**Fortinet Tehditleri Bir Saniyeden Kısa Sürede Tespit Edebilen Yeni Yapay Zeka Çözümünü Tanıttı**

*FortiAI tehditleri otomatik bir şekilde tespit edebilmek ve ortadan kaldırabilmek için derin sinir ağlarını kullanarak Fortinet’in yapay zekadan güç alan güvenlik çözümlerini büyütüyor*

Kapsamlı, entegre ve otomatik siber güvenlik çözümlerinde dünya lideri Fortinet® (NASDAQ: FTNT), tehditleri daha hızlı ortadan kaldırmak ve zaman tüketen manuel güvenlik analiz görevlerini yönetmek için kendi kendine öğrenen Derin Sinir Ağı’ndan (Deep Neural Networks, DNN) faydalanan türünün tek örneği şirket içi çözümü [FortiAI](https://www.fortinet.com/fortiai)’yı tanıttı. FortiAI’ın Virtual Security Analyst™ ürünü, [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta) tarafından geliştirilen çözüm, siber güvenlik tehdit istihbaratını doğrudan kurumun ağına ekleyerek gelişmiş tehditleri bir saniyeden kısa sürede tespit edebiliyor.

**Kurumlar Gün Geçtikçe Büyüyen Bir Savaşın İçinde**

Güvenlik mimarları, tehditleri keşfederken ve ortadan kaldırırken aşağıdaki gibi birçok sorunla karşı karşıya kalıyor:

* **Siber suçlular daha da akıllı hale geliyor**.Geleneksel siber tehditler devam ederken, gelişmiş tehditler, çoğunlukla yapay zeka, öğrenen makineler ve açık kaynak toplulukları üzerinden daha akıllı hale geliyor. Bu yüzden kurumlar ve savunma mekanizmaları, tehditlerin bu dönüşümü karşısında güçlük çekiyor.
* **Saldırı zemini genişliyor**. Milyonlarca yeni uygulamalar, bulutun daha fazla benimsenmesi ve bağlı cihazlarının sayısının artması, güvenlik ekiplerinin düzgün bir şekilde korumasını ve yönetmesini gerektiren milyarlarca sınır/uç nokta oluşturuyor. Birçok potansiyel giriş noktasından ötürü şirketler tehditlere karşı zorluk yaşıyor.
* **Şirketler siber beceri eksikliğinden dolayı kısıtlanıyor**. Siber güvenlik sektörünün karşılaştığı beceri eksikliği, kurumlar için en önemli sorunlardan biri olarak öne çıkıyor. Potansiyel ve aktif tehditler arasında düzgün bir şekilde öncelik belirleyecek, araştıracak ve karşılık verecek yeterli beceriye sahip profesyonel sayısı gerekenden az. Böylece siber suçlular geleneksel güvenlik süreçlerinin ve araçlarının önüne kolayca geçebiliyorlar**.**

**Kendi Kendine Öğrenen Yapay Zeka Kurumların Tehdit Korumasına Uyum Sağlıyor**

FortiAI, hizmete alındığı kuruma özel olarak tehditlerin bilimsel analizinden yola çıkarak karmaşık kararlar verebilmek için insan beynindeki nöronları taklit eden ve Derin Sinir Ağları olarak da bilinen Derin Öğrenim teknolojisinden avantaj kazanıyor. FortiAI’ın yapay zekası gelişmeye devam ederken, şirketler de tehdit korumasını etkili bir şekilde dönüştürmek ve benimsemek için FortiAI’ın Virtual Security Analyst™ ürününden faydalanıyor.

**FortiAI Şartları Eşitliyor**

Fortinet’in DNN yaklaşımı, [FortiAI](https://www.fortinet.com/fortiai)’ın aşağıdaki özellikleriyle tehdit korumasında önemli gelişmeler yaratıyor:

* **Tehditleri gerçek zamanlı olarak tespit etmek ve sınıflandırmak için zaman tüketen manuel araştırmaları otomatikleştiriyor:** Geleneksel güvenlik işlemleriyle birlikte sınırlı güvenlik çalışanlarına sahip kurumlar, genelde her tehdit alarmına karşı manuel araştırma gerçekleştiremiyor. Bu durum, yavaş tepki süresinden ötürü veri ihlali veya güvenlik olayı gibi fazladan risk yaratıyor. FortiAI, bu sorunun önüne geçebilmek, tüm tehdit hareketini tanımlamak, ilk defa ortaya çıkan tehditleri ve devamındaki olayları bir saniyeden kısa sürede tespit etmek için DNN’yi kullanarak araştırmaları otomatikleştiriyor.
* **Saldırıları anında tespit etmek ve ortadan kaldırmak için güvenlik süreçlerini dönüştürüyor:** FortiAI’ın Virtual Security Analyst™ ürünü, tehditlerin karakteristik özelliklerini bilimsel bir şekilde analiz ederek ve tehdide karşılık verme süresini hızlandırmak için doğru kararlar oluşturarak kurumların tehdide maruz kaldığı süreyi büyük ölçüde azaltıyor.
* **Yanlış alarmları büyük ölçüde azaltmak için özelleştirilmiş tehdit istihbaratı sunuyor**: Yanlış alarmlar, araştırılması gerektiği ve tehdit ile tehdit olmayan ögeleri ayırt etmek zaman aldığı için güvenlik analistlerine zaman kaybettiriyor. Özelleştirilmiş tehdit istihbaratı sayesinde FortiAI yeni kötü amaçlı yazılım özelliklerini öğrenerek anında yeni saldırılara uyum sağlıyor ve yanlış alarm sayısını azaltıyor.

**Hava Boşluğu Olan Ağlar için Şirket İçi Koruma**

Hava boşluğu olan ağlara sahip kurumlar için uyumlu şirket içi yapay zeka sunan FortiAI, bu alanda da öne çıkıyor. Operasyonel teknoloji ortamlarının, devlet kurumlarının ve bazı büyük şirketlerin sıkı uyumluluk yasalarıyla ve/veya internetle olan bağlantıyı sınırlayan güvenlik ilkeleriyle uyumlu olması gerekiyor. Kendi kendine öğrenen yapay zeka modeliyle FortiAI, internet bağlantısına ihtiyaç duymayarak kapalı ortamları veya sıkı güvenlik ilkeleri olan kurumların tehditlerin bir adım önünde olmasını sağıyor.

**Fortinet’in Yapay Zekadan Güç Alan Teknolojileri Tehdit Korumasını Otomatikleştiriyor**

Fortinet uzun zamandır yapay zekayı kullanarak müşterilerinin güvenliklerini güçlendirmelerine yardımcı oluyor. Yeni FortiAI ile tamamlanan aşağıdaki Fortinet ürün ve hizmetlerinin bazıları, en küçük kareler yöntemi ve Bayes olasılık metrikleri gibi yapay zekanın çeşitli formlarından avantaj kazanıyor:

* **FortiGuard Labs Tehdit İstihbaratı:** [FortiGuard Labs](https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html?utm_source=nreleaseblog&utm_campaign=2018-q2-fortiguardlabs-cta), her gün yaklaşık 100 milyar güvenlik olayını toplamak ve analiz etmek için ispatlanmış ve gelişmiş yapay zeka ve öğrenen makineler teknolojilerinden faydalanıyor. FortiGuard Labs’ın geliştirdiği tehdit istihbaratı, amiral gemisi FortiGate Yeni Nesil Güvenlik Duvarları gibi Fortinet’in çeşitli ürünleri için oluşturulan abonelik hizmeti aracılığıyla müşterilere ulaşıyor. Böylece müşteriler tehditlerin önüne daha hızlı geçebilmek için küresel laboratuvarlarda hizmete alınan yapay zekadan faydalanıyor.
* **FortiSandbox:** Fortinet, ihlal korumasını otomatikleştirmek için kum havuzu (sandboxing) alanında yapay zeka sunan ilk güvenlik sağlayıcısı olarak öne çıkıyor. Sıfırıncı gün tehditlerini statik ve dinamik olarak analiz edebilmek için iki öğrenen makine modeli bulunan [FortiSandbox](https://www.fortinet.com/products/sandbox/fortisandbox.html), fidye yazılımları ve kripto-gasp gibi sürekli gelişen kötü amaçlı yazılımları daha iyi bir şekilde tespit edebiliyor. Kötü amaçlı yazılımları kategorilere ayırmak için evrensel bir güvenlik dili kullanan FortiSandbox, ağ ve güvenlik ekiplerini birbirine bağlayarak güvenlik operasyonlarının daha da gelişmesini ve entegre olmasını sağlıyor.
* **FortiEDR:** Gelişmiş tehditlere karşı uç nokta korumasını otomatikleştiren FortiEDR, gerçek zamanlı ve dikkatlice organize edilmiş olaya müdahale özelliklerine sahip öğrenen makineleri kullanıyor.
* **FortiInsight**: [FortiInsight](https://www.fortinet.com/products/ueba.html), alışılmışın dışında, kötü amaçlı davranışları ve iç riske karşı ilke ihlallerini tespit etmek amacıyla uç noktaları, veri hareketini ve kullanıcı aktivitelerini etkili bir şekilde gözlemleyebilmek için öğrenen makineleri kullanıyor.
* **FortiWeb:** [FortiWeb](https://www.fortinet.com/products/web-application-firewall/fortiweb.html), web uygulamalarını ve API’ları daha iyi korumak amacıyla her uygulamaya farklı savunmalar geliştirmek için öğrenen makineleri kullanıyor. Böylece FortiWeb, son kullanıcı deneyimini etkileyebilecek yanlış alarmları en aza indirirken tehditleri de hızlıca engelleyebiliyor.
* **FortiSIEM**: [FortiSIEM](https://www.fortinet.com/products/siem/fortisiem.html) konum, saat, kullanılan cihaz ve erişilen belirli sunucular gibi tipik kullanıcı davranışlarındaki benzerlikleri tanımak için öğrenen makineleri kullanıyor. FortiSIEM, devamında farklı konumlardan sürekli çevrimiçi olmak gibi normalin dışındaki aktiviteler gerçekleştiğinde otomatik olarak güvenlik operasyonları ekibine haber veriyor.

Siber suçlular, gelişmiş saldırılarla genişleyen dijital saldırı zeminini istismar etmek için yollar arıyor. [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/enterprise-security.html)’teki yapay zekadan güç alan gelişmiş teknoloji, müşterilere benzeri olmayan, anında gerçekleşen ve otomatik bir tehdit koruması, tespit etme ve karşılık verme imkanı sunuyor.

**Fortinet Güvenlik Yaklaşımları ve Global Tehdit Ortaklığı Başkanı Derek Manky** konuyla ilgili şunları söyledi: “Fortinet olarak FortiGuard Labs’ın bulut tabanlı yapay zekadan güç alan tehdit istihbaratına büyük yatırımlar yaparak daha fazla tehdidi daha hızlı ve doğru şekilde tespit edebiliyoruz. FortiAI, FortiGuard Labs’ın yapay zeka bilgisini alıyor ve özellikle şirket içinde hizmete alımlar için paket haline getiriyor. Böylece müşteriler, doğrudan ortamlarında gelişmiş tehditleri bir saniyeden kısa sürede tespit edebilme, tanımlama ve araştırma özelliklerine sahip FortiGuard Labs’ın gücünden faydalanabiliyor.”

**Ek Kaynaklar**

* Gelişmiş tehditleri bir saniyeden kısa sürede tespit etmek, sınıflandırmak ve araştırmak için [FortiAI’ın kendi kendisine öğrenen yapay zekası](https://www.fortinet.com/blog/business-and-technology/fortiai-virtual-security-analyst-revolutionizes-threat-protection.html) hakkında daha fazla bilgi için bağlantıya tıklayabilirsiniz.
* Fortinet’in [yapay zekadan güç alan güvenliğiyle ilgili uzun geçmişi](https://www.fortinet.com/blog/business-and-technology/fortinet-history-ai-driven-security.html) hakkında daha fazla bilgi için bağlantıya tıklayabilirsiniz.
* Fortinet’in [siber güvenlik becerilerindeki eksikliği gidermek](https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2020/growth-in-nse-institute-programs-tackles-cybersecurity-skills-gap.html) için neler yaptığı hakkında daha fazla bilgi için bağlantıya tıklayabilirsiniz.
* [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 [portföyleri](https://www.fortinet.com/support-and-training/support-services/fortiguard-security-subscriptions.html?utm_source=blog&utm_campaign=2018-blog-security-services) hakkında daha fazla bilgi için bağlantıya tıklayabilirsiniz.
* [Fortinet’in Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=blog&utm_campaign=2018-security-fabric)’in kurumların tüm dijital saldırı zemininde kapsamlı, entegre ve otomaik korumayı nasıl sağladığını öğrenmek için bağlantıya tıklayabilirsiniz.
* [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 [portföyü](https://www.fortinet.com/support-and-training/support-services/fortiguard-security-subscriptions.html?utm_source=blog&utm_campaign=2018-blog-security-services) hakkında daha fazla bilgi için bağlantılara tıklayabilirsiniz.
* Fortinet Kullanıcı topluluğunda (Fuse) fikirlerinizi ve geribildirimlerinizi paylaşmak, ürünler ve teknolojiler hakkında daha fazla bilgi almak veya benzer iş kollarındaki kişilerle iletişime geçebilmek için [bağlantıya](https://fusecommunity.fortinet.com/home?utm_source=blog&utm_medium=campaign&utm_campaign=2020-fusecommunity) tıklayabilirsiniz.
* [Network Security Expert program](https://www.fortinet.com/support/training/network-security-expert-program.html?utm_source=blog&utm_campaign=2019-q2-nse-landing), [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 [FortiVet program](https://www.fortinet.com/corporate/careers/vets.html?utm_source=blog&utm_campaign=2018-q2-fortivet)’ımımız hakkında ayrıntılı bilgi için bağlantılara tıklayabilirsiniz.
* Fortinet’i [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 büyüyen saldırı zemininde müşterilerine eksiksiz görünürlük ve kontrol sağlar, günümüzde artan ve gelecekte de artacak olan performans ihtiyaçlarını karşılamak için onları güçlendirir. Ağlardaki uygulamaların, çoklu bulut sistemlerinin ve sınır ortamlarının karşılaştığı en kritik güvenlik sorunlarına karşı tek çözüm olan Fortinet'in Security Fabric platformu, tüm dijital altyapıda veriyi korur. Fortinet global çapta sevkiyatı yapılan en güvenilir çözümler alanında dünyanın bir numarasıdır ve dünya genelinde 440 binden fazla müşteri ticari faaliyetlerini korumak için Fortinet'e güvenmektedir. Hem bir teknoloji şirketi hem de öğrenen bir şirket olan Fortinet’in Ağ Güvenlik Enstitüsü, sektördeki en büyük ve kapsamlı siber güvenlik eğitim programlarından birini sunmaktadır. Daha fazla bilgi için: <http://www.fortinet.com/>, [Fortinet Blog](https://blog.fortinet.com/) sayfası veya [FortiGuard Labs](https://fortiguard.com/).