aa teknoloji

Palo Alto Networks ML-Powered NGFW

Palo Alto Networks ML-Powered Next-Generation Firewall Makine öğrenimi odaklı yeni nesil güvenlik duvarı; App-ID, User-ID ve Content-ID ile tüm trafiği analiz eder. Sıfır gün tehditlerini Advanced WildFire ile durdurarak Zero Trust mimarisini destekler.

Ağ Güvenliği Zorlukları

Sürekli form değiştiren siber saldırılar ve ağa kontrolsüz eklenen yeni cihazlar, kurumların saldırı yüzeyini genişletmektedir. Geleneksel güvenlik ürünleri, manuel müdahalelere mecbur bırakarak operasyonel kaynakları tüketir ve altyapıyı tehditlere açık hale getirir.
Saldırganlar, güvenlik cihazlarını atlatmak için şifrelenmiş trafikleri kullanmaktadır. Phishing ve çalınan kimlik bilgilerinin sömürülmesi, 2021 yılındaki güvenlik ihlallerinin %90'ını oluşturan en büyük kör noktalardır.
Geleneksel imza ve parmak izi tabanlı sistemlerin yetersiz kalması, bilinmeyen tehditlerin ve SaaS uygulamalarının tespitini imkansızlaştırır.

⚠ Hang Ekiplere Hitap Eder?

- Şifreli trafikteki (TLS 1.3 ve HTTPS/2) tehditleri göremeyen ekipler için
- Kimlik hırsızlığı ve evasive phishing saldırılarına karşı koruma arayanlar için
- İzinsiz SaaS uygulamalarını (Shadow IT) ve veri sızıntılarını engellemek isteyenler için
- Ağdaki yönetilmeyen IoT cihazlarını tespit edip güvenceye almak isteyenler için

Temel İlkeler

Zero Trust
Konumdan bağımsız tam doğrulama

Görünürlük
Uygulama, içerik ve kimlik tespiti

SaaS Denetimi
Yeni nesil CASB ile veri koruması

Önleme
ML destekli sıfır gün engellemesi

Teknik Özellikler

Trafik ve Kimlik Kontrolü
- App-ID ile uygulama bazlı tam görünürlük
- User-ID ve Cloud Identity Engine uyumu
- Dynamic User Groups (DUG) otomasyonu
- TLS 1.3 ve HTTPS/2 için şifre çözme

Gelişmiş Tehdit Önleme
- Advanced WildFire ile zero-day analizi
- Advanced URL Filtering ve Web Koruması
- Makine öğrenimi destekli inline IPS
- DNS Security ile C2 trafik engellemesi

SaaS ve Bulut Güvenliği
- Next-Gen CASB ile SaaS uygulama yönetimi
- Gerçek zamanlı SaaS veri koruması
- Prisma Access SASE entegrasyonu
- Donanım, VM ve Container formları

Merkezi Yönetim ve Görünürlük
- Panorama ile tek ekrandan cihaz yönetimi
- Enterprise IoT ile NIST uyumlu koruma
- Cortex Data Lake üzerinden merkezi loglama
- Geniş API desteği ile 3. parti otomasyonu

NGFW Nasıl Çalışır?

ML-Powered Next-Generation Firewall, trafiği portlar yerine App-ID, User-ID ve Content-ID ile inceler. Single-pass mimarisiyle tek geçişte sıfır gün tehditlerini engeller ve Zero Trust politikalarını güvenle uygular.

Çalışma Akışı

1. Trafik Sınıflandırma
- App-ID tüm uygulamaları doğrudan tespit eder.
- User-ID ağ trafiğiyle kullanıcıyı eşleştirir.
- Gerektiğinde SSL/TLS trafiğinin şifresi çözülür.
- Tüm IoT cihazları imzasız şekilde tanımlanır.

→

2. İçerik ve Tehdit Analizi
- Bilinmeyen dosyalar analiz için WildFire'a iletilir.
- Inline ML ile zararlı yazılımlar anında engellenir.
- DNS Security ile karmaşık DNS atakları bloklanır.
- URL Filtering, evasive phishing sitelerini bulur.

→

3. Karar ve Optimizasyon
- Zero Trust temelli güvenlik politikaları işletilir.
- Single-Pass mimari ile gecikmesiz işlem yapılır.
- Next-Gen CASB ile riskli SaaS uygulamaları engellenir.
- Cortex Data Lake log korelasyonu gerçekleştirir.

Merkezi Yönetim ve Küresel İstihbarat
Panorama yönetim altyapısı, tüm şube, veri merkezi ve bulut cihazlarındaki politikaları tekilleştirir. Shared Threat Intelligence ile tespit edilen yeni bir tehdidin koruma kalkanı saniyeler içinde tüm küresel ekosisteme dağıtılır.

Avantajlar

Single-Pass Mimarisi
Geleneksel katmanlı analizi terk eder. Uygulama, kullanıcı ve içerik analizini tek geçişte yaparak öngörülebilir performans sağlar.

Kapsamlı IoT Güvenliği
Ağdaki yönetilmeyen tüm IoT cihazlarını ML ile tespit eder. Bağlam farkındalıklı segmentasyon ile Zero Trust mimarisini güçlendirir.

Next-Generation CASB
Kurumsal SaaS hesaplarına erişimi sağlarken riskli uygulamaları (Shadow IT) gerçek zamanlı veri korumasıyla engeller.

Zero Trust Uygulaması
Cloud Identity Engine ile her lokasyondaki kullanıcıyı doğrular. Uygulama ve kimlik bazlı kısıtlamalarla riskleri azaltır.

aa teknoloji

AA Teknoloji, modern haber merkezleri için geliştirilen yapay zekâ destekli medya teknolojileri platformudur. Haber akış sistemlerinden dijital arşiv çözümlerine, gerçek zamanlı yayın altyapılarından çok kanallı içerik yönetimine kadar uzanan entegre çözümlerimiz; medya kuruluşlarının dijital dönüşüm süreçlerini hızlandırır ve ölçeklenebilir yayın operasyonları sunar.

Daha fazla bilgi için, aateknoloji.tr'yi ziyaret edin veya @aateknoloji LinkedIn hesabını takip edin.