Palo Alto Networks

Bugününüzün ve Geleceğinizin

Güvenliğini Sağlar!

Siber güvenlik sektöründe lider Palo Alto Networks, bireylerin ve kurumların çalışma şeklini değiştiren teknolojisiyle geleceği şekillendiriyor. Yapay zeka, analiz, otomasyon ve orkestrasyondaki en son yenilikleri içeren, kapsamlı, yenilikçi çözümler sunar. İş ortakları ekosistemini her yıl güçlendirerek, bulutta, ağ altyapısında ve mobil cihazlarda on binlerce kurumun güvenliğini sağlar.

paloalto® NETWORKS

EXCLUSIVE NETWORKS

STRATA
BY PALO ALTO NETWORKS

Altyapınızın güvenliğini sağlayın!

Strata ™, donanım, yazılım ve bulut tabanlı alt yapılarda entegre ve etkili bir ağ güvenliği platformudur.


Yeni Nesil Güvenlik Duvarı

VM-Serisi

CN-Serisi

Panorama


App-ID


Content-ID


Device-ID


User-ID


WildFire


Tehdit Önleme

DNS Güvenliği


IoT Güvenliği

URL Filtreleme

DLP

Global Protect

SD-WAN

paloalto NETWORKS

EXCLUSIVE NETWORKS

Yeni Nesil Güvenlik Duvarı

Fizikselde, Sanalda ve Bulutta Güvenlik

Palo Alto Networks Yeni Nesil Güvenlik Duvarı, tümü merkezi olarak yönetilen fiziksel, sanal ve bulut tabanlı altyapılarda sunulan, entegre ve en gelişmiş ağ güvenliği çözümüdür. Gartner'ın Ağ Güvenlik Duvarı Magic Quadrant'tında 9. kez Lider kategorisinde yer alan Palo Alto Networks ile, kampüsünüzü, hibrit bulutunuzu, şubelerinizi ve mobil kullanıcılarınızın bugün ve gelecekte güvenliklerini sağlayın.

VM-Serisi

Sanal Yeni Nesil Güvenlik Duvarı

VM Serisi Sanal Yeni Nesil Güvenlik Duvarları, fiziksel güvenlik duvarlarını dağıtmanın zor veya imkansız olduğu ortamlar için idealdir. VM Serisi Güvenlik Duvarları, Palo Alto Networks'ün Yeni Nesil Güvenlik Duvarının tüm özelliklerini aynı şekilde sanal ortamda sunar. Genel ve özel bulutun, sanallaştırılmış veri merkezlerinin ve şubelerin uyumlu bir şekilde, güvenliğini sağlar.

CN-Serisi

Konteyner Yeni Nesil Güvenlik Duvarı

CN Serisi, Konteyner Yeni Nesil Güvenlik Duvarları, güvenlik kontrollerini konteyner iş yüklerine mümkün olduğunca yaklaştırmak ve politika değişikliklerinde kullanılmak üzere, Palo Alto Networks'ün Yeni Nesil Güvenlik Duvarının tüm özelliklerini sunar. Bu çözüm, sayesinde konteyner güvenlik duvarı tehditleri önleyebilir. Ayrıca, konteyner kapsülleri, konteyner uygulamaları ile sanal makineler ve fiziksel sunucular arasında izin verilen trafikte — giden, gelen veya yanal — IPS ve URL filtreleme gibi diğer gelişmiş ağ güvenliği hizmetlerini sağlar.

Panorama

Yönetim Çözümü

Panorama ™, Palo Alto Networks Güvenlik Duvarlarınız için, özelliklerinden ve lokasyondan bağımsız olarak, merkezi bir ağ güvenlik yönetim çözümü sunar. Güvenlik politikalarınızın konfigürasyonunu, konumlandırılmasını ve yönetimini basitleştirir. Panorama, günlük ağ trafiğiniz ve olası tehditler hakkında görünürlük ve ihtiyaç duyduğunuz kapsamlı bilgileri sağlar. Güncellemeleri yönetmeye yardımcı olurken, politika tabanlı tehdit yanıtlarını otomatikleştirir. Böylece, iş yükünü azaltır.

Panorama, firmanızın iç güvenlik politikalarını ve güvenlik güncellemelerini yönetmenizi sağlayan, esnek ve basit bir arayüz sunar.

App-ID

Uygulama Sınıflandırma Özelliği

App-ID ™, yalnızca Palo Alto Networks Güvenlik Duvarlarında bulunan patentli bir trafik sınıflandırma teknolojisidir. Bağlantı noktası, protokol, TLS / SSL / SSH şifrelemesi (TLS 1.3 ve HTTP / 2 dahil) veya uygulamanın kullanabileceği diğer taktiklerden bağımsız olarak, bir uygulamanın kimliğini belirler. Uygulamalarınızı doğru bir şekilde tanımlamak için, ağ trafiği akışınıza uygulama imzaları, uygulama protokolü kod çözme gibi, birden çok sınıflandırma uygular. Bağlantı noktası tabanlı eski güvenlik duvarı kurallarından, App-ID ™ teknolojisi tabanlı kurallara geçiş, olası saldırıları büyük ölçüde azaltır. PAN-OS • Policy Optimizer bunu kolaylaştırır.

Content-ID

İçerik Sınıflandırma Özelliği

Content-ID™ teknolojisi, tek bir taramada izin verilen tüm trafiğin eksiksiz analizini gerçekleştirmek için, çok sayıda gelişmiş tehdit önleme teknolojisini kullanır. Content-ID ile, Palo Alto Networks Yeni Nesil Güvenlik Duvarları, olası güvenlik açıklarını ve bağlantı noktası taramalarını engelleyebilir, giden kötü amaçlı yazılım iletişimlerini durdurabilir ve yetkisiz dosyaların, verilerin aktarılmasıyla ilgili riskleri azaltabilir.

paloalto® NETWORKS

EXCLUSIVE NETWORKS

Device-ID

Cihaz Sınıflandırma Özelliği

User-ID'nin kullanıcı tabanlı ve App-ID'nin uygulama bazlı politika sağlaması gibi, Device-ID, IP adresindeki veya konumundaki değişikliklerden bağımsız olarak, bir cihaza dayalı politika kuralları sağlar. Device-ID, cihazlar için izlenebilirlik sağlarken, belirli cihazlarda ağlar arasındaki bağlantıyı takip etmenize ve kullanıcılar, konum veya IP adresleri yerine cihazlarla ilişkili zamanla değişebilen kurallar yazmanıza imkan tanır. Device-ID, Güvenlik, Şifre Çözme, QoS ve Kimlik Doğrulama ilkelerinde kullanabilirsiniz. Device-ID, IoT Güvenlik hizmetiyle birlikte PAN-OS 10.0 veya sonraki bir sürümünü çalıştıran Makine Öğrenimi Destekli Yeni Nesil Güvenlik Duvarı için, kullanılabilir. (Machine Learning Powered NGFW)

User-ID

Kullanıcı Sınıflandırma Özelliği

User-ID ™ teknolojisi, trafik yönünde kullanıcılara veya kullanıcı gruplarına göre, uygulamaları güvenli bir şekilde tanıma politikaları geliştirilmesine yardımcı olur. Örneğin, standart bağlantı noktalarında SSH ve FTP'yi yalnızca BT departmanının kullanmasına izin verebilirsiniz. User-ID ile, kullanıcılarınızı lokasyon (merkez, şube veya ev) ve cihaz bağımsız takip edebilirsiniz. Yalnızca IP adresine göre değil, kullanıcı düzeyinde uygulama etkinliğine ilişkin görünürlük elde edebilir ve kullanıcı etkinlikleri hakkında bilgilendirici raporlar oluşturabilirsiniz. Ek olarak, uygulamalarınızda herhangi bir değişiklik yapmadan kullanıcılarınız için, çok faktörlü kimlik doğrulamasını (MFA) zorunlu kılabilirsiniz.

User-ID ile kurumsal kimlik bilgilerinin kurumunuzdan çıkmasını önleyebilir ve saldırganların ağınızda hareket etmek için çalınan kimlik bilgilerini kullanmasını önleyebilirsiniz.

WildFire

Kötü Amaçlı Yazılım Önleme

WildFire® kötü amaçlı yazılım önleme hizmeti, sektörün en gelişmiş, yenilikçi bulut tabanlı analiz ve önleme çözümüdür.

Bilinmeyen tehditleri tespit etmek için kullanılan geleneksel yaklaşımların ötesine geçen WildFire, dinamik analiz, statik analiz ve makine öğrenimi dahil olmak üzere tutarlı ve kapsamlı bir çözüm sunar.

Sürekli olarak bulutta geliştirilen olası tehdit modellerinden yararlanan WildFire, ayrıca fiziksel ve sanal Yeni Nesil Güvenlik Duvarları içinde sunulan devrim niteliğindeki makine öğrenimi tabanlı çözümden de faydalanır.

Herhangi bir WildFire kullanıcısı olası bir saldırı ile karşılaştığında, (zero-day exploit / malware) saniyeler içinde, dünyanın herhangi bir yerindeki tüm aboneler için yüksek güvenlik duvarından kaçmaya dirençli koruma uygulanmasını otomatik olarak düzenler. Otomatik Odaklama ve sorunsuz entegrasyon sayesinde WildFire, güvenlik ekiplerinin zamandan tasarruf etmesine yardımcı olur.

paloalto® NETWORKS

EXCLUSIVE NETWORKS

Threat Prevention (TP)

Tehdit Önleme

Palo Alto Networks'ün Tehdit Önleme lisansı, IPS özellikleri ile bilinen olası güvenlik açıklarını otomatik olarak durdurur. TP bağlantı noktası, protokol veya şifreleme ne olursa olsun tüm trafiği tehditlere karşı inceler. Dahil edilen IPS korumaları, imzaları ve kuralları Snort ve Suricata ◦ gibi popüler formatlarda içe aktarma ve otomatik olarak uygulama özelliği ile imza eşleştirme ve anomalileri algılamaya dayanmaktadır. TP, tehditleri yalnızca ağa girdiklerinde değil, tüm noktalarda arayarak, Zero-Trust modeliyle güvenli bir çözüm sağlar.

Tüm tehditler için, tek tip bir imza formatı, tüm analizlerin tek bir taramada yapılmasını sağlayarak, gereksiz işlemleri ortadan kaldırır. TP, Yeni Nesil Güvenlik Duvarlarından geçerken her paketi tarar ve paket başlıkları ve yüklerindeki bayt dizilerini yakından inceler. Bu analizden, kullanılan uygulama, kaynağı ve hedefi, protokolün RFC uyumlu olup olmadığı ve yükün bir açıktan yararlanma veya kötü amaçlı kod içerip içermediği dahil olmak üzere her paket hakkında önemli ayrıntıları belirleyebiliriz. Tüm bunlar tek bir taramada gerçekleşir, böylece ağ trafiğiniz ihtiyacınız olduğu kadar hızlı kalır.

DNS Güvenliği

DNS Kullanarak Saldırıların Önlenmesi

Kötü amaçlı yazılımların %80'i, bir komut ve kontrol (C2) kanalı oluşturmak için, DNS kullanıyor. Saldırganlar genellikle DNS'de saklanır; çünkü trafik hacmi o kadar yüksektir ki, birçok kurum bunu izleyecek araçlardan yoksundur.

DNS Güvenliği lisansı, DNS kullanan saldırıları engellemek için, tahmine dayalı analitik, makine öğrenimi ve otomasyon uygular. ML Destekli NGFW ile, kullanıcılara otomatik koruma sağlar, saldırganların güvenlik önlemlerini atlatmasını önler.

DNS Güvenliği raporlaması, tehditlere ilişkin her zamankinden daha derin iç görüler sağlar ve makro, sektörel ve organizasyon düzeyinde DNS trafiğine tam görünürlük sağlar. Bulut tabanlı korumalar sınırsız ölçeklendirir ve her zaman günceldir, kurumunuza DNS kullanan saldırıları durdurması için, kritik bir yeni kontrol noktası sağlar.

IoT Güvenliği

Kurumsal IoT Güvenliği

Palo Alto Networks, tüm IoT cihazlarını korumak için, IoT Güvenliği içeren sektörün TEK Yeni Nesil Güvenlik Duvarı çözümünü sunar. Bulut üzerinden sağlanan IoT Güvenlik lisansını eklemeniz ve mevcut altyapınızdan yararlanarak IoT cihazlarınızın güvenliğini sağlamanız mümkündür. ML ve App-ID teknolojisi ile daha önce hiç görülmemiş cihazlar dahil olmak üzere ağınızdaki tüm IoT ve OT cihazlarını doğru bir şekilde tanımlayabilirsiniz. Bu sayede, güvenlik ekipleri, her cihaz için Device-ID, risk seviyesini ve her türlü davranışsal anomaliyi tespit ederek, hızlı şekilde aksiyon alabilir.

IoT Güvenliği lisansı; sağlık, akıllı şehir altyapı sistemleri, enerji, kamu hizmetleri ve ulaşım gibi alanlarda, baştan uca güvenlik çözümü sağlar. .

paloalto® NETWORKS

EXCLUSIVE NETWORKS

URL Filtreleme

Kötü Amaçlı Siteler ve Kimlik Avını Önleme

URL Filtreleme, web'i kurumsal ihtiyaçlarınız için, güvenle kullanmanızı sağlar. Bulut üzerinden sağlanan URL Filtreleme lisansı, benzersiz statik analiz ve makine öğrenimi aracılığıyla tehditleri belirleyerek, web filtrelemenin bir adım ötesine geçer. Kimlik avı sayfaları ve JavaScript tabanlı saldırılar milisaniyeler içinde tespit edilir. Her gün oluşturulan binlerce yeni kötü amaçlı URL ile, kötü amaçlı web sayfalarını anında tanımlama özelliği, web kaynaklı saldırılara karşı koruma sağlamak için bir gerekliliktir. Otomatik korumalar, kötü amaçlı yazılım dağıtan ve kimlik bilgilerini çalan kötü amaçlı sitelere erişimi engelleyerek veri kaybını durdurur. App-ID ve User-ID tabanlı politikalar, karmaşık web güvenlik kurallarını basitleştirerek operasyonel yükü azaltır.

Veri Kaybı Önleme

Veri Koruma ve Uyumluluk

Palo Alto Networks Kurumsal Veri Kaybını Önleme lisansı, tüm trafik uygulamaları ve tüm kullanıcılar için, kişisel kimlik bilgileri (PII) ve IP gibi hassas verilerin tutarlı ve güvenilir bir şekilde korunmasını sağlayan bir bulut hizmetidir. Palo Alto Networks ürünleriyle yerel entegrasyon, konumlandırmayı kolaylaştırır ve gelişmiş makine öğrenimi, yönetim karmaşıklığını en aza indirir. Kurumsal DLP, kurumların gizli verileri bulundukları her yerde tutarlı bir şekilde takip etmelerine, sınıflandırmalarına, izlemelerine ve korumalarına imkan tanır. Office 365 ™ ve Salesforce® gibi hem şirket içinde hem de bulutta veri ihlali riskini en aza indirmeye yardımcı olur ve KVKK, CCPA, PCI DSS, HIPAA ve diğerleri dahil olmak üzere veri gizliliği ve bu süreçteki uyumluluk düzenlemelerinin karşılanmasına yardımcı olur.

Global Protect

Mobil Kullanıcı Güvenliği

GlobalProtect ™ lisansı, cihazları veya lokasyonları ne olursa olsun, Yeni Nesil Güvenlik Duvarı özelliklerinden yararlanan tüm kullanıcıların erişimini güven altına alarak, mobil iş gücünüzü korumanıza imkan tanır. Global Protect, tüm uygulama trafiğini (tüm bağlantı noktalarında) her zaman inceleyerek ayrıntılı görünürlük sağlar ve daha verimli güvenlik politikaları oluşturmanıza ve bunları uygulamanızı sağlar.

VPN ile Global Protect, bulut ve veri merkezlerindeki uygulamalara erişim için güvenli seçenekler sunar.

SD-WAN

Güvenli Şube Bağlantısı

Palo Alto Networks SD-WAN lisansı, en gelişmiş güvenlik ve kesintisiz bağlantı ile uçtan uca bir SD-WAN mimarisine kolayca geçmenizi sağlar. Prisma Access'i SD-WAN hub'ı olarak kullanarak, kullanıcı deneyimini geliştirmek için, optimize edebilirsiniz. Ek olarak, Güvenli Prisma Access SD-WAN hub'ımız, SD-WAN hub altyapısını oluşturmanın karmaşıklığını ortadan kaldırır. Alternatif olarak, hub ve ara bağlantı altyapısını Palo Alto Networks Yeni Nesil Güvenlik Duvarlarını kullanarak kendiniz oluşturabilirsiniz. Dağıtım modelinden bağımsız olarak, bu entegrasyon, ağınızı en güvenli şekilde yönetmenize olanak sağlar.

paloalto® NETWORKS

EXCLUSIVE NETWORKS

PRISMA
BY PALO ALTO NETWORKS

Bulut Güvenliği

Prisma ™, sektörde en gelişmiş bulut güvenliği teklifidir. Günümüzün karmaşık BT altyapılarının güvenliğini sağlamak için, tasarlanmış bir çözüm paketiyle bulut deneyiminizi hızlandırın!

Prisma Access

Prisma Cloud

Prisma SaaS

paloalto NETWORKS

EXCLUSIVE NETWORKS

Prisma Access

Bulutta Sağlanan Mobil Kullanıcı Güvenliği

Prisma ™ Access, kurumunuzun uzak ağlarına ve mobil kullanıcılarınıza tutarlı bir güvenlik sağlamanıza yardımcı olan bir erişim hizmetidir (SASE). İster merkez ofisinizde, ister şubede veya mobil olsun tüm kullanıcılarınız, bulut ve veri merkezi uygulamalarını ve interneti güvenle kullanmak için Prisma Access'e bağlanır. 76 ülkede, dünya çapında 100'den fazla konumda bulunan Prisma Access, tüm noktalardaki trafiği tutarlı bir şekilde denetler ve şubeden şubeye ve şubeden Merkez Ofise trafiği sağlamak için, çift yönlü ağ iletişimi sağlar.

Geniş ölçekte koruma sağlayan Prisma Access, global kapsamlıdır, böylece şubede donanımsal güvenlik duvarlarını boyutlandırma ve dağıtma konusunda endişelenmenize gerek kalmaz. Prisma Access, merkezi analiz ve raporlama için Cortex Data Lake'i kullanır.

Prisma Cloud

Bulut Yerel Güvenlik Platformu

Prisma ™ Cloud, hibrit ve çoklu buluttaki, tüm uygulamalar ve veriler için, sektörün en geniş güvenlik ve uyumluluk kapsamına sahip, güvenlik platformudur. Prisma Cloud, bulut yerel uygulamaları ve bulut platformları genelinde veri merkezlerini, konteynerleri, sunucusuz konumlandırmaları, depolama ve diğer hizmet sunumu olarak platformları (PaaS) korur. Kaynakları dağıtırken dinamik olarak tespit eder ve bulut uygulamalarınız için güvenlik ve uyumluluk içgörüleri sağlamak için sağlanan veri bulut hizmetleriyle (kaynak yapılandırmaları, akış günlükleri, denetim günlükleri, ana bilgisayar ve kapsayıcı günlükleri, v.b.) ilişkilendirir. Gelişmiş tehditleri önlemek için kullanıcı, iş yükü ve uygulama davranışlarını profillemek için, makine öğrenimini kullanır. Güvenlik düzenleme araçlarıyla sorunsuz entegrasyon, güvenlik açıklarının hızla düzeltilmesini sağlar.

Prisma SaaS

Güvenli SaaS Erişimi

Prisma ™ SaaS, bulut uygulamaları ve önemli veriler için görünürlük, uyumluluk kontrolleri ve güvenlik sağlar. Office 365 ve Salesforce, ve G Suite gibi kurumsal SaaS uygulamalarına güvenli erişim sağlamaya yardımcı olur ve bulutta veri ihlali riskini azaltır.

Prisma SaaS, birden çok SaaS uygulaması genelinde sürekli olarak görünürlük, uyumluluk kontrolleri ve koruma sağlayan bir bulut hizmetidir. Kurumları ve verilerini bulut siber ataklarına karşı korur. Palo Alto Networks güvenlik duvarlarının entegre bir özelliği olan Prisma SaaS, tüm internet trafiğinde ve tüm ağ trafiğinin denetimi ve SaaS uygulamaları için, API tabanlı güvenlik çözümü sunar.

paloalto® NETWORKS

EXCLUSIVE NETWORKS

CORTEX™
BY PALO ALTO NETWORKS

Geleceği Güvenceye Alın

Cortex ™, güvenlik operasyonları için sektörün en kapsamlı çözüm paketidir. Kurumları sınıfının en iyisi algılama, inceleme, otomasyon ve yanıt verme özellikleriyle güçlendirir.

Otomatik Odaklama


Cortex


Cortex XDR


Cortex XSOAR

paloalto® NETWORKS

EXCLUSIVE NETWORKS

AutoFocus

Tehdit İstihbaratı

AutoFocus ™ tehdit istihbaratı hizmeti, yüksek güvenlik duvarı tehdidi istihbaratından oluşan, kaynaklara anında erişim sağlar. Sektörün en büyük ağ, uç nokta ve bulut istihbarat kaynaklarından, tüm dünyadaki saldırılara ilişkin benzersiz ön görüler elde edebilirsiniz. Her tehdit, dünyaca ünlü Unite 42 tehdit araştırmacılarının yorumları ile zenginleştirilir. Bu sayede, analistleriniz, önemli ölçüde zamandan tasarruf sağlar.

Cortex

Güvenlik Analitiği için Oluşturulmuş Veriler

Cortex ™ Data Lake, Cortex XDR, Prisma Erişimi ve Yeni Nesil Güvenlik Duvarları dahil olmak üzere Palo Alto Networks çözümlerini etkinleştirmek için, kurumunuzun güvenlik verilerini toplamanızı, dönüştürmenizi ve entegre etmenizi sağlar.

Cortex XDR

Genişletilmiş Tespit ve Yanıt

Cortex XDR ™, karmaşıklığı ortadan kaldırmak ve tehditlere odaklanmak için, güvenlik operasyonlarınızı güçlendirir. Cortex XDR çözümü, ağ ve bulut verileriyle saldırıları nasıl tespit edebileceğinizi yeniden kurgular. Cortex XDR, davranış analizi ve makine öğrenimi ile, verileri analiz ederek tehditleri doğru şekilde tanımlar. Her vakanın tam görüntüsünü çeker ve temel nedeni ortaya çıkararak tehditleri öncekinden 8 kat daha hızlı araştırmanıza imkan tanır. Buna ek olarak, uyarı önceliklendirmesi, tehdit avlama, zaman tasarrufu sağlayarak, kolay ve kullanıcı dostu bir güvenlik operasyon deneyimi sunar.

Cortex XSOAR

Genişletilmiş Güvenlik Düzenleme, Otomasyon ve Yanıt (XSOAR)

Cortex ™ XSOAR, sektörün genişletilmiş güvenlik düzenleme, otomasyon ve yanıt (SOAR) platformuyla SOC verimliliğini güçlendirir. Güvenlik ekipleri, vaka yönetimi, otomasyon, gerçek zamanlı işbirliği ve tehdit istihbaratı yönetimine yönelik kapsamlı bir şekilde operasyonlarını takip edebilir. Cortex XSOAR sayesinde, ekipler, tüm kaynaklardaki uyarıları yönetebilir, herhangi bir işlemi standart hale getirebilir, tehdit istihbaratı üzerine aksiyon alabilir ve her güvenlik kullanım durumu için yanıtı otomatikleştirebilir - bu da %90 daha hızlı yanıt süreleri ve insan müdahalesi gerektiren uyarılarda %95 azalma sağlar.