

plus

LinkPlus
a Redington company

ŞUBAT 2020 + SAYI 65



Kapak Konusu

2020 GÜNDEMİ: YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİ

Trend Micro ve Hitachi Vantara'nın
Yetkili Eğitim Merkezi LinkPlus

Başarı Hikayeleri

İstanbul Havalimanı - Splunk
Siber Güvenlik Operasyon Merkezi Projesi

LC Waikiki - Hitachi All-Flash Solutions
Altyapı Yenileme Projesi

splunk>

TREND
MICRO

HITACHI
Inspire the Next

Red Hat

VERSA
NETWORKS

MobileIron

ptc

VERITAS

+tableau

corelight

plus

İÇİNDEKİLER

Yönetim Yeri

LinkPlus Bilgisayar Sistemleri
San. ve Tic. A.Ş.
Kısıklı Mah. Hanımseti Sok.
No: 46, 34692
Üsküdar / İstanbul
+90 216 316 50 50
www.linkplus.com.tr

Yayın Kurulu

Cem BORHAN
Hilal PİYADE GÖKSU

İçerik Yönetmeni

Özlem ÖZKAN

Grafik Tasarım

Gülstan ŞENOL

Fotoğraflar

Dolunay KAZDAL

Üretim Koordinatörü

Metin SÖZÜER

Baskı

Set Pozitif Matbaacılık ve
Promosyon Hzm. Ltd. Şti.
+90 212 286 49 33

Yayına Hazırlayan

Terminal Medya
Sun Plaza Bilim Sk. No: 5 Kat: 13
Maslak / İstanbul
+90 212 367 49 88
www.terminaliletisim.com.tr

Plus, LinkPlus
Bilgisayar Sistemleri
San. ve Tic. A.Ş.'nin
Yerel Süreli Yayınıdır.

ŞUBAT 2020 • SAYI: 65



KAPAK KONUSU

LinkPlus Çok Markalı Global Kimliği ile Ekosistemini
Büyütüyor: Global Markaların Lokal Gücü 4
2020 Gündemi: Yapay Zekâ ve Makine Öğrenmesi 6
“Yeni Çağın Yeni Fırsatları İçin Hazırız”
Trend Micro Uzmanlarının Yolu 12
LinkPlus Yetkili Eğitim Merkezi’nden Geçiyor 14
Hitachi Vantara Yetkili Eğitim Merkezi Açıldı 16
LinkPlus, Tableau’nun Türkiye Distribütörü Oldu

SPLUNK

Splunk Discovery Day’de Geleceği Keşfetme Fırsatı 18
Dünyanın İlk Havalimanı Siber Güvenlik
Operasyon Merkezinde Splunk Var! 20
Seynur ve Soitron Splunk İçin Güçlerini Birleştirdi 22

TREND MICRO

Global Telekom Suçları İnternet Güvenliğini
Tehlikeye Atıyor 26
Trend Micro, Cloud Conformity ile
Liderliğini Sağlamıştı 30
E-posta, Ağ, Uç Nokta, Sunucu ve Bulut
İş Yükleri İçin XDR 32

HITACHI VANTARA

LC Waikiki, Hitachi All-Flash Solutions ile Büyüyor 34
İş Dünyasının Veri Hakimiyeti Pentaho ile Artıyor 37
Endüstriyel IoT, Üretim Alanına Taşınıyor 38
Büyük Veri Pazarı 2023’te 520 Milyon Dolara Ulaşacak 40
NEXT 2019’da Yapay Zekâyı Öne Çıkaran Duyurular 42

RED HAT

Günümüzün Popüler Teknolojileri 46
Bizlere Neler Vaat Ediyor?

VERSA NETWORKS

Versa Networks’e NSS Labs’den Tavsiye Notu 50

MOBILE IRON

Makine Öğrenmesiyle Mobil Tehdit Tespiti 52

PTC

PTC, SaaS Platformu Onshape ile KOBİ’lere
Ulaşmayı Hedefliyor 58

VERITAS

Veritas Backup Exec
Backup Exec Çözümüne Geçmek İçin 10 Neden! 60

Yıkıcı teknolojilerin izinde, büyük dönüşümün eşiğinde...

Yıkıcı Teknolojiler (Disruptive Technologies) ve *Yıkıcı Yenilik* (Disruptive Innovation) kavramları, ilk olarak 1995 yılında Prof. Clayton Christensen tarafından, Harvard Üniversitesi’nde dile getirildi. Christensen bu kavramları, 1997 ve 2003’te yayınladığı *The Innovator’s Dilemma* ve *The Innovator’s Solution* kitaplarında uzun uzun anlattı. *Yıkıcı Yenilik*, halihazırda pazara hakim olan ürün ve hizmetleri yıkan, yok eden, onların yerini alan yenilikçi ürün veya hizmetleri tariflerken; *Yıkıcı Teknolojiler*, söz konusu ürün ve hizmetlerin ardındaki teknolojileri ifade etmek için kullanıldı. Christensen, aynı zamanda müşteri deneyimini farklı bir boyuta taşıyan yepyeni bir döneme de işaret ediyordu. Harvard’lı Profesör’ün 25 yıl önce “...çağ değiştirecek bir döneme giriyoruz” sözleri ile dikkat çektiği *Yıkıcı Teknolojilerin* dönüştürücü etkisini bugün hayatımızın içinde birebir yaşıyoruz. Netflix, Airbnb, Spotify, Bitaksi, Getir, Glovo gibi dünyadan ve Türkiye’den pek çok *Yıkıcı Yenilik* örneğinin ardında, bugünün *Yıkıcı Teknolojilerinin* gücü var.

2020 yılında hem tüketici hem de üretici konumundaki kurumların, şirketlerin ve hatta devletlerin ana gündemlerinde hangi konuların olduğu hiçbirimiz için sır değil. Akla en kolay gelen iki başlık: Yapay Zekâ ve Makine Öğrenmesi. Ve elbette bu ikisinin sürüklediği daha fazlası... Derin Öğrenme, Akıllı Sanal Yardımcılar (Chatbot), Sanal/Artırılmış Gerçeklik, Robot Teknolojileri, Ses/Yüz Tanıma Sistemleri, Blockchain/Cryptocurrency, Nesnelerin İnterneti, Bulut Bilişim, Giyilebilir Teknolojiler, Nanoteknoloji, Kuantum Teknoloji, Akıllı Şehirler, Endüstri 4.0, Mobil Teknolojiler, 5G... İşte bunlar, kurumların, şirketlerin, devletlerin gündemini meşgul eden günümüzün *Yıkıcı Teknolojileri/Yenilikleri*...

Geçtiğimiz yıllara kadar Yapay Zekâ entegrasyonu büyük ölçekli şirketler sahasının önemli bir rekabet unsuruken, şimdilerde orta ölçekli şirketlerin rekabeti için bile zorunlu hale geldi. Bağımsız araştırma şirketlerinin raporları, bize 2025 itibarıyla müşteri ilişkilerinin %95’inin yapay zekâlar aracılığıyla sürdürüleceğini söylüyor. Elbette Yapay Zekâ’nın hayatımıza etkileri iş dünyası ile sınırlı değil. Yıkıcı Teknolojilerin bilimin her alanından başlayarak, iş dünyasına ve günlük hayatımıza yapacağı etkinin boyutları üzerine biraz düşünmek, eşiğinde bulunduğumuz büyük dönüşüm de fark etmemizi sağlıyor. Bu öyle bir dönüşüm ki bundan sadece beş yıl sonrasında, çok çok farklı bir dünyada yaşıyor olabiliriz.

Geçtiğimiz 24 Ocak’ta, Elazığ, Sivrice’de yaşanan deprem ülkemizi yasa boğarken, erken uyarı teknolojilerine dair gelişmeleri de gündeme taşıdı. Harvard Üniversitesi’nde gerçekleştirilen bir çalışmaya göre Yapay Zekâ, deprem sensörlerinin tespit ettiği çok küçük kırılmaları dahi analiz ederek, yaklaşan büyük depremler hakkında alarm verebiliyor. Bilim insanları bu yöntemi kullanarak, ABD’de önceki yöntemlere göre 17 kat daha fazla depremi doğru tahmin etmeyi başardılar. Bu konudaki teknolojilerin hızla gelişmesini ve ülkemizde de kısa zamanda hayata geçirilmesini diliyoruz.

2019 yılında iki yeni global markanın daha distribütörlüğünü üstlenerek, 2020 yılını marka sayımızı 10’a yükselterek karşıladık. Her biri yıkıcı teknolojilerden güç alan, yeni nesil teknolojiler geliştiren bu 10 markanın iş ortaklarımızla birlikte Türkiye’de yaygınlaştırılmasını sağlarken, bizim de gündemimizin ana başlıkları Yapay Zekâ ve Makine Öğrenmesi olacak. 2020 yılında, Yıkıcı Teknolojileri takip ederek distribütörlük kavramını yeniden tanımlamayı ve yine Yıkıcı Teknolojiler perspektifinden hareketle iş ortaklarımızla birlikte büyümeyi, bu sayede Türkiye’nin büyük dönüşümüne de katkıda bulunmayı hedefliyoruz.

2020’nin tüm iş ortaklarımızın, müşterilerimizin ve Türkiye’nin hedeflerine ulaştığı bir yıl olmasını diliyorum.

Saygılarımla,

CEM BORHAN Genel Müdür



CEM BORHAN - GENEL MÜDÜR

“2020 yılında, Yıkıcı Teknolojileri takip ederek distribütörlük kavramını yeniden tanımlamayı ve yine aynı perspektiften hareketle iş ortaklarımızla birlikte büyümeyi, bu sayede Türkiye’nin büyük dönüşümüne de katkıda bulunmayı hedefliyoruz.”

LinkPlus çok markalı global kimliği ile ekosistemini büyütüyor:

GLOBAL MARKALARIN LOKAL GÜCÜ

2020 yılında sektördeki çeyrek asırlık markaların arasına dahil olan LinkPlus, Redington satın alması sonrası gerçekleştirilen yatırımlarla yeni kazanımlar elde etti ve yeni hedeflere odaklandı.

LinkPlus, 1995 yılında kurulan ve çeyrek asırdır IT sektöründe faaliyetlerini sürdüren köklü bir kuruluş. 2015 yılına dek tek bir markanın distribütörlüğünü sürdüren LinkPlus, bu süreçte katma değerli iş ortaklığı anlayışının öncüsü oldu ve çok ciddi bir know-how biriktirdi. İş ortaklığı ağını pazarlama ve tanıtım faaliyetleri ile desteklemesinin yanı sıra teknik uzmanlarıyla da iş ortakları ve müşterilerinin yanında oldu. Ayrıca en ileri altyapı ve teknolojilerle donatılan demo ve eğitim merkezini iş ortakları ve müşterilerinin kullanımına sundu, onları en iyi eğitmenlerle bir araya getirdi, yaz okulları düzenledi. İş ortaklarına sadece Türkiye'deki değil, bölgedeki büyüme hedeflerinde de destek oldu.

2015 yılına kadar tek markalı yapısıyla iş ortakları ile birlikte büyüyen ve katma değerli distribütörlük alanında önemli başarılarla imza atan LinkPlus, Türkiye'deki pazarı yakından takip eden Redington'ın dikkatini çekti. Global çapta 8 milyar dolarlık bir dağıtım ve tedarik zinciri çözümleri sağlayıcısı olan Redington'ın başlangıç hikâyesi ile LinkPus'ın başlangıcı benzerlik gösteriyor. 1993 yılında kurulan ve tek marka ile tek bir pazarda faaliyetine başlayan Redington, bugün gelişmekte olan 34 ülkede, bilgi teknolojileri (BT) ve mobilite alanlarında 200'den fazla global marka ile yer alıyor. LinkPlus ise 2018 yılının Ocak ayında hisse devrinin tamamlanmasıyla birlikte yüzde 100 Redington kuruluşu olarak global bir

kimlik kazanırken, marka sayısını 10'a çıkarmış bulunuyor.

FINANSAL GÜÇ ARTIŞI VE BÜYÜME

LinkPlus Redington tarafından satın alındıktan sonra, öncelikle finansal gücünü arttırdı. 2015 yılından bu yana çalışan sayısı %50'nin üzerinde artarken, dijital pazarlamaya yatırım yapıldı. LinkPlus, DNA'sında kodlanmış olan geleneksel öncü tavrını bir Redington kuruluşu olarak da sürdürdü. Redington'ın global birikiminden gelen know-how'ı 25 yıllık birikimine ekleyerek, Türkiye'deki distribütörlük kavramını da değiştirdi. Distribütörlüğün artık dağıtıcı olarak değil "Katma Değerli Çözüm Sağlayıcısı" olarak algılanmasını sağladı. Bunu, finansal gücü, eğitim ve demo merkezi, pazarlama

faaliyetleri, bünyesindeki her marka özelinde uzmanlaşmış güçlü teknik ekibi ile başardı. Öte yandan Redington tarafından satın alınma ile birlikte LinkPlus, "Multi Vendor" yani çok markalı bir oyuncu haline geldi. Hemen ardından da tüm Redington iştiraklerinde olduğu gibi logosunu yeniledi. LinkPlus'ın logosundaki yeşil renk, "sürdürülebilirlik", doğaya katkı ve çevreciliği temsil ederken, yazı karakteri ile "sadeleşme" öne çıkıyor. Logonun sembolü ise tam bir uyumu, çok boyutlu bir entegrasyonu ve sinerji içinde çalışmayı vurguluyor.

GLOBAL VİZYON LOKAL STRATEJİ

Yapay Zekâ (AI), Robotik, Makine Öğrenmesi, Büyük Veri ve Analitik,

Nesnelerin İnterneti (IoT) ve 5G iletişimi gibi yeni nesil teknolojilerin sunduğu olanakları ve fırsatları global bir bilgi birikimi ve bakış açısıyla takip eden LinkPlus, distribütörlüğünü üstlendiği markalarla bugünün ve yarının yeni ihtiyaçlarına cevap veriyor. 2016 yılında Splunk ve Trendmicro; 2017 yılında Hitachi Vantara, Red Hat, Versa Networks; 2018 yılında MobileIron, PTC, Veritas; 2019 yılında ise Tableau ve Corelight ile iş ortaklığı yaparak, marka sayısını 10'a yükselten LinkPlus, üretici ile beraber pazarı büyütme adına çalışmalar yapıyor, pazardan en fazla payı almayı hedefliyor. Tek distribütörü olduğu Splunk, Versa, MobileIron, Tableau ve Corelight gibi Türkiye'de ofisleri olmayan markalar için ayrıca pazara yaklaşarak strateji

belirliyor ve satış-pazarlama başta olmak üzere uçtan uca bütün operasyon desteğini sağlayabiliyor. Bu doğrultuda, iş ortaklarını ve müşterileri bir araya getiren önemli etkinlikler de düzenliyor. 2019 yılı içerisinde ilk olarak organize edilen MobileIron ve Splunk Day etkinlikleri 2020 yılında da gerçekleştirilecek. 2019'da yeni logosu, yeni kimliği ve çok markalı yapısı ile başarılı bir yıl geçiren LinkPlus, 2020'ye de yeni bir enerji, yeni bir yön ile adım atıyor. Sorumluluğunu üstlendiği markaları ve iş ortaklarını bir sonraki büyüme ve yaygınlaşma seviyesine götürme konusunda Redington ile ortak bir vizyona sahip olan LinkPlus, kendi ufkunu da her yönden genişletmeye devam ediyor.

2020 GÜNDEMİ: YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİ

“Yeni Çağın Yeni Fırsatları İçin Hazırız”

LinkPlus 2020 yılında, dünyanın öncü teknoloji üreticilerini barındıran çok markalı yapısı ve gelişen ekosistemiyle birlikte yeni çağın beklentilerine cevap verecek teknoloji ve çözümleri yaygınlaştırmaya yönelik stratejiler doğrultusunda ilerliyor. Daha dinamik ve çevik bir yapılanma ile yılı karşılayan LinkPlus’ın 2020 için odaklandığı konular arasında, Yapay Zekâ ve Makine Öğrenmesi kavramları öne çıkıyor.

LinkPlus, 2020’yi nasıl karşılıyor?

CEM BORHAN: 2020 yılında sektördeki çeyrek asırlık kuruluşlar arasına dahil olan LinkPlus, bir Redington şirketi olmasıyla birlikte hem global bir kimlik hem de ciddi bir finansal güç kazandı. Bu yılı, dünyanın en yenilikçi teknolojilerini üreten markalarımız ve gelişen ekosistemimizle birlikte, yeni çağın beklentilerine cevap vermeye hazır bir şekilde karşılıyoruz.

2020 için belirlediğiniz stratejilerden söz eder misiniz?

CEM BORHAN: Bir Redington kuruluşu olarak, yerel stratejilerimiz ile Redington’ın global stratejilerini uyum içerisinde birleştiriyoruz. 2019 yılı son çeyreğinde Dubai’de düzenlenen teknoloji fuarı GITE’X’e, Redington

çatısı altında katıldık. Bizim için son derece verimli geçen etkinlik boyunca hem Redington ile birlikte 2020 stratejilerimizin üzerinden geçtik hem de birçok üretici ile bir araya gelerek 2020 yol haritamızı belirleyecek önemli görüşmeler gerçekleştirdik. Stratejik bir kararla, distribütörlük faaliyetlerimizi Redington’da olduğu gibi dikey iş alanları altında kategorize ediyoruz. Geçmiş dönemlerde sürdürdüğümüz ürün odaklı yapılanmamızı artık “iş” merkezli bir yapıya dönüştürmüş durumdayız. Bulunduğumuz noktada, “Güvenlik”, “Analitik” ve “Bulut” olmak üzere üç temel dikey belirledik ve markalarımızı bunların altında konumlandık. Bu yeni yapılanmanın sağlıklı bir şekilde uygulanabilmesi bizim için son derece

önemli. Bunu sağlarken, geçmişteki çeyrek asırlık bilgi birikimimizin de bize büyük katkısı oluyor. LinkPlus’ın en güçlü olduğu alanlardan ikisi teknik altyapısı ve teknik ekibi. Her marka özelinde uzmanlaşmış ekiplerimizle teknik destek verebiliyoruz. Bu özelliğimizden aldığımız güçle, üç temel dikey altında hem iş ortaklarını hem de kullanıcıları desteklemeyi amaçlayan bir “Danışmanlık ve Servis” bacağı kuruyoruz. Danışmanlık ve servis hizmetlerini, markalarımızı güçlendirecek ve iş ortaklarına teknik destek vererek pazardaki hareket kabiliyetlerini artıracak stratejik bir hedef olarak görüyoruz. Bu konu, özellikle Türkiye’de ofisi ve ekibi olmayan markalarımızın büyümesi için son derece önemli.

“Güvenlik”, “Analitik” ve “Bulut” dikeyleri altında büyüme stratejimiz doğrultusunda, kendisini yenilikçi teknolojilerle farklılaştırmış yeni markaları da 2020 yılında LinkPlus ailesi içerisinde görmeye başlayacağız.

Distribütörlüğünü yaptığınız markaların pazardaki gücünü artırmaya yönelik başka faaliyetlerinizden de söz eder misiniz?

CEM BORHAN: Ne kadar yenilikçi ve dikkat çekici olursa olsun, pazara yeni giren bir teknolojinin yaygınlaşabilmesi için öncelikle yaratıcı ve üretken bir iş ortağı ağı oluşturmanız, teknik uzmanlığa sahip insan kaynağının artmasını sağlamanız, o teknolojinin nasıl çalıştığını, nasıl işe yaradığını gösterebileceğiniz bir platform kurmanız

“2020’de LinkPlus’ta, global markalarımızın sahip olduğu Yapay Zekâ ve Makine Öğrenmesi’ne yönelik teknoloji know-how’ını da yanımıza alarak, yapısal ve/veya yapısal olmayan verinin uçtan uca tüm yolculuğunu adresleyebilen bir yapı oluşturacağız.”

CEM BORHAN
Genel Müdür
LinkPlus



ve pazarda farkındalığı yaratacak etkinlikler düzenlemeniz gerekiyor. LinkPlus’ın iş ortağı ağı oluşturma konusundaki çeyrek asırlık deneyimi zaten açıkça ortada. İş ortaklarımızın üretkenliğinden ve yenilikçi çözümler geliştirme yeteneklerinden hiç kuşukumuz yok. Teknik uzmanlığa sahip insan kaynağının geliştirilmesi konusunda, İstanbul ve Ankara’daki ofislerimizde kurduğumuz eğitim merkezlerimiz ile markalarımıza destek oluyoruz. Hitachi Vantara ve Trend Micro’nun Yetkili Eğitim Merkezi’yiz. Eğitim merkezlerimizde son derece kapsamlı teknik eğitimler verebiliyoruz. PoC çalışmaları yapmaya uygun, en ileri teknolojilerle donatılmış demo ve test merkezimizle de iş ortaklarımız ve

müşterilerimizin yanındayız. Ayrıca, Türkiye ofisleri bulunmayan markalarımızın satış-pazarlama ve teknik aktivitelerini de üstlenerek, aynı zamanda bir nevi Türkiye irtibat ofisleri gibi çalışıyoruz. Ayrıca, yurt dışından gelen ekiplerin çalışmaları için ofis alanı sunuyoruz. Türkiye’deki öncü kuvvetleri olarak, pazarı onlar için hazırlıyoruz ve bunu bir bayrak yarışı gibi düşünüyoruz. Örneğin, bu doğrultuda 2019 yılında iki önemli etkinlik düzenledik. Mart ayında düzenlediğimiz “MobileIron Customer Day” ve Ekim ayında düzenlediğimiz “Splunk Discovery Day”, iş ortaklarımızı müşterilerle bir araya getiren, gerçek anlamda sinerji yaratılmasına katkıda bulunan başarılı etkinlikler oldu. Bu etkinlikleri geleneksel hale getirerek her yıl devam ettirmeyi hedefliyoruz.

Bu yıl LinkPlus'ın teknoloji gündeminde neler var?

CEM BORHAN: Sorumluluğunu üstlendiğimiz global markalar, içinde bulunduğumuz dijital dönüşümün yarattığı bu yeni çağın en ileri teknolojilerini üretiyorlar. Onlarla çalışmanın doğal sonucu olarak da 2020 gündemimizde iki temel başlık öne çıkıyor: Yapay Zekâ ve Makine Öğrenmesi. Yeni dünyamızda, Buluttan IoT'ye akla gelebilecek her kavram, aslında artık Yapay Zekâ ve Makine Öğrenmesi kavramlarının çatısı altına girmiş durumda.

Geçtiğimiz yıl, yani 2019'da ağırlıklı olarak Bulut ve IoT (Nesnelerin İnterneti) teknolojilerini konuştuk. Distribütörlüğünü üstlendiğimiz tüm markalarımızla ve ekosistemimizle birlikte de Türkiye'deki kamu kuruluşlarının, KOBİ ve kurumsal şirketlerin dijital dönüşümlerini sağlamaya hizmet edecek Bulut ve IoT odaklı projeler üzerinde çalışmalar ve farkındalıklarını artıracak etkinlikler gerçekleştirdik.

Bulut'ta kat edilen yol ile birlikte Yapay Zekâ, Robotik, Büyük Veri ve Analitik, Nesnelerin İnterneti (IoT) ve 5G iletişimi gibi teknolojilerin çok yeni olanaklar ve fırsatlar sunduğunu görüyoruz. Özellikle IoT tarafında Türkiye'de önemli projelerin hayata geçirildiğini ve bu konuda hız kazanıldığını görüyoruz. Yapay Zekâ ve Makine Öğrenmesi alanında da deneysel projeler başlamış durumda. 2020'de, bu alanlara yaptığımız yatırımların sonuçlarını göreceğimizi memnuniyetle söylemek isterim.

Güvenlik, Analitik ve Bulut olmak üzere üç temel dikeyde yoğunlaşacağınızı belirttiniz. 2020 yılında bu alanlarda odaklandığınız özel konular olacak mı?

CEM BORHAN: Öncelikle Güvenlik başlığını ele alacak olursak, bu yılın öne çıkan en önemli konularından birisinin KVKK (Kişisel Verilerin Korunması Kanunu) olduğunu söyleyebiliriz. Bir süredir herkesin diline dolanmış olsa da özellikle BT dünyasında hâlâ pek

çok bilinmezi barındırıyor. Verilerin güvenliği hayatımızı ne kadar etkiliyor, hangi veri kritiktir, hangi veri daha az kritiktir, hangi veri paylaşılabilir, hangi veri paylaşılabilir konularında halen belirsizlikler var. KVKK, Türkiye'deki en genele yayılmış güvenlik yönergesi diyebiliriz. Halka açılmış bütün kuruluşları kapsayan bir yönerge bu. Bugüne kadar BDDK'nın ve TCMB'nin finans sektörüne yönelik, keza BTK'nın Telekom sektörüne yönelik yayınladığı yönergeler, kanun ve yaptırımlar bulunuyor. KVKK'nın da oluşmasıyla birlikte, bütün sektörlerde daha yaygın bir şekilde uyarlanan bir güvenlik ihtiyacı ortaya çıktı. İşte LinkPlus, 2020'de bu alanda danışmanlık verebilen ve çözüm sunabilen bir yapı kazanacak.

Analitik alana bakış açınızı öğrenebilir miyiz?

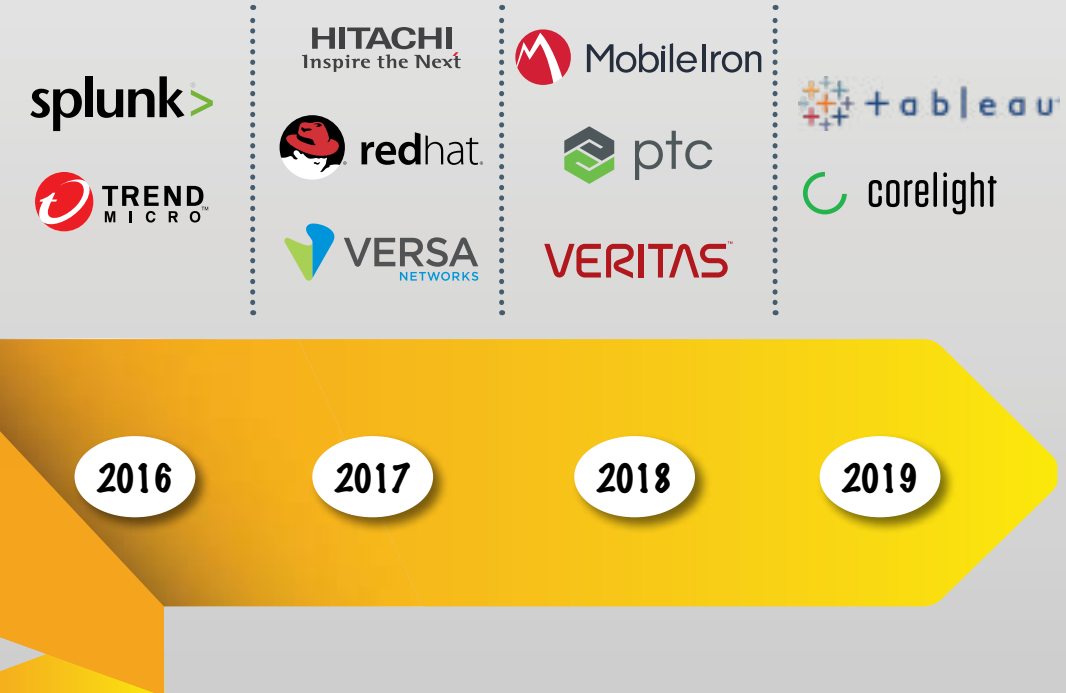
CEM BORHAN: Analitik dediğimiz zaman akla hemen "raporlama", "veri ambarı", "veri analizi" geliyor. Evet, eski nesil teknolojiler yapısal verileri analiz etme ihtiyacı ile ortaya çıktılar ve işlerini de gayet güzel yapmaya devam ediyorlar. Ancak artık hayatımıza yapısal olmayan veriler de girdi. Tam anlamıyla ıslah edilemez gibi görünen, son sürat akan bir veri ırmağının içindeyiz. Aklınıza gelecek her cihazdan bağlandığımız her platform, sosyal medya, mobil uygulama üzerinde iz bırakıyor, veri üretiyoruz. Big Data kavramı ile açıklanan bu devasa boyuttaki veriyi analiz edebilmek için Analitik kavramı ve bu kavram altında geliştirilmiş yeni nesil teknolojiler hayatımıza zaten girdi. Ancak bu

“Türkiye’de ofisleri bulunmayan markalarımızın satış-pazarlama ve teknik aktivitelerini de üstlenerek, bir nevi Türkiye irtibat ofisi gibi çalışıyoruz. Onların Türkiye’deki öncü kuvvetleri olarak, pazarı onlar için hazırlıyor ve bunu bir bayrak yarışı gibi düşünüyoruz.”

CEM BORHAN Genel Müdür / LinkPlus

ÇOK MARKALI YAPI

Global çapta 8 milyar dolarlık bir dağıtım ve tedarik zinciri çözümleri sağlayıcısı olan Redington'ın başlangıç hikayesi ile LinkPus'ın başlangıcı benzerlik gösteriyor. 1993 yılında kurulan ve tek marka ile tek bir pazarda faaliyetine başlayan Redington, bugün gelişmekte olan 34 ülkede, bilgi teknolojileri (BT) ve mobilite alanlarında 200'den fazla global marka ile yer alıyor. LinkPlus ise 2018 yılının Ocak ayında hisse devrinin tamamlanmasıyla birlikte yüzde 100 Redington kuruluşu olarak global bir kimlik kazanırken; 2016 yılında Splunk ve Trend Micro, 2017 yılında Hitachi Vantara, Red Hat, Versa Networks, 2018 yılında MobileIron, PTC, Veritas, 2019 yılında ise Tableau ve Corelight ile iş ortaklığı yaparak, marka sayısını 10'a yükseltmiş bulunuyor.



“Bir Redington kuruluşu olarak, yerel stratejilerimiz ile Redington'ın global stratejilerini uyum içerisinde birleştiriyoruz. 2019 yılı son çeyreğinde Dubai'de düzenlenen teknoloji fuarı GITEX'e, Redington çatısı altında katıldık. Burada hem Redington ile 2020 stratejilerimiz üzerine fikir alışverişinde bulunduk hem de birçok üretici ile bir araya gelerek 2020 yol haritamızı belirleyecek önemli görüşmeler gerçekleştirdik.”

CEM BORHAN Genel Müdür / LinkPlus

kapsamda geliştirilen tüketici/kullanıcı kimlik ve davranış analizleri gibi örnekler, bakış açımızı biraz daha genişletip bizi yeni yeni ufuklara sürüklüyor. Artık yeni bir farkındalık ile çözüm üretmemiz, bu güne kadar sahip olduğumuz birikimi Yapay Zekâ ve Makine Öğrenmesi ile buluşturmamız gerekiyor.

2020'de LinkPlus'ta, global markalarımızın sahip olduğu Yapay Zekâ ve Makine Öğrenmesi'ne yönelik teknoloji know-how'ını da yanımıza alarak, yapısal ve/veya yapısal olmayan verinin uçtan uca tüm yolculuğunu adresleyebilen bir yapı oluşturacağız. Distribütörlüğünü üstlendiğimiz marka ve teknolojileri de bu bakış açısıyla bir araya getirmeyi, iş ortaklarımız üzerinden kullanıcılara ulaştırmayı hedefliyoruz.

Üçüncü dikey olan alan ise oldukça deneyim sahibi olduğunuz Bulut Bilişim. Bu alanda öncelikli gördüğünüz 2020 hedefiniz nedir?

CEM BORHAN: Bulut Bilişim, gerçekten üzerinde çok konuşulan ve bizim de uzun zamandır deneyimlediğimiz bir alan. Bulut Bilişimi doğru bir şekilde konumlamak gerekiyor çünkü bir takım yaptırım ve zorunlulukları da beraberinde getirebiliyor. Bu zorunluluklar ve yasal sınırlandırmalar her ülkede belli oranda bulunuyor. Verinin ülke dışına çıkarılamaması, regülasyonlar, konjonktürel koşullar, veri merkezlerinin millileştirilmesi gibi zorunluluklar ve ihtiyaçlar yan yana geldiğinde, Bulut Bilişim'in hibrit yapısı da ortaya çıkmış oluyor. Bazı verilerin kuruluş içerisinde kalması, bazılarının üretici firmaların veri merkezinde durması, bazılarının da ülke içerisinde

“2020 yılında, Bulut'un Türkiye'de doğru şekilde konumlanabilmesine katkıda bulunmayı ve iş ortaklarımızı bunun etrafında kenetlemeyi hedefliyoruz. Bu doğrultuda, AWS, Google Cloud, Ali Baba gibi Bulut Bilişim'in başarılı örneklerini yakından takip ediyoruz.”

CEM BORHAN Genel Müdür / LinkPlus

milli veri merkezlerinde tutulması söz konusu. Bu açıdan baktığımızda, ciddi bir oyuncusu olmayı hedeflediğimiz Bulut Bilişim'in dünyada ve Türkiye'de nasıl konumlanacağını çok iyi izlememiz, değerlendirmemiz gerekiyor. 2020 yılında, Bulut'un Türkiye'de doğru şekilde konumlanabilmesine katkıda bulunmayı ve iş ortaklarımızı bunun etrafında kenetlemeyi hedefliyoruz. Bu doğrultuda, AWS, Google Cloud, Ali Baba gibi Bulut Bilişim'in başarılı örneklerini yakından takip ediyoruz.

Markalarınızı kamu sektöründe konumlandırmaya yönelik özel çalışmalarınız var mı? Kamu sektörünü nasıl değerlendiriyorsunuz?
CEM BORHAN: 2018 ve 2019, çeşitli nedenlerle BT projelerinin yavaşladığı yıllar oldu. Ancak önümüzdeki dönemde bu durumun değişmesini bekliyoruz ve kamuda markalarımız için önemli bir potansiyel olduğunu görüyoruz. Bu nedenle de Ankara'ya yönelik yatırımlar yaptık. Tüm markalarımız, kamu sektöründe çok önemli ihtiyaçlara cevap verebilecek nitelikte. Bu yıl sık sık vurgulayacağımız Yapay Zekâ ve Makine Öğrenmesi kapsamında

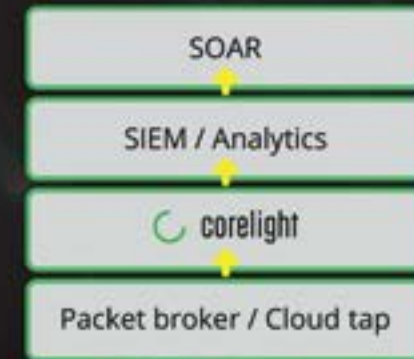
markalarımızı bir araya getirdiğimizden ve iş ortaklarımızı da bu doğrultuda yönlendirdiğimizden söz etmiştim. Biz bu anlamda da kamu tarafında ciddi bir potansiyel görüyoruz. Bu potansiyelden hareketle, Ankara ofisimizi Maidan İş Merkezi'ne taşındık ve orada da bir eğitim merkezi kurduk. Ayrıca Ankara'da ofisi olmayan iş ortaklarımız ve markalarımız için Ankara ziyaretleri sırasında çalışabilecekleri alanlar da yarattık. Özetleyecek olursak, 2020'de kamu sektörü için de hazırız.

2020 senesinde büyüme beklentileriniz neler?

CEM BORHAN: 2020 yılında, şu anda distribütörlüğünü yürüttüğümüz markalarda insan kaynağı anlamında büyümenin yanı sıra 2019 yılına göre ciro olarak da yaklaşık yüzde 30 büyüme sağlamayı öngörüyoruz. Ciddi anlamda büyüme vaat ettiğine inandığımız, yeni çağın beklentilerine yönelik teknolojileriyle inovatif atılım yapan markalarla yolumuza devam ediyoruz. Ayrıca, şu anda 10 olan marka sayımızın, 2020 yılında yine Güvenlik, Analitik ve Bulut dikeyleri çerçevesinde hızla artmasını bekliyoruz.

Turn network traffic into security **evidence.**

Corelight Sensors transform raw network packets into rich logs, extracted files, and custom insights via the power of open-source Zeek (formerly Bro).



Upgrade your security stack with Corelight cloud, appliance, or virtual sensors:

- Achieve 20x faster incident response
- Unlock threat hunting capabilities
- Customize and tune threat detection
- And much, much more..

 **corelight**

www.corelight.com | info@corelight.com

From the creators of Bro / Zeek.

Trend Micro Uzmanlarının Yolu LinkPlus Yetkili Eğitim Merkezi'nden Geçiyor

LinkPlus, Trend Micro'nun Yetkili Eğitim Merkezi oldu. Kurumsal Güvenlik ürünlerine yönelik olarak düzenlenecek eğitimlere katılarak bünyesinde sertifikalı mühendis barındıran iş ortakları, Trend Micro'nun belirlediği en üst seviyedeki iş ortaklığı unvanlarına sahip olabilecekler.

LinkPlus, 25 yıllık yolculuğu boyunca farklı ihtiyaçlara karşılık veren teknik eğitimleri ile iş ortaklarının ve müşterilerinin yanında oldu ve bu alandaki deneyimi ve başarılarıyla da öne çıktı. Temsil ettiği üreticilerin yeni teknolojilerini hem iş ortaklarıyla hem de Türkiye'deki son kullanıcılarla daha etkin bir şekilde buluşturmak için söz konusu teknolojilere yönelik eğitimlere büyük önem veren LinkPlus, Aralık 2019 itibarıyla de Trend Micro'nun Yetkili Eğitim Merkezi oldu. Yenilikçi güvenlik teknolojileriyle öne çıkan Trend Micro'nun 2016 yılından bu yana Yetkili Distribütörü olan LinkPlus, bu gelişmeyle birlikte Trend Micro iş ortakları ve son kullanıcılarına Trend Micro tarafından onaylanmış sertifika eğitim programları düzenleme yetkisi elde etti.

SERTİFİKA ALMA ADIMLARI

Trend Micro'nun ürünleriyle ilgili sertifika alarak, Sertifikalı Mühendis olmak isteyenlerin, öncelikle bir yetkili eğitim merkezindeki sınıf ortamında, yetkili eğitmen tarafından verilen

eğitilmeye katılmaları gerekiyor. Bu eğitime katılanlara Eğitime Katılım Sertifikası veriliyor ve eğitim sonunda hepsine birer ID, yani kimlik numarası tanımlanıyor. Katılımcılar, bu ID ile birlikte Trend Micro'nun online sistemlerinde yer alan sınava girmeye hak kazanıyorlar. Bu sınavdan geçen kişiler de Trend Micro'nun Sertifikalı Trend Micro Mühendisi oluyorlar.

NEDEN SERTİFİKA ALMAK GEREKİYOR?

LinkPlus İş Birim Yöneticisi Onur Demirel, sertifika eğitimlerine Trend Micro iş ortaklarının ve Trend Micro kullanan kurumsal kullanıcıların ihtiyaç duyduklarını şu sözlerle ifade ediyor: "Trend Micro İş ortaklarının, iş ortaklığında belli seviyelere ulaşabilmeleri için bazı gereksinimleri yerine getirmeleri söz konusu. Bünyelerinde yetkili Sertifikalı Mühendis bulundurmaları da bu gereksinimler arasında yer alıyor. LinkPlus Yetkili Eğitim Merkezi'nde, tüm Trend Micro iş ortaklarının Trend Micro ürünlerine yönelik eğitim ihtiyaçlarına

cevap verecek bir platform sunuyoruz. Trend Micro ürünlerini kullanan kuruluşlar ise kendi ekiplerinin Trend Micro ürünlerine dair eğitimlerini sağlamak için merkezimizden yararlanabilecekler." Onur Demirel, eğitimlerin periyodik olarak düzenlenmek üzere, Trend Micro ile birlikte oluşturulacağını ve iş ortaklarının ve kurumsal kullanıcıların söz konusu eğitimlere davet edileceklerini belirtiyor.

EĞİTİMLER HANGİ ÜRÜNLERİ KAPSAYACAK?

LinkPlus İş Birim Yöneticisi Onur Demirel, Yetkili Eğitim Merkezi'nde verilecek eğitimlerin, Trend Micro'nun kurumsal ürünlerini kapsadığına dikkat çekiyor. Kurumsal Uç Nokta Güvenliği, Kurumsal Veri Merkezi Güvenliği ve Kurumsal Network Güvenliği ürünlerine yönelik eğitimleri alan ve bünyesinde sertifikalı mühendis barındıran iş ortakları, Trend Micro'nun belirlediği en üst seviyedeki iş ortaklığı unvanlarına sahip olabilecekler. Bu seviyelere

“Trend Micro'nun 'Kurumsal Güvenlik' konusundaki eğitimleri, son kullanıcıların ihtiyaçlarını daha iyi anlama ve onlara doğru ihtiyaçları önerme konusunda da önemli bir destek sağlayacak.”

ONUR DEMİREL
İş Birim Yöneticisi
LinkPlus



ulaşan iş ortakları, Trend Micro'nun sağlamış olduğu bazı avantajlardan da faydalanabilecekler. Demirel, "Trend Micro'nun Kurumsal Güvenlik konusundaki eğitimleri, son kullanıcıların ihtiyaçlarını daha iyi anlama ve onlara doğru ihtiyaçları önerme konusunda da önemli bir destek sağlayacak" diyor ve sözlerine şöyle devam ediyor: "Dolayısıyla, bu eğitimlerin sadece iş ortaklarının belli seviyelere ulaşmasını değil, aynı zamanda o iş ortaklarının kendi portföylerini genişletmelerinde ve var olan portföylerindeki müşterilere daha doğru ve daha etkin çözümler sunmalarında da etkili olacağına inanıyoruz."

EĞİTİMLER OCAK SONUNDA BAŞLIYOR

Ocak 2020 sonunda "Kurumsal Uç Nokta Güvenliği-Apex ONE ve bağlı ürünler" için ilk Trend Micro eğitimlerini vermeye başlayan LinkPlus, kendi bünyesindeki teknik bir uzmanı, Trend Micro Sertifikalı Eğitimci olarak yetiştirmiş bulunuyor.

TREND MICRO EĞİTİMLERİ HANGİ ÜRÜNLERİ KAPSIYOR?

Kurumsal Uç Nokta Güvenliği – Apex ONE ve Bağlı Ürünler

- ✓ Trend Micro Apex One™, kurumsal ağları kötü amaçlı yazılımlardan, web tabanlı tehditler, casus yazılımlar ve karışık tehdit saldırıları ile ağ virüslerinden koruyor.
- ✓ Apex One, uç noktada bulunan bir Security Agent programından ve bir sunucudan oluşuyor. Tek bir ajan ile uygulama kontrolü, zafiyet analizi ve EDR (Endpoint Detection and Response-Uç Nokta Tespit ve Yanıt) gibi güvenlik katmanları ile Entegre bir çözüm sağlıyor.
- ✓ Sunucu, web tabanlı yönetim konsolu aracılığıyla eşgüdümlü güvenlik politikaları oluşturmayı ve güncellemeleri her güvenlik ajanına dağıtmayı kolaylaştırıyor.
- ✓ Kurumsal Veri Merkezi Güvenliği – Deep Security Ailesi
- ✓ Fiziksel, bulut ve sanal alanlardaki modern veri merkezinin, imaj ve konteynerlerin güvenliğini sağlıyor.
- ✓ Network Security, System Security ve Malware Prevention olarak 7 modül ile veri merkezini koruyor.
- ✓ Sunuculardaki kurumsal uygulamaları ve verileri ihlallerden ve iş kesintilerinden koruyor.
- ✓ Merkezi olarak yönetilen platform, yasal düzenlemelere uyumu sağlarken ve yatırım getirisini hızlandırırken güvenlik prosedürlerini basitleştiriyor.

Kurumsal Ağ Güvenliği – Deep Discovery Ürün Ailesi

- ✓ İleri tehditleri ve hedefli saldırıları tespit etmek, analiz etmek ve önlemek için gelişmiş kum havuzu (sandbox) teknolojisi ile ağınıza koruyor.
- ✓ İş ağındaki trafiği dinliyor ve gelişmiş paket analizi ile zararlı hareketleri tanımlıyor.
- ✓ Kum havuzu teknolojisi sayesinde bilinmeyen dosyalar üzerinde analiz gerçekleştirerek sizi bilgilendiriyor.
- ✓ Uç noktalarınızda Trend Micro çözümü olması durumunda tespit ettiği zararlı dosya, URL bilgilerini içeren şüpheli objeleri güvenlik istihbaratı olarak Apex Central ile paylaşıyor ve böylece uç noktalarda gerekli güvenliği sağlıyor.

Hitachi Vantara

Yetkili Eğitim Merkezi Açıldı

Hitachi Vantara Türkiye, Linkplus'ı yetkili eğitim merkezi olarak atadı. LinkPlus bünyesinde açılan Hitachi Vantara Yetkili Eğitim Merkezi, müşterilerin ve iş ortaklarının Hitachi Vantara çözümlerini çok daha etkin ve yetkin bir şekilde kullanabilmelerini sağlayacak.

Dijital altyapı ve çözümleri alanında dünyanın önde gelen şirketlerinden Hitachi Vantara, Türkiye'de distribütörlük faaliyetlerini başarıyla sürdüren Linkplus'ı Yetkili Eğitim Merkezi olarak atadı. LinkPlus bünyesinde yer alan yeni Hitachi Vantara Yetkili Eğitim Merkezi, müşterilerin ve iş ortaklarının Hitachi Vantara ürün, çözüm ve sistemlerini çok daha etkin ve yetkin bir şekilde kullanabilmelerine olanak tanıyor.

PLATFORMDA HANGİ ÜRÜNLER YER ALIYOR?

Kapsamlı eğitim takvimi ile müşteri ve iş ortaklarına sürekli teknik eğitimler sunan Yetkili Eğitim Merkezi, yeni veri depolama platformu Jupiter'in yanı sıra Lumada ile yapay zekâ, Pentaho ile analitik platform ve Rean Cloud ile bulut teknolojileri alanında katılımcıların uzmanlıklarını ve yetkinliklerini



Hitachi Vantara Yetkili Eğitim Merkezi'nin açılışı, Hitachi Vantara Gelişen Ülkeler Başkan Vekili Tom Pegrume (solda), Hitachi Vantara Genel Müdürü Önder Sönmez (ortada) ve LinkPlus Genel Müdürü Cem Borhan'ın katılımıyla gerçekleşti.

artırıyor. Hitachi Vantara ürün ve çözümlerini daha etkin kullanabilmeyi hedefleyen katılımcılara, her biri 3

ila 5 gün arasında süren eğitimleri tamamladıklarında Hitachi Vantara sertifikası veriliyor.



LinkPlus İş Geliştirme Direktörü Cenk Soyluoğlu ve Hitachi Vantara Kıdemli Kanal Müdürü Özlem Köklü Avcı

BÜYÜME ODAKLI İŞBİRLİĞİ

Yetkili Eğitim Merkezi olarak LinkPlus'ın seçilmesinin en büyük nedeninin Hitachi Vantara'ya yaptığı katkılar olduğunu belirten Hitachi Vantara Kıdemli Kanal Müdürü Özlem Köklü Avcı, "LinkPlus'la olan ilişkilerimizi eğitim alanında geliştirmek, büyütmek, müşterilerimiz ve iş ortaklarımızın ürünlerimizi ve çözümlerimizi daha yetkin ve etkin bir şekilde kullanabilmelerini sağlayacak bir ortam oluşturmak ve eğitilmiş bir kullanıcı kitlesi yaratmak bizim en büyük önceliklerimiz arasında yer alıyordu. Bu eğitim merkezi, Türkiye'deki müşterilerimizin yetkinliklerini ve uzmanlıklarını en üst düzeye çıkararak ürün ve çözümlerimizden en iyi faydayı elde edebilmeleri açısından çok büyük önem taşıyor. İhtiyaç duyulabilecek her türlü kaynağın ve deneyimli eğitmenlerin

bulunduğu eğitim merkezimiz, müşterilerimizin hayatına dokunarak iş problemlerine yardımcı olmamıza ve hayatlarını kolaylaştırmamıza olanak tanıyacak" diyor. Distribütör oldukları ilk günden itibaren Türkiye'de bir eğitim merkezine ihtiyaç duyulduğunu ve bu görevi üstlenmek istediklerini Hitachi Vantara yetkilileri ile paylaştıklarını ifade eden LinkPlus İş Geliştirme Direktörü Cenk Soyluoğlu ise sözlerine şöyle devam ediyor: "Bu hayalimizin gerçeğe dönüşmesinden dolayı son derece mutluyuz. Eğitim merkezimiz sahip olduğumuz bilgi birikimini ve deneyimlerimizi müşterilerimize ve iş ortaklarımıza aktarabilme fırsatı sağlıyor. Tüm eğitimler bizim binamızda gerçekleştiriliyor. Hitachi Vantara, ilk distribütör olduğumuzda sadece bir veri depolama çözüm

üreticisiyken zaman içerisinde satın alınan şirketlerle birlikte kurumların dijital dönüşüm yolculuğunda ihtiyaç duyabilecekleri tüm çözümleri tek tek portföyüne kattı. Dolayısıyla, eğitim merkezimizde verilecek eğitimlerde gerek Hitachi Vantara'nın son derece güçlü olduğu kurumsal veri depolama çözümleriyle ilgili, gerekse yeni nesil bulut teknolojileri ve verinin çok daha iyi kullanılabilmesine olanak tanıyacak, kurumların gerçekten fayda sağlayacakları eğitimler de yer alacak."

EĞİTİMLER BAŞLADI

Hitachi Vantara'nın içinde bulunduğu bölgede Dubai'den sonra açılan ikinci merkez olarak 6 Ocak 2020 tarihi itibarıyla hizmet vermeye başlayan İstanbul'daki yetkili eğitim merkezine, sadece Türkiye'den değil yurtdışından da katılımcılar büyük ilgi gösteriyor.

LinkPlus, Tableau'nun Türkiye Distribütörü Oldu



LinkPlus, 2020 yılını karşılarken, çatısı altındaki markalar arasına Veri Analitiği ve İş Zekâsı alanında öncü marka Tableau'yu da dahil etti. Tableau, Türkiye pazarında LinkPlus'ın deneyimini de yanına alarak yaygınlaşmaya devam edecek.

Uzun yıllar Redington çatısı altında farklı markalarla katma değerli distribütörlük deneyimini genişleten LinkPlus, 2020 yılında Veri Analitik ve İş Zekâsı alanında Tableau'yu da çatısı altına almaktan büyük memnuniyet duyuyor. Tableau'nun Veri Analitik platformu, tüm sektörlerdeki şirketlerin iş kararlarını vermelerinde verileri kullanmalarına yardımcı oluyor. LinkPlus ve Tableau işbirliği, Türkiye'de daha fazla kuruluşun veriden en yüksek değeri elde etmesi için gereken gücü sağlayacak. Tableau'nun self-servis analitik platformu, herhangi bir beceri düzeyindeki kişilere verilerle çalışma imkânı sunuyor. Bireylerden ve

kâr amacı gütmeyen kuruluşlardan devlet kurumlarına ve Fortune 500 kuruluşlarına kadar, dünya çapında on binlerce müşteri, hızlı bilgi almak ve etkili, veri odaklı kararlar verebilmek için Tableau'yu kullanıyorlar. Platform, görsel analitiği sezgisel hale getirerek, kişilerin cevap beklenen soruları hızlı bir şekilde veriye dayanarak yanıtlamasına ve kuruluşlarındaki bilgileri paylaşmasına olanak tanıyor. Küresel işletmeler, başlangıç dönemindeki startup'lar, hükümetler ve sivil toplum kuruluşları, verilerini aksiyona geçmelerini sağlayacak iç-görülere dönüştürebilmek için Tableau'yu tercih ediyorlar.

“Tableau, 2019 Gartner Magic Quadrant’a göre son yedi yıldır peş peşe Analitik ve İş Zekâsı alanının lideri olarak tanındı. Türkiye’de de kuruluşların Tableau gibi birinci sınıf bir analiz platformundan yararlanma potansiyelinin yüksek olduğunu görüyoruz. LinkPlus olarak, Tableau’nun verilerin görülmesi ve anlaşılmasına yardımcı olma misyonunu destekliyoruz ve iş ortaklarımızla birlikte Türkiye’de bu misyonu genişletmeyi hedefliyoruz.”



VOLKAN NALCI
İş Birim Yöneticisi
LinkPlus

KURULUŞLARIN “VERİ ODAKLI” OLMALARINA YARDIM EDİYOR

Tüm dünyada kurum ve kuruluşlar, daha fazla veri odaklı olabilmek adına trilyonlarca dolar yatırım yapıyorlar. Ancak Mckinsey Analytics Anketi, kuruluşların yaptığı analizlerin yalnızca %8’inin veriden değer elde etmeyi sağlayan bir başarı ile sonuçlandığını ortaya koyuyor. Tableau ve LinkPlus işbirliğinin, Türkiye pazarındaki müşterilerin bu alandaki artan ihtiyaçlarına cevap vermeye hizmet etmesinin yanı sıra, kuruluşların bir “Veri Kültürü” oluşturmalarının değerini anlamalarına da yardımcı olması bekleniyor. Her büyüklükteki şirketin veri-odaklı bir işleyişe kavuşmasına

katkıda bulunacak veri projeleri geliştirecek olan LinkPlus iş ortakları, aynı zamanda iş zekâsına yeni bir bakış açısı getirilmesini sağlayacak Tableau atölyeleri ve etkinlikleri de düzenleyecekler. LinkPlus İş Birim Yöneticisi Volkan Nalci, “Tableau ile ortaklığımızdan heyecan duyuyoruz ve analizin “yeni neslini” şekillendirmeye ve Türkiye’deki İş Zekâsı algısını modernize etmeye yardımcı olmak istiyoruz” diyor. Zaten Türkiye’de Tableau’nun self-servis analitik platformunu kullanan müşterileri bulunuyor. LinkPlus, iş ortaklarının yardımıyla daha fazla veri odaklı olmak için Tableau kullanan kuruluşların sayısını artırmayı hedefliyor.

Mckinsey Analytics Anketi, kuruluşların yaptığı analizlerin yalnızca %8’inin veriden değer elde etmeyi sağlayan bir başarı ile sonuçlandığını ortaya koyuyor. Tableau ve LinkPlus işbirliği, Türkiye pazarındaki müşterilerin bu alandaki artan ihtiyaçlarına cevap vermeye hizmet ederken, kuruluşların bir “Veri Kültürü” oluşturmalarının değerini anlamalarına da yardımcı olacak.

Splunk Discovery Day'de Geleceği Keşfetme Fırsatı

LinkPlus, geleneksel hale dönüştürmeyi hedeflediği Splunk Discovery Day etkinliğinin ilkinin Ekim ayında Adile Sultan Sarayı'nda düzenledi. Splunk veri platformunu ve bu platform üzerine konumlandırılmış çözüm ve teknolojileri tanıtmak amacıyla düzenlenen etkinliğe, Destel Bilişim Çözümleri, Netsmart, SoftwareONE, Soitron Siber Güvenlik Sistemleri ve Seynur Bilgi Teknolojileri 'Gold Sponsor'; Konsalt Proje Yönetim ve İnşaat ile Platin Bilişim Teknolojileri 'Silver Sponsor' olarak destek verdi.

LinkPlus, distribütörlüğünü gerçekleştirdiği Splunk'ın çözüm ve teknolojilerini müşterilerine daha yakından tanıtmak amacıyla Splunk Discovery Day etkinliğini düzenledi.

Sektör liderleri ve teknoloji uzmanlarının bir araya geldiği etkinliğin açılışında konuşan LinkPlus Genel Müdürü Cem Borhan, hızla değişen ve hayatın içine nüfuz eden teknolojilerle birlikte iş yapış şekillerinin de dönüştüğüne dikkat çekerek, sözlerine şöyle devam etti: "Birçok kurumun halihazırda işlediği veya işlemediği veri boyutu dramatik bir şekilde büyüyor. Nesnelerin İnterneti (IoT), Endüstri 4.0, Yapay Zekâ (AI) ve Robot teknolojileri alanlarındaki gelişmeler artarak devam ederken, hayatımızın içine daha fazla girmeye başlıyor. Katma Değerli Distribütör olarak iş ortaklarının oluşturduğu ekosistemi geliştiren, toparlayan, sinerji oluşturacak ortamları yaratan bir kimliğimiz var. Bu kimliğin bir yansıması olan Splunk Discovery Day'de müşterilerimize, ellerindeki verileri kurumları için nasıl daha faydalı hale getirip,

günümüz teknolojilerine uydurabileceklerini göstermeyi hedefledik. Kurumların yarın için ihtiyaç duyduğu çevikliği, vizyonu ve performansı anlatırken yeni yaklaşımlar hakkında da bilgi paylaşma fırsatı yakaladık" dedi.

TÜRKİYE'DE %50 ÜZERİNDE BÜYÜME

Splunk'ın 2017 yılında 1 milyar dolar global ciro elde ederken bugün 2-2,5 milyar dolarlık düzeye ulaştığını vurgulayan Borhan, sözlerine şöyle devam etti: "Bu, dünya genelinde yüzde 40 civarı bir büyümeye karşılık geliyor. Splunk, bizim coğrafyamızda Türkiye'nin de içinde bulunduğu gelişmekte olan ülkelerde yüzde 50'nin üzerinde bir büyümeye ilerliyor. Türkiye özelinde konuşursak daha yüksek oranlı bir büyümemiz var. Kurumların ihtiyaçlarına cevap verebilmek için yapımızı giderek büyütüyoruz. Hem insan kaynağı hem iş ortaklarımızın artışıyla birlikte her konuda destek verebileceğimiz bir yapıyı kurmak için buradayız."

VERİ HERKES İÇİN ERIŞİLEBİLİR VE DEĞERLİ

Sektör liderleri ve teknoloji uzmanlarının bir araya geldiği etkinlikte, Splunk bölge yönetiminden gelen isimler de sunumlarıyla yer aldı.

Splunk EMEA Gelişmekte Olan Pazarlar Bölgesi Başkan Yardımcısı Nordine Aamchoune ve Splunk Batı Avrupa Bölgesi Satış Direktörü Amit Stark, şirketlerin daha üretken, kârlı, rekabetçi ve güvenli olmasını sağlayan Splunk platformu hakkında detaylı bilgiler paylaştı.

Fortune 100 listesindeki şirketlerin yüzde 92'sinin Splunk çözümlerini kullandığını belirten Nordine Aamchoune, "5.000'den fazla çalışmamız ve dünya çapında 15.000'den fazla müşterimiz var. Geçen her yıl, dünya çapında yüzde 40 ila 50 oranında büyümeyi hedefliyoruz. Referanslarımıza baktığınızda, hepsinin farklı ve geniş alanlarda faaliyet gösterdiğini, Splunk'ın sektörler, ülkeler ve özel kuruluşlar arasında fiilen en çok tercih edilen güvenlik çözümü



“ Splunk, Türkiye'nin de içinde bulunduğu gelişmekte olan ülkeler bölgesinde yüzde 50'nin üzerinde bir büyümeye ilerliyor. Türkiye'deki büyümenin bölgedeki oranların da üzerinde bir seyir gösterdiğini görüyoruz. ”

CEM BORHAN
Genel Müdür
LinkPlus



Splunk Doğu Avrupa Bölge Satış Direktörü Amit Stark, Splunk'ın anlamlı veriye ulaşım yolculuğunun detaylarını anlattı.



Splunk EMEA Gelişen Pazarlar Başkan Yardımcısı Nordine Aamchoune, Splunk Discovery Day'de Splunk'ın dünden bugüne gelişimini ve sunulan önemli çözümleri katılımcılarla paylaştı.

sağlayıcısı olduğunu görebilirsiniz" dedi. Dünyada büyük bir değişim yaşandığına dikkat çeken Aamchoune, sözlerine şöyle devam etti: "Artık daha karışık, telefona daha bağlı bir dünyamız var. Bugün buluttan, drone'lardan, sensörlerden, Nesnelerin İnterneti'nden (IoT), Makine Öğrenmesi'nden ve Yapay Zekâ'dan konuşuyoruz. Tüm bunlar, inanılmaz büyüklükte veriyi açığa çıkarıyor ve çoğu müşterimiz bu verilerden

avantaj sağlıyor. Biz müşterilerimize zaman ve bütçe yönetimi, etki azaltımı, daha düşük risk konusunda destek veriyoruz."

SPLUNK İLE BAŞARI HİKAYELERİ

Sektör ya da ölçekten bağımsız olarak, veri üreten bütün işletmelerin kullanabileceği bir çözüm olan Splunk'ın şirketlere kattığı katma değeri ise Garanti BBVA IT Güvenlik Müdürü Çağlayan Kılıç ve IST Systems, IT Altyapı

ve Güvenlik Sistemlerinden Sorumlu Genel Müdür Yardımcısı Emrah Bayarçelik anlattı. Bayarçelik, dünyada bir ilki gerçekleştirerek İstanbul Havalimanı'nda kurdukları Siber Güvenlik Operasyon Merkezi hakkında verdiği bilgilerle büyük ilgi gördü. Etkinlikte ayrıca, IT operasyon analitiği ve güvenlik konularında teknik bilgilerin uzmanları tarafından paylaşıldığı sunumlar gerçekleştirildi.

Dünyanın İlk Havalimanı Siber Güvenlik Operasyon Merkezinde Splunk Var!

İstanbul Havalimanı'nın ICT (Information & Communication Technology - Bilgi ve İletişim Teknolojisi) altyapısını, havacılık sistemlerinin tasarımını ve uygulamasını gerçekleştiren IST Systems, havalimanının siber güvenlik sisteminin kalbine, kurumsal log yönetiminin öncü teknoloji çözümü Splunk'ı konumlandırdı. İş ortağı Destel Bilişim ile birlikte hayata geçirilen bu proje ile İstanbul Havalimanı, “Siber Güvenlik Operasyon Merkezi” kurulan dünyanın ilk havalimanı oldu.

IST Systems, 2018 yılında İstanbul Havalimanı için ICT altyapı (Information & Communication Technology - Bilgi ve İletişim Teknolojisi), havacılık sistemleri tasarımı ve uygulamasını gerçekleştirmek amacıyla kurulmuş bir şirket. IST Systems'in hedefi, havacılık endüstrisinde güçlü bir girişimci olmanın yanı sıra, aynı zamanda uzman ekibiyle Türkiye ve bölgedeki yeni nesil teknolojileri kullanan akıllı bina sistemlerini inşa etmek ve işletmek üzere lider bir entegratör olmak.

IST Systems, havalimanı işletmeciliği konusundaki geniş bilgi birikimi ve akıllı sistemler dünyasındaki kapsamlı uzmanlığı ile İstanbul Havalimanı'na hizmet veren çeşitli kritik havacılık sistemlerinin entegrasyonunda Ana Sistem Entegratörü olarak yer aldı. Havalimanları göz önüne alındığında BT sistemleri bütün işleyişin merkezini oluşturuyor. BT sistemleri sayesinde havalimanları en verimli tesislere dönüştürülürken, seyahat eden halka en yüksek düzeyde müşteri hizmetleri ve güvenlik sağlanmasında çok önemli bir bileşen olarak karşımıza çıkıyor. İstanbul Havalimanı'nı bilgi teknolojileri

açısından da Türkiye'de ve dünyada ilk yapan pek çok özelliği bulunuyor:

- ✓ Türkiye'nin ilk H-VPLS Network Altyapısına sahip havalimanı
- ✓ Türkiye'nin ilk Wi-Fi operatör kurulumu
- ✓ Türkiye'nin ilk 5G hazır havalimanı
- ✓ Dünyanın ilk Tier-3 Havalimanı Veri Merkezi
- ✓ Dünyanın ilk siber güvenlik operasyon merkezi kurulan havalimanı

DÜNYANIN İLK HAVALIMANI SİBER GÜVENLİK OPERASYON MERKEZİ

Bir havalimanı için BT sistemleri bu kadar kritik hale gelince, bir de müşteri deneyimi gereği internet artık her noktada devredeyken, siber güvenlik konusu da çok önemli hale geliyor.

IST Systems IT Altyapı ve Güvenlik Sistemleri'nden sorumlu Genel Müdür Yardımcısı Emrah Bayarçelik, İstanbul Havalimanı'nda ortaya konulan siber güvenlik ihtiyacının yenilikçi bir bakış açısıyla değerlendirilmesinin zorunlu olduğunu belirtiyor. Doğru ekibi kurmak, projenin hak ettiği değeri sağlayabilecek deneyimli danışmanları ve global iş ortaklarını bir

araya getirmek, projenin sağlam temellere oturtulması ve başarısı için çok önemliydi. IST Systems ve ihaleyi en yüksek teknik puan ile kazanan iş ortağı Destel Bilişim ekiplerinin bu proje kapsamında ele aldığı ilk konu, IGA Güvenlik Operasyon Merkezi'nin, Yeni Nesil Siber Güvenlik Operasyon Merkezi olarak nasıl yaratılacağı oldu.

IGA operasyonunun işletimindeki en önemli noktalardan biri 26 farklı kalemde oluşan Siber Güvenlik projesindeki çok çeşitli üreticilerin ürünlerinin kullanıldığı bir ortamda kusursuz bir entegrasyon ortamı oluşturarak merkezi izleme platformunu hayata geçirmektir. Bu anlamda global ölçekte referans sahibi olan pek çok ürün masaya yatırıldı. IGA'nın ihtiyaç duyduğu hız ve sürekliliği performans olarak sağlayabilen en uygun platformun Splunk olduğuna karar verildi. Böylelikle Splunk Core ve Splunk Enterprise Security ürünleri projede konumlandırıldı. Sistem ve ürünler belli aşamaya geldikten sonra da Splunk UBA ürünü ile kullanıcı davranışlarına yönelik analizler yapıya eklendi. Şu anda Güvenlik Operasyon Merkezi ekibi bütün güvenlik olaylarını tek bir ekranda izleyebiliyor ve

gerektiğinde hızlıca aksiyon alabiliyor. Bu proje ile İstanbul Havalimanı, siber güvenlik operasyon merkezi kurulan dünyanın ilk havalimanı oldu. Destel Bilişim'in deneyimli ekibi ve Splunk uzmanları başından sonuna kadar sürecin yönetiminde yer aldı. Bütün sistem, en başından, en güncel teknolojilerle en doğru konseptler kullanılarak tasarlandı. Siber Güvenlik bakış açısıyla bakıldığında tehditlerin gelebileceği her noktaya kurulmuş olan sistemlerle tam entegre bir merkez yaratıldı. Süreç içerisinde karşılaşılabilecek tüm zorluklar ve tehditler düşünülerek hem birbiriyle gerekli koşullarda entegre hem de birbirinden bağımsız çalışabilecek bir tasarım gerçekleştirildi. Splunk, sadece SIEM olarak değil aynı zamanda analitik ve entegrasyon platformu olarak da konumlandırıldı. Splunk'ın sunduğu çok geniş entegrasyon yetenekleri ile operasyon başlamadan, güvenlik cihazlarının kurulumu aşamasında bile fayda görülmeye başlandı.

NEDEN SPLUNK TERCİH EDİLDİ?

- ✓ Entegrasyon seçeneklerinde neredeyse sonsuz esneklik sağlıyor.

“Tamamı akıllı sistemlerden oluşan İstanbul Havalimanı'nda, toplam sayısı 40bin'in üzerinde olan sensor verilerini de Splunk'a entegre ederek, Yapay Zekâ ve Makine Öğrenmesi özellikleri ile IoT Analytics Platformu oluşturmayı hedefliyoruz.”

EMRAH BAYARÇELİK
Genel Müdür Yardımcısı
IT Altyapı ve Güvenlik Sistemleri
IST Systems

- ✓ Farklı fonksiyonları üstlenen, farklı üreticilere sahip, 26 farklı Siber Güvenlik Ürününün kalbi olarak çalışıyor.
- ✓ Kurulum aşamasında, sistemlerin entegrasyonları sırasında, maksimum görünürlük ile zaman tasarrufu sağlıyor.
- ✓ Güvenlik ile ilgili bütün log'lara ve alarmlara tek arayüzden erişilmesini sağlıyor. Analiz ve aksiyon işlemleri en üst düzeyde verimlilikle yapılabilir.

GELECEK HEDEFLER

İstanbul Havalimanı, Splunk'ın siber güvenlik teknolojileriyle kurulan operasyon merkezi ile kendilerini geleceğe de taşıyacak güçlü bir altyapıya kavuştu. Söz konusu altyapının mimarı ve uygulamacısı olan IST Systems Genel Müdür Yardımcısı Emrah Bayarçelik, bundan sonraki hedeflerini de şu sözlerle ifade ediyor: “Tamamı akıllı sistemlerden oluşan İstanbul Havalimanı'nda, toplam sayısı 40 binin üzerinde olan sensor verilerini de Splunk'a entegre ederek, Yapay Zekâ ve Makine Öğrenmesi özellikleri ile IoT Analytics Platformu oluşturmayı hedefliyoruz.”

SİBER GÜVENLİK OPERASYON MERKEZİ İÇİN SPLUNK

İstanbul Havalimanı'nda kurulan Siber Güvenlik Operasyon Merkezi, Splunk'ın Güvenlik Operasyon Merkezleri oluşturmaya yönelik olarak geliştirdiği kurumsal log yönetimi ve otomasyon teknolojileri kullanılarak tasarlandı. Splunk SOC ve Splunk UBA çözümlerinden yararlanan IST Systems'in hayata geçirdiği merkezin sunduğu özellikler ve avantajları aşağıdaki gibi özetlemek mümkün:

- ✓ İki veri merkezinde MultiSite Cluster olarak Aktif/Aktif kesintisiz çalışma,
- ✓ Firewall ve diğer tüm güvenlik cihazları log'larına tek noktadan erişim,
- ✓ Farklı üreticilerin ürünleri arasında entegrasyonların sağlanmasıyla bilgi paylaşımı (Identity Awareness-Kimlik Farkındalığı),
- ✓ Yerli ve yabancı istihbarat servislerine entegrasyon,
- ✓ UCMDDB ve Service Manager sistemlerine entegrasyon,
- ✓ Google YouTube entegrasyonu ile dinamik öğrenen proxy blacklist yönetimi,
- ✓ Splunk üzerinden, kullanıcıyı 802.1x ile karantinaya alma, zararlı trafik durumunda firewall'a kural ekleme ve benzeri entegrasyonlar.

Seynur ve Soitron Splunk İçin Güçlerini Birleştirdi

Splunk uzmanlığı ile öne çıkan, Professional Services Partner yetkinliğine sahip Seynur BT ve Soitron Group'un ortağı Sekom'un kuruluşu olan Soitron Siber Güvenlik Hizmetleri, Türkiye'de Kurumsal Log Yönetimi dönemini başlatmak üzere yeni bir işbirliğini hayata geçirdi.



SELİM SEYNUR
Genel Müdür
Seynur BT

REHA AKBAŞ
Yönetici Direktör
Soitron Siber Güvenlik Servisleri

Log Yönetimi, bugün veri güvenliği ve veri analizinde en önemli rolü oynayan kavram olarak öne çıkıyor. Özellikle siber güvenlik ihtiyaçları arttıkça, kuruluşlar adacıklar halinde, farklı operasyonlar için ayrı ayrı log izleme ve yönetme teknolojileri kullanımını terk ediyorlar. Artık kuruluşları rekabette öne çıkarmayı ve konsolidasyonun getirisiyle maliyetleri düşürmeyi hedefleyen yeni bir yaklaşıma, Kurumsal Log Yönetimi'ne geçiliyor.

Bu alandaki teknoloji öncülüğünü ise Splunk Professional Services Partner yetkinliğine sahip Seynur BT ve Soitron Siber Güvenlik Hizmetleri üstleniyor. Seynur BT ve Soitron Siber Güvenlik Hizmetleri tarafından hayata geçirilen işbirliğinin ayrıntılarını, Seynur BT Genel Müdürü Selim Seynur ve Soitron Siber Güvenlik Servisleri'nin Yönetici Direktörü Reha Akbaş ile konuştuk.

Önce Seynur BT ve Splunk ile iş ortaklığı hakkında kısa bir bilgi alabilir miyiz?
SELİM SEYNUR: Seynur, 2006 yılında kuruldu ve 2010 yılından bu yana Splunk ile iş ortaklığımız bulunuyor. Aslında Türkiye'yi Splunk ile ilk kez 2010 yılında tanıştıran teknoloji şirketi olarak da biliniyoruz. Splunk'ın Türkiye'deki tek, bölgedeki çok az sayıdaki Professional Services Partner yetkinliğine sahip iş ortağıyız. Güvenlik, veri analizi ve veri inceleme alanlarındaki uzmanlığımız ile öne çıkıyoruz. Müşterilerimize veri odaklı çözümler sunmayı hedefliyoruz. Bu doğrultuda SIEM, yani log izleme ve log yönetimi projeleri faaliyetlerimiz içerisinde önemli yer tutuyor.

Soitron Siber Güvenlik Hizmetleri hakkında da sizden bilgi alabilir miyiz?
REHA AKBAŞ: Sektörün farklı alanlarında 20

yıllık deneyime sahip kişilerden oluşan bir ekiple güvenlik alanında hizmet vermek üzere kurduğumuz şirketimizi, yaklaşık üç sene önce Soitron Group'un stratejik iş ortağı olan Sekom İletişim Sistemleri satın aldı. Siber güvenlik alanında uçtan uca çözümlere odaklanmış bir kuruluş olarak, 2019 yılına kadar Sekom bünyesinde hizmet verdik. Ancak bilindiği gibi siber güvenlik çok hızlı büyüyen, çok dinamik bir alan. Bu nedenle 2019 yılı başında, yabancı ortağımız Soitron'un adı ile ayrı bir şirket olarak devam etmeye karar verildi.

Soitron'un yolu Splunk ve Seynur ile nasıl kesişti?

REHA AKBAŞ: Burada anahtar kelimeler, Selim'in de söz ettiği gibi "log izleme" ve "log yönetimi". Konuyu açmak için

önce yaptığımız işlerden söz etmeliyim. Biz işlerimizi üç ana tema üzerinde yönetiyoruz. İlki bizim yıllardır yürütmekte olduğumuz "Proje Hizmetleri". Çeşitli ürünleri ele alıp, katma değerli hizmetlerimizle birleştirip müşterilerimiz için ihtiyaçları olan projeleri hayata geçiriyoruz. İkincisi "Yönetilen Hizmetler". Güvenlik Operasyon Merkezi (SOC) servislerini bu başlık altında sunuyoruz. Üçüncüsü de "Tamamlayıcı Hizmetler". Bu başlık altında danışmanlık, sızma testleri, risk analiz hizmetleri gibi alanlar var. Tabi bütün bu alanlarda artık veri ve verinin izlenebilirliği, yani log izleme (SIEM) ve log yönetimi çok önemli bir ihtiyaç olarak belirliyor. 2000'li yılların başlarında güvenlik deyince, akla ilk gelen firewall kurmaktı. Biz de o zamanlar, firewall sağlayan bir şirkettik. Ancak güvenliğin değişen dinamikleri

içerisinde kendimizi yeni teknolojilere adapte etmemiz gerekti. Splunk ve Seynur ile de bu noktada buluştuk.

SELİM SEYNUR: Teknoloji dünyası, internetle birlikte çok hızlı bir şekilde dönüşüm geçirdi, geliştirdi ve büyüdü. Güvenlik ihtiyaçları çeşitlendi, giderek daha karmaşık hale geldi. Çok farklı operasyonlar için çok farklı teknolojilerin ortaya çıktığı bir zemin üzerindeyiz. Dünyada güvenlik alanında faaliyet gösteren belki binlerce üretici firma var. Akla gelebilecek en niş alandaki ihtiyaç için bile birden fazla alternatif ürün bulabiliyorsunuz. Bu da beraberinde bu yapıların yönetilebilirliği konusunu gündeme getiriyor. Çünkü teknoloji bu kadar hızlı ilerlerken, içeride bu yapıları izleyecek uzman insan kaynağı aynı hızda oluşamıyor. Dolayısıyla bu alanda da çözülmesi gereken

SPLUNK HAKKINDA

Splunk, IT operasyonlarının yönetimi/izlenmesi ve yüksek güvenlik ihtiyaçlarına çözüm getiren web tabanlı bir yazılım platformu. Log dosyaları, config dosyaları, diğer uygulamalardan gelen uyarı mesajları gibi onlarca farklı kaynaktan gelen bilgileri gerçek zamanlı olarak analiz edip indeksliyor, içerisinde arama yapılmasını sağlıyor ve bunlardan grafikler, raporlar, uyarılar ve izleme ekranları oluşturabiliyor.

Kuruluşların IT'ye yönelik güvenlik risklerini ortadan kaldıran, kullanımı kolay, bakım gerektirmeyen Splunk, dünyada kurumsal big data projelerindeki başarılı kullanımı ile de dikkat çekiyor.



REHA AKBAŞ
Yönetici Direktör
Soitron Siber Güvenlik Servisleri

“Biz bu işbirliği ile Sekom’un, Seynur’un ve Soitron’un uzmanlığını tek bir noktada birleştirmiş ve büyük bir sinerji yaratmış olduk. Bu durum tabi en çok müşterilerimiz için önemli. Çünkü bu hizmetleri ayrı ayrı yerlerden alıp, bir problem çıktığında ayrı muhataplarla karşılaşmak zorunda olmayacaklar.”

en büyük sorun, aslında yapılan yatırımların iyi yönetilmesi, iyi gözlemlenmesi olarak karşımıza çıkıyor.

REHA AKBAŞ: Çok doğru. Yıllardır bu işin içerisindeyiz, güvenlik hizmetleri artık “tamamlayıcı” hizmet olmaktan çıktı ve son yıllarda kendi başına ayrı bir segment haline geldi. Çünkü müşterilerimizin karşısına, olayın tek bir fazını değil, uçtan uca projeyi kapsayarak çıkmamız gerekiyor. Bu bakış açısına ulaştığımızda, bu alanda teknoloji geliştiren farklı üreticilerle görüştük. Splunk, hem vizyonu hem de ulaştığı teknolojik üstünlükle bize en doğru seçim olarak görüldü. Pazardaki gücünü ve öncülüğünü tekrar tekrar söylemeye hiç gerek yok. Özetle, Splunk ile yollarımızın kesişmesi kaçınılmazdı. Elbette bir de bu işin uzmanlık tarafı var ki onu da Seynur’un en iyi şekilde adreslediğini, uzun yıllara dayanan tanışıklığımız dolayısıyla biliyoruz.

Bu tanışıklık, bugün sizleri nasıl bir iş ortaklığına yöneltti?

REHA AKBAŞ: Şirketlerimizin faaliyet gösterdiği farklı alanlar, birbirini çok iyi bir şekilde tamamlıyor. Güvenlik projeleri, asla ürün satışıyla bitmeyen, katma değerli hizmet sunulması ve takip edilmesi gereken projelerdir. Sattığınız şey, uçtan uca yönetmeniz gereken, yaşayan bir süreçtir aslında. Hiçbir güvenlik projesi yoktur ki “Biz ürünü teslim ettik, hadi hoşça kalın” diyerek, ayrılabilersiniz. Seynur ile gelişen bu işbirliği, özel bir proje vesilesiyle kendiliğinden oluştu diyebiliriz. Seynur’un Splunk ile olan geçmişini, engin tecrübesini, uzmanlığını yanımıza almak, projenin başarısında çok önemli bir rol oynadı. Proje sonrasında da “Biz bu işbirliğini neden genişletmeyelim” diye düşündük ve daha yapısal bir hale getirmeye karar verdik.

Soitron Group, aslında bu işbirliğinin benzer bir uygulamasını Slovakya’da hayata geçirdi. Biz de orada oluşmuş know-how ile birlikte Slovakya’daki altyapıyı İstanbul’a getiriyoruz.

Bu işbirliği nasıl bir strateji ile ilerleyecek ve şu anda nasıl bir noktadasınız?

SELİM SEYNUR: Öncelikle, Veri Güvenliği ve Operasyonel Veri Analizi olmak üzere, iki temel işbirliği alanı belirledik. Operasyonel Veri Analizi tarafında Splunk’ın üzerine kurulması gereken altyapının pek çok bileşeni var. Bir Sekom kuruluşu olarak Soitron, bu anlamda yazılım ve donanım maliyetlerini üstlendi. Bu yatırım, bütünüleyici bir çözüm sunma konusunda bizi çok özel bir yere taşıyor. Yine bu altyapının oluşmasında, Sekom’un Red Hat konusunda sayılı katma değerli iş ortaklarından biri olması ve ayrıca Soitron’un iyi bir network ekibine ve veri merkezi konusunda uzmanlara sahip olması çok önemli artılardı. Soitron’un yeni yatırımlarıyla kurulan altyapılar, bu alanda müşterilere uzaktan yönetim hizmetleri verilmesine olanak tanıyacak. O noktada Sekom ve dolayısıyla iştiraki olan Soitron’un çok önemli yatırımları oldu.

SEYNUR BT HAKKINDA

2006 yılında kurulan ve 2010 yılından bu yana Splunk ile iş ortaklığı olan Seynur BT, güvenlik, veri analizi ve veri inceleme alanlarındaki uzmanlığı ile öne çıkıyor ve müşterilerine veri odaklı çözümler sunmayı hedefliyor. Splunk’ın Professional Services Partner yetkinliğine sahip Türkiye’deki tek iş ortağı olan Seynur BT, Türkiye’yi Splunk ile ilk kez 2010 yılında tanıştıran teknoloji şirketi olarak da biliniyor.

REHA AKBAŞ: Veri güvenliği ve veri analitiği işine girdiğinizde bu işin sadece bir yazılım işi olmadığını görüyorsunuz. Böyle bir altyapının, software defined yani yazılım tanımlı bir network’e dayanması ve üzerinde platformların, depolama araçlarının, sanallaştırma ve container yapılarının çalışması gerekiyor. Elbette bunun bir de orkestrasyonu var. Biz bu işbirliği ile Sekom’un, Seynur’un ve Soitron’un uzmanlığını tek bir noktada birleştirmiş ve büyük bir sinerji yaratmış olduk. Bu durum tabii en çok müşterilerimiz için önemli. Çünkü bu hizmetleri ayrı ayrı yerlerden alıp, bir problem çıktığında ayrı muhataplarla karşılaşmak zorunda olmayacaklar.

SELİM SEYNUR: Yani Splunk çerçevesinde, Level 1’den Level 4’e kadar, yani mimarisinden ilk seviye desteğine, 7/24 desteğine kadar her ihtiyacı kapsayan bir çözüm sunabiliyoruz. Ayrıca, iyi anlaşılan uyumlu ekiplere sahibiz ve bu da bizim için üstlendiğimiz projelerin çok daha eğlenceli ve verimli olması anlamına geliyor.

SOITRON SİBER GÜVENLİK HİZMETLERİ HAKKINDA

Soitron’un yolculuğu, 1996 yılına dayanıyor. Ülkemizde henüz Internet altyapısı yeni yeni oluşurken, günümüzde de güvenlik altyapılarının temel taşı olan Firewall sistemlerini sağlamaya, bunlarla ilgili servisleri sunmaya başlayan ekip, güvenlik ihtiyacı ve bunu destekleyen teknolojiler geliştikçe bir dönüşüm geçiriyor.

Siber Güvenliğin sağlanmasında aslında ürünlerin yeterli olmadığını gören ekip, birbirleri ile entegre çalışan ve sık sık güncellenen farklı teknolojileri etkin ve en verimli şekilde kullanacak insan kaynağının yetiştirmesine de katkı sağlıyor. Üç yıl önce Soitron Group’un Türkiye’deki stratejik iş ortağı Sekom İletişim Sistemleri tarafından satın alınan şirket, siber güvenlik alanında uçtan uca çözümlere odaklanmış bir kuruluş olarak, 2019 yılına kadar Sekom bünyesinde hizmet veriyor. 2019 yılı başında ise sektörün büyümesiyle birlikte yabancı ortak Soitron’un adı ile ayrı bir şirket olarak yoluna devam ediyor.

REHA AKBAŞ: Elbette asıl hedefimiz işi büyütmek! Artık log tutma işlemi küçük adacıklar halinden çıkıp, kurumsal seviyede loglamaya dönüşüyor.

SELİM SEYNUR: Bu dönüşümün pazarın olgunluğuyla da çok ilgisi var elbette. Türkiye’de pazar, dünyaya göre biraz daha geriden geliyor olsa da Splunk gibi bir çözüme pek çok sektörde ihtiyaç olduğu görülüyor. Ekim ayında gerçekleştirilen Splunk Day etkinliğindeki ilgi, bize bunu açıkça gösterdi.

Müşterilerinizin, kurumsal seviyede loglama yaklaşımından ne gibi kazançları olacak?

SELİM SEYNUR: Kurumsal log yönetimi, konsolidasyonun doğası gereği öncelikle her zaman maliyet avantajları ile gelir. Bu yaklaşım, sahip olma maliyetlerini makul bir seviyeye çekerken, yeni teknolojilerle birlikte veri analizi yeteneklerini de en üst seviyeye çıkaracak. Buradan elde edilen sonuçlar, kuruluşların çevikliğini, verimliliğini, yönetimin daha isabetli kararlar almasını sağlayacak.



SELİM SEYNUR
Genel Müdür
Seynur BT

“Kurumsal log yönetimi, konsolidasyonun doğası gereği öncelikle her zaman maliyet avantajları ile gelir. Bu yaklaşım, sahip olma maliyetlerini makul bir seviyeye çekerken, yeni teknolojilerle birlikte veri analizi yeteneklerini de en üst seviyeye çıkaracak.”

Global Telekom Suçları İnternet Güvenliğini Tehlikeye Atıyor

Telekomünikasyon alanında yaşanan gelişmeler devam ettikçe, güvenliğin de aynı doğrultuda gelişmesi gerekiyor. Günümüzün tehdit durumunu anlamak telekom sahtekârlıkları gibi suçların yol açabileceği zararların etkisini azaltmaya yardımcı olurken, IoT çağında karşılaşılabilecek tehditlere karşı da işletmelerin ve kullanıcıların hazır olmasını sağlıyor.



Yazan:

HASAN GÜLTEKİN

Türkiye ve Yunanistan Ülke Müdürü
Trend Micro

Telekomünikasyon, nesnelerin interneti ve kablosuz teknolojilerin 5G'ye dönüşümünde büyük bir etkisi olan, teknolojiye gelişmelere ve toplumun değişen taleplerine cevap olarak sürekli gelişmeye ve genişlemeye devam eden önemli bir alan olarak öne çıkıyor.

Telekom operatörlerinin ağı aynı zamanda kullanıcıların daha fazla internet içeriği yüklemelerini ve daha hızlı veri aktarmalarını sağlamak için birer içerik dağıtım ağı (CDN) haline geliyor. Telekomünikasyon, şirketlerin iş yapış şeklini, hizmet verme yöntemlerini, bilgi yaymayı ve modern yaşamı birçok yönden etkilediği için bu alandaki gelişmelerin devam etmesi gerekiyor.

Telekomünikasyon alanının kapsamı genişlemeye devam ettikçe, bu alanı anlama şeklinin kapsamının da genişlemesi büyük önem taşıyor. Başlamak için en uygun yer ise telekomünikasyon teknolojilerinin büyümesi ve evrim geçirmesi ile genişleyen tehdit ortamları. Telekomünikasyon alanıyla bağlantılı tehditlerin var olmasının nedeni, paranın telekomünikasyon operasyonları ile olan sıkı ilişkisi. Kullanıcılar, aldıkları telekomünikasyon hizmetleri için para ödüyorlar. Çevrimiçi olmak, arama yapmak, mesaj göndermek gibi işlemlerin hepsi kullanıcının seçtiği operatöre göre değişen mali değerlere sahip. Paraya olan bu doğrudan

“Telekomünikasyon alanıyla bağlantılı tehditlerin var olmasının nedeni, paranın telekomünikasyon operasyonları ile olan sıkı ilişkisi. Paraya olan bu doğrudan bağlantı, sistemden doğrudan kâr elde etmek ya da suçtan elde ettikleri parayı aklamak isteyen saldırganları çekiyor.”

bağlantı, sistemden doğrudan kâr elde etmek ya da suçtan elde ettikleri parayı aklamak isteyen saldırganları çekiyor. Telekomünikasyona yönelik tehditlerin ve diğer bileşenlerin derinlemesine ve kapsamlı bir şekilde incelendiği Europol Siber Suç Merkezi (EC3) ile birlikte hazırladığımız Siber-Telekom (CyTel) Suç Raporu 2019'da telekomünikasyon alanı ile ilgili öne çıkan tehditleri fiziksel telekom altyapıları üzerinden gerçekleştirilenler ve ağ tabanlı olanlar olarak ikiye ayırdık.

FİZİKSEL ALTYAPI SALDIRILARI

Doğru araçlara sahip olan bir suçlu, telekomünikasyon alanında kullanılan altyapılar üzerinde kolaylıkla sahtekarlık yapabilir. Telekomünikasyon altyapısının en basit işlevi yapılan çağrı ve veri aktarımı trafiğini en üst düzeye çıkarmaktır. Kullanıcılar, akıllı

telefon gibi cihazlardaki SIM kartlar aracılığıyla bu altyapıya erişirler. Bir suçlu bir SIM kartın kontrolünü ele geçirdiğinde telekom altyapısının faturalama yetkinliklerine de erişebilir. Kendi telekom altyapılarına sahip olan suç yapıları tek bir telekom operatörü altında faturalanabilecek şekilde SIM kartları üzerindeki trafiği yönlendirebilirler. Bu tür bir sahtekarlık başka bir ülkedeki telekom operatörü üzerinden gerçekleştirilir, böylece sektör araştırmacılarının ve kanun güçlerinin kendilerine ulaşmalarını zorlaştırırlar.

Telekom altyapıları üzerinden gerçekleştirilebilecek saldırılara baktığımızda:

✓ **SIM Kutusu Sahtekarlığı:** Yüzlerce SIM kartın tutulduğu cihazlar olan SIM kutularının kullanıldığı bir sahtekarlık şeklidir. SIM kutusu

kartlarını kullanmak, suçluların rasgele operatör meta verilerini değiştirmek için gelen trafiği VOIP üzerinden yönlendirebilmelerine ve hatta telefon dinlemeleri ve Belgelerin İbrazı Emri gibi hukuki yaptırım süreçlerini atlatabilmelerine olanak tanır.

✓ **Uluslararası Gelir Paylaşımı Sahtekarlığı (IRSF):** Para aklayan ve CyTel hackleme gibi eylemler yoluyla fiili sahtekarlıklar gerçekleştiren iki tür suçlunun yaptıkları için kullanılan bir terimdir.

✓ **Ön Ödemeli Yükleme Suistimali:** Ön ödemeli SIM kartların taşınabilir ve anonim olma özelliğine dayanan bu saldırı yasadışı gelirlerin aktarılması potansiyeline sahiptir.

AĞ TABANLI SALDIRILAR

Fiziksel telekom altyapıları, suçluların saldırılarını gerçekleştirmek için kötü amaçlı kullanabileceği tek araç değildir. Ayrıca fiziksel yapılar ve uç nokta cihazları bağlayan ağları da hedefleyebilirler. Suçlular ağların farklı yönlerini telekomdan kazanç sağlamak için kullanabilir. Telekom ağları üzerinden gerçekleştirilebilecek saldırılara bakıldığında:

✓ **Özel Santral ya da PBX Sistemlerini Ele Geçirme:** Bu sahtekarlık türünde saldırgan gelir oluşturan trafiği yönlendiren telekom PBX

bilgisayarlarının kontrolünü ele geçirir. Bu PBX bilgisayarlar genellikle ya üretim aşamasında tanımlanmış ya da zayıf şifrelerle korunur. Bu da hackerlar tarafından ele geçirilmesi çok kolay birer hedef haline getirir.

✓ **Üyelik Sahtekarlıkları:** Bu saldırı türünde saldırgan yasal bir telekom kullanıcı hesabına erişir ve arkasından da hesabın sahibine eşit bir kontrol elde eder. Bu erişim aynı zamanda saldırganın yasal kullanıcının faturalama hesabını etkilemesine ve hatta hesabına erişememesine neden olabilir.

✓ **Wangiri:** Otomatik bir sahtekarlık yolu olan Wangiri'de birçok numara ya da kişi otomatik olarak aranır ama aranan kurbanın telefonu yalnızca bir kez çalar. Çağrıyı cevaplayamayan kurban, arayan numarayı geri aradığında anında faturalama gerçekleştirilir. Eğer saldırganın numarası özel bir numaraysa, fatura daha da yüksek olur.

✓ **Ses Oltalama / Vishing:** Bu sosyal mühendislik tekniğinde otomatik olarak gerçekleştirilen sesli arama ya da mesajlar kullanılır. Kurban, önemli kişisel bilgilerini vermesi için ikna edilir.

NASIL DAHA GÜVENDE OLABİLİRİZ?

Bahsedilen tehditler, sektörler ve kullanıcılar için vazgeçilmez hale gelen

altyapılar, süreçler ve telekomünikasyon teknolojilerinin birebir benzerlerinin kullanımı sayesinde gerçekleştirilir. Siber suçlular, cihazlara ve ağlara bulaşacak zararlı yazılımların kurulumu gibi bilindik tehditleri de bu altyapılara karşı kullanabilirler. Bu tehditler, siber suçluların kritik sektörler tarafından kullanılan tesisler aracılığıyla kendilerini zenginleştirecek fırsatları nasıl yarattığını gösteriyor. Telekomünikasyon teknolojilerini gerçek amacı olan kullanıcıları birbirine bağlamak ve dünyanın geri kalanıyla iletişim kurmalarına yardımcı olmak için kullanmak, aynı zamanda saldırılara karşı hazırlıklı olmayı ve korunmayı da içermesi gerekiyor. Sektörlerin ve kullanıcıların birbirleriyle nasıl bağlantı kurduklarının temelini ekleyen bu tehditlere karşı telekomünikasyon alanında hizmet veren paydaşların işbirliği çok önemli. Kullanıcılar, telekomünikasyon şirketleri, hükümetler ve kolluk güçleri tamamen durduramasalar bile telekom sahtekarlıklarının etkilerini azaltmakta büyük rol sahibidir. Telekomünikasyon sektörü 5G gibi uzun zamandır beklenen teknolojilerle büyümeye devam ettikçe, mevcut ve olası tehditlere karşı fiziksel ve siber altyapıların güvenliğini geliştirmek için, özel sektör ve kamunun bilgi paylaşarak birlikte çalışması her zamankinden daha önemli hale gelmiş durumda.

Trend Micro, Cloud Conformity ile Liderliğini Sağlamlaştırdı

Cloud Conformity satın almasıyla Trend Micro, sahip olduğu buluta yönelik hizmet ve çözümlerini daha da genişletirken, bulut altyapısının yanlış yapılandırmasının neden olduğu çoğu zaman gözden kaçırılabilen güvenlik sorunlarına da çözüm getiriyor.

Bulut güvenlik çözümlerinin küresel lider şirketlerinden Trend Micro, bulut güvenliği durumunun yönetimine (Cloud Security Posture Management – CSPM) olanak tanıyan yenilikçi ürünlere sahip Cloud Conformity'yi satın aldı. Trend Micro'nun stratejisi müşterilerin işlerinde herhangi bir aksamaya neden olmadan bulut güvenliği sağlamaya dayanıyor. Bulut güvenliği alanındaki yeniliklerine hız kesmeden devam eden Trend Micro, bu satın alma ile birlikte bulut altyapısında meydana gelebilecek sorunları otomatik olarak tanımlayabilecek ve düzeltebilecek yetenekleri çözümlerine ekliyor. Cloud Conformity'nin ürünleri maliyetleri optimize etmenin yanı sıra PCI, GDPR, HIPAA ve NIST gibi önemli düzenlemelerle uyumluluğun sağlanmasına yardımcı oluyor.

BULUT RİSKLERİNE KARŞI EN İYİ ÇÖZÜMLER

Bulut teknolojilerinin kullanıma başladığı günden bu yana diğer üreticilerin aksine bulut alanında tümleşik güvenlik oluşturmaya odaklandıklarını belirten Trend Micro CEO'su Eva Chen "Buluta taşınan kurumların sayısı arttıkça, müşterilerimiz kendilerini yönetilmeyen risklere açık bırakan bulut uygulamalarıyla çalıştıkları hissine kapılıyorlar. AWS'nin 2019 Yılı Teknoloji İş Ortağı olan Cloud Conformity, bu uygulamaları ve getirdiği riskleri çok iyi anlıyor. Cloud Conformity'nin önerdiği çözümler, portföyümüzü mükemmel bir şekilde tamamlayacak ve müşterilerimize çok hızlı bir şekilde katma değer sunacak. Cloud

Conformity, hem çalışanları hem de teknolojisiyle Trend Micro'ya tamamen uyum sağlayacak" diyor.

EKİP DE TREND MICRO AİLESİNE KATILDI

Belirli bir amaca yönelik satın almalarda çalışanlar da teknoloji kadar büyük önem taşıyor. Trend Micro, pazar lideri bulut güvenliği stratejilerinin bir parçası olarak Cloud Conformity'nin hem çalışanları hem de teknolojisi sayesinde büyümesini sürdürmeye devam edecek. Çalışanların Trend Micro ailesine katılması, teknolojinin yanı sıra işletmelerin bulut teknolojilerini sadece güvenli bir şekilde değil aynı zamanda verimli bir şekilde kullanabilmelerini sağlayacak deneyimi ve uzmanlığı da beraberinde getirecek.



Trend Micro COO'su **KEVIN SIMZER** ve Cloud Conformity CEO'su **MICHAEL WATTS**

“En iyi yaptığımız işi daha da iyi yapma ve çözümlerimizi çok daha geniş bir kitleye sunabilme olanağı elde edeceğiz. Müşterilerimizin AWS, Azure ve Google Cloud dahil olmak üzere tüm bulut ortamlarında kendilerine daha fazla güvenlik ve uyumluluk sağlayacak bu sade yaklaşımı beğeneceklerini umuyoruz.”

MICHAEL WATTS
CEO
Cloud Conformity

MÜŞTERİLER GÜVENDE HİSSEDİYOR

Gartner'a göre 2023 yılında bulut güvenliğinde meydana gelen sorunların en az yüzde 99'u müşterilerin yaptıkları hatalardan kaynaklanacak. Yine Gartner'a göre 2024 yılında CSPM (Bulut Güvenliği Durumu Yönetimi) çözümlerini uygulayan ve geliştirme süreçlerine genişleten kuruluşlar, yanlış yapılandırmadan kaynaklanan bulutla ilgili güvenlik olaylarını yüzde 80 oranında azaltacak(*). Trend Micro'nun bulut güvenliği hizmetlerinden oluşan kapsamlı çözümleri, aynı anda uyumlulukla ilgili standartların karşılanmasını sağlarken risklerin de etkin bir şekilde yönetildiğine dair güvence sunuyor.

(* Gartner, Inc.; Innovation Insight for Cloud Security Posture Management; 25 Ocak 2019 | G00377795)

Konuyla ilgili görüşlerini aktaran Virgin Australia Baş Mimarı Russel Jones, "Güvenlik ve uyumluluk konusundaki kararlılığımızla tamamlanan AWS ile hızlı bir şekilde büyüme sürecimiz, Cloud Conformity sayesinde ölçeklenebilir ve eyleme geçilebilir bir hale geldi. Ürünleri büyüdükçe sürekli esneklik sağlayarak bize daha fazla görünürlük, performans iyileştirme ve maliyetleri optimize etme yeteneği sağladı" diyor. Araştırmalar, küçükten büyüğe tüm kuruluşların bulut tabanlı dağıtımı benimsediğini ve yalnızca bilgi işlem hizmetlerini değil aynı zamanda depolama, mesajlaşma ve diğer birçok hizmeti de kullandıklarını net bir şekilde gösteriyor. Bu satın alma ile Trend Micro, güvenlik

önerilerini, sadece bilgi işlem iş yüklerini güvence altına almanın ötesinde bulut güvenliği konusunda yardıma ihtiyaç duyan kuruluşlara da sunabiliyor. Lider bulut güvenliği çözümleri sağlayıcısı olan Trend Micro'nun bir parçası olmanın getireceği fırsatların heyecanını yaşadıklarını belirten Cloud Conformity İcra Kurulu Başkanı Michael Watts, "En iyi yaptığımız işi daha da iyi yapma ve çözümlerimizi çok daha geniş bir kitleye sunabilme olanağı elde edeceğiz. Müşterilerimizin AWS, Azure ve Google Cloud dahil olmak üzere tüm bulut ortamlarında kendilerine daha fazla güvenlik ve uyumluluk sağlayacak bu sade yaklaşımı beğeneceklerini umuyoruz" diyor. Trend Micro, Cloud Conformity çözümünü hemen kullanıma hazır hale getirmiş bulunuyor.

E-posta, Ağ, Uç Nokta, Sunucu ve Bulut İş Yükleri İçin XDR

Trend Micro, e-posta, ağ, sunucu ve bulut iş yüklerine entegre edilmiş tespit ve karşılık verme (XDR – X Detection & Response) yetkinliklerini sunan ilk şirket oldu. Daha hızlı tespit için daha geniş çaplı görüntüleme ve uzman güvenlik analitiği ile güvenlik ekiplerinin verimliliği en üst düzeye çıkarılıyor.

ESG araştırması kurumların yüzde 55'inin 25'ten fazla farklı siber güvenlik teknolojisi kullandığını gösteriyor⁽¹⁾. Ama buna rağmen saldırılar artıyor ve var olan kontrolleri aşıyorlar. 2018 SC Media Araştırması'na göre BT güvenlik ekipleri her gün 10.000'den fazla güvenlik uyarısı alıyor. Bunun sebep olduğu küresel boyuttaki sorunlar ve verimsizlik de ortada. Verizon 2018 Veri Sızıntısı İnceleme Raporu'na göre "bir sızıntının tespit edilme süresi 197 güne çıkarken önemli bir ihlal olduğunun anlaşılma süresi ise 69 güne çıkmış". Bu da suçluların neredeyse 9 ay boyunca bir kurumun içinde saklandığını ve zarara yol açtığını gösteriyor.

Siber güvenlik çözümlerinin küresel lider şirketlerinden Trend Micro, e-posta, ağ, sunucu ve bulut iş yüklerine entegre edilmiş tespit ve karşılık verme yetkinliklerini yani XDR çözümünü sunan ilk şirket oldu. Ürün, fark edilmeden kurumunuza yerleşen ve tehdit altında bırakan karmaşık saldırıların tespit edilebilmesi için güvenlik silolarındaki küçük olayları birbirine bağlarken işletmelere risk durumunun daha geniş açıdan görüntülenebilmesini sağlamak üzere tasarlandı.

Trend Micro ağ savunma ve hibrit bulut güvenliği başkanı yardımcısı Steve Ouane tehdit tablosunun yavaşlamadan sürdüğünü ve istihdam açığının ise neredeyse çözümsüz olduğunu, dolayısıyla kendilerine çok iş düştüğünü belirtiyor. "İşletmelerin güvenliği yalnızca uç noktalara dayanmamalı. E-posta gibi kilit tehdit vektörlerini görmezden gelen geleneksel EDR ürünlerinin aksine biz mümkün olan en kısa sürede ortaya çıkanları en eksiksiz tespitler için çok daha fazla kaynakta ölçeklendirme gerçekleştiriyoruz." E-posta, ağ, uç nokta ve bulut iş yüklerinde tespitleri, telemetriyi, veri işlemeyi ve ağ meta verilerini birbirine bağlamak insan eliyle yapılan işleri en aza indirirken ekiplerin farklı ürün silolarındaki günlük uyarı yoğunluğunu işlemekten geçirmelerinin mümkün olmadığı olayları da hızla birbiriyle ilişkilendiriyor. Trend Micro'nun küresel tehdit istihbaratı, olay verileri çevresine daha fazla uygunluk ve içerik ekliyor. Ayrıca en yüksek öncelikli tehditleri hedef alan şirket güvenlik uzmanlarının önde gelen tespit kuralları ile de sürekli geliştiriliyor. Trend Micro'nun XDR çözümünde "X", saklı tehditleri bulmak için kritik olan daha

fazla koruma noktasından daha kapsamlı veri setleri elde etme anlamına geliyor. Sonuçlanan tespitler daha kesin, daha hızlı gerçekleştiriliyor ve hiç olmadığı kadar daha iyi içerik sağlıyor. Yorumlanan uyarılar için tek bir güvenlik doğrusu ve standart hale getirilmiş bir şemaya sahip olmak, BT güvenlik ekipleri için hayatı daha kolay hale getiriyor. Gartner'a⁽²⁾ göre, "Tehditler, inceleme yap-bozunun eğer tek bir parçasına bakıyorsanız çok daha karmaşık, çok yönlü ve kaçırması kolay hale geliyor. Birçok güvenlik teknolojisinden birlikte yararlanmak ve büyük resmi anlamak için iç ve dış kaynaklardan gelen verileri geniş çaplı kullanmak tehditleri kurum için gerçek bir problem haline getiriyor. Modern güvenlik problemlerini gerçekten çözmek için işbirliği, içerik, sistem zekâsı ve sanallaştırmaya ihtiyaç var." Kapsamlı XDR çözümü, büyük ölçekli şirketlerdeki Trend Micro çözümlerinden toplanan veri setlerine en etkili uzman analitiklerini uygulayarak, saldırıları tanımlamak ve durdurmak için daha hızlı bağlantılar oluşturuyor. Trend Micro'nun Yönetilen XDR'ı 7/24 kapsamlı tehdit analizi, tehdit avcılığı, karşılık verme planları ve düzeltme tavsiyeleri de sunuyor.

XDR: GELİŞMİŞ TEHDİTLERE KARŞI İLERİ DÜZEY GÜVENLİK

Daha sofistike hale gelen ve gelişen siber saldırılar standart tespit yöntemlerinden kaçınıbiliyor. Trend Micro'nun bu saldırıların tespit edilmesini ve hızla yanıt verilmesini sağlayan XDR teknolojisi işletmelere üst düzey koruma sağlıyor.

Trend Micro'nun üst düzey koruma sağlayan çözümleri hakkında bilgi almak için:

www.trendmicro.com.tr



THE ART OF CYBERSECURITY

⁽¹⁾ ESG, Siber Güvenlik Tablosu: Büyük Ölçekli Şirket Sınıfı Üreticilerin Evrimi, Jon Olsik, Bill Lundell, Kasım 2018

⁽²⁾ Gartner, Gelişmekte Olan Teknoloji Analizi: SOAR Çözümleri, Baskı 7 Aralık 2018

LC Waikiki, Hitachi All-Flash Solutions ile Büyüyor

LC Waikiki’de kurulan yeni Hitachi All-Flash Solutions altyapısı sayesinde, kuruluş artık global çaptaki ciddi büyüme hedeflerine doğru daha emin adımlarla ilerliyor.

AMAÇ: Miyadını doldurmak üzere olan altyapıyı yeni büyüme planları ve artan veri miktarına yanıt verecek şekilde güncellemek.

ÇÖZÜM: Esnek, yüksek performanslı ve güvenilir All-Flash çözümleri.

İŞ HEDEFLERİ

Orta doğu ve Asya pazarının en büyük tekstil perakendecisi olan LC Waikiki, Türkiye’deki merkezinden tüm bölgeye hizmet veriyor. Herkesin iyi giyinme hakkının olduğuna inanan firma, kaliteli ürünleri uygun fiyatla tüketici ile buluşturmayı hedefliyor. Günümüzde 43.200 çalışanı olan LC Waikiki 45 farklı ülkede 950 mağaza ile hizmet veriyor. 2023’te Avrupa’nın en iyi üç moda perakendecisinden biri olmayı hedefliyor.

Bu hedefe ulaşmak için firmanın her yıl %25-30 büyüme gerçekleştirmesi ve giderek artan müşteri taleplerine yanıt vermesi gerekiyor. LC Waikiki altyapı ve destek direktörü Ayşen Güney, “Giyim perakende pazarında çok büyük bir rekabet söz konusu” diyor ve ekliyor: “Başarılı olmak için çok iyi bir lojistik

operasyonunuz olması gerekli. Doğru ürün doğru zamanda doğru mağazada olmalı. Herhangi bir gecikme müşteri sadakatini, firmanın imajını zedeliyor ve doğal olarak da satışlara yansıyor.” Dağıtım, satış, müşteri davranışları, stoklar, müşteri geribildirimi... Bunların hepsi çok önemli veriler. LC Waikiki’nin IT Depolama ve Veritabanı Yöneticisi Gökhan Belindir de moda ve tekstil pazarının çok hızlı değişen bir pazar olduğuna dikkat çekiyor ve verinin kritik önemine şu sözlerle değiniyor: “Müşteri tercihlerinin değişimine paralel olarak firmaların kendisini hızla değiştirmesi gerekiyor. Dolayısıyla pazardaki değişimlere ayak uydurabilmek için yeni stratejiler geliştirmek durumundayız ve bunun için gerekli olan verinin doğru ve güvenli bir şekilde depolandığından,

hızlı bir şekilde erişilebildiğinden emin olmalıyız.”

HEDEFLERE ULAŞTIRACAK BİR BT ALTYAPISI

LC Waikiki, söz konusu büyüme stratejisi kapsamında önce BT varlığını gözden geçirdi ve görev-kritik SQL veri tabanı ve ürün dağıtım planlama uygulamalarının baskı altında kalmaya başladığını tespit etti. “Fiziksel ve online mağazalarımızın sayısı arttıkça veri miktarı da artıyor” diyen, LC Waikiki altyapı ve destek direktörü Ayşen Güney, bu verinin aynı zamanda LC Waikiki yönetiminin daha hızlı ve daha iyi karar alabilmesi için de kritik önem taşıdığını belirtiyor. Avrupa’nın en iyi üç moda markasından biri olmak için operasyonlar hızlı olmalıydı ve çabuk tepki verilebilmeliydi.

FAYDALAR

- ✓ IT altyapısı basitleştirildi.
- ✓ Maliyetler ve kaplanan alan azaldı.
- ✓ Karar alma süreçleri iyileştirildi ve hızlandı.
- ✓ Büyüme planları altyapı tarafından da desteklenir hale geldi.

Böylece, depolardan mağazalara dağıtım sırasında gecikmelerin yaşanmaması için, veriyi hızla erişilebilir kılmak ve güvende durmasını sağlamak üzere altyapının yenilenmesine karar verildi.

ÇÖZÜM

LC Waikiki altyapı yenilemesi için bir ihale açtı ve sektörün üç lider firmasını davet etti. Güney, “Hitachi’nin sunduğu güvenlik, performans ve yüksek teknolojiden etkilendik. Özellikle Hitachi patentli flash sürücülerin (FMD) performansı etkilemeden verilerimizi sıkıştırmaya imkân vermesi çok işimize yaradı” diyor. Hitachi Vantara projede kurulum ve premium destek servislerini sağladı. Bunların arasında yeni mimariyi uygulamak ve verileri transfer edip 24/7 saha içinde destek hizmeti vermek

de vardı. Güney “Yeni mimarinin uygulanması, 7/24 Sahada Destek ve Veri Transferi, yerel Hitachi Vantara ekibinin desteği ile sorunsuz bir şekilde uygulandı” diyor. Hitachi Virtual Storage Platform (VSP) G serisi ve all-flash VSP F serisi, LC Waikiki’nin karar verme süreçlerini ve ürünlerin mağazalara dağıtımını kontrol eden kritik hizmetlerin temelini oluşturuyor. Çözümde ayrıca Hitachi Advanced Server platformu kullanıldı. Virtual Storage Platform G400 ve Hitachi NAS Platform (HNAS) sistemlerinin sağladığı dosya paylaşımı ve yerel uygulamalar için veri ambarı kullanıldı. İş uygulamalarını optimize etmek için veri depolama performans yönetimi ve bakımı Hitachi Infrastructure Analytics Advisor (HIAA) tarafından

LC WAIKIKI BAŞARI HİKAYESİ

ENDÜSTRİ

- ✓ Perakende

ÇÖZÜM

- ✓ Sınır bilişimden Buluta veri altyapısı
- ✓ Veri depolama
- ✓ All-Flash Çözümleri
- ✓ Veri koruma

DONANIM

- ✓ Hitachi Virtual Storage Platform G1500 ve VSP G400, Hitachi NAS Platform (HNAS)
- ✓ Hitachi Virtual Storage Platform F900

YAZILIM

- ✓ Hitachi Data Instance Director
- ✓ Analyzer

SERVİSLER

- ✓ Hitachi Vantara’dan hizmet alımı
- ✓ Premium Destek Hizmetleri



“ Hitachi Vantara çözümü, esnek, yüksek performanslı, stabil ve güvenli. Büyürken gerekli olan desteği sağlaması ve kesintisiz, problemsiz bir lojistik operasyonuna sahip olmak, rekabetçi moda sektöründe olmazsa olmaz değer taşıyor. ”

AYŞEN GÜNEY
Altyapı ve Destek Direktörü
LC Waikiki

gerçekleştirildi. Veri koruma ve yönetimi de Hitachi Data Instance Director (HDID) uygulamasına emanet edildi. Bu yazılımlar sayesinde LC Waikiki disk klonlama ve yedekleme işlemlerini daha kolay halleder oldu.

SONUÇ

LC Waikiki Hitachi Vantara sayesinde altyapısını hem sadeleştirdi hem de de tek noktada toplamayı başardı. Veritabanı sorgulamaları büyük ölçüde hızlandı. Lojistik daha kolay ve daha hızlı hale geldi, envanter kontrolü daha iyi yapıldı. Güney, “Yeni altyapı lojistik operasyonlarımızı hızlandırdı ve stoklarımızdaki ürünleri mağazalara daha hızlı göndermeye başladık” diyor ve ekliyor: “Kazanılan bu zamanı da karar süreçlerinde kullanıyoruz ve bu sayede daha geniş bir ürün yelpazesi üretme imkânını kazandık.”

LC Waikiki IT Veri Depolama ve Yedekleme Uzmanı Abdurrahman Erol da, “All-flash çözümüne geçtikten sonra farklı departmanlarda çalışan elemanlarımız veriye artık daha hızlı erişebildiklerini belirttiler” diyor. Stok kontrolünün iyileştirilmesi sayesinde müşteriler artık mağaza raflarında aradıkları her şeyi bulabiliyorlar. LC Waikiki yeni altyapıya geçtikten sonra mağazadan satın alma yapmadan çıkan müşteri sayısında da bir düşme gözlemlendi. Müşteri sadakatının artması, LC Waikiki’nin rekabette kendi pazar payını koruması ve geliştirmesi anlamına geliyor. FMD’nin veri sıkıştırma imkânı sunması sadece maliyetleri düşürmekle de kalmıyor. Hitachi all-flash veri depolama çözümleri performansı da artırıyor. Veri depolamanın sanallaştırılması, işlemleri kolaylaştırıyor ve yönetimi tek noktada

toplamaya imkân veriyor. Uyarlamalı veri azaltma servisleri, veri depolama için gerekli olan kapasiteyi minimize ediyor ve enerji tüketimini düşürüyor. Bunun yansıması daha uygun maliyetli barındırma, enerji ve soğutma hizmetleri oluyor. LC Waikiki’de kurulan yeni Hitachi altyapısı sayesinde firma artık ciddi büyüme hedeflerine doğru daha emin adımlarla ilerliyor. Güney son olarak; “Hitachi Vantara çözümü esnek, yüksek performanslı, kararlı ve güvenli bir çözüm. Büyümemiz için gerekli olan desteği sağlıyor ve kesintisiz, problemsiz lojistik operasyonlarını garanti ediyor. Bu da rekabetçi perakende sektöründe başarının anahtarlarından biri. Hitachi’ye güveniyor ve artık firma olarak işimizi geliştirmek ve gelecek hedeflerimize doğru ilerlemek için yoğunlaşıyoruz” diyor.

İş Dünyasının Veri Hakimiyeti Pentaho ile Artıyor

Sahip oldukları kurumsal veriden en yüksek katma değeri, veriyi daha etkin biçimde yönetebilmeyi başaran şirketler elde edebiliyor.

Büyüyen şirketlerin ürettiği kurumsal verinin hacmi her geçen gün artarken, bu veriyi farklı bulut ve sınır bilişim ortamlarında daha etkin yönetme ihtiyacı da derinleşiyor. Sahip oldukları veriden daha fazla katma değer elde etmek isteyen kurumlar, Hitachi Vantara’nın yakın zamanda yeni sürümünü yayınladığı veri entegrasyon ve analitik platformu **Pentaho 8.3** ile çalışıyor. Pentaho 8.3, şirketlerin sahip oldukları veriden en yüksek faydayı sağlamaları için kullanılan ortak veri yönetim yaklaşımı DataOps’u destekleyen yeni özelliklerle donatıldı. Yeni versiyon ile birlikte veriye yönelik gizlilik, güvenlik ve yönetim (*governance*) ihtiyaçları karşılanırken, sınır bilişimden çok bulutlu çalışma ortamlarına çevik veriden faydalanıyor.

EA ACCESS SONUNDA PS4’TE

DataOps yaklaşımının doğru veriyi, doğru zamanda ve doğru yerde elde etmeyi hedeflediğine dikkat çeken **Hitachi Vantara Portföy Pazarlama Başkan Yardımcısı John Magee**, Pentaho 8.3’ün tam da bu hedefe ulaşmayı sağlayan özelliklerle güçlendirildiğine dikkat çekiyor ve şöyle devam ediyor: “Pentaho 8.3, verinin sadece doğru hizmet düzeyinde en düşük maliyetlerle saklanması

sağlamakla kalmıyor, aynı zamanda aranabilmesini, kolayca erişilebilmesini, doğru bir idari akış çerçevesinde işlenebilmesini de garanti altına alıyor. Bu sayede karar almayı destekleyici analizler üretiliyor ve verinin sahip olduğu ekonomik değer tam kapasite ile kullanılıyor” diye konuştu.

VERİ AKTARIMINDA “SÜRÜKLE BIRAK” KOLAYLIĞI

Şirketlerin veri yönetimi uygulamalarını modernleştiren Pentaho 8.3, veri ile bilgi arasındaki tüm pürüzleri ortadan kaldıran bir dizi yenilik de barındırıyor. Sürükle bırak yöntemiyle çalışan yeni veri hattı, standart yöntemlerle ulaşılması zor olan veriyi kolayca elde etmeyi kolaylaştırıyor.

DAHA İYİ YÖNETİM İÇİN VERİ GÖRÜNÜRLÜĞÜ

Büyüyen içerik havuzlarını desteklemek için geliştirilen dağıtık nesne depolama sistemi Hitachi Content Platform (HCP) ile geliştirilen entegrasyon, kullanıcıların HCP’deki özelleştirilmiş üst veriyi ve sorgu nesnelerini sistemdeki üst veriyle okumalarını, yazmalarını ve güncellemelerini sağlıyor. Böylelikle veri üzerinde arama yapmak ve veriyi idare etmek kolaylaşıyor.

Pentaho 8.3 ile birlikte devreye alınan IBM Information Governance Catalog (IGC) entegrasyonu, veri yönetiminde elle yapılan müdahaleleri en aza indirmek için Pentaho’dan gelen kök veriyi IGC üzerinde görüntüleme olanağı sunuyor. Öte yandan AMQP, JMS, Kahka ve MQTT gibi yaygın kullanılan protokollerle gerçek zamanlı veriyi takip etmek kolaylaşıyor.

ÇOK BULUTLU ORTAMLARA TAM DESTEK

AWS bulut ortamında S3’ten Redshift’e toplu yüklemeleri tekrarlayan SQL betikleriyle yönetme dönemi Pentaho 8.3 ile sona eriyor. Hitachi Vantara’nın yeni toplu yükleme özellikleri, Redshift’e yüklemeleri otomatik hale getirerek, kurumların verimliliğini artırıyor. Üstelik veriyi içe alma sırasında gerekli politikaları ve zamanlamaları belirlemek bu yöntemle mümkün oluyor. Bulut tabanlı veri ambarları için yaygın olarak tercih edilen Snowflake ile kurulan bağlantı, buradaki verinin diğer veri kaynaklarıyla harmanlanıp zenginleştirilmesini ve analizini sağlıyor. Pentaho kullanıcıları ayrıca AWS ve Google Cloud gibi desteklenen diğer bulut platformlarındaki veriye de erişebiliyor.

Endüstriyel IoT, Üretim Alanına Taşınıyor

Hitachi Vantara'nın duyurduğu yapay zekâ özellikli endüstriyel analitik çözüm paketi Lumada Manufacturing Insights, Üretim 4.0 için makine, üretim ve kalite sonuçlarını optimize ediyor.

Hitachi Vantara, veri odaklı içgüdülerden dönüşüm yaratacak sonuçlar elde ederek imalat endüstrisini güçlendirecek olan Endüstriyel Nesnelerin İnterneti (IIoT) çözümleri paketi Lumada Manufacturing Insights'ın lansmanını gerçekleştirdi. Yapay Zekâ (AI) ve Makine Öğrenimi (ML) tekniklerini kullanan Lumada Manufacturing Insights, Üretim 4.0 için gerekli olan dijital inovasyon altyapısını güçlendiren makine, üretim ve kalite sonuçlarını optimize edecek şekilde tasarlandı. Hitachi Vantara'nın Ürün ve Strateji Sorumlusu Brad Surak "Veri ve analitik, üretim operasyonlarını modernize etme ve dönüştürme gücüne sahip. Ancak bugün çok fazla üretici için, eski altyapı ve bağlantısı kesilmiş yazılımlarla yürütülen süreçler inovasyonu yavaşlatıyor ve rekabet avantajını etkiliyor," diyor. "Lumada Manufacturing Insights ile müşteriler çalışma süreleri, verimlilik ve kalite ile ilgili anında elde edecekleri kazanımları işletmek ve geleceğe

yönelik dönüşümlerini başlatmak üzere halihazırda sahip oldukları sistem ve yazılımlarla uyumlu çalışan dijital inovasyon süreçleri için gerekli temeli oluşturabilecekler." **ÜRETİMDE DÖNÜŞÜMLERİ HIZLANDIRMAK** Lumada Manufacturing Insights, iyileştirme çalışmaları için düzenli olarak öngörülebilir analitiğe dayalı veri bilimi uyguluyor. Lumada mevcut uygulamalarla entegre çalışır ve maliyetli üretim ekipmanlarının veya uygulamalarının söküp değiştirilmesine gerek kalmadan eyleme geçirilebilir iç görüler sunar. Lumada Manufacturing Insights, çeşitli dağıtım seçeneklerini destekler ve şirket içi veya bulutta çalışabilir. Hitachi Vantara, Çözüm ve Hizmetler Baş Sorumlusu Bobby Soni "Hitachi Vantara ile müşterilerimiz, operasyonel teknoloji uzmanlığımızdan ve dijital yolculuklarını hızlandırmak için yaratıcı yaklaşımlarımızdan yararlanıyorlar.

Kanıtlanmış yöntemlerimiz ve gelişmiş araçlarımızla, verimliliği geliştiren, teslimat hızını artıran ve nihayetinde daha iyi iş sonuçları sağlayan müşterilerimiz için uygun çözümler tasarlayabiliyoruz" diyor. Makine, üretim ve kalite analitiği sunan Lumada Manufacturing Insights, müşterilerine şu tavsiyelerde bulunuyor:
✓ Akıllı üretim olgunluk modeli üzerine kendi yaklaşımınızı inşa edin ve aralıksız süreç iyileştirme için dijital inovasyon altyapısını güçlendirin;
✓ Rekabet avantajı elde etmek amacıyla veri silolarını, mahsur kalan varlıkları ve video, LiDAR ve diğer gelişmiş sensörlerden gelen verileri entegre edin;
✓ İstenilen ölçekte kök-neden analizi için 4M (Makine, İnsan, Malzeme ve Yöntemler) korelasyonlarını kullanın;
✓ Gelişmiş AI ve ML tekniklerine dayanarak Genel Ekipman Etkinliğini (OEE) ve geliştirme önerilerini değerlendirin;



- ✓ Zamanlama verimliliğinizi değerlendirin ve değişen iş yükleri, üretim oranları ve iş emri biriken dönemler için optimize edin;
- ✓ Ürün kalitesini tahmini öngörülerle izleyin ve yönlendirin;
- ✓ Talep tahmin hassasiyetine, üretim planlarına ve üretime uyumu arttırın.

ERKEN KULLANANLAR İLK FAYDALARI GÖRDÜLER

Ericsson Inc. Stratejik Endüstriyel Ortaklıklar ve Girişimlerden Sorumlu Başkan Yardımcısı Angelica Moden, Ericsson ve Hitachi Vantara gerçekleştirdikleri iş birliği sayesinde Lumada Manufacturing Insights'ı test ederek yeni ürün lansmanlarında beklenen artışa yanıt verebilmek için dijital bir inovasyon temelini oluşturduğunu ifade etti. Moden ayrıca, "Hitachi Vantara ile kurduğumuz ortaklığımız aracılığıyla ortak müşterilerimize sunacağımız çözümün ayrınsını kullanarak güç kazanıyoruz ve 5G teknolojilerimize dayanarak Endüstriyel

IoT kullanım şemalarımızı genişleteceğiz" dedi. "Vizyoner bir üretici olarak odak noktamız dönüşümsel değişimi hızlandırmak, veri silolarını ortadan kaldırmak ve dijital inovasyon için Üretim 4.0'a doğru olan yolculuğumuzu hızlandıracak bir temel oluşturmaktır" diyen Logan Aliminium İşte Dönüşüm Lideri Vijay Kamineni sözlerine şöyle devam etti; "Kullanım şemalarımızı işletme dönüşümü öncelikleriyle uyumlu hale getirmek ve Lumada Manufacturing Insights ile başarıya ulaşmak için bir yol haritasına sahip olmak amacıyla IIoT atölye çalışmasını kullandık. Hitachi Vantara ile gerçekleştirdiğimiz iş birliği, dönüşümümüzün her aşamasında iş hedeflerini tanımlamamızı, verimlilik, kalite, güvenlik ve sürdürülebilir üretimdeki kazanımları hızlandıracak net sonuçlar ortaya koymamızı sağlıyor. Hitachi Vantara uzun vadede bize yardımcı olacak benzersiz bir IT/OT avantajını da beraberinde getiriyor. Precision Drilling Corporation'da CTO

olan Shuja Goraya ise konu ile ilgili olarak şu yorumda bulundu; "Hitachi Vantara ile teçhizat başına saniyede 20.000'den fazla veri akışını işleyebilmek için endüstriyel analizler ve güçlü Lumada platformu ile zaman kazanıyoruz ve bu sayede doğru kişilere doğru zamanda harekete geçirilebilir bilgiler sağlıyor, optimal kararlar alınmasına yardımcı oluyoruz. Bu da operasyonel mükemmelliğimizi ve sonuç olarak rekabet avantajımızı ortaya koyuyor. İş sonuçlarının sunumu için video ve LiDAR'dan gelen bilgileri kullanarak Lumada Manufacturing Insights ile bütünleştiriyoruz." Shuja sözlerine şunları da ekledi; "Gelişme fırsatlarını etkin bir şekilde belirleyerek, müşterilerimiz için teslimat sürelerini kısaltarak süreç optimizasyonunu mümkün kılıyoruz. Her şey daha iyi kararlar almak ve daha sonra bu öğrendiklerimizi tutarlı bir şekilde yürütebilmek için verilerin verimli kullanımı ile mümkün olabiliyor. Hitachi Vantara ile kurduğumuz stratejik ortaklığımızdan heyecan duyuyoruz."

Büyük Veri Pazarı 2023'te 520 Milyon Dolara Ulaşacak

Hitachi Vantara'nın sponsorluğunda IDC tarafından gerçekleştirilen araştırmaya göre, Türkiye'deki kurumların yüzde 55'i şirket içi (on-prem) Büyük Veri işleme konusunda çalışmalarını sürdürüyor.

International Data Corporation'ın (IDC) açıkladığı son tahminlere göre, Türkiye'de Büyük Veri ve Analitik yatırımları 2018 yılında 247 milyon dolar olarak gerçekleşti. 2023 yılına kadar ise pazarın yıllık yüzde 16 oranında büyüyerek, 520 milyon dolara ulaşacağı öngörülüyor. IDC'nin Hitachi Vantara'nın sponsorluğunda yaptığı en son araştırmaya göre, Türkiye'de her geçen gün daha fazla şirket, hayatın her alanında ve hemen her sektörde fark yaratacak bir güç olan Büyük Veri'nin önemini kavramaya başlamış durumda. Türkiye'deki her 10 kurumdan 8'i "makine öğrenmesi"ni, kurumu için anlamlı ve değerli görürken, her iki şirketten biri, yani katılımcıların yarısı, geçmiş verileri analiz etmek için çok sayıda veri kaynağını bir araya getirmekte zorluklar yaşadığı belirtiyor.

BÜYÜK VERİ YATIRIMLARI İKİYE KATLANACAK

Türkiye'deki kurumların tamamına yakını (%98), önümüzdeki iki yıl içinde, Büyük Veri analizi ve yönetimi ile ilgili çözümlere ayrılan bütçenin artmasını bekliyor.



Araştırmaya katılan kurumların yüzde 15'i ise, yine bu bütçenin önümüzdeki iki yıl içerisinde yüzde 100'ün üzerinde artacağını tahmin ediyor.

BÜYÜK VERİ NEREDE KULLANILIYOR?

Büyük Veri ve Analitik çözümleri kurumlara birçok farklı konuda çalışma imkânı sunarken, katılımcıların yüzde 70'i "Müşteri hizmetlerini ve deneyimini geliştirmek" ve "İş süreçlerini ve operasyonlarını geliştirmek ve optimize etmek" konularının öncelikli alanlar olduğunu vurguluyor.

UYGULAMA VE KULLANIM KOLAYLIĞI ARANIYOR

Büyük Veri işleme platformlarının kullanımında kurumların karşılaştığı en önemli zorluklar arasında yüzde 52 ile "Şirket içi bilgi ve deneyim eksikliği" ilk sırada yer alırken, "Farklı sistemler ve farklı veri türleri" yüzde 30 ile ikinci sırada bulunuyor. Türkiye'deki kurumlar Büyük Veri ve Analitik çözümlerini değerlendirirken, "uygulama kolaylığı" ve "kullanım kolaylığı"nın en çok önem verilen kriterler olduğu belirtiliyor.

ENTEĞRE VERİ YÖNETİMİ 'OLMAZSA OLMAZ' KONUMA GELDİ

Türkiye'de giderek artan sayıda kurum ve şirketin, Büyük Veri'nin önemini kavramaya başladığını belirten IDC Türkiye'nin Baş Analisti Eren Eser, "Kurumlar, Büyük Veri ve Analitik Teknolojilerinin yetkinliğinin artması ve sunduğu imkânlarla birlikte, veriye dayalı karar verme yönünde bir istek ve yönelim içinde bulunuyor. Büyük Veri ve analitik yatırımlarının başlıca kısa vadeli hedefi, iş operasyonlarını ve müşteri deneyimini iyileştirmek olsa da, birçok kurum Büyük Veri ve Analitik çözümlerini daha uzun vadede yeni iş ve gelir akışları yaratmak için kullanmayı hedefliyor" şeklinde konuştu.

IDC Türkiye'nin Yazılım Çözümleri Araştırma Müdürü Yeşim Öztürk de, "Şirket içi ve bulut uygulamalarında üretilen verilerin harmanlanması, yükselen bir eğilim veya zorluk olmaya devam ediyor. Bu nedenle entegre veri yönetimi ve analizi sağlayacak çözümlere artık daha fazla ihtiyaç duyuyoruz. Entegre veri yönetimi, mükemmel müşteri ve çalışan deneyimi için olmazsa olmazdır" ifadelerini kullandı.

HITACHI'DEN VERİ YÖNETİMİNE MODERN VE ETKİN BİR YAKLAŞIM

Araştırma sonuçlarını değerlendiren Hitachi Vantara Türkiye Genel Müdürü Önder Sönmez de büyüyen şirketlerin ürettiği veri hacminin her geçen gün arttığına, bu veriyi farklı bulut ve şirket içi bilişim ortamlarında daha etkin yönetme ihtiyacının derinleştiğine dikkat çekti. Sönmez, "Sahip oldukları veriden daha fazla katma değer elde etmek isteyen kurumlara, Hitachi'nin ortak veri



yönetim yaklaşımı DataOps ile hizmet veriyoruz. Bu yaklaşımın temel prensibi, doğru veriyi, doğru zamanda ve doğru yerde elde etmek. Bunun için şirketlerin veri yolculuğunda SEAM (Store, Enrich, Activate, Monetize) olarak adlandırdığımız dört adımlı bir yaklaşım öneriyoruz. Müşterilerimizin sahip oldukları veriyi 'Depolama' adımıyla doğru yönetmelerine destek oluyoruz. DataOps, Hitachi Vantara'nın yakın zamanda yeni sürümünü yayınladığı veri entegrasyon ve analitik platformu yazılımı Pentaho 9 ile çalışıyor. Bu

yeni versiyon, veriye sadece en hızlı bir biçimde ulaşılmasını sağlamakla kalmıyor, aynı zamanda bu verinin 'sürükle-bırak' yöntemlerle analize hazırlanmasını ve makine öğrenme gibi ileri seviye analitik işlemlerin yapılmasını kolaylaştırıyor. Bu sayede, verinin hazırlanması için harcanan büyük zaman kayıplarının önüne geçiliyor ve veri bilimcilerin analizler yapabilmesi için daha fazla zamanları olmasını sağlayarak, verinin sahip olduğu ekonomik değer tam kapasitede kullanılmasına olanak veriyor" şeklinde konuştu.

NEXT 2019'da Yapay Zekâyı Öne Çıkaran Duyurular

Hitachi Vantara, geçtiğimiz Ekim ayında Las Vegas'ta düzenlenen NEXT 2019'da yenilikçi duyuruları ile yapay zekâ çağına vurgu yaptı.

YAPAY ZEKÂ ÇAĞININ VERİ YÖNETİM KONSEPTİ

Hitachi Vantara, NEXT 2019'da yeni DataOps'un kullanımına yönelik yenilikçilik vizyonunu ve uçtan çekirdeğe, çekirdekten çoklu buluta giden dünyaya hazırlanan müşteriler ve iş ortakları için bu vizyonunun faydalarını ortaya koyan açıklamalarda bulundu.

DataOps, içinde olduğumuz yapay zekâ (AI) döneminde büyük kurumlara yönelik veri yönetimini gerçekleştiriyor. Bir kurumun verilerindeki tüm değeri bulup kullanmak için veriyi tüketenlerle veriyi üretenler arasında sıkı bir bağ kuran DataOps, bir ürün, hizmet veya çözüm değil. Daha çok, daha iyi veri kalitesi, daha düşük döngü ve üstün veri

yönetimi ile bir kurumun veri kullanımını geliştirmek için bir metodoloji, teknolojik ve kültürel bir değişimi ifade eden bir kavram. İşletmeler, eski yöntemlerden dolayı sahip oldukları verilerin çoğunu analiz etmedikleri için, Hitachi Vantara, DataOps'un önceden kullanılmamış büyük miktardaki verilerin büyük bölümünü kilidini açarak BT'nin geleceği üzerinde önemli bir etkiye sahip olacağına inanıyor.

Hitachi Vantara, NEXT 2019'da yaptığı duyuru ile ürün, çözüm ve hizmetlerden oluşan portföyünde bu alana yönelik önemli güncellemeler yaptığını açıkladı. Portföy, her büyüklükte ve her sektördeki kurumlardaki DataOps girişimleri için geniş ve kapsamlı bir temel sunuyor.

Hitachi Sanal Depolama Platformu (VSP) 5000 serisi ve Hitachi Ops Center yazılımı, her ölçekte her bir iş yükü için yeni bir ölçeklendirme, ölçek büyütme mimarisi ile şirketin güçlü gelecek nesil depolama ve altyapı temelini oluşturuyor. Hitachi Vantara, şirketin yeni oluşturduğu bulut hizmetleri portföyünün ilk önemli duyurusunda bulut hizmet yeteneklerini de genişletti ve geliştirdi. Portföyde, buluta geçiş hizmetleri, uygulama modernizasyon hizmetleri, operasyon yönetim hizmetleri, danışmanlık hizmetleri ve Hitachi Enterprise Cloud (HEC) yer alıyor. Portföy, şirketin 2018'de REAN Cloud'u satın almasından sonra elde ettiği kritik yetenekleri ve sektör lideri uzmanlığı güçlendiriyor.

KURUMSAL DEPOLAMA BAŞTAN TANIMLANIYOR

Hitachi VSP 5000 serisi, tüm dijital iş operasyonları için mevcut iş yüklerine hız ve ölçeklenebilme katmanının yanı sıra, çoklu bulut ve yapay zekâ odaklı ortamlardan doğan yeni, veri yoğun iş yükleri için temel veri depolama altyapısını sağlıyor. Blok ve dosya verilerini depolamak için gereken çevikliği sağlıyor ve geleneksel kritik iş uygulamalarından konteynerlere ve ana sistemlere kadar iş yükü çeşitliliğini destekliyor. Hitachi VSP 5000 serisi, operasyonel verimliliği en üst düzeye çıkaran tüm iş yükünün birleştirilmesini mümkün kılıyor.

YEPYENİ BİR MİMARİ

VSP 5000 serisi, SAS mimarisi, NVMe ve depolama tipi bellek (SCM) avantajlarından yararlanarak sınıfının en iyisi performansı ve dayanıklılığı sunmak için en iyi hâle getirilmiş, tamamen yenilenmiş, büyük işletme tipi flaş dizisi sunuyor. Yeni Hitachi Accelerator Fabric ile güçlendirilmiş dünyanın en hızlı NVMe flaş dizisi, kullanıcıların 21 milyon IOPS'ye kadar hızlandırılmış iş çıktıları ve içgörüler almasına yardımcı oluyor. Kaynak yoğun uygulama sahipleri de yanıt sürelerini 70 mikro saniyeye kadar düşüren önemli bir gelişme elde edebiliyorlar. Yeni veri tekilleştirme iyileştiricisine sahip VSP 5000 serisi, blok büyüklüğü ve diğer özelliklere dayalı veri tekilleştirme süreçlerinin anında iyileştirilmesini

gerçekleştirmek için gelişmiş makine öğrenim (ML) algoritmaları kullanıyor. Böylece en az performans etkisiyle azami veri azaltma için çevrimiçi ve süreç sonrası tekilleştirme arasında iyileştirme yapıyor ve toplam 7:1 oranına kadar azalma sağlıyor. VSP 5000 serisi günümüzün hep ağa bağlı olan dijital işleri için amaca yönelik üretilmiş. Kendini koruyan IO mimarisi ve dörtlü yedekli yapısı sektör lideri düzeyinde %99,999999 oranında kullanılabilirlik sunuyor.

VERİ MERKEZİ OPERASYONLARINI DÖNÜŞTÜRÜN

VSP 5000, geniş bir iş yükü yelpazesinde ve uçtan çekirdeğe çoklu bulut yayılma modellerinde

talepkâr hizmet seviyesi gereksinimlerini karşılamak için veri merkezlerini modernleştirmek isteyen kuruluşlar için önemli bir gelişme. Yeni Hitachi Ops Center, karar almaya destek olma ve azami yatırım getirisi için kaynak dağıtımını modernize etmede altyapı yönetimine ve operasyonlara yapay zekâyı ekliyor. Ops Center, görevlerin %70'ini otomatikleştirerek müşterilerin bağımsız bir veri merkezine geçişini hızlandırıyor ve sistem sağlığı teşhisi ve veri operasyonlarını en iyi durumda tutmak için daha hızlı ve doğru içgörüler sunuyor. Müşteriler, mevcut depolama altyapılarına anında yeni değer katmak için VSP 5000 modeliyle var olan sistemlerini sanallaştırabiliyor, TCO'yu %20 düşürebiliyorlar. Sanallaştırma, VSP 5000 serisinde mevcut tüm veri hizmetlerini eski sistemlere taşıyor. VSP Bulut Bağlantı Paketi, ek veri merkezi kapasitesi açmak için verileri herkese açık

buluta taşımak için bir HNAS 4000 dosya depolama ağ geçidini sisteme ekliyor. Herkese açık buluta taşınan veriler, meta verilerle zenginleştirilerek dizine eklenebiliyor ve aranabilir hâle getiriliyor.

HER İŞ YÜKÜNÜ EN İYİ HÂLE GETİRECEK ESNEKLİK

Hitachi Depolama Sanallaştırma İşletim Sistemi (SVOS), VSP 5000 serisine güç veriyor ve ölçek büyütme mimarileri, NVMe performansı ve SCM dahil yeni nesil depolama ortamları için en iyi hâle getirilmiş bulunuyor. Her bir iş yükü performansında iyileştirme, depolama maliyetlerini düşürmek ve operasyona olumsuz etki edecek hataları tahmin etmek için değişen koşullara adapte olan yapay zekâyı içeriyor.

VSP 5000 serisi, endüstride NVMe ve SAS flaş depolamayı aynı sistem dizisinde karıştırarak iş yükleri arasında performans ve fiyatı iyileştirmek için esneklik sunan tek depolama sistemi. Akıllı katmanlama,

uygulamaları hızlandırmak için verileri en iyi hâle getirilmiş bir katmana dinamik olarak tanıtmak ve indirmek için yapay zekâ ve makine öğreniminden faydalıyor.

VSP 5000 serisi, müşterilerin kestirilebilir hizmet seviyeleri sunarken, aynı zamanda küçük ölçekten ihtiyaç olursa devasa ölçeğe büyüebilmeleri için tasarlanmış bulunuyor. Her türden (geleneksel işlemsel sistemler, konteyner kullanan modern uygulamalar, analitik ve hatta ana bilgisayarlar) çoklu iş yükünü hızlandırmak, birleştirmek, maliyet tasarrufu ve veri merkezi ayak izini azaltmak için her zamankinden daha fazla uygulamayı birleştiriyor.

Güncellemeye açık mimarisi, sağlam depolama teknolojilerinden tepeden tırnağa altyapı yenilemesi ya da daha fazla donanım yatırımı yapmadan, Fabrics üzeri SCM ve NVMe (NVMe-oF) gibi son gelişmelere geçiş yapmaya hazır bulunuyor.

Hitachi VSP 5000 Serisi, Hitachi Ops Center ve SVOS'un Sunduğu Ek Faydalar:

- ✓ Giriş seviyesinde fiyatlandırılan Hitachi VSP 5100, tam depolama yönetimi, güçlü sistem analizi ve yerel kopya veri yönetimi sağlayan katma değerli yazılımlar yüklü gelir.
- ✓ Yeni VSP 5000 serisi dahil tüm VSP modelleri için %100 veri kullanılabilirliği garantisi sunar.
- ✓ Bölgesel bir kesintiden etkilenmeyen, kesintisiz operasyona ihtiyaç duyan müşteriler için Hitachi'nin Global-Aktif Cihaz (GAD) özelliği VSP 5000

Serisinde yer alır ve uzaklığı 500 kilometreye kadar olan konumlar arasında uygulamaların eşzamanlı kümelenmesini sağlar.

- ✓ Kullanımı kolay Hitachi Ops Center yönetici şablonları, yönetimi basitleştirir ve BT iş akışını düzenler.
- ✓ Hitachi Ops Center ile kullanıcılar, BT operasyonel verimliliğini artırmak için hızlandırılmış yönetim otomasyonunu deneyimlerken yaptıkları insan kaynağı tasarrufuyla yeniliklere odaklanabilirler.



GET YOUR DATAOPS ADVANTAGE

DataOps is your data practice for the AI era. Connect your data consumers and data creators to accelerate collaboration and digital innovation. We help you place the right data in the right place at the right time. We are analytics, industry expertise, technology and outcomes rolled into one great solution partner. We listen. We understand. We work with you.

Get your DataOps advantage today with Hitachi Vantara.

hitachivantara.com

Günümüzün Popüler Teknolojileri Bizlere Neler Vaat Ediyor?

Günümüzün çok ciddi potansiyele sahip popüler teknolojilerinden faydalanabilmek için şirketlerin doğru kararlar vermesi gerekiyor. Fortune 500 listesinde yer alan şirketlerin güvenilir danışmanı Red Hat olarak bu alandaki uzmanlığımızı sizlerle paylaşmak için sabırsızlanıyoruz.



Yazan:
HALUK TEKİN
Red Hat Türkiye Genel Müdürü

Yirmi beş yıl önce dünya çok farklı bir yerd. İçi köpük malzemeye doldurulmuş tüylü oyuncaklar yeni çıkmış, Jurassic Park gişe rekorlarını en çok kıran film olmuş, Nelson Mandela Nobel Barış Ödülü'nü almış, Buckingham Sarayı ilk kez kapılarını halka açmış, CERN kaynak kodunu internette paylaşımına açmıştı. Bu arada küçük bir işletme sahibi, bir teknoloji konferansında çok yetenekli, genç bir teknoloji meraklısıyla tanışmış ve Red Hat Inc. doğmuştu. Bugün ise açık kaynak araçları, araştırma sonuçlarına göre Nesnelerin İnterneti çözümlerinin lideri. Buzdolaplarından kapı zillerine kadar güçle çalışan her türlü cihaz akıllı hale getirilebiliyor ve piyasaya her gün milyonlarca ağ bağlantılı cihaz giriyor. IDC raporuna göre, dünyayı saran Nesnelerin İnterneti ağına yapılan harcamaların 2020 yılında 1 trilyon doları aşacağı tahmin ediliyor. Nesnelerin İnterneti çözümlerinin

hızının artmasıyla yaşanan gelişmelerle birlikte kurumlar da bu tür ürün ve hizmetler geliştirebilen, hizmete alabilen ve yönetebilen teknoloji ve araçlara aktif bir şekilde yatırım yapıyorlar. Nesnelerin İnterneti alanında çözüm geliştirme söz konusu olduğunda hangi teknolojinin kullanıldığını daha iyi görmek amacıyla RTInsights araştırma şirketine, Nesnelerin İnterneti çözümleri geliştiren veya önümüzdeki 12-18 ay içinde geliştirmeyi planlayan büyük ve çok büyük kurumlardaki 253 BT yetkilisinin katıldığı bir araştırma yaptık. Araştırma, özellikle, Nesnelerin İnterneti uygulamaları geliştirmenin, geleneksel uygulama geliştirmeden hangi açılardan farklılaştığını, Nesnelerin İnterneti çözümleri geliştirirken gereken en önemli yetenekleri ve açık kaynak araçları ile Nesnelerin İnterneti çözümleri arasındaki ilişkiyi inceledi.



Sorulan ilk sorulardan biri şuydu: “Nesnelerin İnterneti ile geleneksel uygulama geliştirme arasındaki en önemli farklar nelerdir?” Bu soruya en çok verilen cevaplar ise şöyle oldu:

- ✓ Yapısal olarak güvenilir ve ölçeklenebilir geliştirme çözümlerinin önemi (yüzde 51)
- ✓ Veri & uygulama uyumluluğu & ömrüne yönelik standartların önemi (yüzde 48)
- ✓ Akıllı sınır cihaz ve sensörlerinin sayısının çokluğu (yüzde 45)
- ✓ Veri ve uygulama güvenliğine yönelmenin önemi (yüzde 41)

Her iki sürecin birbirinden ayrıldığı yerleri tespit ederek, Nesnelerin İnternetinde en başarılı çözümlerini geliştirebilmek için neler gerektiğini daha iyi belirleyebiliriz. Nesnelerin İnterneti çözümlerinin hem yüksek hacimli verileri üretme hem de tüketme eğilimi göz önüne alındığında, güvenilir ve ölçeklenebilir çözümlerin listenin en başlarında yer alması hiç de şaşırtıcı değil.

Nesnelerin İnterneti veya geleneksel geliştirme faaliyetleri arasındaki farkı nasıl ayırt ettiğini sorarken, bu Nesnelerin İnterneti uygulamalarını kuran BT yetkililerinin hangi yazılım araçlarına başvurduğunu öğrenmek istedik. Araştırmada, son on yıl içinde, uygulama geliştirme ve kurumda bunları hizmete alma uygulamalarında açık kaynak yazılımlarının defacto seçildiği öğrendik. Ve yine araştırma sonuçlarına göre Nesnelerin İnterneti çözümleri geliştirilirken de açık kaynak araçları tercih ediliyor.

Hali hazırda Nesnelerin İnterneti çözümleri geliştiren kurumlardan katılan katılımcıların yüzde 39'u markalı seçeneklerden ziyade açık kaynak

çözümlerini tercih ediyor. Buna karşın, kendilerini Nesnelerin İnterneti liderleri olarak sınıflandıran kurumlara aynı soru sorulduğunda, Nesnelerin İnterneti çözümleri geliştirmek için açık kaynaktan faydalandığı söyleyenlerin oranı yükselerek yüzde 43'e çıkıyor. Nesnelerin İnterneti çözümleri geliştirmek için öncelikle açık kaynak kullanan kurumların kendilerini lider olarak tanımlama oranı ise, markalı araç kullanan kurumlara göre yüzde 50 daha fazla. Nesnelerin İnterneti çözümleri geliştirirken en önemli gerekliliklere baktığımızda, açık kaynak çözümleri etrafındaki destek şaşırtıcı gelmiyor. Çünkü Nesnelerin İnterneti çözümleri geliştiren kurumların, tam da açık kaynağın ayırıcı çözüm özellikleri olan ölçeklilik, güvenilirlik, karmaşıklık ve hacim gereklilikleri gibi konulara cevap bulmaları gerekiyor.

Red Hat olarak kurumsal BT dönüşümünü destekleme taahhüdü verirken, ihtiyaçlarını Red Hat teknolojiyle karşılayarak Nesnelerin İnterneti çözümleri geliştirecek kullanıcılarla çalışmayı da heyecanla bekliyoruz.

ÇOKLU BULUT

Çoklu bulut, birden fazla bulut sağlayıcısından (genel veya özel) birden fazla bulut hizmeti almak anlamına geliyor.

Diyelim ki, kurumunuz bulut altyapısını genişletmek istiyor. Çıplak metal dediğimiz sunucularınızı sanallaştırmaya dayalı iş yükleriyle değiştiriyor ve genel bulut seçeneklerinin arasında neler var diye bakıyorsunuz. Buraya bir not düşelim; genel bulutu her şey için istemiyorsunuz, sadece son derece değişken kullanım

oranları olan belli bir müşteri uygulamasını desteklemek için ona ihtiyacınız var. Biraz araştırma yaptıktan sonra sizin istediğiniz hizmet seviyesi anlaşmalarının güzel bir karmasını sunan, güvenlik protokollerini ve uygulamanızı barındırma koşulları uygun bir genel bulut sağlayıcısı buluyorsunuz. Fakat bir noktada müşteriler sadece başka bir sağlayıcının markalı bir uygulaması aracılığıyla ulaşılacak bazı özellikleri talep etmeye başlıyor. O özellikleri sizin uygulamanıza entegre etmeniz için hem o sağlayıcının markalı uygulamasını almanız, hem de bu uygulamayı o sağlayıcının markalı genel bulutunda saklamanız gerekiyor (çünkü ancak bu şekilde her iki uygulamayı da talebe göre ölçeklendirebiliyorsunuz). Sonuçta bir çoklu bulutunuz oluyor. Buraya bir parantez açabiliriz. Zaman zaman insanların aklına çoklu bulut ile hibrit bulutun ne farkı var sorusunun geldiği görülüyor. Aslında birçok fark var. Çoklu bulut en baştaki tanımda da anlatıldığı üzere genel ya da özel aynı tip buluttan birden fazlasını kullanıyor olmanız demek. Hibrit bulut ise genel ya da özel birçok farklı bulut kullanımının, aynı entegrasyon ya da orkestrasyon biçimiyle var olması demek. Dünya çapında 870'ten fazla müşterisinin teknoloji yolculuklarındaki konumuna ve hedeflerine dair önemli istatistikler sunan Red Hat Global Customer Tech Outlook araştırmamızda müşterilerimize bulut stratejilerini sordüğümüzda en popüler cevap yüzde 31 ile hibrit bulut oldu. Hibrit bulutun tercih edilme sebepleri arasında genel veri güvenliği, maliyet avantajı ve veri entegrasyonu ilk sıralarda yer alıyor. Çoklu bulut konusuna değinmişken

şu noktayı tekrar vurgulamakta fayda var: Çoklu bulut kullanmanın en büyük avantajlarından biri de kurumların tek bir sağlayıcıya bağımlı kalmanın getirebileceği sıkıntılardan kurtulması. İş yüklerini çoklu bulut sağlayıcılarına dağıtmak kurumlara esneklik kazandırıyor; bulutu diledikleri zaman kullanıyorlar veya bırakabiliyorlar. Birden fazla bulut kullanmakta hiçbir problem yok. Aksine bu yaklaşım, gayet faydalı ve açık kaynak yazılımları bu faydaları ikiye üçe katlayabiliyor.

KONTEYNER NEDİR?

Diyelim ki bir deniz nakliyat ve kargo şirketiniz var ve büyük bir ikilem yaşıyorsunuz; öyle ki işinizi daha fazla sürdüremeyecek hale gelmişsiniz. Geminiz her seferinde sadece bir kargo nakliyatı yapabiliyor. Bu çok ciddi bir problem. Açıkçası bu durum çok maliyetli ve ayrıca kaynak israfı anlamına geliyor; her gemide tek kargo kullanmak çok zorlayıcı, çok can sıkıcı bir durum. Ta ki bir arkadaşınız sizi bambaşka, çok daha inovatif bir sistemle tanıştıran kadar. Bu yeni paketleme sistemi hem hafif hem kolayca istiflenebilir hem de gemileriniz her seferde aynı anda birçoğunu taşıyabiliyor! Şimdi, kargo gemileri ile teknoloji arasında nasıl bir benzerlik var diyebilirsiniz. Aslında bu hikayedeki unsurlar, konteyner teknolojisinin özellikleriyle aynı: gemiler işletim sistemlerini, kargo ise uygulamaları ve işlemleri temsil ediyor. Yeni paketleme sistemi ise konteyner teknolojisi. Deniz nakliyat ve kargo şirketi olarak çözmeniz gereken sorunlar, bugün birçok teknoloji geliştiricisinin uğraştığı zorluklarla aynı: işletim sistemleri her seferinde yalnızca bir uygulamayı ya da bir prosesi destekleyebiliyorlar.

Bu da ciddi bir problem demek çünkü geliştiricilerin teknolojinin potansiyelinden faydalanmasını engelliyor, verimi düşüyor. Konteynerler; içinde dosyalar, kütüphaneler ve diğer hayati bilgilerin hepsiyle donatılmış ve izole edilmiş ve kompakt işlem kümeleridir. Neredeyse ağırlıksızdır ve o kadar sıkı paketlenmişlerdir ki taşıma ve aktarma tamamen zahmetsizdir. Yani herhangi bir kesinti olmadan, herhangi bir yere kolayca taşınabilirler. Konteynerleştirilmemiş uygulamalar ve işlemler yalnızca hazırlandıkları ortamda çalışabileceği için, başka bir yere taşınamazlar. Bununla birlikte, konteynerleri bu kadar özel yapan şey, tüm hayati bilgilerini içlerinde bulundurmalarıdır, yani bu, bir yerden bir yere taşınırken ve taşındığında bile sürekli çalışabilecekleri anlamına gelir. Bu teknoloji, geliştiricilerin, genellikle çok zaman alan, zor ve büyük bir baş ağrısı olan kodu yeniden yapılandırmak zorunluluğu yerine konteynerlerini teknolojik ortamlarına uyarlamalarına olanak tanıyor.

Konteynerlerin modülerliği, uygulanabilir ve etkili bir teknolojik gelişme olarak kabul edilmelerini sağladı. Bununla birlikte, yetenekli tüm makineler gibi, bunların da potansiyelinin tam olarak kullanabilmesi için ürün üzerinde uzmanlık gerekiyor. Herkesin konteynerler kullanmak için hazır araçları ve eğitimi olmadığı için, dışarıdan bir kaynaktan yardım istemeleri çok önemli. Red Hat olarak bu ihtiyacı anladık ve bu alanda fayda sağlamaya karar verdik. Konteyner kullanımının tüm yönlerine yardım sunan bir dizi paket ve hizmet tasarladık. Sunduğumuz ürün ve hizmetler arasında eksiksiz bir konteyner uygulama platformu (Red

Hat OpenShift), ve bağımsız depolama (Red Hat Gluster Storage) ve hizmet sunumunu artırıp işletme maliyetlerini azaltan (Red Hat CloudForms) ve çok daha fazlası yer alıyor. Bunlar, adından da anlaşılacağı gibi, mevcut tüm hizmetleri bir araya getiren lüks bir paket olan Red Hat Cloud Suite'ten de satın alınabiliyor. Ayrıca, güvenliğin her şeyden daha önemli olduğunu biliyor; bu yüzden konteynerleri birbirlerinden korumak için SE Linux gibi izolasyon teknolojilerini kullanmayı seçiyoruz. Altyapı tutarlılığının da ne kadar önemli olduğu malum, yani konteyner tabanlı uygulamaları herhangi bir ortamda güvenle dağıtabilmelisiniz. Bu yüzden Açık inovasyon, yönetim, platformlar, depolama, altyapı ve en önemlisi güven sağlamayı vaat ediyoruz.

PEKİ KUBERNETES NE İŞE YARIYOR?

Kubernetes, konteynerleştirilmiş uygulamaları çalıştırmak için gereken de facto standart. Bir diğer deyişle K8s (K ve s arasında 8 harf bulunmasından dolayı bu kısaltmayla anılır), konteynerleştirilmiş uygulamaların kurulumunu, ölçeklendirilmesini ve yönetimi otomasyona almak için kullanılan bir açık kaynak sistemidir. Yukarıdaki kargo gemisi benzetmesinin devamı olan Kubernetes, dümenci anlamına geliyor; konteynerlerin okyanustaki seyrini düzenliyor. Ayrıca taşınabiliyor ve genişletilebiliyor. Sonuç olarak muhteşem potansiyellere sahip bu teknolojilerden faydalanabilmek için şirketlerin doğru kararlar vermesi gerekiyor. Fortune 500 listesinde yer alan şirketlerin güvenilir danışmanı Red Hat olarak bu alandaki uzmanlığımızı sizlerle paylaşmak için sabırsızlanıyoruz.

Versa Networks'e NSS Labs'den Tavsiye Notu

Siber güvenlik hizmetlerinin değerlendirilmesinde bağımsız ve olgulara dayalı testlerle güvenilir bir kaynak sunan NSS Labs, Yeni Nesil Saldırı Önleme Sistemleri (NGIPS) Grup Testinde Versa Networks'e tavsiye notu verdi.

Güvenli Bulut IP platformunun yaratıcısı Versa Networks, NSS Labs 2019 Yeni Nesil Saldırı Önleme Sistemleri (NGIPS) grup testinde tavsiye notu aldı. NSS Labs, siber güvenlik hizmetlerinin değerlendirilmesinde bağımsız ve olgulara dayalı testlerle güvenilir bir kaynak sunan saygın bir küresel kuruluş. Sunulan rapor, NGIPS ürünleri için Güvenlik, Maliyet ve Performans/Fonksiyonellik başlıklarında ele alınan temel etmenlere odaklanıyor.

DETAYLI TESTLER BAŞARILI SONUÇLAR

Grup testlerinde, Versa'nın amiral gemisi ürünü olarak değerlendirilen FlexVNF, Güvenlik Etkinliği bakımından kaçış vektörlerini yüzde 100 bloke etti ve kabul edilebilir stabilite ve güvenilirlik aralığında statik güvenlik açıkları için yüzde 99,8 saldırı kapsama performansı gösterdi, sıfır yanlış pozitif oluşturdu. Performans testlerinde ise, Versa 1-RU form faktörde korumalı veri hacminde 6Gbps hızla çalışırken, test edilen tüm NGIPS ürünleri arasında en düşük Toplam Sahip Olma Maliyetine (TOC) ulaştı. NSS Labs, sıklıkla karşılaşılan günlük



saldırıları ile güncel tehdit aktörü kampanyalarından hedef odaklı saldırılara ve ileri düzey saldırılara kadar farklı türde saldırıları test ediyor. NSS Labs, bu testte NGIPS'in farklı tehditlere karşı koruma sağlayıp sağlamadığını ve bu ürünlerin işletmelerin ihtiyaçlarına ne ölçüde yanıt verdiğini değerlendirdi. NSS Labs'ın güvenlik etkinliği testleri, NGIPS'in tehditleri kesin olarak bloke ederek kaydederken aynı zamanda yanlış pozitiflere karşı da dirençli olduğunu doğruluyor. NSS Labs bu testlerde,

siber suçlular ve diğer tehdit aktörleri tarafından halen kullanılan saldırı yöntemlerini yansıtan çok çeşitli ticari, açık kaynak ve tescilli araçlar kullanılıyor.

NGIPS TEKNOLOJİSİ NEDEN GEREKLİ?

NGIPS teknolojisi, işletmelerin kurum içinden gelen tehditleri yönetmek için ihtiyaç duydukları dijital inceleme ve olay müdahale kabiliyetlerinin sağlanması bakımından kritik bir rol üstleniyor. Birçok geniş çaplı ihlalle ilişkilendirilen bu

“Versa Networks'ün alanında çığır açan güvenlik portföyünün etkinliği ve düşük toplam sahip olma maliyeti (TCO), NSS Labs'ın testiyle bir kez daha onaylandı. Versa Networks, bu testte yüzde 100 kaçış tespit performansı elde etti ve NSS Labs'tan ayrıca SD-WAN tavsiye notu almayı da başardı.”

KUMAR MEHTA
Kurucu ve CDO
Versa Networks

tehditler, genellikle ilgili alanda kullanılan NGFW (Yeni Nesil Firewall) altyapılarını atlatabiliyor. NGIPS, aynı zamanda NGFW ve IPS kabiliyetlerini birleştiren geleneksel WAN şube/kampus yerleşimlerinde ve yüksek ölçüde adapte edilebilir tehditlerin hafifletilmesine yönelik politika kontrollerinde de kullanılıyor. Alan yerleşimlerini desteklemesinin yanı sıra, NGIPS yeni kullanım vakalarının desteklenmesinde de giderek daha büyük önem kazanıyor. İşletmeler güvenlik orkestrasyon ve otomasyon yanıtı (SOAR) ile güvenlik bilgi ve olay yönetimi (SIEM) aracılığıyla, segmentasyon, operasyonel çeviklik ve müdahale süresi bakımından gelişme kaydetmeyi hedefliyorlar. Bu

VERSA NETWORKS HAKKINDA

“Yazılım Tanımlı Ağ” (SDN) teknolojileri, bir süredir iletişim dünyasındaki fiziksel bariyerleri ortadan kaldırmayı hedefleyerek, bir paradigma değişimine neden oldu. ABD ve Avrupa'da hayata geçirdiği yazılım tanımlı geniş alan ağ projeleri ile parlayan Versa Networks ise yenilikçi bir anlayışla geliştirdiği, uçtan-uca çözümlerle hem kuruluşlar hem de servis sağlayıcılar için SD-WAN alanında devrim yaratıyor.

Sequoia, Mayfield, Verizon Ventures ve Artis Ventures firmalarının önde gelen yatırımcıları tarafından desteklen Versa Networks, ABD ve Avrupa'da başlattığı devrimi, şimdi de Türkiye'de LinkPlus iş birliği ile devam ettiriyor.

Versa Networks, 2012 yılında Silikon Vadisi'ne doğan, yazılım tabanlı ağ teknolojileri üzerine odaklanan bir kuruluş. Kurucularını ağ endüstrisinin önde gelen uzmanları oluşturuyor. “Yüksek performanslı yönlendirme işlemlerini, mevcut cihazların bariyerlerini aşarak, daha esnek, daha yüksek performansla, daha güvenli ve daha düşük maliyetle nasıl yaparız” sorusunun cevabını vermek üzere yola çıkıyorlar.

Versa Networks Türkiye Ülke Müdürü Ahmet Turan Türköl, Versa Networks'ün Sequoia, Mayfield, Verizon Ventures ve Artis Ventures gibi önemli yatırımcılar tarafından desteklendiğine dikkat çekerek, geldiği noktayı şu sözlerle özetliyor: “Teknoloji dünyasının en önemli yatırımcılarını ve dolayısıyla çok büyük bir finansal gücü arkasına alan Versa Networks, ‘Wide Area Network’ alanında yazılım tanımlı ürün olarak en ileri düzeyi temsil eden SD-WAN ürününü, yaklaşık 80 milyon dolarlık bir Ar-Ge çalışmasıyla ortaya çıkardı. Bugün Gardner'ın “Cool Vendor” diye tanımladığı, NSS Labs gibi bağımsız araştırma şirketlerinin üzerine basarak önerdiği bir noktadayız. Yaptığımız iş ise en basit tanımıyla, iletişim teknolojilerindeki bariyerleri tamamen aşmak.”

teknolojiler, IPS sistemlerinden alınan bilgi ve aksiyonları giderek daha fazla kullandıkları için NGIPS açısından yeni gereklilikleri de beraberinde getiriyor.

VERSA NETWORKS'ÜN ETKİN ÇÖZÜMÜ

Versa Networks'ün Güvenli Bulut IP çözümü, işletmelerin şube/çoklu bulut ağları için güvenli bir SD-WAN ortamı geliştirmelerine ve WAN maliyetlerini daha iyi yönetmelerine imkân tanırken aynı zamanda operasyonların sadeleştirilmesini, ağ esnekliğinin geliştirilmesini ve uygulama performansının artırılmasını sağlıyor. Versa'nın çözümü, yönlendirme, ağ

bağlantısı hizmetleri ve SD-WAN'la çoklu aygıtların tek bir platformda birleştirilmesini sağlayan birleşik tehdit yönetimi (UTM) ve NGFW gibi kritik güvenlik fonksiyonlarını entegre ediyor. Çoklu kiracı yapısı, çoklu yerleşim opsiyonları, Zero Touch Provisioning ve çoklu bulut kapsama ortamı sağlayan bu benzersiz çözüm, işletmelerin hızlandırılmış WAN dönüşümü için yeni nesil teknolojileri sorunsuz bir şekilde benimsemelerini mümkün kılıyor. Versa, bu değerlendirmenin ardından NGFW (iki yıl üst üste), SD-WAN, Güvenlik Destekli SD-WAN ve şimdi de NGIPS için NSS Labs tavsiye notunu almayı başardı.

MAKİNE ÖĞRENME Sİ İ YLE MOBİL TEHDİT TESPİTİ



Bilinmeyen,
“Sıfır-Gün”
Mobil Tehditleri
Tespit Etmek İçin
İdeal Teknolojiyi
Bulmak...

Son dönemde MTD (Mobil Tehdit Tespiti) için önemli bir teknoloji olarak benimsenen makine öğrenmesi, bilgisayarların özel bir programlama yapılmasına gerek kalmadan model tanıma gibi daha sofistike davranışlar geliştirmesine imkân tanır. Makine öğrenmesi, zaman içerisinde uygulama ve kullanıcı davranışını sürekli olarak izlemek suretiyle normal ve anormal davranış arasındaki farkı – ve daha da önemlisi, mobil cihazlarda kötü amaçlı faaliyetlere yol açabilecek hususları – tespit edebilen güçlü bir teknolojidir. Geleneksel masaüstü anti-virüs

programları gibi daha yaygın güvenlik yaklaşımlarına kıyasla sağladığı hız, doğruluk ve kapsam nedeniyle, kurumsal güvenlik konularında makine öğrenmesinin kullanımı son yıllarda ivme kazanmıştır. Mobil tehdit ortamının gelişmesiyle birlikte, güvenlik profesyonelleri tehditleri cihaz seviyesinde belirleyerek hızla ortadan kaldırabilen ve kritik tehditleri öncelikli olarak değerlendiren teknolojilere ihtiyaç duymaktadır. Makine öğrenmesine dayalı MTD ise bu noktada önem kazanıyor çünkü söz konusu kabiliyetler bulut tabanlı ve anti-virüs çözümlerden çok

daha fazlasını sunabilmektedir. Örneğin, birçok kuruluş aşağıda bir kısmına yer verilen mobil güvenlik sorunlarına çözüm getirmek için makine öğrenmesinden yararlanmaktadır:

✓ **Makine-hızı saldırıları:** Günümüzde bilinmeyen, sıfır günlük tehditler de dahil olmak üzere ilgili saldırılar makine hızı üzerinden yapıldığı için, IT'nın bu saldırılara aynı hızda yanıt verebilmesi gerekmektedir. Makine öğrenmesi, admin'lerin bu tehditleri hızla tespit etmelerine ve uygun şekilde aksiyon almalarına yardımcı olur.

✓ **Cihaz güvenliği:** Dünyada milyarlarca cihaz bulunmaktadır ve bunların büyük bir çoğunluğu, mobil saldırılara karşı son derece hassastır. Makine öğrenmesine dayalı tehdit tespitini dünyanın her noktasında milyonlarca cihazda uygulayabilen UEM, büyük ölçekli mobil filolarını bu tür saldırılardan korumanın ideal yöntemini sunmaktadır.

✓ **Mobil tehdit zekâsı:** Hedefe yönelik saldırılar genellikle cihazda çok karmaşık bir değişiklik yaratır. Bu değişikliklerin önemli bir kısmı analistler tarafından fark edilemez. Bazı durumlarda, bunun için makine öğrenmesiyle binlerce cihaz parametresinin korelasyonunun gerçekleştirilmesi gerekir.

✓ **IT admin sayısının yetersizliği:** Günümüzde güvenlik tehditlerinin fazlalığı karşısında makul bir

sürede tehditleri tespit etmek ve bunlara yanıt vermek için gerekli insan gücünü sağlamak mümkün olmamaktadır. Makine öğrenmesi, IT admin'lerini tehdit işleme yükünden kurtarabilir.

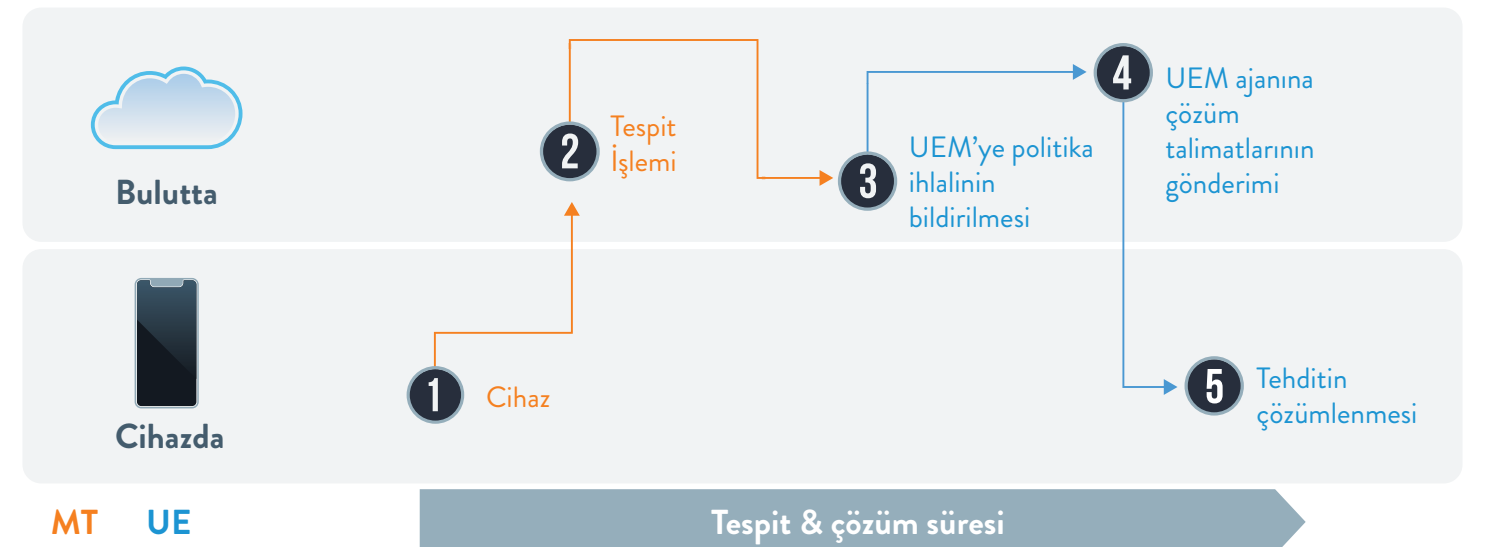
GÜNÜMÜZDE TEHDİT ORTAMI

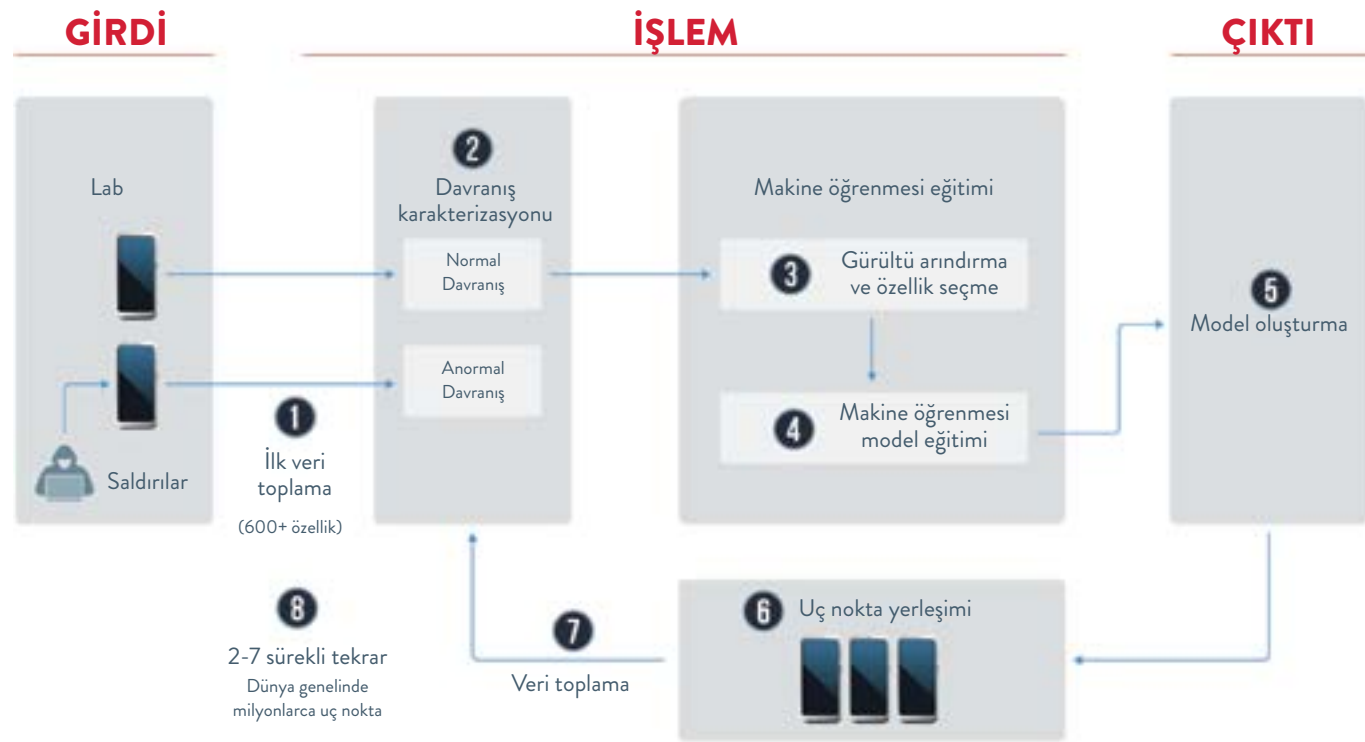
Bazı ortak çözümlerin modern tehditler karşısında arzu edilen etkiyi sağlamamasının nedenleri

Bulut tabanlı tehdit tespiti, çözümü geciktirebilir

Bulut tabanlı tehdit tespit çözümleri, MTD açısından bir yaklaşım sunmakla birlikte, bazı dezavantajları beraberinde getirir. Birincisi, bu çözümler cihaz tehditlerine yanıt süresini geciktirebilir çünkü bu çözümler öncelikle cihazı tarar ve sonrasında ilgili verileri cihazdan kaldırarak buluta gönderir. Ardından, bulut ajanı potansiyel güvenlik ihlalinin UEM çözümüne bildirerek cihazdaki UEM ajanına gerekli talimatları gönderir

– bu bakımdan, cihaz taramasından çözüme kadar beş adımdan oluşan uzun bir sürecin uygulanması gerekir. Bu süreç kapsamında, kullanıcının lokasyonu gibi hassas veriler buluta aktarılır. Bu veri aktarımı, “ortadaki adam” (MITM) saldırısına karşı hassas olabilir ve bu nedenle, çözümün cihazda uygulanması imkansız hale gelebilir. Bu süreçte hassas verilerin filtrelenmesi de, Genel Veri Koruma Yönetmeliği (GDPR) gibi birçok uyum yönetmeliğinin ihlal edilmesine neden olabilir. Ayrıca, günümüzün bulut tabanlı çözümleri öncelikle bilinen tehditleri tespit eder. Makine öğrenmesi algoritmalarını kullanmadıkları için, bilinmeyen, sıfır günlük tehditlerin tespit edilmesinde yeterince etkili değildir. Modern siber saldırılar, tespit edilmemek için tehdidin bir kısmını değiştirme konusunda ciddi bir beceri kazanmış olduğundan, MTD çözümleri bu anormallikleri derhal tespit edebilmelidir.





Geleneksel anti-virüs yazılımları mobil tehditlere karşı reaktif bir yaklaşım sergiler

Başlangıçta virüsler geleneksel masaüstü cihazları ve sunucuları hedef alırken, saldırganlar da çoğunlukla hacker faaliyetlerinin verdiği heyecanın peşinden giden “yalnız kurtlar”dı. Ancak günümüzde çok daha sofistike bir hal alan saldırılar, kazancın temel motivasyon haline gelmesiyle birlikte, organize siber suç ağları tarafından düzenleniyor.

Geleneksel güvenlik yaklaşımları, bu tehditlere yanıt vermek için genellikle imza ve ‘sandboxing’ kullanımına odaklanırlar. Bu teknikler, öncelikle bir güvenlik açığı (exploit) örneğinin tespit edilmesini ve alınmasını gerektirir. Ardından bir güvenlik uzmanı güvenlik açığını “sandbox” üzerinde çalıştırarak bir imza oluşturur. Bu işlemle, makine hızında hareket eden adaptasyon

kabiliyeti son derece yüksek mobil tehditleri durdurmak için gereken reaksiyon süresi hedefine ulaşılması mümkün değildir. Mobil OS saldırı imzalarının geliştirilmesi kolay değildir çünkü güvenlik çözümlerinin verilere erişimi, anti-virüs çözümlerinin geleneksel uç noktalarda eriştiği ayrıntılı dosya kütükleri gibi verilerle aynı seviyede değildir. Mobil cihazlarda bulunan “sandboxing” kısıtlamaları, kullanıcı verilerine erişimi sınırlandırır. Bunun sonucunda, güncellenen imza dosyasının (eğer çözüm cihazda tespit imkânı tanırıyorsa) cihazlara veya (bulut tabanlıysa) buluta gönderilmesi gerekir. Fazlasıyla yavaş olan bu işlem, arzu edilen verimliliği sağlamamaktadır. İmzalar ve “sandboxing” işlemi yavaş işleyen veya eskide kalmış tehditler için yeterli oluyordu ancak günümüzde gizli ve kalıcı olmak üzere tasarlanan kötü amaçlı, bilinmeyen ve hedef odaklı saldırılar

karşısında yeterli etkiyi yaratmamaktadır. Bu işlemler bilinen saldırılar karşısında ve bazı müdahale girişimleri bakımından faydalı olsa da, geleneksel teknikler bilinmeyen mobil saldırılarla ve güvenlik açığı varyasyonlarıyla mücadelede yetersizdir.

Makine öğrenmesi: Mobil güvenlik şartı

Hacker’lar hedefe yönelik mobil saldırılarda genellikle üç teknik kullanır:

1. Tespit edilmemek için bilinmeyen ya da şekil değiştirmeye dayalı saldırılara başvururlar.
2. Saldırını sürdürmek ve cihazı kontrol altında tutmak için cihaz güvenliğine zarar vermeye odaklanırlar.
3. Cihaz güvenliğine zarar vermek için gerekli güvenlik açıklarını sağlamak için MTIM saldırılarından veya

BULUT TABANLI EĞİTİM NASIL ÇALIŞIR?

BULUTTA

1. **İlk veri toplama.** Öncelikle, model normal kullanım kapsamında olan düzinelerce cihazdan yüzlerce özellik toplar ve analiz eder.
2. **Davranış karakterizasyonu.** Analiz edilen davranışların her biri “normal” veya “anormal” (potansiyel açıdan kötü amaçlı) olarak nitelendirilir.
3. **Gürültü arındırma ve özellik seçme.** Her bir DNA saldırısı, sistem verilerinde görülebilecek “reaksiyonlardan” veya değişikliklerden oluşan benzersiz bir profile sahiptir. Yanlış sonuçlara neden olabilecek veri noktaları belirlenir ve ortadan kaldırılır. Her bir saldırı türünde, ilgili özellikler seçilir ve ağırlıklandırılır.
4. **Makine öğrenmesi model eğitimi.** Motor, gerekli tekrarları yapar ve optimum tespit kesinliği için eğitilir.
5. **Model oluşturma.** Makine öğrenmesi motoru, her bir DNA tehdidi için benzersiz, optimum ve gürültüden arındırılmış veri noktalarının kombinasyonuna dayalı uç nokta tehdit tespit modelleri oluşturur.

CIHAZDA

6. **Veri toplama.** Makine öğrenmesinin önemli bir kısmı bulutta meydana gelir. Dünya genelindeki milyonlarca cihazdan milyarlarca veri noktası toplanarak bulutta analiz edilir. Cihazlardan alınan veriler daha sonra öğrenme sürecinin tamamını sürekli olarak tekrar etmek ve modelleri iyileştirmek için kullanılır. Sonrasında bu veriler uç noktalara aktarılır.
7. **Uç nokta yerleşimi.** Modeller cihazlara teslim edildiğinde, gerçek zamanlı olarak cihazda fiili tespit yapılır. İmzaların aksine, optimum davranışsal tespit modellerinin yeni tehditler için güncellenmesine gerek yoktur çünkü her bir tehdidin benzersiz sistem kombinasyonu aynıdır ve modeller tarafından kolaylıkla tespit edilir. Saldırganlar yeni bir saldırı yöntemi belirleyene kadar, makine öğrenmesi modelleri bilinmeyen, sıfır günlük tehditleri tespit etmeye devam edebilir.

kimlik avı (phishing) tekniklerinden yararlanırlar. Bu teknikler, App Store veya Google Play’e bir uygulama ekleyip hedeflenen kuruluşun bunu yüklemesini beklemekten çok daha etkilidir.

İyi habere gelirsek, kuruluşlar MTD yardımıyla UEM’in sağladığı temel güvenliği daha da geliştirebilirler. Cihaza eklenecek MTD aşağıdaki özelliklere sahip olmalıdır:

- ✓ Geleneksel anti-virüs güvenlik unsurlarını bilinmeyen veya şekil değiştirmiş saldırıları durdurmak için makine öğrenmesine dayalı tespit özellikleriyle güçlendirmek.
- ✓ Cihaz (çekirdekten itibaren), ağ ve uygulama genelinde tüm saldırı

vektörlerini eş zamanlı olarak kapsamak. Bu sayede tek bir arıza noktasının cihazı tehdit etmesi engellenebilir.

- ✓ Tehditlere gerçek zamanlı müdahale edilmesini geciktirebilecek bulut tabanlı unsurları kullanmadan tehditleri doğrudan tespit etmek.
- ✓ En etkili kurumsal mobil güvenlik yaklaşımı olarak, bulut tabanlı, makine öğrenmesi eğitimiyle cihazda yerleşik tespit özelliklerini birleştirmek.
- ✓ Doğru sorun için doğru ortamı kullanmak. Bunun için analiz gerektiren milyarlarca veri noktasına ilişkin makine öğrenmesi eğitiminin bulutta çevrimdışı olarak verilmesi gerekir. Ancak MITM’nin ve bulut tabanlı yaklaşımlarla ilişkili diğer

risklerin ortadan kaldırılması için tespit işlemi cihazda yapılmalıdır.

Makine öğrenmesi motorları için bulut tabanlı eğitim

Mobil tehditlerin yüksek hassasiyetle öngörülmesini sağlamak için makine öğrenmesine dayalı motorun milyarlarca veri noktasını analiz (ve yeniden analiz) etmesi gerekir. Bu motor, fazla miktarda verinin işlenebilmesi için bulut ortamında bulunan yüksek performanslı hesaplama kümelerini makine öğrenmesi modellerine aktarır. Ardından, modeller – internet bağlantısı olmayan durumlarda bile – daha önceden bilinmeyen tehditleri derhal tespit etmek için cihaza dağıtılır.

Cihaza ekli, makine öğrenmesine dayalı tehdit tespiti avantajları

Bulut tabanlı tehdit tespitine ve geleneksel anti-virüs çözümlerine kıyasla, makine öğrenmesine dayalı MTD çözümleri modern mobil tehditlerin belirlenmesi açısından bir dizi avantaj sağlar. En önemli avantajlar aşağıda belirtilmiştir:

- ✓ **Bilinmeyen tehdit tespiti:** Geleneksel anti-virüs çözümlerinin aksine, makine öğrenmesi daha önce

bilinmeyen veya sıfır günlük tehditleri algılar.

- ✓ **Makine hızı tespiti:** Mobil saldırılar makine hızında gerçekleştirildiği için, koruma amaçlı önlemlerin de aynı hızda karşılık verebilmesi gerekir. Bulut tabanlı çözümler, ağların ileri geri hareketlerinden kaynaklanan gecikmeler nedeniyle makine öğrenmesine dayalı sistemlerle aynı hıza ulaşamaz.

- ✓ **Optimum gizlilik koruması:** Tüm tespit işlemleri cihazda yapıldığı için, hassas verilerin filtrelenerek bulut ortamına aktarılması gerekmez.

- ✓ **Ağ bağlantısı gerektirmez:** Cihaza yerleşik tespit sistemi, bulut tabanlı tespiti işe yaramaz hale getirebilen MITM gibi ağ saldırılarına karşı hızlı koruma sağlar. Yalnızca cihaza yerleşik bir sistem, ağ bağlantısının olmadığı durumlarda dahi sistemi korumaya devam edebilir.

DOĞRU MAKİNE ÖĞRENMESİ ÇÖZÜMÜNÜ NASIL BULACAKSINIZ?

Günümüzde, birçok mobil güvenlik sistemi tedarikçisi, MTD'ye makine öğrenmesine dayalı bir yaklaşım getirebileceğini iddia ediyor. Bu sistemlerin kabiliyetlerini nasıl değerlendireceğinizi aşağıda açıkladık.

Aşama 1:

DOĞRU SORULARI SORUN

- ✓ Makine öğrenmesine dayalı sistem saldırı kaynağı veya günah keçisi bilinmeden de çalışabilir mi?
- ✓ Makine öğrenmesine dayalı matematiksel model ne kadar yoğundur ve kaç yıl süreyle test edilmiştir?
- ✓ Çözümün en yeni tehditleri belirlemek için yeni imzalar dahil ne sıklıkla güncellenmesi gerekir?
- ✓ Makine öğrenmesi hem bağlı hem de bağlı olmayan ortamlarda nasıl çalışır?
- ✓ Çözüm CPU'ya ve batarya kullanımına minimum düzeyde etki ederek milisaniyelerle ifade edilen sürelerde harekete geçebilir mi?

Aşama 2:

LİTERATÜRÜ İNCELEYİN

Bu sorulara ek olarak, her bir tedarikçinin bloglarını ve diğer açıklamalarını inceleyin. Saldırıların cihazları ilk olarak hedef aldığı zamanla keşfedildiği zaman arasında geçen süreye özellikle dikkat edin. Bu sayede tedarikçinin makine öğrenmesi modelinin arzu edilen sonuçları verip vermediğini tespit etmeniz kolaylaşacaktır. Örneğin, eğer bir tedarikçi aylarda App Store'larda satışına devam edilen ve milyonlarca kez yüklenen bir kötü amaçlı uygulama hakkında açıklama yaparsa, keşif ve doğrulama işlemleri büyük ihtimalle manuel olarak gerçekleştirilmiştir. Öte yandan, sadece birkaç bin kez yüklenen bir uygulamayı etkileyen saldırılarla ilgili açıklama yapılması, makine öğrenmesi MTD çözümünün etkili olduğunu gösterir.

Aşama 3:

KENDİNİZ DENEYİN

Çözümün nasıl çalıştığını bizzat görmek için tedarikçiden demo ya da konsept kanıtı talep edin. Böylelikle, şirketin uygulama ve destek hizmetlerinin kalitesi hakkında da bilgi sahibi olabilirsiniz.

ÇÖZÜM: MOBILEIRON THREAT DEFENSE

Bulut tabanlı mobil tehdit tespiti, sandboxing ve imza yöntemlerinin aksine, MobileIron kurumsal mobil güvenlik için özel olarak tasarlanan makine öğrenmesine dayalı bir yaklaşım kullanır. Zimperium ortaklığıyla geliştirilen makine öğrenmesi motoru, kötü amaçlı davranışları belirlemek için sistem verilerini analiz eder ve sonrasında cihazda tespiti mümkün kılan sofistike matematiksel modeller oluşturur. Motor bilinen kötü amaçlı tehditleri izlemek yerine, cihaz, ağ ve uygulama (DNA) saldırılarını tespit ederek sürekli olarak öğrenmeye ve



işlem hassasiyetini geliştirmeye devam eder. Bu bakımdan, tehdit olduğunu ya da olabileceğini gösteren spesifik aksiyonları analiz ederek daha önce hiç karşılaşılmamış saldırıları bile hızla tespit edebilir. Ayrıca, makine öğrenmesi ve tehdit çözümleme kabiliyetlerimiz tek bir uygulamaya entegre edilmiş olup, kullanıcıların istemciyi etkinleştirmek veya güncellemek için herhangi bir aksiyon almasına gerek kalmadan bu uygulamanın tüm mobil cihazlara eklenmesi mümkündür.

HİBRİT KURULUŞLAR İÇİN MOBİL MERKEZLİ, “ZERO TRUST” MİMARİ



PTC, SaaS Platformu Onshape ile KOBİ'lere Ulaşmayı Hedefliyor

PTC, bilgisayar destekli tasarımın buluttaki öncülüğünü üstlenen SaaS platformu Onshape'i satın aldı. Ürün tasarımını bulutun avantajlarıyla SaaS ortamında daha düşük maliyetlerle gerçekleştirmeye izin veren Onshape, PTC uzmanlığıyla üretim alanında faaliyet gösteren KOBİ'lerin gelişiminde önemli rol oynayacak.

PTC CEO'su Jim Heppelmann, geçtiğimiz Ekim ayı sonunda, bir SaaS Platformu olan Onshape'i satın almak üzere kesin bir anlaşma imzalandığını duyurdu. Jim Heppelmann, yeni iş birliğini şu sözlerle paylaştı: "Sağlam bir bilgisayar destekli tasarımı (CAD), güçlü veri yönetimi ve işbirliği araçlarıyla bir araya getiren ürün geliştirme platformu Onshape'i satın almak için kesin bir anlaşma imzaladığımızı sizinle paylaşmaktan büyük heyecan duyuyorum. Bir SaaS platformu olan Onshape, SolidWorks'ün yaratıcı ekibi ve eski yöneticileri olan Jon Hirschtick, John McEleney ve Dave Corcoran dahil CAD alanında uzmanlaşmış bir ekip tarafından kuruldu. Bildiğiniz gibi, çoğu yazılım endüstrisi sahip olma maliyetini düşürmesi ve pazara yeni yetenekler getirilmesini hızlandırması sebepleriyle SaaS modelini benimsiyor. SaaS, yüksek ücretli sunucu donanımına olan ihtiyacı ortadan



JIM HEPPELMANN

CEO
PTC

kaldırıyor ve kullanıcıların, yöneticilerin düzenli güncellemeler gerçekleştirmelerine gerek kalmaksızın, her zaman yazılımların en güncel versiyonlarını kullanmalarını sağlıyor. PTC, iş değerini artıran ve rekabet gücünüzü geliştiren yenilikçi teknoloji sağlama konusundaki kararlılığımızın bir yansıması olarak Onshape'i satın alıyor. Bu stratejik satın alma ile PTC, CAD ve PLM

alanındaki kapsama alanını ikiye katlıyor. Müşterilere tercihlerine göre SaaS (Onshape) ya da kendi bünyelerinde (Creo ve Windchill) konumlayabilecekleri en güçlü seçenekleri sunuyoruz."

ONSHAPE SATIN ALMASI NE ANLAMA GELİYOR?

Creo ve Windchill ürünleri, PTC'nin ana faaliyetlerini temsil ediyor. Her iki ürün de pazar payının artmasıyla beraber çok iyi performans gösteriyor. PTC, bu kritik ürünlere süresiz olarak yatırım yapmaya devam edecek ve istikrarlı bir şekilde yeni performans ve işlevsellik geliştirmelerini hayata geçirecek. Bir taraftan da SaaS platformu kullanmaya hazır olan müşterilerini, ürün geliştirme ihtiyaçları için zengin özelliklere sahip, pazarda kendisini kanıtlamış bir platform olan Onshape çözümü ile destekleyecek. Bu işbirliğiyle birlikte PTC, Türkiye'deki 3 milyonu aşkın KOBİ'ye ulaşmayı hedefliyor.



PTC, SİZİ VUFORIA VIEW İLE YENİ DENEYİMLERE DAVET EDİYOR!

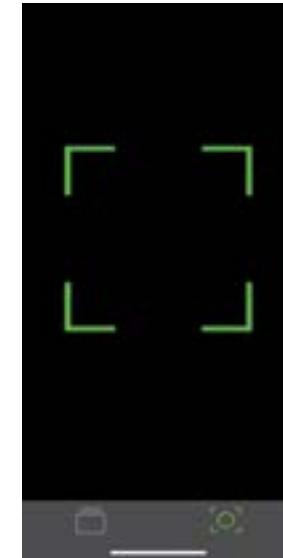
1. IOS veya Android işletim sistemli cihazlarınıza "Vuforia View" uygulamasını indirin.



2. Uygulama içinde galeriden hazır deneyimleri sol alt köşede bulunan butona basarak açabileceğiniz gibi dilerseniz sağ alt kısımdan kod okutma seçeneğiyle aşağıdaki kodları okutabilirsiniz.



Motosiklet



Pro Engine



VERITAS BACKUP EXEC

Backup Exec Çözümüne Geçmek İçin 10 NEDEN!



Kurumunuz da başka pek çok kurum gibiye, IT ortamınız ister sanal ister fiziksel, bulutta ya da hibrit olsun, giderek daha karmaşıklaşan bir yedekleme ve kurtarma süreciyle uğraşıyorsunuz demektir. Veritas Backup Exec™ zaman ve maliyet tasarrufu sağlamanıza; güvenilirliği, RTO (kurtarma süresi hedefleri) ve RPO'yu (kurtarma noktası hedefleri) iyileştirmenize yardımcı olabilecek pek çok güçlü özelliği sayesinde bütün veri koruma ihtiyaçlarınızı karşılayan, basit bir yedekleme ve kurtarma çözümü sunarak bu karmaşayı ortadan kaldırır. Halihazırda Backup Exec kullanıyorsanız, çözümünüzü en yeni sürüme yükseltmek daha da büyük fayda sağlayacaktır.

1. KOLAY KULLANIM



Backup Exec, her bir yedekleme, replikasyon ve kurtarma işlemini hızla takip ve kontrol edebilmek için

ihtiyaç duyduğunuz görünürlüğü sağlayan, kullanımı kolay bir arayüz, akıllı kullanıcı konsolları ve sezgisel sihirbaz uygulamaları ile tam bir paket halinde sunulur. Ayrıca zaman tasarrufu sağlar ve yedekleme korumasının uygulanmasını kolaylaştırır; birkaç tıklamayla yedekleme işlerinin zaman ayarlarını yapabilir, yedekleme durumunu görebilir ve kurtarma işlemleri yapabilirsiniz. Azure Site Recovery entegrasyonu sayesinde buluttaki replikaları Azure üzerinden kolayca görebilirsiniz.

2. DAHA MODERN VERİ KORUMA



Uzun vadeli veri saklama ve felaket kurtarma için Microsoft Azure, Amazon Web Services

(AWS) ve Google Cloud gibi genel veri depolama ortamlarını kullanmak, depolama maliyetlerinizi düşürmenin yanı sıra kurumunuzun modernizasyonu ve dijital

dönüşümü açısından da akıllıca bir hareket olacaktır. İşletmeler dönüşürken veri koruma uygulaması geçmişte yaşamaya devam etmektedir. Hatta çoğu kurumda hâlâ teyp bazlı çözümler devrededir. Yedekleme verilerinizi kurum-İçi teyplerden doğrudan bulutta depolamaya taşımak, iş başlamak için harika bir adım olacaktır. Backup Exec bu geçişi kolayca yapmanızı sağlar.

3. BULUT, SANAL VE FİZİKSEL ORTAMLAR İÇİN TEK BİR ÇÖZÜM



Artık hiç kimsenin birden fazla yedekleme çözümüyle uğraşacak zamanı ve maddi kaynağı yok. Backup Exec sayesinde tek bir arayüz üzerinden tüm yedekleme ve kurtarma durumunuzu görebilir, böylece yedekleme yöneticisi olarak sizin için çok değerli olan zamandan tasarruf edebilirsiniz. Başarısı kanıtlanmış bu yedekleme ve kurtarma çözümü, fiziksel ve çoklu-bulut ortamlarında ister tek bir

fiziksel sunucuda ister binlerce sanal makinede bulunan tüm verileri korur.

4. AWS VE AZURE BULUT İLE ENTEGRASYON



Backup Exec, Azure ve AWS mağazalarından alınabilir. Tek yapmanız gereken, Mağaza şablonunu kullanarak Backup

Exec yazılımını tek tıklamayla bulutta barındırılan bir sunucuya yüklemek. Hepsi bu kadar. Backup Exec, AWS ve Azure bulut ile kusursuz entegrasyon sağlayarak tüm verilerinizi korur. Backup Exec'in Azure Site Recovery (ASR) destekli Instant Cloud Recovery (Anında Buluttan Kurtarma) özelliği, bulut yedeklemelerini tamamlayıcı olması için Servis Olarak Azure Felaket Kurtarma (DRaaS) çözümünden yararlanır ve böylece Azure bulut entegrasyonunuzu daha da geliştirir. Instant Cloud Recovery sayesinde, tam bir felaket durumunda bile çalışmama süresini (RTO) ve veri kaybını

(RPO) en aza indirebilirsiniz, çünkü iş açısından kritik olan Hyper-V ve VMware sanal makinelerindeki verileri anında Azure buluta kopyalayabilirsiniz. Backup Exec ile AWS bulutun entegrasyonu, verileriniz Glacier ve Glacier Deep Archive da dahil olmak üzere herhangi bir AWS depolama katmanında güvenle depolamanızı sağlar.

5. SANAL MAKİNE KORUMASINI OPTİMİZE EDEN TASARIM



Backup Exec; Microsoft® Volume Shadow Copy Service (VSS) ve VMware vStorage™ APIs for Data

Protection (VADP) ile entegre olarak tüm sanal makineleriniz için uygulamaya-duyarlı, güvenilir ve tutarlı yedeklemeler sunar. İleri teknolojiyi kullanan Backup Exec CPU'yu, bellek kullanımını ve I/O yük performansının sanal ana makinedeki etkisini en aza indirir. Kayıt kesme, meta-veri toplama ve katalog oluşturma gibi

NEDEN BACKUP EXEC 20 KULLANMALISINIZ?

1. Kullanım kolaylığı.
2. Modern, güvenilir veri koruma.
3. Bulut, sanal ve fiziksel ortamlar için tek bir çözüm.
4. AWS ve Azure bulut ile entegrasyon.
5. Optimize sanal makine koruması.
6. Fidy yazılımlarına karşı koruma.
7. Hızlı, verimli yedekleme ve kurtarma.
8. Akıllı veri tekilleştirme sayesinde optimize depolama.
9. Hemen hemen tüm depolama cihazlarında yedekleme.
10. Merkezi yönetim.

yedekleme penceresini etkilemeyen post-processing görevlerini uygulayan Backup Exec, yüksek düzeyde optimize yedekleme sunar ve parça düzeyinde uygulama verilerinin doğrudan depolama alanından hızlı ve çevik bir şekilde kurtarılmasını sağlar.

6. TÜM VERİLERİNİZ İÇİN FİDYE YAZILIMLARINA KARŞI KORUMA

Fidye saldırılarının sıklığı giderek artıyor. Çoğumuzun bildiği gibi, bu riskle savaşmanın tek etkili yöntemi önemli verileri yedeklemektir. Özellikle de fidye saldırıları karşısında ayakta kalma mücadelesi veren küçük ve orta ölçekli işletmeler açısından bu işlem büyük önem taşır. Verileri giderek daha çok lokasyona dağılmış halde bulunan birçok şirket, her dosyayı yakalayabilmek için farklı yedekleme çözümleriyle uğraşmak zorunda kalır. Ama bu yöntem verimsizdir. İster sanal ister fiziksel ya da çoklu-bulut ortamında olsun, her yerdeki tüm verilerinizi Backup Exec ile koruyabilirsiniz.

7. SON DERECE HIZLI YEDEKLEME VE KURTARMA

Backup Exec 20, önceki versiyonlarından bile daha hızlı yedekleme ve kurtarma sunar. Yedeklemeyi ister kurum-içi veriler (fiziksel sunucular, VMware ya da Microsoft Hyper-V sanal makineler) ister bulut tabanlı iş yüklerinizde Instant GRT® ve sanal makinelerde Instant Recovery gibi özelliklerle yapın, düşündüğünüzden de kısa sürede ve güvenilir yedekleme ve kurtarma gerçekleştirebilirsiniz. Backup Exec'in güçlü performansı, veri koruma pencerelerinin sayısını azaltarak size zaman kazandırır.

8. AKILLI TEKİLLEŞTİRMEYLE DAHA AZ DEPOLAMA

Entegre, blok seviyesinde veri tekilleştirme sayesinde, giderek büyüyen veri hacimlerini kontrol altına alın. Her bir yedekleme işi için ayrı ayrı tekilleştirme yapan noktasal çözümlerin aksine Backup Exec sanal ve/veya fiziksel ortamınızın tamamında tekilleştirme

yaparak daha fazla depolama tasarrufu sunar. Ayrıca Backup Exec değiştirilmiş blok takip sistemi de kullandığı için, her sanal makinedeki her blok yerine, sadece değişmiş blokları yedeklemek mümkün olur. Genel bulut depolama alanında entegre, sıralı tekilleştirme sayesinde depolama maliyetleri daha da optimize edilir. Bu yaklaşım, sadece tek verilerin depolanmasını sağlamanın yanı sıra ağ üzerindeki trafiği de azaltarak bant genişliği tasarrufu sunar ve toplam sahip olma maliyetinizi (TCO) en aza indirir.

9. HEMEN HEMEN TÜM DEPOLAMA CİHAZLARINDA YEDEKLEME

Kritik verileri depolamak konusu olduğunda, Backup Exec'in esnek seçenekleri sektörün en kapsamlı donanım ve yazılım uyumluluğunu sunar; böylece disk, teyp, tekilleştirme depolama alanı, uygulama, özel bulut genel bulut, hatta çoklu-bulut da dahil olmak üzere hemen hemen tüm depolama cihazlarında yedekleme yapılabilir. Belirli bir depolama cihazı ya da bulut platformu satın alarak depolama maliyetlerinizi artırmanıza gerek kalmaz.

10. MERKEZİ YÖNETİM

Backup Exec'in merkezi yönetim konsolu dağıtık Backup Exec sunucularının ölçeklendirilebilir şekilde yönetimini sağlar ve böylece yedekleme operasyonlarını yönetmek için gerekli zamanı ve kaynakları azaltır. Bu süreç aynı zamanda iş yükü dengeleme ve yük devretme işlemlerinde güvenilirliği de artırarak donanım verimliliğini ve operasyonel esnekliği maksimum seviyeye çıkarır. Ayrıca merkezi takip, raporlama ve bildirimlerle ortamınız hakkında proaktif bilgi edinebilirsiniz.



Veritas, bilginin gücünden faydalanmanızı sağlıyor.

Veritas platformunu kullanarak, işletmeler dijital dönüşüm süreçlerini hızlandırabilir; çoklu-bulut yönetimi, veri koruma, veri depolama optimizasyonu, uyumluluk ve iş yükü taşınabilirliği gibi BT ve iş zorluklarını kolaylıkla aşabilir.

Veritas size, bilgiyi gerçek anlamda değer yaratan bir varlığa dönüştürme özgürlüğü kazandırıyor. Veriyi sadece maliyet tasarrufu ya da risk azaltımı için değil, gerçekten fark yaratmak için kullanın.

Bilginin içindeki gerçekleri ortaya çıkarın.

VERITAS TECHNOLOGIES LLC HAKKINDA

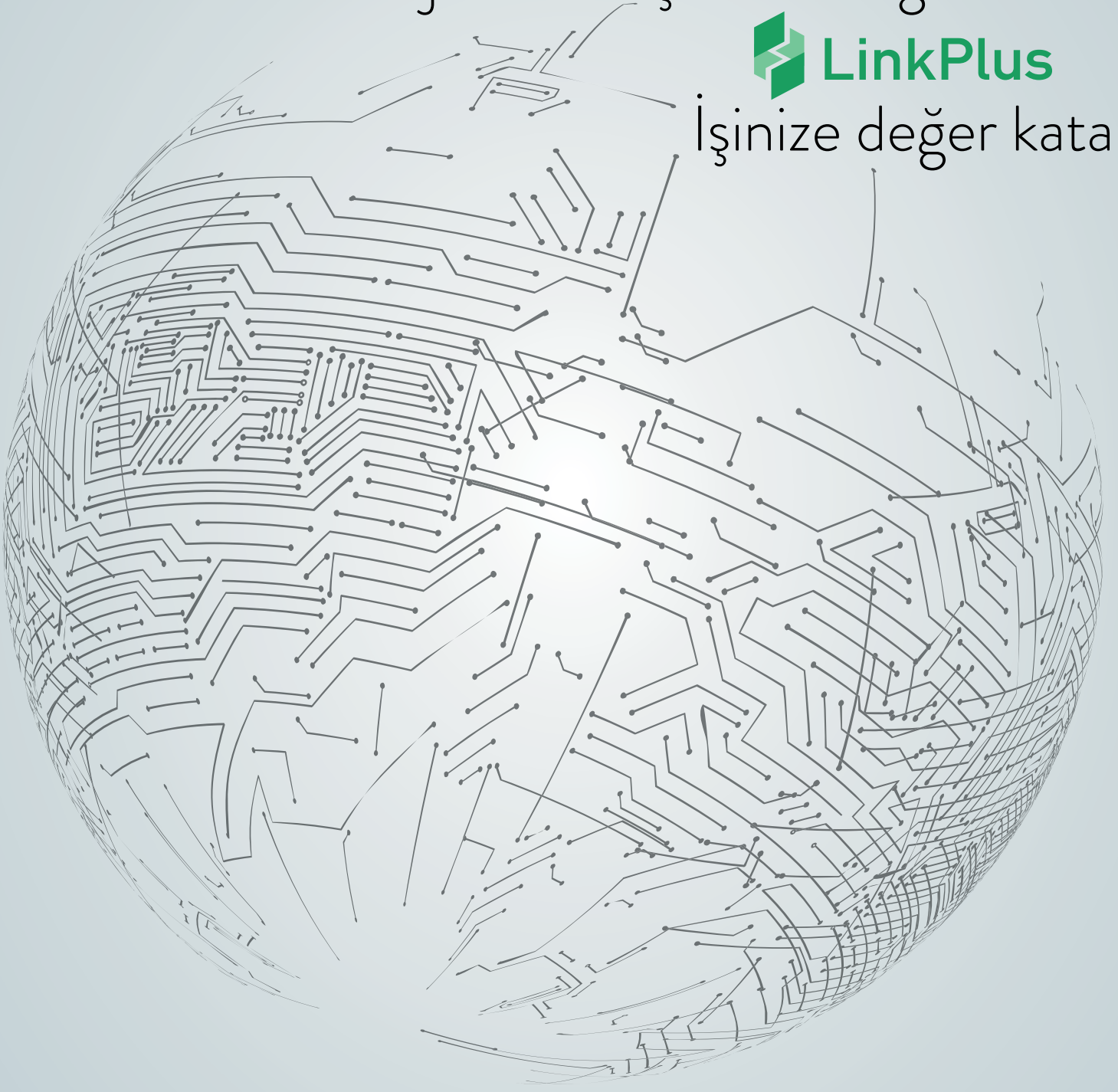
Veritas Technologies kurumsal veri yönetiminde bir dünya lideridir. Fortune 500 listesindeki işletmelerin %90'ı da dahil olmak üzere 50 binden fazla kuruluş, BT ortamlarındaki karmaşıklığı azaltmak ve veri yönetimini sadeleştirmek için Veritas'a güvenmektedir. Kurumsal Veri Servisleri Platformumuz herhangi bir yerdeki verilerin korunmasını otomatize eder, veri kurtarma süreçlerini düzenler, işletme için kritik uygulamaların 7/24 erişilebilir olmasını sağlar ve kurumlara, sürekli değişen veri mevzuatlarına uyum için gerekli içgörülerini sunar. Her ihtiyaca göre ölçeklendirme ve uygulama modeli konusunda güvenilirliğiyle tanınan Veritas, 500'den fazla veri kaynağını ve 50 adet bulut depolama hedefi de dahil olmak üzere 150'den fazla depolama hedefini destekler.

Dijital dönüşümün doğru adresi



LinkPlus

İşinize değer katar



splunk>



HITACHI
Inspire the Next



VERITAS

