**BASIN BÜLTENİ**

**Fortinet, Security Fabric görünürlüğünü ve korumasını endüstriyel Nesnelerin İnterneti’ni (IoT) de kapsayacak hale getiriyor**

Yüksek performanslı siber güvenlik çözümlerinde küresel lider olan [Fortinet](http://ctt.marketwire.com/?release=11G067974-001&id=7377526&type=0&url=http%3a%2f%2fwww.fortinet.com)® (NASDAQ: FTNT) yeni FortiGuard Industrial Security Service çözümünün Security Fabric görünürlüğünü, kontrolünü ve korumasını endüstriyel Nesnelerin İnterneti’ni de kapsayacak hale getirdiğini duyurdu.

**Fortinet Türkiye Sistem Mühendisi Özgür Köse** konuyla ilgili yaptığı açıklamada“IoT tabanlı saldırılar bizlere milyarlarca cihazın bir anda bir silaha dönüşüp küresel olarak dijital ekonomilere, kritik altyapılara zarar verebileceğini ve milyonlarca kullanıcının verilerini çalabilecek boyutlara ulaşabileceğini gösterdi. Nesnelerin İnternetinin (Nİ) neden olabileceği bu büyüklükteki saldırıları etkisiz hale getirmek için kurumların tüm altyapılarının eksiksiz görünürlük, segmentasyon ve uçtan-uca korumasını sağlayacak ölçeklenebilir mimariye ihtiyaçları var. Fortinet Security Fabric kurumları Nİ saldırılarının neden olacağı çeşitli saldırı yüzeylerini öğrenme, segmentasyon ve koruma ile kapsamlı bir çözümle donatıyor” dedi.

* FortiGuard Industrial Security Service (ISS) FortiGuard Labs’in ödüllü tehlike bildirme hizmetlerini kullanarak petrol ve gaz, ulaşım, imalat ve kamu hizmeti gibi kritik altyapılara sahip farklı sektörlerden kurumlara özel olarak kontrol ve savunma çözümleri sunuyor.
* İmalattan doğal kaynaklara, havacılıktan devlet kurumlarına birçok alanda faaliyet gösteren dünyanın dört bir yanından müşteriler Fortinet’in Security Fabric ile sunduğu IoT çözümlerinin zenginliğinden faydalanıp karmaşık ağlarını ve uç nokta cihazlarını koruma altına alıyorlar.
* Fortinet uzun bir süredir Nİ güvenliği konusunda yaptığı çalışmalar ve büyüyen patent portföyü ile IoT inovasyonlarındaki kararlılığını ortaya koydu.

**FortiGuard Threat Intelligence ile Endüstriyel IoT’yi koruma altına alın**

Kurumlardan ve kullanıcılardan gelen talepler küresel ağlara bağlı IoT cihazlarının sayısında bir patlama yaşanmasına neden oldu. McKinsey 2020’ye geldiğimizde bir ağa bağlı Nİ cihazlarının sayısının 20 ila 30 milyar arasında olacağını öngörürken 2015’teki rakamın 10 ila 15 milyar önünde olacağının altını çiziyor. Ancak cihazların sayısı hızla çoğalırken güvenlik riskleri de aynı ölçekte büyüyor.

Ticari ve endüstriyel ağlar ve onların kullandığı Nİ cihazları daha önceleri izole halde çalışırken giderek daha fazla karşımıza çıkan akıllı şehirler veya ağa bağlı evler Nİ cihazlarının yerel, ulusal ve küresel ölçekteki altyapılara bağlı olmasını sağladı. Bu durum kurumların Nİ, BT ve OT (Operasyonel Teknoloji) dünyalarının giderek birbirine yaklaştığı günümüzde ne kadar güvende olduklarını tekrar düşünmelerini gerektiriyor. Birleşik bir Security Fabric’e sonsuz sayıda güvenlik aracı entegre edebilen kurumlar tehdit bilgilendirme hizmetini gerçek zamanlı ve doğru bir şekilde toplayıp ilişkilendirerek normal olmayan hareketleri fark edebiliyor ve otomatik iletilebilen bir cevap geliştirebiliyor.

FortiGuard ISS en çok tercih edilen Industrial Control System (ICS) ve Supervisory Control and Data Acquisition (SCADA) cihaz ve uygulamalarını güvenli hale getiriyor. Bu yeni hizmet ICS ve SCADA sistemleri üzerinde var olabilecek açıklara karşı koruma, derin görünürlük ve detaylı kontrol seçeneklerini sunarken eş-zamanlı tehdit bilgilendirme güncellemeleri ile desteklenerek kurumların erişimi kısıtlayıp saldırının yapıldığı kritik IoT altyapısını korumaya yardımcı oluyor. Fortinet’in endüstriyel güçteki güvenlik cihazları en zorlu ortamlarda bile çalışmak için tasarlandı.

**Küresel kurumlar Fortinet sayesinde IoT’nin nimetlerinden güvenle faydalanıyor**

Her ölçekten ve her sektörden kurumlar Fortinet Security Fabric ile karşılaştıkları Nİ güvenlik zorluklarına çözüm buluyorlar.

* **Gibsons Energy –** Çıkarma ve satış alanlarında çalışan petrol ve gaz şirketi olan Gibsons oldukça dağıtık halde bulunan bir BT altyapısına sahipti ve sahada kurulu halde olan Nİ cihazlarının idaresi ile buluta geçişlerini daha güvenli hale getirecek bir çözüme ihtiyaç duyuyordu. Gibsons Energy Bilgi Hizmetleri Başkan Yardımcısı Richard Hannah bu ihtiyaçla ilgili şöyle dedi: “Sahada konuşlandırdığımız binlerce cihazımız bulunuyor, eskiden bu cihazların hepsini manuel olarak kontrol etmek zorundaydık. Şimdi ise onları buluta bağlayacak bir planımız ve operasyon analizlerini sağlayacak bir sistemimiz var. Fortinet ile birlikte çalışan operasyon ekiplerimiz şimdi cihazların eş-zamanlı takibini gerçekleştirebilirken altyapımızın güvenliğini sağlamak için harcadığımız binlerce saate ulaşan bakım derdinden de kurtulmamızı sağlıyor.”
* **Mumbai Şehri –** Maharashtra Hükümeti Mumbai şehrinin tümünde kablosuz internet erişimi sağlayacak Mumbai WiFi projesi için Fortinet’i seçerek vatandaşların kalabalık alanlarda faydalanabilecekleri ve akıllı toplu taşıma ve akıllı park etme sistemleri için de kullanılabilecek açık WiFi erişim noktaları oluşturuyor. Maharashtra Hükümeti Bilgi Teknolojileri Baş Sekreteri Vijay Kumar Gautam “Mumbai WiFi projesi vatandaşlarımızı dijital olarak daha güçlü hale getirme konusunda çok önemli bir role sahip. Hedefimiz şehrin tamamını açık WiFi erişimiyle donatıp önemli kamu hizmetlerine online erişimi kolay hale getirmek. Altyapımızın hiper-bağlantılı doğası böylesi bir projenin esnek ve ölçeklenebilir bir teknoloji ile her geçen gün daha fazla kullanıcıya, cihaza ve uygulamaya erişimini sağlamalı.”

**IoT güvenliği için entegre bir çözüm**

Fortinet, IoT güvenliğini sağlayıp saldırı alanının her bir noktasını koruma altına alacak geniş ve entegre çözümleri ile Nİ güvenlik sorununa cevap bulabilecek özel bir konuma sahip. Kurumlar Nİ tehditlerine karşı altyapılarını daha güçlü hale getirirken öğrenme, segmentasyon ve korumadan oluşan üç stratejik ağ güvenlik yetkinliğine ihtiyaç duyacaklar. Fortinet’in geniş Nİ güvenlik çözümleri FortiOS, FortiGate, FortiSIEM, Secure Access, FortiGuard Threat Intelligence ve Advanced Threat Protection gibi çözümlerden oluşuyor. Bunlara ek olarak Fortinet’in dayanıklı Fabric Ready Partner ekosistemi ForeScout, Nozomi Networks ve SentinelOne gibi Nİ ve uç nokta güvenlik markaları ile gelişmiş entegrasyon ve eksiksiz koruma sağlayacak teknik işbirliklerini de destekliyor.

**Endüstriye yön veren IoT güvenlik inovasyonu**

Fortinet yıllardır güvenlik inovasyonlarını kullanıcılarına ulaştırırken endüstrideki en güçlü IoT güvenlik patentlerini de portföyünde taşıyarak en yakın takipçisine fark atıyor. Bu patentler Fortinet’in kesintisiz liderliğini perçinlerken çığır açıcı Nİ güvenlik çözümlerini müşterilerinin hizmetine sunuyor.

* Nesnelerin İnterneti için Güvenlik ve/veya Yönetim Sistemi
* Fiziksel seviyede Nesnelerin İnternetine izinsiz giriş tespiti
* Nesnelerin İnterneti kapsamında ‘Stateless Autoconfiguration’ mekanizmasında IPv6 istemciler üzerinde bilgi toplama
* Bulgusal temelli teknikler ile WiFi üzerinden gerçekleşen IoT saldırılarının tespiti

**Fortinet hakkında**

Fortinet (NASDAQ: FTNT) dünya genelinde büyük ölçekli şirketlere, servis sağlayıcılarına ve kamu kurumlarına güvenlik sunar. Fortinet, her geçen gün artan sanal saldırılara karşı müşterilerine akıllı ve sorunsuz koruma sağlar, sınırların ortadan kalktığı ağların artan performans ihtiyaçlarını karşılar. Ağlardaki uygulamaların, bulut sistemlerinin ve mobil cihazların karşılaştığı en kritik güvenlik sorunlarına karşı performanstan ödün vermeden güvenlik sunan tek çözüm sadece Fortinet’in Security Fabric mimarisidir. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 330 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.