**Fortinet En Zorlu Ortamlarda bile Operasyonel Teknolojiyi Koruma Altına Alıyor**

*Fortinet’in kapsamlı Security Fabric Mimarisi sayesinde, çevresel korumalı ya da çevresel olmayan korumalı kurumsal tesislerde entegre güvenlik sağlanıyor.*

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri [Fortinet](http://ctt.marketwire.com/?release=11G067974-001&id=7377526&type=0&url=http%3a%2f%2fwww.fortinet.com)® (NASDAQ: FTNT), kritik altyapılara ve endüstriyel kurumlara yönelik Operasyonel Teknoloji (OT) Güvenlik çözümünü duyurdu. Bu yeni çözüm, kurumların OT altyapıları üzerinde, çevresel anlamda korumalı olmayan alan ve tesislerde hizmete alınan endüstriyel kontrol sistemlerinde (ICS) ve veri tabanlı kontrol ve gözetleme sisteminde (SCADA) entegre bir siber güvenlik koruması sağlamak için FortiGuard endüstriyel tehdit istihbaratı ile sağlamlaştırılmış güvenlik duvarı, devre açıp kapama/anahtarlama ve kablosuz erişim noktası cihazlarını içeriyor.

* Fortinet Security Fabric, kritik altyapıların ve endüstriyel kurumların ileri düzey segmentasyon, erişim kontrolü ve kötücül yazılım kontrolü yapabilmelerini sağlıyor. Kurumlar bu şekilde, güvenlik mimarilerini tek bir çatı altında toplayabiliyor ve işlem yaptıkları ortamın türünden bağımsız bir şekilde OT ağlarını koruyabiliyorlar
* Fortinet’in sağlamlaştırılmış güvenlik ürünleri, endüstriyel kurumların OT altyapılarını ve cihazlarını koruyabilmelerini sağlıyor. Hatta başka güvenlik cihazlarının çalışamaz hale geldiği zorlu ortamlarda bile koruyabiliyor.
* Fortinet’in endüstri-sınıfı cihazları, yakın zamanlarda duyurulmuş olan [FortiGuard Industrial Security Services](https://www.fortinet.com/products/security-subscriptions/industrial-control-systems.html) avantajlarını kullanıyor. Petrol, gaz, ulaşım ve imalat ve kamu hizmetleri dahil endüstriyel kurumlara ve bu kurumların kritik altyapılarına özgü bir savunma ve uygulama kontrolü sağlıyor.

**Fortinet Sistem Mühendisi Cengiz Türkmen,** “Akıllı şehirlere geçiş ve birbiriyle bağlantı halindeki kamu hizmetleri gibi uygulamaların; BT, Operasyonel Teknoloji (OT) ve Nesnelerin İnternetini(IoT) birbiriyle bütünleştirdiği bir ortamda kritik altyapıları siber saldırılara karşı korunması giderek daha da acil bir öncelik olarak ön plana çıkıyor. Birbiriyle birleşen bu ağları başarılı bir şekilde korumak isteyen kurumlar, tüm altyapılarını eksiksiz bir şekilde görünür kılabileceği, segmentasyon ve bütünlüklü bir koruma sağlayabileceği biçimde ölçeklendirebileceği bir mimariye ihtiyaç duymaktadır. Fortinet’in son OT çözümü kritik altyapılara sahip kurumları geleneksel BT ortamlarına kadar uzanan kapsamlı bir güvenlik çözümüyle donatıyor ve kritik OT altyapılarını korumak için gereken ileri düzey yetenekler sağlıyor” dedi.

**OT ile BT’nin birbirine yakınlaşması, birleştirilmiş ve otomatikleştirilmiş güvenlik gerektirmektedir**

Kritik altyapılar her geçen gün daha fazla siber saldırıya maruz kalıyor. Bir araştırmada kurumların yüzde 51’inin son 12 ay içinde bir SCADA/ICS güvenlik ihlali yaşadığı aktarılıyor. Saldırıların başarılı olması durumunda ciddi arızalar yaşanabilir hatta su, elektrik ve yakıt gibi temel hizmetler ve fiziksel varlıkların zarar görmesine yol açılabilir.

Kamu hizmetleri, petrol, gaz, ulaşım ve imalat sektörlerinde, birbirine bağlı kontrol sistemleri ve endüstriyel IoT (Nesnelerin İnterneti) cihazlarının kullanılma oranı arttıkça, saldırılabilecek alanların genişliği de artıyor. Bu cihaz ve sistemlerin birbirine bağlı olması, ciddi bir problem yaratıyor çünkü geleneksel BT’nin ağ altyapılarını, kablosuz erişim noktalarını ve mobil ağlarını kullanmaya başlıyorlar. OT altyapı teknolojilerinin kendine özgü doğası, aynı zamanda, güvenlik ve tehdit istihbarat çözümlerinin çoğu tarafından (kritik altyapılara yapılan saldırılara karşı savunma yeteneği olmaması bir yana) görünebilir bile olmadığı anlamına geliyor.

2014 Forrester raporuna göre, “Geleneksel bilgi teknolojileri (BT) ile operasyonel teknoloji (OT) arasında temel farklılıklar bulunmaktadır. . . . IT ve OT’nin güvenlik ve risk uzmanları birbirine saygı duymalı, birbirlerinin farklılıklarını kabul etmeli ve birlikte çalışmayı öğrenmeliler.”1

Fortinet’in Operasyonel Teknoloji Güvenlik çözümü, kritik altyapı ve endüstriyel kurumlara özgü güvenlik problemlerine çözüm getirirken, Fortinet Security Fabric aracılığıyla da hem OT hem de geleneksel BT altyapılarının yönetimi ile idaresini tek bir yapı içinde buluşturuyor.

**OT altyapısına özel olarak tasarlanmış Security Fabric koruması**

Fortinet’in açık havada kullanılmaya yönelik sağlam ürünleri, aşırı zor hava koşulları ya da benzer güçlükler içeren fiziksel ortamlar için olduğu kadar kötücül saldırılarla karşılaşabilecek kritik kontrol sistemleri için de kurumsal sınıfta bağlanabilirlik ve güvenlik özelliği taşıyan ve endüstriyel olarak sağlamlaştırılmış cihazlardır.

* [FortiGate Rugged Serisi](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_Rugged_Series.pdf) kritik endüstri ve kontrol ağlarını kötücül saldırılara karşı korumak için uzmanlaştırılmış bir tehdit koruması sunan ‘hepsi bir arada’ güvenlik duvarlarıdır.
* [FortiSwitch Rugged Serisi](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitchRugged.pdf), Fortinet’in güvenilen FortiSwitch hattındaki tüm performans ve güvenliği sağlıyor ama buna bir de ekstra bir güçlendirme ekleyerek ürünü, zorlu dış ortamlarda hizmete alınan uygulamalar için ideal hale getiriyor. Yönetimin FortiGate tarafından yapılıyor olması operasyonu basitleştiriyor ve güvenlik politikalarını anahtar yuvalarını (switchleri) da kapsayacak şekilde genişletiyor.
* [FortiAP Dış Mekan Serisi](http://www.corex.at/Produktinfos/FortiAP_Outdoor_20170322.pdf), FortiGate sayesinde entegre kablosuz kontrol işlevi tarafından yönetilerek güvenli ve kimlik odaklı WiFi erişim noktaları sunuyor. FortiSwitch de buna eklenince, ortak güvenlik politikaları ile gerçekten birleşik hale gelmiş bir erişim katmanı oluşuyor.
* Fortinet’in dış mekanlara yönelik sağlam cihazları, arızalar arasında üstün bir ortalama zaman, elektromanyetik çıkarım koruması, titreşim toleransı, hava girişi korumalı suya dayanıklılık, geniş termal işletim aralıkları, fansız soğutma ve eternet gücü (PoE) gibi çeşitli özelliklere sahip olacak şekilde sunuluyor.

Bu cihazlar Fortinet’in, FortiOS güvenlik işletim sistemi tarafından kontrol altında tutuluyor ve en çok kullanılan ICS ve SCADA cihaz ve uygulamalarını korumak için FortiGuard Industrial Security Service/ FortiGuard Endüstriyel Güvenlik Hizmeti ile yedekleniyor. FortiGuard Endüstriyel Güvenlik Hizmeti markalı ICS ve SCADA protokollerinde zayıflıkları koruma altına almak, derin bir görünürlük ve her noktada kontrol sağlamak için OT özelinde gerçek zamanlı tehdit istihbaratı gerçekleştiriyor.

Fortinet Fabric-Ready İşbirliği Programı ayrıca, kurumların üçüncü taraf OT güvenlik çözümlerini Fortinet Fabric Security ile sorunsuzca entegre edebilmelerini de mümkün kılıyor. Bir ön-doğrulama niteliği taşıyan bu derin teknik entegrasyonlar, istikrarlı bir şekilde birlikte işlerlik ve kurulum kolaylığı sağlarken karmaşıklığı azaltıp otomasyonu artırıyor.

Konuyla ilgili görüş bildiren Innogy SE, Telekomünikasyon Başkanı Dr. Jürgen Tusch, “Enerji sektörü giderek daha da dijitalleşiyor, dolayısıyla yenilenebilir çok sayıda enerji kaynağının kritik şebeke kontrol merkezlerine güvenli bir şekilde bağlanması çok önemli ve gitgide büyüyen bir problem olarak karşımıza çıkıyor. İletişim altyapıları gibi kritik misyonlara yönelik güvenlik çözümleri için Fortinet ile birlikte çalışmaktan heyecan duyuyoruz. Fortinet ile girdiğimiz işbirliği, kamu hizmetlerine özgü gereklilikleri karşılamak için ihtiyaç duyduğumuz derin denetimi geliştirmemizle sonuçlandı. Bu gelişme, OT ağlarımızda güvenlik ve görünürlüğü bir ileri seviyeye taşımamız için büyük bir önem taşıyordu” diyor.

Nozomi Networks, İşbirlikleri &Kurumsal Geliştirmeden sorumlu Başkan yardımcısı Chet Namboodri konuyu şöyle değerlendiriyor: “Nozomi Networks, OT sistemleri üzerinde yenilikçi siber güvenlik ve operasyonel görünürlük çözümlerinde lider bir firmadır. Fabric-Ready programı çerçevesinde Fortinet ile birlikte çalışan Nozomi olarak, OT ağ gözetim ve davranışsal analitiğimizi entegre ederek gerçek zamanlı görünürlük elde edebiliyor, tehditleri saptayabiliyoruz. Bunun yanı sıra, Fortinet’in Fortigate Rugged serisi güvenlik duvarlarıyla sorunsuz bir otomasyon da gerçekleştirmiş bulunuyoruz. OT alanında kapsamlı saptama ve onarım çözümü sunmak için Fortinet ile işbirliği yapmak bize gurur veriyor.”

**Ek Kaynaklar**

* Fortinet’in Operasyonel Teknoloji altyapılarındaki güvenlik çözümleriyle ilgi ilgili daha fazla bilgi için Fortinet Kritik Altyapı Güvenliği [anasayfa](https://www.fortinet.com/solutions/industries/scada-industrial-control-systems.html) ‘sını ziyaret edebilirsiniz.
* Fortinet’ [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet) ve [Facebook](https://www.facebook.com/fortinet/) üzerinde takip edebilirsiniz.
* [Fortinet blog](http://blog.fortinet.com) üzerindeki sohbetlere katılabilirsiniz.
1. Forrester Brief: S&R Pros Can No Longer Ignore Threats To Critical Infrastructure, Rick Holland, Stephanie Balaouras, Katherine Williamson, Temmuz 2014

**İlgili Kişi**

Eray Çoşan Akkuş

Marjinal Porter Novelli

0533 927 23 97 erayc@marjinal.com.tr

**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 320 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet’e güvenmektedir. Daha fazla bilgi için: http://www.fortinet.com, Fortinet Blog sayfası veya FortiGuard Labs.