**Gelişmiş Yapay Zeka ve Karşı Tehdit İstihbaratı Siber Suçluların Uzun Süredir Sahip Olduğu Avantajı Ellerinden Alacak**

*Kurumların Proaktif Olarak Modern Saldırılara Karşı Korunabilmesi için Entegrasyonu, Gelişmiş Yapay Zekayı ve Aksiyon Alınabilen Tehdit İstihbaratını En Yüksek Seviyede Kullanan Güvenlik Stratejilerini Benimsemesi Gerekiyor.*

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet® (NASDAQ: FTNT), [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta)’in 2020 ve ilerisi için tehdit zeminine yönelik yaptığı tahminleri açıkladı. Açıklanan tahminler arasında Fortinet’in siber suçluların yakın zamanda kullanmayı planladığı yöntemlerin yanı sıra kurumların gerçekleşecek saldırılara karşı kendilerini koruyabilmelerine yardımcı olacak stratejiler yer alıyor.

**Siber Saldırılar Değişiyor**

Siber saldırı metodolojileri yakın zamanda daha akıllı hale gelerek, saldırıların etkisini ve hızını artırdı. Bu trendin devamı ise kurumların güvenlik stratejilerine olan yaklaşımının değişmesine bağlı. Günümüzün küresel tehdit zeminin hacmi, hızı ve gelişmişliği göz önünde bulundurulduğunda, kurumların agresif saldırılara karşı etkili bir şekilde karşılık verebilmesi için gerçek zamanlı ve makine hızında hareket etmesi gerekiyor. Yapay zeka ve tehdit istihbaratındaki gelişmeler, bu mücadelede hayati öneme sahip.

***Sistem olarak Yapay Zeka’nın (AI as a System) Dönüşümü***

Fortinet, bir süredir insan vücudundaki bağışıklık sistemi görevi görecek güvenlik odaklı bir yapay zeka (AI) geliştiriyor. Birinci nesil AI, öğrenmek, ilişki kurmak ve belirli bir eylem planı oluşturmak için öğrenen makineler modelini kullanacak şekilde tasarlandı. İkinci nesil AI ise öğrenme düğümlerini bir çevreye dağıtarak erişim kontrolü gibi alanları önemli ölçüde geliştirmek için düzenleri tespit etme yeteneğinden faydalanıyordu. Öte yandan üçüncü nesil AI, gücünü merkezi ve modası geçmiş bir işleme merkezinden almak yerine, bölgesel öğrenen düğümleri birbirine bağlayacağı ve böylece yerel olarak toplanan verilerin daha dağıtık bir şekilde paylaşılabileceği, ilişkilendirilebileceği ve analiz edilebileceği alan haline geldi. AI’nın geçirdiği bu dönüşüm, özellikle genişleyen sınır ortamlarını emniyete almak isteyen kurumlar için önemli bir gelişme.

***Birleşmiş Öğrenen Makineler***

Öğrenen makineler, akışlardan veya iç trafik ve veri analizinden elde edilen geleneksel tehdit istihbaratından faydalanmaya ek olarak yeni sınır cihazlarından yerel öğrenen düğümlere gelecek ilgili bilgilerden de güç alacak. AI, gerçek zamanlı bilgiyi takip ederek ve aralarında bağ kurarak tehdit zeminine dair eksiksiz bir görüntü oluşturmanın yanında yerel sistemlerin yerel olaylara nasıl tepki vereceğini de iyileştirebilecek. AI sistemleri, ağ üzerinde bilgi paylaşarak tehditleri görebilecek, onların arasında bağ kurabilecek, takip edebilecek ve onlara karşı hazırlıklı olabilecek. Birleşmiş öğrenen bir sistem, tüm bunların sonunda veri setlerinin kendi içinde bağlı olmasını sağlayarak öğrenme modellerinin dönüşen ortamları ve olay trendlerini benimsemesini sağlayacak. Böylece bir noktada yaşanan olay, tüm sistemin zekasını geliştirecek.

***AI ve Rehberler Saldırıları Öngörebilmek için Birleşecek***

Kurumlar, AI’a yatırım yaparak görevlerini otomatikleştirebildiği gibi gerçekleşmeden önce veya gerçekleşirken saldırılara bakabilecek ve onları keşfedebilecek otomatik bir sisteme sahip oluyor. Öğrenen makineler, istatistiksel analizlerle birleştiğinde kurumların tehditleri tespit etme ve onlara cevap verme özelliklerini geliştirmek için AI’larına bağlı özel aksiyon planları geliştirmelerini sağlayacak. Bu tehdit rehberleri, AI’ların saldırganların bir sonraki hamlelerini, saldırının yüksek ihtimalle nerede gerçekleşeceğini ve hangi aktörlerin sorumlu olduğunu belirlemesini sağlayan şablonlarını açığa çıkarmasına yardımcı olabilir. Eğer bu bilgi AI’ın öğrenme sistemine eklenirse, uzaktaki öğrenen düğümler daha gelişmiş ve proaktif bir koruma sunabilecek. Bu korumayla tehdit tespit edilebilecek, hareketleri tahmin edilebilecek, proaktif olarak engellenecek ve diğer düğümler birbiriyle koordine olarak saldırının tüm alanları aynı anda kapatılabilecek.

***Karşı İstihbarat ve Yanıltma Fırsatı***

Casusluk dünyasındaki en kritik kaynaklardan birisi karşı istihbarat ve aynısı hareketlerin dikkatlice gözlendiği ortamlara saldırırken veya onları savunurken de geçerli. Siber suçluların genelde erişiminin olmadığı tehdit istihbaratına sahip sistem yöneticilerinin belirgin bir avantajı var. Bu avantajı öğrenen makineler ve AI ile güçlendirmek de mümkün. Yanıltma teknolojilerinin daha sık kullanılması, siber saldırganlar tarafından karşı istihbarat hamlesine neden olabilir. Bu durumda saldırganların doğru ve yanlış trafik arasındaki farkı yakalanmadan veya trafiği gözetlemeden fark edebilmesi gerekiyor. Kurumlar da bu stratejinin önüne daha fazla rehber ekleyerek ve yanıltma stratejilerinde her yere nüfuz eden bir AI kullanarak geçebilir. Bu strateji, doğru trafiği tespit etmeye çalışan suçluları fark etmenin yanında yanıltıcı trafiğin de gelişmesini sağlayarak gerçeğinde gerçekleşen işlemlerle arasında bir fark olmamasını sağlayacaktır. Sonuç olarak kurumlar karşı istihbarat çalışmaları gerçekleşmeden onlara karşı cevap vererek, üstün kontrol konumlarını devam ettirebilecek.

***Kolluk Kuvvetleriyle daha Sıkı Çalışma***

Siber suçluların gizlilik ve erişim gibi özel ihtiyaçları oluyor. Aynı zamanda siber suçluların bir sınırı da yok. Dolayısıyla kolluk kuvvetleri de küresel komuta merkezleri ve özel sektörle ilişki kuruyor. Böylece siber suçluları gerçek zamanlı görmeye ve onlara karşılık vermeye bir adım daha yaklaşıyor. Kolluk kuvvetlerinin yanı sıra kamu ve özel sektör ilişkilerinin yapısı, siber suçluları tespit etmeye ve onlara cevap vermeye yardımcı olabiliyor. Farklı uluslararası ve yerel kolluk kuvvetleri, devletler, kurumlar ve güvenlik uzmanları arasında köprü kurmak için daha birleştirici bir yaklaşımı öne çıkaran inisiyatifler, kritik altyapıları korumak ve siber suçlarla mücadele edebilmek için bilginin doğru zamanda ve güvenle aktarılmasının hızlandırılmasına yardımcı oluyor.

**Siber Suçlular Gelişmeye Devam Ediyor**

Stratejide yapılan değişikliklere siber suçlulardan da karşılık geliyor. Siber suçlular, saldırıları tespit etmek ve onlara karşılık vermek için gelişmiş yöntemler kullanan ağlara ve kurumlara daha güçlü bir yöntemle karşılık vermek için çalışıyor. Daha gelişmiş saldırı yöntemlerinin yanı sıra büyüyen potansiyel saldırı zemini, daha akıllı ve AI’dan güç alan sistemlerle siber suçlular gelişmeye devam ediyor.

***Gelişmiş Kaçınma Teknikleri***

Yeni yayınlanan [Fortinet Tehdit Görünümü Raporu](https://www.fortinet.com/blog/threat-research/fortinet-q2-2019-threat-landscape-report.html), tespit edilmekten kaçınmak, güvenlik özelliklerini ve cihazlarını etkisiz kılmak, mevcut yüklenmiş yazılımı istismar eden ve kötü amaçlı trafiği doğru gibi gösteren ‘yasal görünen araçlardan faydalanma’ (living off the land, LotL) stratejileriyle yakalanmamak için gelişmiş kaçınma tekniklerinin kullanımında artış olduğunu gösteriyor. Birçok modern kötü amaçlı yazılım araçları halihazırda antivirüs programlarından veya tehditleri tespit eden diğer önlemlerden kaçınmak için özellikler barındırıyor. Ancak siber suçlular tespit edilmekten kaçınmak için kendilerini gizleme ve anti-analiz çalışmalarını daha da geliştiriyor. Bu tarz stratejiler, güvenlik kaynaklarında ve çalışanlarındaki zaafiyeti en yüksek seviyeye çıkarıyor.

***Toplu Saldırı Teknolojisi***

Son birkaç yılda ağlara ve cihazlara saldırmak için öğrenen makineler ve AI gibi teknolojilerden faydalanan [toplu saldırı teknolojisinde](https://www.fortinet.com/blog/industry-trends/defending-against-an-automated-attack-chain--are-you-ready-.html) yaşanan artış, yeni bir potansiyel olarak dikkat çekiyor. Toplu saldırı teknolojisinde yaşanan gelişmeler; ilaç, ulaşım, mühendislik ve otomatik problem çözme alanlarında güçlü etki yaratıyor. Ancak eğer kötü amaçla kullanılırsa ve şirketler güvenlik stratejilerini güncellemezlerle, siber suçlular için de aynı şekilde önemli etkiye sahip oluyor. Toplu saldırı teknolojisi, siber suçlular tarafından ağa sızmak, iç savunmalara aşırı yüklenmek ve etkili bir şekilde veriyi çıkartmak için kullanılabiliyor. Özelleştirilmiş botlar, belirli özelliklerle donatıldığında gerçek zamanlı toplanan istihbarat verilerini paylaşabiliyor ve aralarında bağlantı kurabiliyor. Böylece toplu saldırı teknolojisinin bir veya birden çok hedefi aynı anda açığa çıkartmak için seçim yapmasını ve saldırıyı ona göre özelleştirmesini sağlıyor.

***5G’yi ve Sınır Bilişimi Silahlaştırmak***

5G’nin gelişmesi, toplu saldırı teknolojisini temel alan kullanışlı saldırıların gelişmesini başlatacak bileşen olabilir. Bu noktada 5G için de bilgiyi ve uygulamaları hızlıca paylaşabilen ve işleyebilen, özel bir amaç için kurulan yerel ağları oluşturabilmek gerekiyor. 5G ve sınır bilişim silahlaştırıldığında, bireysel olarak istismar edilen cihazlar, kötü amaçlı kodun aktarılması için gerekli aracı olabilir ve gizliliği açığa çıkmış cihazlar da hedeflerine 5G hızında saldırmak için birlikte çalışabilir. Böylesi bir saldırının hızı, zekası ve yerelleştirilmiş doğası düşünüldüğünde geleneksel güvenlik teknolojileri, inatçı saldırılara karşı mücadele ederken zorlanabilir.

***Siber Suçluların Sıfırıncı Gün Saldırısını Farklı Şekillerde Kullanabilir***

İstismar edecek bir sıfırıncı gün zafiyeti bulmak ve geliştirmek eskiden çok maliyetliydi. Dolayısıyla siber suçlular da genellikle saldırı bertaraf edilene kadar mevcut portföye yüklenirdi. Saldırı zeminin genişlemesi ve yapılan keşiflerin kolaylaşmasıyla potansiyel olarak istismar edilebilen sıfırıncı gün zafiyetleri de gün yüzüne çıkıyor. [Yapay zeka fuzzing tekniği ve sıfırıncı gün madenciliği](https://www.fortinet.com/blog/industry-trends/predictions--ai-fuzzing-and-machine-learning-poisoning-.html) de sıfırıncı gün saldırılarının hacmini artırma potansiyeline sahip. Bu trende karşı çıkabilmek için güvenlik önlemlerinin yerinde olması gerekiyor.

**Fortinet Bölge Teknoloji Direktörü Melih Kırkgöz konuyla ilgili şunları söyledi:**

“Siber saldırganların elde ettiği birçok başarının arkasında genişleyen saldırı zemininden ve dijital dönüşüm sonucunda ortaya çıkan güvenlik boşluklarından faydalanma özellikleri yatıyor. Çok yakın zamanda saldırganların saldırı metodolojileri, öncü yapay zeka ve toplu saldırı teknolojileriyle daha akıllı hale geldi. Öte yandan kurumlar da siber suçluların onları hedef almak için kullandığı teknolojileri kendilerini savunmak için kullanırsa yakın zamanda bu gidişat değişecek. Nesnelerin İnterneti’nden dinamik bulutlara birçok sınırın yanı sıra ağ bölümlerinde koruma ve görünürlük için kurumların kapsamlı, entegre ve otomatik olan birleşik bir yaklaşım benimsemesi gerekiyor.”

**Daha Fazla Okuma için Ek Kaynaklar:**

* Öngörüler hakkında daha fazla bilgi için [blog](https://www.fortinet.com/blog/industry-trends/fortinet-2020-threat-landscape-predictions.html) yazımızı okuyabilirsiniz.
* Fortinet Tehdit Görünümü raporunun en sonuncusuna ve 2018’in 3. Çeyreğindeki botnet, kötü amaçlı yazılım ve istismarları hakkında detaylı bilgiye [blog](https://www.fortinet.com/blog/threat-research/fortinet-q3-threat-landscape-report.html) üzerinden erişebilirsiniz.
* [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta) ve FortiGuard Güvenlik Hizmetleri [portföyüne](https://www.fortinet.com/support-and-training/support-services/fortiguard-security-subscriptions.html?utm_source=blog&utm_campaign=2018-blog-security-services) ulaşmak için tıklayın.
* Güvenlik denetimleri ve en iyi uygulamalar sunan FortiGuard [Güvenlik Derecelendirme Hizmeti](https://www.fortinet.com/support-and-training/support-services/fortiguard-security-subscriptions/security-rating.html?utm_source=blog&utm_campaign=2018-blog-security-rating-service) için tıklayın.
* Haftalık [FortiGuard Tehdit İstihbarat Özetlerine](https://fortiguard.com/resources/threat-brief) abone olmak için tıklayın.
* [Network Security Expert program](https://www.fortinet.com/support-and-training/training/network-security-expert-program/nse-1.html?utm_source=blog&utm_campaign=2018-q2-nse-training), [Network Security Academy program](https://www.fortinet.com/support-and-training/training/fortinet-network-security-academy.html?utm_source=blog&utm_campaign=2018-fnsa-program) veya [FortiVets program’ımımız](https://www.fortinet.com/corporate/careers/vets.html?utm_source=blog&utm_campaign=2018-q2-fortivet) hakkında ayrıntılı bilgi için tıklayın.
* [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=blog&utm_campaign=2018-security-fabric) veya [Third Generation of Network Security](https://www.fortinet.com/blog/business-and-technology/executive-insights--the-third-generation-of-security-is-here.html) bağlantılarından ayrıntılı bilgiler edinebilirsiniz.
* Fortinet’i on [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/), [YouTube](https://www.youtube.com/fortinet), ve [Instagram](https://www.instagram.com/behindthefirewall/)’dan takip edebilirsiniz.

**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 425 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Daha fazla bilgi için: <http://www.fortinet.com/>, [Fortinet Blog sayfası](https://blog.fortinet.com/) veya [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta).