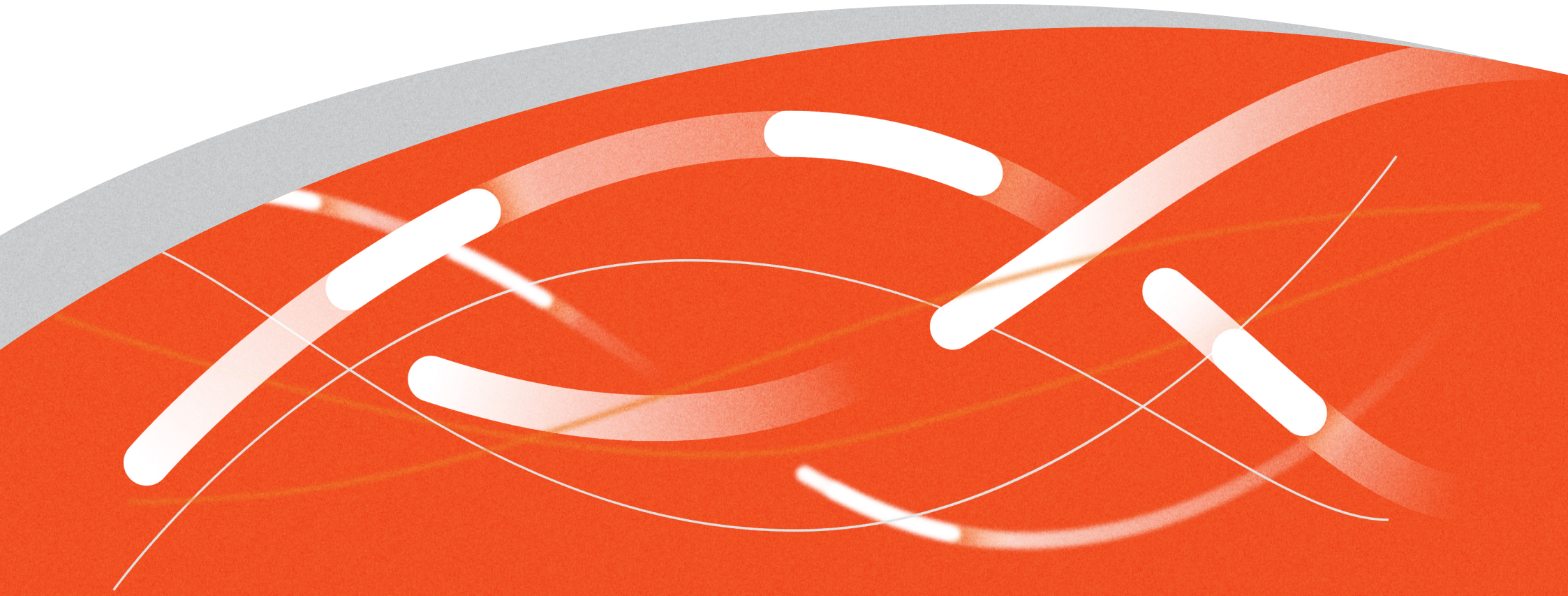
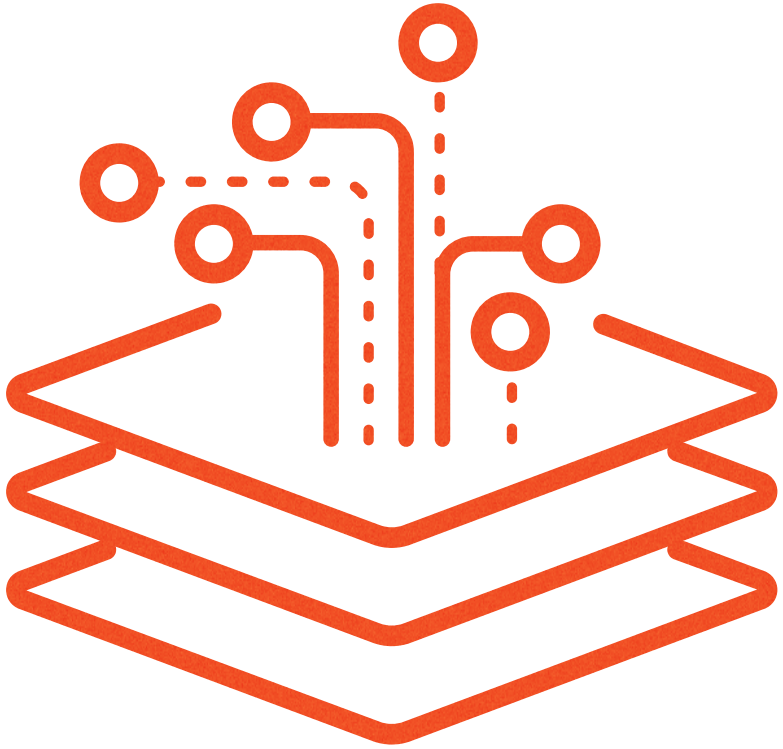
paloalto®
NETWORKS



S KAŽDÝM NOVÝM DNEM MŮŽE BÝT SVĚT JEŠTĚ BEZPEČNĚJŠÍ

Technologie Palo Alto Networks udávají krok na poli kybernetické bezpečnosti a mění způsob, jakým lidé a organizace fungují. Naším posláním je stát se vaším partnerem v kybernetické bezpečnosti a chránit digitální způsob života nás všech. Pomáháme našim zákazníkům čelit komplexním bezpečnostním výzvám dnešní doby pomocí neustálých inovací, které využívají nejnovější poznatky v umělé inteligenci, analytice, automatizaci a orchestraci. Díky naší integrované platformě a neustále rostoucí síti partnerů chráníme desítky tisíc organizací od cloudu, přes sítě až po mobilní zařízení.



Takto vás chráníme...

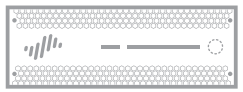
Security Operating Platform

Bezpečnost vyžaduje jednoduchost. Security Operating Platform® byla navržena tak, aby vaše týmy mohly chránit vaši organizaci jednoduše a efektivně. Naše platforma zabraňuje kybernetickým útokům a zároveň zastavuje již probíhající útoky, čímž chrání vaši organizaci, cloud a budoucnost.

STRATA™
BY PALO ALTO NETWORKS

ZABEZPEČENÍ ORGANIZACE

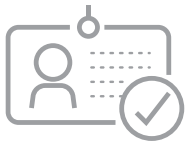
Strata™ zabraňuje útokům s využitím platformy síťové bezpečnosti, která určuje trend v této oblasti. Naše vzájemně spolupracující technologické moduly jsou navržené jako velmi efektivní, snadno se s nimi pracuje a ochrana, kterou poskytují v síťových prostředích, v cloudu i pro mobilní uživatele, je účinná a konzistentní.



Next-Generation Firewall

App-ID

Content-ID



User-ID

Panorama

DNS Security

Threat Prevention

URL Filtering

WildFire

GlobalProtect

SD-WAN

Next-Generation Firewalls
(Fyzický a virtuální)

Palo Alto Networks Firewally nové generace zastavují kybernetické útoky a zároveň zjednodušují bezpečnost. Inovace jsou úzce integrovány do platformy a nahrazují jednoúčelové produkty. Fyzické, virtualizované a cloudové možnosti nasazení poskytují konzistentní ochranu bez ohledu na to, kde jsou vaše data a aplikace umístěny.

Až 80 % průniků do společností souvisí s odcizením uživatelského jména a hesla. Next-Generation firewally od Palo Alto Networks nabízejí unikátní ochranu uživatelských údajů před odcizením, kdy nedovolí zadat firemní uživatelské údaje jinam, než je předem definováno. Zároveň tyto Next-Generation firewally umožňují prosadit multifaktorovou autentizaci i pro aplikace, které ji nativně nepodporují. Tím společnost chrání před nejčastějším zdrojem průniků.

App-ID
Technologie pro identifikaci aplikací

App-ID™ je patentovaná technologie klasifikace provozu dostupná pouze na firewallech Palo Alto Networks. Určuje identitu aplikace bez ohledu na port, protokol, šifrování SSH/SSL nebo jakoukoli jinou maskovací techniku, kterou může aplikace použít. K přesné identifikaci aplikací používá několik mechanismů klasifikace včetně podpisů aplikace, dekódování aplikačního protokolu a heuristiky v rámci síťového provozu.

Když je aplikace identifikována, bezpečnostní politika vám umožní určit, jak s ní zacházet. Každou aplikaci můžete snadno zablokovat nebo povolit, vyhledat hrozby v jejím provozu, kontrolovat neoprávněný přenos souborů a přenášeného obsahu, nebo na její provoz aplikovat QoS.

Content-ID
Technologie pro identifikaci obsahu

Technologie Content-ID™ přináší nový přístup založený na úplné analýze veškerého povoleného provozu a využívá více pokročilých technologií prevence hrozeb v jediném sjednoceném enginu. S Content-ID mohou naše Next-Generation firewally blokovat pokusy o zneužití zranitelnosti, přetečení vyrovnávací paměti a skenování portů; chránit před invazivními a maskovacími metodami útočníků; zastavit odchozí škodlivé komunikace; blokovat přístup ke škodlivým a phishingovým webům; a snížit rizika spojená s přenosem nepovolených souborů a dat.

User-ID
Technologie pro identifikaci uživatelů

Technologie User-ID™ pomáhá definovat pravidla, která bezpečně povolují aplikace na základě uživatelů nebo uživatelských skupin, a to pro odcházející nebo přicházející komunikaci. Například jen IT oddělení může používat nástroje jako SSH, telnet a FTP, a to jen na standardních portech. Díky User-ID mají vaši uživatelé jednotná pravidla, bez ohledu na to, kde právě jsou, v ústředí, na pobočce nebo doma - a také bez ohledu na to, jaká zařízení pro přístup k síti používají. Přehledy o aktivitách uživatelů můžete vytvářet pomocí vlastních nebo předdefinovaných šablon.

Vhled do aplikací na úrovni uživatelské identity umožňuje efektivněji spravovat aplikace procházející sítí. Používání aplikací tak může být v dobrém souladu s potřebami podniku a v případě potřeby je možné snadno informovat uživatele, že porušují pravidla nebo je přímo zablokovat.

Panorama
Centrální management

Panorama™ poskytuje centralizovanou správu síťové bezpečnosti, zjednodušuje administraci a poskytuje přehled o bezpečnostních hrozbách v síťovém provozu. Panorama spravuje pravidla a dynamické aktualizace, takže můžete držet krok s neustále se vyvíjejícími síťovými hrozbami. Díky sjednocení pravidel na firewallech, Threat Prevention, URL filtering, App-ID, User-ID a blokování souborů a dat lze snadno snížit administrativní zátěž a dosáhnout vyšší úrovně celkového zabezpečení.

Panorama dokáže spravovat všechny vaše firewally, ať se nacházejí kdekoliv: na perimetru, v datovém centru nebo v cloudu. Prostřednictvím API a dynamických skupin IP adres pomáhá Panorama s automatizací procesů, jako je například přidávání, přesouvání nebo odstranění serverů. Vestavěný Application Command Center poskytuje komplexní pohled na současné a historické údaje o síti a informace o hrozbách v ní.

DNS Security

Ochrana před útoky přes DNS

Služba DNS Security používá prediktivní analýzu na detekci útoků, které používají DNS ke komunikaci s Command and Control (C2) nebo ke krádeži údajů. Úzká integrace s Palo Alto Networks Next-Generation firewally vám poskytuje automatickou ochranu a eliminuje potřebu použití jiných nástrojů. Sdílené zdroje o hrozbách a strojové učení rychle identifikují hrozby ukryté v DNS komunikaci. Služba DNS Security předpovídá a blokuje škodlivé domény vytvořené útočnými nástroji pro generovaní domén (DGA), a zároveň rychle odhalí C2 komunikaci nebo krádež dat využívající tunelování přes DNS. Next-Generation firewall dokáže takto automaticky najít infikovaná zařízení a dynamicky pro ně změnit pravidla. Tato ochrana je doručovaná z cloudu, takže je dobře škálovatelná a vždy aktuální pro efektivní zastavení útoků využívajících DNS.

Threat Prevention

Ochrana před exploity, škodlivým softwarem a C2

Threat Prevention – ochrana před hrozbami – využívá signatury, které blokují známé zranitelnosti na straně klienta a serveru, škodlivý software a Command and Control komunikaci. Kontroluje se celý provoz na hrozby, bez ohledu na port nebo protokol. Threat Prevention poskytuje ochranu ve více vrstvách, přesně v souladu se Zero Trust modelem, a hledá a zastavuje hrozby nejen při prvním vstupu do sítě, ale ve všech fázích životního cyklu kybernetického útoku.

Signatury Threat Prevention jsou přizpůsobené pro skenování provozu v jediném průchodu. Tím se eliminují zbytečné procesy, a také související zpoždění, které známe při používání tradičních technologií, které obvykle spoléhají na několik zřetězených skenů. Threat Prevention zkoumá každý paket procházející Next-Generation firewally a podrobně zkoumá sekvenci bajtů jak v rámci hlavičky paketu, tak i přenášená data. Z této analýzy můžeme identifikovat důležité podrobnosti o každém paketu, včetně použité aplikace, jeho zdroje a cíle, jestli exploit nebo škodlivý kód. Kromě jednotlivých paketů analyzujeme také kontext v sekvenci více přicházejících paketů, a to mimo jiné i pro zjištění případných technik maskování útoku. To vše se děje v rámci jednoho skenu, takže rychlost síťového provozu zůstane zachována.

URL Filtering

Ochrana před škodlivými stránkami a phishingem

URL Filtering vám umožňuje bezpečně používat web. Tato cloudová služba významně vylepšuje základní filtrování webu a nebezpečné hrozby zjišťuje pomocí unikátní kombinace statické analýzy a strojového učení. Automatická ochrana blokuje přístup na stránky, které doručují škodlivý software a snaží se ukrást přihlašovací údaje. Organizace může minimalizovat riziko nasazením granulárních bezpečnostních pravidel a využívat výhody této průběžně aktualizované ochrany. Pravidla založená na aplikacích a identitě uživatelů zjednodušují složité předpisy pro přístup na web a snižují provozní náklady.

URL Filtering klasifikuje webové stránky na základě obsahu, funkcionality a jejich pověsti z pohledu bezpečnosti. Každá URL adresa je vyhodnocena v rámci několika kategorií, včetně rizikovosti této stránky (pravděpodobnost, s jakou vás tato stránka vystaví hrozbám).

WildFire

Ochrana před neznámým škodlivým obsahem

WildFire® je sandboxová služba pro prevenci před škodlivým softwarem. WildFire posouvá hranice tradičního sandboxu a pomáhá bezpečnostním týmům držet krok s nejnovějšími útočnými technikami díky nástrojům jako strojové učení, statická analýza, dynamická analýza a profilování sítě. WildFire používá vlastní hypervizor a unikátní analýzu přímo na fyzických zařízeních pro odhalení malwaru, který se snaží vyhnout analýze v sandboxu.

V okamžiku, kdy Palo Alto Networks firewall detekuje neznámý vzorek (soubor nebo odkaz obsažený v e-mailu), je vzorek odeslán na analýzu do WildFire sandboxu. Na základě vlastností, chování a aktivit, které vzorky vykazují při analýze, WildFire vygeneruje verdikt: “neškodný”, “grayware”, “phishing” nebo “škodlivý”. WildFire potom automaticky vytvoří nové signatury popisující škodlivý software a okamžitě je distribuuje ke všem zákazníkům, kteří službu používají. Všechny firewally Palo Alto Networks tak mohou automaticky zastavovat nově zjištěný malware, který před krátkou dobou objevil firewall někoho jiného.

GlobalProtect

Ochrana pro mobilní uživatele

Mobilita pracovní síly zvyšuje produktivitu a flexibilitu, ale současně přináší značná bezpečnostní rizika. Vždy, když uživatelé opustí budovu s notebookem nebo chytrým telefonem, obcházejí firemní firewall a jeho bezpečnostní pravidla, která jsou určena pro jejich ochranu i pro ochranu sítě. GlobalProtect™ poskytuje veškerou funkčnost Next-Generation firewallu bez ohledu na to, kde se uživatelé nacházejí.

GlobalProtect "Clientless VPN" poskytuje bezpečný vzdálený přístup k firemním webovým aplikacím. Uživatelé využívají výhodu zabezpečeného přístupu přes webový prohlížeč s podporou SSL bez nutnosti instalace jakéhokoli agenta.

SD-WAN

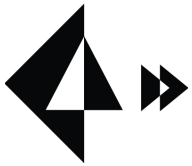
Softwarově definované WAN připojení

Software-Defined Wide Area Network (SD-WAN) je technologie, která vám umožňuje používat více internetových privátních linek vytvoření inteligentní dynamické WAN sítě, která pomáhá snižovat náklady maximalizovat kvalitu připojení použitelnost aplikací. Místo použití nákladných MPLS linek komponenty, jako jsou routery, firewally, WAN kontrolery WAN optimalizátory pro připojení do internetu, vám SD-WAN na Next-Generation firewallu umožňuje používat levnější internetové služby menší počet zařízení. Nemusíte kupovat spravovat další WAN komponenty.

PRISMA™
BY PALO ALTO NETWORKS

ZABEZPEČENÍ CLOUDU

Prisma™ představuje nejkomplexnější nabídku pro ochranu cloudu na trhu. Urychlete i vy vaši cestu do cloudu se sadou produktů vytvořenou právě pro dnešní komplexní IT prostředí!



Prisma™ Access

Prisma™ Cloud

Prisma™ SaaS

VM-Series

VM-Series

Virtuální Next-Generation firewall pro privátní a veřejná cloudová prostředí

VM-Series je virtualizovaná podoba našeho Next-Generation firewallu, která se dá nasadit v nejrůznějších privátních a veřejných cloudových prostředích. VM-Series účinně chrání aplikace před hrozbami v privátních a veřejných cloudech. Klasifikuje provoz na základě aplikací, nikoli portů, takže poskytuje ucelený přehled o rizikách v síti. Bezpečnostními pravidly založenými na aplikacích tak můžete zúžit prostor pro úspěšné kybernetické útoky a zabránit úniku dat.

Automatizační funkce VM-Series umožňují urychlit nasazení zabezpečení v privátních a veřejných cloudech. Například spouštěcí skript může automaticky nakonfigurovat VM-Series firewall s veškerými licencemi a předplatnými. Následně se firewall automaticky zaregistruje u centrálního managementu - Panoramy. Změny konfigurace VM-Series se dají taky automatizovat, aby se dynamicky projevovaly i v bezpečnostních pravidlech.

Prisma Access

Cloudová ochrana pro mobilní uživatele

Prisma™ Access poskytuje vaší organizaci konzistentní bezpečnost pro vzdálené sítě a mobilní uživatele. Je to generační krok vpřed v oblasti bezpečnosti, využívající cloudovou infrastrukturu pro připojení veškerých uživatelů ke všem aplikacím. To v praxi znamená, že všichni uživatelé, ať už jsou v sídle společnosti, na pobočkách, na cestách či doma, se připojují k službě Prisma Access a mohou tak bezpečně používat aplikace v cloudu, v datovém centru a na internetu. Prisma Access konzistentně kontroluje veškerý provoz na všech portech a poskytuje obousměrně zabezpečené propojení pobočkám mezi sebou a mezi pobočkami a ústředím.

Prisma Access poskytuje ochranu s důrazem na škálovatelnost a globální dostupnost, takže není třeba nasazovat na vašich pobočkách fyzické firewally ani zajišťovat provoz v pronajatém datovém centru. Prisma Access používá Cortex Data Lake (datové úložiště) pro centralizovanou analýzu, vytváření přehledů a forenzní analýzu.

Prisma Cloud

Cloudová služba pro ochranu před hrozbami, dohled a dodržování předpisů

Prisma™ Cloud dynamicky mapuje vaše zdroje a citlivé údaje v rámci cloudových prostředí GCP™, AWS® a Azure®. Následně detekuje rizikové konfigurace, identifikuje síťové hrozby, podezřelé chování uživatelů, škodlivý kód, únik údajů a zranitelnosti v jednotlivých instancích. Eliminuje slepá místa ve vašich cloudových prostředích a kombinací bezpečnostních pravidel a strojového učení poskytuje nepřetržitou ochranu.

Prisma Cloud také výrazně zjednodušuje vynucování předpisů napříč několika cloudovými prostředími a poskytuje přehledy pro audit v souladu s nařízeními jako jsou GDPR, ISO, SOC 2, PCI a další. S vašimi cloudovými prostředími se integruje pomocí API, může tak nabídnout bezproblémovou uživatelskou zkušenost, bez agentů nebo proxy serverů.

Prisma SaaS

Ochrana SaaS služeb

Při přesunu vašich IT aplikací do cloudu se zvyšuje riziko kompromitování citlivých údajů a distribuce malwaru. Prisma™ SaaS analyzuje data ve vašich software-as-a-service aplikacích, jako např. Office 365, Gmail, Dropbox a jiných a na základě nastavených pravidel upozorňuje na nalezená rizika, která případně i eliminuje.

Prisma™ SaaS je cloudová služba, která se připojí přímo na vaše SaaS aplikace prostřednictvím API a následně poskytuje klasifikaci dat, přehled o sdílení a nastavení oprávnění k souborům, a také detekci hrozeb v rámci aplikace. Dále nabízí kompletní informace o aktivitách uživatelů, o složkách a souborech pro snadné zjištění nechtěného sdílení nebo porušení stanovených předpisů.

Prisma Cloud Compute (Twistlock)

Bezpečnost pro kontejnery, hosty a funkce, během celého životního cyklu

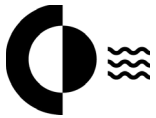
Prisma Cloud Compute je unikátní bezpečnostní platforma, která dokáže plně zabezpečit cloud-native prostředí, od hostů, přes kontejnery, až po serverless aplikace, a to od zranitelností i před aktivními hrozbami. Využívá k tomu strojového učení, pomocí kterého vytváří 4D modely známého správného chování aplikací. Chrání procesy, síťovou komunikaci, souborový systém i systémová volání, v průběhu celého životního cyklu CD/CI.

CORTEX™
BY PALO ALTO NETWORKS

ZABEZPEČENÍ BUDOUCNOSTI

Cortex™ je otevřená a integrovaná bezpečnostní platforma založená na umělé inteligenci, která se neustále vyvíjí, aby byla schopná zabránit i těm nejpokročilejším hrozbám.

Cortex™



Cortex™ Data Lake

Cortex™ XDR

Cortex™ XSOAR

Cortex™ AutoFocus

Cortex

Bezpečnostní platforma založená na umělé inteligenci

Cortex™ přináší jednoduchost a díky automatizaci a bezprecedentní přesnosti výrazně zlepšuje celkovou bezpečnost. Platforma využívá bohatá data ze senzorů na koncových bodech, ve firewallech a v cloudu. Pro sběr informací lze využít i již nasazené aplikace od Palo Alto Networks, případně také informace z vybraných bezpečnostních řešení jiných výrobců. Cortex se neustále vyvíjí, aby rychle přinášel nové inovace v bezpečnosti, analytice a automatizaci. Automatizací vašich IT procesů ušetříte čas při řešení specifických a složitých problémů.

Cortex Data Lake

Cloudová služba pro sběr, ukládání a analýzu dat

Cortex Data Lake ukládá obohacené logové záznamy z produktů Palo Alto Networks včetně Next-Generation firewallů, Prisma Access, Cortex XDR a z firewallů jiných výrobců. Tato cloudová služba je plně škálovatelná, eliminuje potřebu lokálního úložiště a garantuje vašim datům bezpečnost a důvěrnost. Většina Cortex aplikací používá Cortex Data Lake pro čtení těchto dat, analyzuje je a zpřístupní výsledky.

Cortex XDR

Cloudová služba pro detekci a reakci

Cortex XDR přináší zcela jedinečný přístup ochrany proti známým i neznámým hrozbám typu malware i exploit, a to bez využití signatur. Nezaměřuje se pouze na detekci, ale především na okamžitou prevenci. Pro analýzu neznámých souborů je využívána již zmiňovaná služba WildFire. Exploity jsou detekovány a zastaveny pomocí znalosti útočných technik, které mohou vést k ovládnutí operačního systému.

Cortex XDR sbírá podrobná data o aktivitě v síti, na koncových bodech a v cloudu, tato data vyhodnocuje pomocí algoritmů vytvořených s podporou strojového učení. Dokáže tak rychle odhalit kompromitované koncové body, najít a zastavit cílené útoky a zabránit odcizení citlivých informací. Aplikace Cortex XDR čte a koreluje data z Cortex Data Lake a odhaluje aktivitu hrozeb a útoky v časové posloupnosti. Je to váš nástroj pro kompletní vhled do síťového provozu a chování uživatelů.

Cortex XSOAR (Demisto)

Pokročilý SOAR (Security Orchestration, Automation and Response)

Cortex XSOAR (původně Demisto) je jednotná platforma zabezpečující orchestraci, automatizaci a reakci (SOAR), která kombinuje orchestraci bezpečnosti, správu incidentů a jejich interaktivní vyšetřování tak, aby sloužila bezpečnostním týmům v průběhu celého životního cyklu incidentu. Tato orchestrace umožňuje přijímat upozornění z různých zdrojů a prostřednictvím standardizovaných a automatizovaných šablon (playbooks) na ně urychleně reagovat. Šablony ke své činnosti využívají stovky integrací a tisíce bezpečnostních akcí a vytvářejí tak ideální rovnováhu mezi strojovou automatizací a dohledem analytika. Šablony jsou navíc obohacené o možnost vyšetřování v reálném čase, což umožňuje okamžité řešení vznikajících hrozeb.

Každý incident v Cortex XSOAR má vyhrazenu interaktivní místnost (War Room), ve které mohou analytici vzájemně komunikovat, spouštět příkazy v reálném čase a dokumentovat svoje aktivity řešení incidentů. Pro kompletní viditelnost do životního cyklu útoku jsou k dispozici plně přizpůsobitelná shrnutí, nástěnky a přehledy. Cortex XSOAR umožňuje bezpečnostním týmům zkrátit průměrný čas na odezvu, udržovat konzistentní incident management a zvýšit svou produktivitu.

AutoFocus

Znalostní databáze o hrozbách

AutoFocus urychluje schopnost analyzovat hrozby a reagovat na kybernetické útoky a šetří vašim analytikům čas díky možnosti rychlého přístupu ke komunitním údajům ze služby WildFire a k informacím od našeho výzkumného týmu Unit 42. Váš bezpečnostní tým může využívat vestavěné značky (tags) od Unit 42, které identifikují rodiny malwaru, útočníky, kampaně, škodlivé chování a exploity, a nemusí provádět vlastní zdlouhavý výzkum.

Tato cloudová služba zrychluje a zpřesňuje odezvy na útoky tím, že poukazuje na hrozby s největším dopadem, čímž vám usnadňuje stanovení priorit během vyšetřování. Automatizovaná ochrana poskytovaná vaším Next-Generation firewallem ulehčuje praktické nasazení nasbíraných informací v reálném čase, napříč celým chráněným prostředím. Získané informace lze přes jednoduché API odesílat například i do nástrojů SIEM. Všechny interní údaje a údaje třetích stran konsolidované do jednoho systému umožňují rychlé vyšetřování, korelaci a určení hlavní příčiny škodlivé aktivity bez specializovaných bezpečnostních výzkumníků nebo dalších nástrojů.

Palo Alto Networks

3000 Tannery Way
Santa Clara, CA 95054
Support: +1.866.898.9087
www.paloaltonetworks.com