Palo Alto Networks

Dnešní zabezpečení určuje podobu zítřka

paloalto NETWORKS

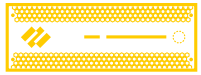
Palo Alto Networks je jediný dodavatel řešení kybernetického zabezpečení, se kterým se digitální podniky nemusí rozhodovat mezi zabezpečením, které potřebují dnes, a tím, co jim vydrží do budoucna. Jde nám o to, aby naše zabezpečení nekompromisně splňovalo oba požadavky.

Podívejte se, jak vás chráníme.

STRATA™
BY PALO ALTO NETWORKS

Strata

**Zabezpečte svůj podnik už dnes proti zítřejším hrozbám.
Chraňte uživatele, aplikace a data inteligentním zabezpečením sítě
od Palo Alto Networks.**



Next-Generation Firewall

PA-Series

VM-Series

CN-Series

App-ID

Content-ID

User-ID

Device-ID

Panorama

DNS Security

Enterprise DLP

Threat Prevention

URL Filtering

WildFire

IoT Security

GlobalProtect

5G Security

SD-WAN

Next-Generation Firewall

Fyzické, virtuální nebo cloudové řešení ochrany

Pusťte se s jistotou do digitální transformace, když zkonsolidujete několik dílčích zabezpečovacích produktů do uceleného řešení zabezpečení sítě. Palo Alto Networks Next-Generation Firewall (NGFW) je konzistentní a integrované řešení zabezpečení sítě, které poskytuje nejlepší ochranu ve své třídě. Dodává se jako fyzické nebo virtuální zařízení, formou softwarového kontejneru i v cloudu – a ve všech konfiguracích se dá centrálně spravovat. První NGFW s technologií strojového učení (ML) na trhu dokáže bránit neznámým hrozbám, dohlížet a jistit všechno – včetně IoT – a zamezovat chybám pomocí automaticky doporučovaných pravidel. Zabezpečte svůj kampus, hybridní cloud, pobočky i mobilní uživatele devítinásobným lídrem z analýzy Gartner Magic Quadrant pro síťové firewally.

PA-Series

Fyzický Next-Generation Firewall

Fyzické firewally PA-Series jsou konstruované pro vysoce výkonné zpracování zabezpečovacích úloh. Kvůli požadavkům na maximální propustnost jsou vybavené několika vysokorychlostními rozhraními. PA-Series NGFW poskytují vhled, zabezpečení a kontrolu nad provozem v podnikových sítích (včetně provozu IoT a 5G) pro datové centrum, perimetr kampusu, pobočkové kanceláře, průmyslové instalace a mobilní infrastrukturu 5G.

VM-Series

Virtuální Next-Generation Firewall

Virtuální firewally VM-Series jsou ideální pro prostředí, kde by nasazení hardwarových firewallů bylo složité nebo nemožné. Firewally VM-Series poskytují všechny možnosti Palo Alto Networks NGFW ve virtuálním provedení. Zabezpečením procházejícího síťového provozu a prevencí hrozeb konzistentně chrání veřejné a privátní cloudy, virtualizovaná datová centra a pobočkové kanceláře.

App-ID

Klasifikace aplikací

App-ID™ je patentovaná technologie klasifikace provozu, kterou mají jenom firewally Palo Alto Networks. Dokáže určit identitu aplikace bez ohledu na port, protokol, šifrování TLS/SSL/SSH (včetně TLS 1.3 a HTTP/2) nebo jakoukoli jinou úhybnou taktiku, kterou může aplikace používat. Provoz nejrůznějších aplikací ve vašem síťovém toku rozpoznává pomocí celé řady klasifikačních mechanismů včetně signatur aplikací, dekódování aplikačních protokolů a heuristiky. Jakmile je aplikace identifikována, kontrolou politik můžete určit, jak se s ní má naložit. Můžete její provoz zablokovat, povolit a prověřit na přítomnost hrozeb, identifikovat vzorce neoprávněných přenosů souborů a dat nebo provoz řídit pomocí QoS. Přechod ze starších firewallových pravidel založených na portech na pravidla využívající App-ID podstatně omezuje prostor pro útok. Policy Optimizer, funkce PAN-OS®, umožňuje pomocí jednoduchých pracovních postupů a poznatků získávaných systémem PAN-OS snadno přejít na ovládání založené na App-ID a posílit vaše zabezpečení.

CN-Series

Kontejnerový Next-Generation Firewall

Kontejnerové firewally CN-Series poskytují všechny možnosti Palo Alto Networks NGFW formou kontejneru, který umožňuje přesunout zabezpečení co nejblíž ke kontejnerovým úlohám a využívat při formulování pravidel tak důležitý kontext kontejneru. Kontejnerový firewall CN-Series tak může uplatňovat prevenci hrozeb a další pokročilé služby zabezpečení sítě včetně IPS a filtrování adres URL na povolený provoz – odchozí, příchozí i obousměrný – mezi kontejnerovými pody, aplikacemi v kontejneru i staršími úlohami, jako jsou třeba virtuální počítače nebo klasické hardwarové servery.

Content-ID

Klasifikace obsahu

Content-ID™ pomocí několika vyspělých technologií prevence hrozeb provádí komplexní analýzu veškerého povoleného provozu při jediném prověřování. Pomocí Content-ID dokážou naše firewally blokovat zneužití zranitelností, přetečení zásobníku a skenování portů; chrání taky před úhybnými a matoucími metodami, které používají útočníci. Naše cloudové zabezpečovací služby jako Threat Prevention a URL Filtering pomocí Content-ID zastavují odchozí komunikaci malwaru, blokují přístup ke známým webům na stahování malwaru a phishingu a omezují rizika spojená s přenosem neautorizovaných souborů a dat. Content-ID umožňuje komplexní ochranu před hrozbami pomocí jednorázového prověření síťového provozu. Optimalizuje tak výkon NGFW.

User-ID

Klasifikace uživatelů

Technologie User-ID™ pomáhá definovat pravidla, která bezpečně umožňují používat aplikace na základě uživatelů nebo jejich skupin, v odchozím i příchozím směru. Můžete tak například umožnit pouze IT oddělení používat SSH, telnet nebo FTP, a jen na standardních portech. User-ID se stará o to, aby pravidla sledovala uživatele, ať pracují kdekoli – v ústředí, v pobočce, nebo doma – a na libovolném zařízení, které používají. Můžete získat přehled o aktivitách aplikací na úrovni uživatelů – nejen podle IP adres – a generovat o tom informativní výkazy. Navíc od uživatelů můžete vyžadovat vícefaktorové ověřování (MFA), aniž byste museli jakkoli upravit aplikace.

Pomocí User-ID se dá zabránit tomu, aby se firemní přihlašovací údaje dostaly z vašeho podniku. Zastavíte tak útočníky, kteří by mohli chtít použít ukradené přihlašovací údaje k přístupu do vaší sítě. Dynamické skupiny uživatelů (DUG) umožňují správcům dynamicky měnit přístupová oprávnění uživatelů nebo vynucovat MFA, ať už kvůli novým poznatkům o hrozbách, nebo kvůli provoznímu požadavku, jakým může být třeba poskytnutí dočasného přístupu skupině uživatelů.

Device-ID

Klasifikace zařízení

Device-ID™ je nový koncept pravidel, který umožňuje správcům psát pravidla založené na charakteristikách zařízení. Umožňuje bezpečnostním týmům pochopit, jak se události vztahují k zařízením, a psát pravidla spojená se zařízeními namísto jejich IP adres nebo umístění, které se můžou postupem času měnit. Pomocí Device-ID můžou naše NGFW omezit IoT zařízení na známé vzorce dobrého chování, blokovat v síti zařízení se zastaralým operačním systémem, rychle dosledovat hrozby zpátky k jednotlivým zařízením a používat „zařízení“ jako rozměr v jiných typech pravidel. Device-ID můžete používat v pravidlech zabezpečení, dešifrování, kvality služby (QoS) a ověřování. Device-ID podporuje Panorama a všechny NGFW s technologií strojového učení (kromě VM-50 a CN-Series) s PAN-OS 10.0 nebo novějším.

Panorama

Řešení správy

Panorama™ je centralizované řešení správy zabezpečení pro všechny vaše firewally Palo Alto Networks bez ohledu na jejich provedení a umístění. Zjednodušuje jejich konfiguraci a nasazení i správu pravidel zabezpečení. Panorama poskytuje centralizovaný přehled a komplexní vhled do síťového provozu, protokolů a hrozeb. Snižuje pracnost správy tím, že pomáhá spravovat aktualizace, automatizovat odezvu na hrozby pomocí akcí založených na pravidlech a využívat integraci se systémy třetích stran.

Týmy zabezpečení sítí můžou získat lepší přehled a kontrolu nad svou bezpečnostní situací, zkonsolidovat nástrojové vybavení a automatizovat zabezpečení. Panorama se stará o pravidla a dynamické aktualizace zabezpečení, abyste vy mohli držet krok s neustále se vyvíjejícími síťovými hrozbami. Zjednodušte si provoz efektivní správou aktualizací softwaru a automatizujte plánování aktualizací obsahu, které vám pomůžou udržet si nejlepší možný stav zabezpečení. S jediným řešením správy můžete naplno využívat všechny možnosti bezpečnostních funkcí a souvisejících předplatných. Navíc máte všechno pod kontrolou z jednoho místa.

DNS Security

Prevence útoků pomocí DNS

Osmdesát procent malwaru používá DNS k vytvoření řídícího a ovládacího (command-and-control, C2) kanálu. Útočníci svoje data často skrývají v DNS, protože objem tohoto provozu je tak vysoký, že většina organizací nedisponuje nástroji potřebnými k jeho náležitému monitorování. Na ochranu před hrozbami přenášenými přes DNS potřebujete vynikající detekční nástroje ve spojení s analytikou, která poskytne bezpečnostním specialistům kontext potřebný k rychlému vytváření zásad a účinným reakcím na hrozby. Naše služba DNS Security blokuje útoky, které zneužívají DNS, pomocí prediktivních analýz, strojového učení a automatizace. Úzká integrace s NGFW poskytuje automatickou ochranu, která brání útočníkům obejít bezpečnostní opatření, a odstraňuje nutnost nezávislých nástrojů nebo změn směrování DNS. Pomáhá rychle předvídat a bránit přístupu ze škodlivých domén, neutralizuje hrozby skryté v DNS tunelech a automatizuje rychlé vyhledávání a izolaci napadených zařízení.

Reportování služby DNS Security umožňuje daleko hlubší vhled do hrozeb než dřív, protože poskytuje ucelený pohled do provozu DNS na makro, oborové i organizační úrovni. Cloudové ochranné mechanismy mají prakticky nekonečné možnosti škálování, takže poskytnou vaší organizaci důležitý nový kontrolní bod, kde se dají zastavit útoky zneužívající DNS. Řešení Palo Alto Networks spojuje nejlepší detekci ve své třídě s analytikou a vynucováním pravidel v reálném čase přímo na provozu DNS.

Enterprise Data Loss Prevention

Ochrana dat a dodržování předpisů

Palo Alto Networks Enterprise Data Loss Prevention (DLP) je první cloudová bezpečnostní služba, která objevuje, monitoruje a chrání citlivá data, například osobně identifikovatelné informace nebo intelektuální majetek, ve všech sítích, cloudových službách a u všech uživatelů. Jediná cloudová služba a předem nadefinované zásady umožňují snadno a konzistentně zajistit důvěrnost dat a dodržování předpisů, ať už na počítačích ve vlastní síti, u vzdálených pracovníků, nebo v cloudu. Naše technologie Enterprise DLP, která je nativně integrována v ovládacích bodech Palo Alto Networks, až trojnásobně snižuje celkové náklady na vlastnictví proti složitým starším DLP produktům. Zjednodušuje tak nasazení a údržbu a zároveň eliminuje nutnost dodatečné infrastruktury.

Threat Prevention

Prevence zneužití, malwaru a C2

Naše služba Threat Prevention funkcemi IPS automaticky zastavuje známá zneužití bezpečnostních slabin na straně klienta i serveru, nabízí ochranu proti malwaru při přenosu a blokuje odchozí provoz C2. Threat Prevention prověřuje na výskyt hrozeb veškerý provoz bez ohledu na port, protokol nebo šifrování. Nic se tak nedá jen tak zamést pod koberec. Obsažené ochranné mechanismy IPS jsou založené na srovnávání se signaturami a na detekci anomálií. Umožňují importovat a automaticky aplikovat signatury a pravidla v oblíbených formátech jako Snort nebo Suricata®. Threat Prevention hledá hrozby ve všech bodech životního cyklu kybernetického útoku, nejen při prvním vstupu do sítě. Poskytuje tak vícevrstvou ochranu založenou na modelu Zero Trust.

Jednotný formát signatur pro všechny hrozby zajišťuje rychlé zpracování tím, že umožňuje provádět všechny analýzy při jediné integrované kontrole. Odpadají tak nadbytečné procesy běžné u řešení, která používají několikanásobné prověřování. Threat Prevention zpracovává každý paket, který prochází našimi NGFW. Přitom důkladně sleduje bajtové sekvence v hlavičkách paketů a datových částech. Z této analýzy dokážeme identifikovat důležité detaily o každém paketu včetně použité aplikace, zdroje a cíle přenosu, shody protokolu se specifikací RFC a toho, zda datová část obsahuje útok nebo škodlivý kód. Kromě jednotlivých paketů analyzujeme i kontext pořadí při doručení a sekvenci paketů, abychom zachytili a zabránili úhybným technikám. Všechno to probíhá při jediném prověření, takže síťový provoz běží tak rychle, jak potřebujete.

URL Filtering

Prevence škodlivých webů a phishingu

URL Filtering umožňuje bezpečně používat web k pracovním účelům. Tato cloudová služba přesahuje možnosti elementárního filtrování webového obsahu, protože identifikuje hrozby jedinečnou kombinací statických analýz a strojového učení. Phishingové stránky a útoky založené na JavaScriptu identifikuje v řádu milisekund. Vzhledem k tomu, že každý den vznikají tisíce nových škodlivých URL, je schopnost okamžitě identifikovat nebezpečné stránky nutným předpokladem ochrany před útoky na webu. Automatické ochranné mechanismy blokují přístup ke škodlivým webům, které návštěvníkům posílají malware a kradou jejich přihlašovací údaje. Minimalizujte vystavení své organizace vůči útokům rozšiřováním pravidel firewallu a využíváním průběžně aktualizovaných ochranných mechanismů. Politiky založené na aplikacích a uživatelích zjednodušují složitá pravidla zabezpečení webové komunikace, a tím současně snižují provozní režii.

URL Filtering pro přesné určení kategorií a rizikových ratingů prověřuje webové stránky a analyzuje jejich obsah strojovým učením se statickými i dynamickými analýzami. Klasifikuje URL na neškodné a škodlivé. Tyto kategorie pak můžete zahrnout do pravidel NGFW pro důslednou kontrolu nad webovým provozem. Při zjištění nově kategorizovaných škodlivých adres je URL Filtering bez jakéhokoli zásahu analytika okamžitě zablokuje.

WildFire

Prevence malwaru

Služba prevence malwaru WildFire® představuje nejvyspělejší cloudový analytický a preventivní nástroj pro útoky nultého dne a vysoce zákeřný malware. WildFire překonává tradiční pojetí detekce neznámých hrozeb tím, že spojuje přednosti různých komplementárních technik pro účinné odhalování včetně dynamické analýzy, statické analýzy, strojového učení a analýz na úrovni samotného hardwaru. Poradí si tak s nejrůznějšími úhybnými technikami. WildFire souvisle poskytuje inovativní detekční engine s nulovým dopadem na provozní výkon, který jinak nevyhnutelně patří k řešením síťového sandboxingu typu „zadržet a uvolnit“. Pomáhá bezpečnostním týmům šetřit čas a zdroje podrobnými poznatky o chování identifikovaných hrozeb, indikátorů narušení a postupu zablokování.

WildFire navíc vychází z modelů hrozeb, které se průběžně zdokonalují v cloudu, a používá revoluční engine strojového učení provozovaný v rámci fyzických a virtuálních NGFW. Bez čekání na aktualizace signatur tak dokáže inovativně bránit škodlivému obsahu – například neznámým přenosným spustitelným souborům nebo nebezpečným bezsouborovým útokům vycházejícím z PowerShellu. Za plného provozu a bez zasílání vzorků do cloudu.

Komunita WildFire slouží jako jedna z největších světových sítí na analýzy podnikového malwaru. Ke své činnosti využívá poznatky o hrozbách z firemních sítí, koncových bodů, cloudů i od nezávislých partnerů. Když jakýkoli předplatitel služby WildFire odhalí útok nultého dne nebo malware, služba automaticky zajistí globální nasazení přesně cílených ochranných mechanismů, které jsou odolné proti úhybným taktikám. Celá reakce proběhne v řádu sekund od prvního zjištění kdekoli na světě.

IoT Security

Zabezpečení internetu věcí pro podniky a zdravotnictví

IoT Security je nejucelenější řešení zabezpečení internetu věcí, které poskytuje vhled, prevenci i vynucování s využitím strojového učení. Jedná se o jediné řešení na trhu, které využívá strojové učení s naší špičkovou technologií App-ID a pomocí crowdsourcované telemetrie profiluje všechna zařízení – i úplně nová – pro zjišťování, vyhodnocování rizik, analýzu zranitelností, detekci anomálií a doporučení pravidel založených na důvěryhodnosti. Místo samotného upozorňování zajišťuje i prevenci, aby všechna zařízení byla chráněná před všemi hrozbami a zranitelnostmi. Zákazníkům ve zdravotnictví navíc řešení IoT Security umožňuje maximální návratnost investic a vynikající výsledky díky hlubokému přehledu, cíleným vhledům do využití speciálních přístrojů a dokonalejšího zabezpečení lékařských zařízení.

IoT Security se dá snadno nasadit a bezproblémově se integruje do existujících pracovních postupů. Omezuje tak zátěž týmů, které se starají o infrastrukturu, zabezpečení a sítě. Tato předplacená služba například vybaví vaše bezpečnostní týmy poznatky o IoT vycházejícími z rozsáhlého portfolia nativních integrací s řešeními správy majetku (CMMS/ITSM), z řízení přístupu k síti (NAC), správy bezpečnostních informací a událostí (SIEM) a oborově specifických databází poznatků o zařízeních.

IoT Security podporuje nejrůznější modely používání v podnicích, zdravotnických zařízeních, ICS/SCADA systémech, systémech pro správu budov, infrastruktuře chytrých měst, ropném a plynárenském průmyslu, komunálních službách a dopravě.

GlobalProtect

Zabezpečení mobilních uživatelů

Řešení síťového zabezpečení koncových bodů GlobalProtect™ zpřístupňuje naše špičkové funkce prevence hrozeb i mobilním pracovníkům bez ohledu na to, kde přesně pracují. Prisma Access používá GlobalProtect k poskytování šifrovaného přístupu pro vzdálené uživatele bez klienta i s klientem. Řešení umožňuje organizacím zahrnout do korporátních pravidel řízení přístupu i nespravovaná zařízení a aplikace v cloudu a datových centrech. Navíc pomocí integrace s podnikovými řešeními správy mobilních zařízení jako AirWatch®, Microsoft Intune® nebo MobileIron® umožňuje podporovat VPN na úrovni jednotlivých aplikací.

5G Security

Zabezpečení pro sítě 5G

Dnešní podniky budou v rámci své digitální transformace očekávat od sítí 5G skutečnou transformaci na Průmysl 4.0, který využívá cloud, automatizaci, umělou inteligenci a internet věcí. Se sítěmi 5G přichází větší spoléhání na cloud a okrajová počítačová zařízení, čímž vzniká vysoce distribuované prostředí, které zahrnuje infrastruktury různých dodavatelů a cloudů. Nativní zabezpečení Palo Alto Networks pro sítě 5G nabízí nejpodrobnější pravidla pro nativně cloudové 5G jádro, distribuované okrajové cloudy a podnikové sítě 5G. Nativní zabezpečení pro sítě 5G nabízí jednoduchou a dokonale integrovanou bezpečnostní platformu, která využívá automatizaci, nativní orchestraci Kubernetes® a integraci s otevřenými API. Má tak velkou výhodu v provozní jednoduchosti. Na obranu před protivníky, kteří pracují při rychlostech 5G, i na prevenci známých a neznámých hrozeb v sítích 5G v globálním měřítku využijete automatizované poznatky o hrozbách, které používají strojové učení a jsou doručované cloudem. Získejte nové zdroje příjmů nabídkou služeb zabezpečení sítí 5G v podnikových podmínkách a MEC (Multi-Access Edge Computing).

Nativní zabezpečení pro sítě 5G podporují fyzické firewally PA-7000 Series a PA-5200 Series, virtuální firewally VM-Series pro virtualizované implementace 5G a CN-Series pro kontejnerové cloudově nativní implementace 5G. To znamená, že pokud už používáte uvedené NGFW, můžete stejnou platformu nadále používat na zabezpečení 5G infrastruktury poskytovatele služeb nebo podnikových sítí 5G.

SD-WAN

Bezpečné připojení poboček

Předplatné SD-WAN v rámci našich NGFW umožňuje snadno nasadit ucelenou architekturu SD-WAN s nativně integrovaným zabezpečením a konektivitou na světové úrovni. Pokud využijete integraci SD-WAN s řešením Prisma Access, můžete optimalizovat výkon a zlepšit uživatelský komfort. Prisma Access se navíc dá využívat i jako služba. V takovém případě odpadají komplikace spojené s vybudováním centrální SD-WAN infrastruktury pro jednotné připojení k internetu. Další možností je sestavit si celou vlastní SD-WAN infrastrukturu s využitím Palo Alto Networks NGFW.

PRISMA
BY PALO ALTO NETWORKS

Prisma

Prisma® je nejucelenější cloudové portfolio zabezpečení na trhu. Zrychlete svou digitální transformaci produktovou sadou navrženou pro zabezpečení dnešních cloudů před budoucími hrozbami.


Prisma SaaS


Prisma SD-WAN


Prisma Access


Prisma Cloud

Prisma Cloud

Zabezpečení a shoda aplikací SaaS s předpisy

Prisma SaaS umožňuje bezpečné využívání cloudových služeb tím, že poskytuje konzistentní přehled, kontrolu nad dodržováním předpisů a zabezpečení cloudových aplikací (SaaS) a citlivých dat v cloudu. Pomáhá minimalizovat využívání stínového IT, zabezpečit přístup k podnikovým SaaS aplikacím jako Microsoft 365™, Salesforce®, Google Workspace™, Slack® nebo Box a zmírňovat riziko úniku dat v cloudu.

Prisma SaaS chrání organizace a jejich data před kybernetickými riziky v cloudu, aby mohly bezpečně využívat SaaS aplikace a bezpečně ukládat citlivá data v cloudu. Coby integrovaná funkční součást NGFW Palo Alto Networks je služba úzce provázaná se zabezpečením celé společnosti. Umožňuje optimalizované nasazení, které překonává nesystematický přístup dílčích kontrolních prvků jako zprostředkovatel zabezpečení přístupu ke cloudu (CASB).

Prisma SD-WAN

Bezpečné cloudové řešení poboček

Prisma SD-WAN je první řešení SD-WAN na trhu, které umožňuje bezpečné cloudové zajištění poboček. Poskytuje až 243% návratnost investice. Na rozdíl od starších řešení SD-WAN, se kterými jsou spojené vysoké náklady a zbytečné komplikace, zajišťuje Prisma SD-WAN výjimečný uživatelský komfort díky zásadám definovaným podle aplikací. Zjednodušuje síťové a bezpečnostní operace strojovým učením a automatizací.

Prisma Access

Cloudové zabezpečení mobilních uživatelů

Prisma Access proměňuje zabezpečení sítí nejucelenější cloudovou platformou svého druhu, a tak organizacím umožňuje bezpečně podporovat vzdálené pracovníky. Starší řešení zabezpečení sítí nedokážou zprostředkovat přístup a zajistit ochranu pro všechny aplikace – naopak mají v bezpečnostním pokrytí výrazné mezery a nepodporují práci odkudkoli tak spolehlivě, jak organizace vyžadují. Jedině Prisma Access plně prověřuje veškerý provoz aplikací – webových, newebových i šifrovaných pomocí SSL/TLS – obousměrně na všech portech, ať komunikují s internetem, cloudem, datovým centrem, nebo mezi pobočkami. Snižuje tak pravděpodobnost úniku dat o 45 %.

Navíc má Prisma Access ucelenější bezpečnostní pokrytí než jakékoli jiné řešení. Do jediné platformy konsoliduje celou řadu dílčích produktů, mezi které patří firewall jako služba (FWaaS), přístup k sítím založený na modelu Zero Trust (ZTNA), CASB, bezpečná webová brána (SWG) a další. Všechny komponenty se přitom spravují z jediné konzoly. Prisma Access staví na masivně škálovatelné síti, která využívá kombinovanou infrastrukturu Amazon Web Services (AWS®) a Google Cloudu s více než 100 přístupovými body v 76 zemích. Díky tomu Prisma Access poskytuje mimořádně nízkou latenci podpořenou špičkovou úrovní SLA. Koncoví uživatelé se tak můžou spolehnout na skvělou digitální zkušenost.

Prisma Cloud

Nativní platforma cloudové bezpečnosti

Prisma Cloud je komplexní nativně cloudová zabezpečovací platforma (CNSP) s nejširším pokrytím zabezpečení a shody s předpisy na trhu pro celou nativně cloudovou technologickou infrastrukturu, aplikace a data v hybridních i multicloudových prostředích. Prisma Cloud chrání nativní cloudové aplikace napříč hostitelskými počítači, kontejnery, bezserverovými a dalšími cloudovými řešeními typu PaaS (platforma jako služba). Dynamicky zjišťuje nasazené zdroje a koreluje data poskytovaná cloudovými službami (konfigurace zdrojů, protokoly toků, auditní protokoly, protokoly hostitelů a kontejnerů atd.). Poskytuje tak vynikající postřehy o zabezpečení a shodě cloudových prostředí a aplikací s předpisy. Pomocí strojového učení profiluje chování uživatelů, pracovních úloh a aplikací pro účinnou prevenci pokročilých hrozeb.

Protože má nejúplnější knihovnu compliance frameworků na trhu, ohromně zjednodušuje zajištění shody. Prisma Cloud toho dosahuje hloubkovým sdílením kontextu, který zahrnuje infrastrukturu, PaaS, uživatele, vývojové platformy, data a aplikační úlohy. Dokonalá integrace s nástroji na orchestraci zabezpečení navíc zajišťuje rychlou nápravu zranitelností.

Pro zabezpečení celého životního cyklu se Prisma Cloud integruje s řetězci nástrojů DevOps a pomáhá se správou zranitelností. Pomocí široké sady DevOps pluginů, které zahrnují technologie IDE, SCM, CI a CD, můžou bezpečnostní týmy DevOps zabezpečit infrastrukturu a aplikace. Mají přitom pokryté šablony infrastruktury jako kódu (IaC), hostitele, systémové snímky a funkce.

CORTEX®
BY PALO ALTO NETWORKS

Cortex

Cortex® je nejkomplexnější portfolio produktů pro bezpečnostní operace na trhu, které poskytuje podnikům špičkovou správu povrchů vystavených útokům spolu s vynikajícími detekčními, vyšetřovacími, automatizačními a reakčními funkcemi.

AutoFocus

Cortex XDR

Cortex XSOAR

CRYPSIS™
A PALO ALTO NETWORKS COMPANY

Crypsis

CORTEX® XPANSE™
BY PALO ALTO NETWORKS

Cortex XPANSE

AutoFocus

Cortex Kontextové informace o hrozbách

Služba AutoFocus™ poskytuje okamžitý přístup k masivnímu úložišti kontextových informací o hrozbách, který se dá odebírat jako feed. Informace do služby proudí z rozsáhlé sítě koncových bodů a cloudových informačních zdrojů, takže podává jedinečný vhled do útoků probíhajících v reálném světě. Informace o každé hrozbě doplňuje hluboký kontext od renomovaných výzkumníků Unit 42. Feed informací o hrozbách a agilní API pro přístup z jakéhokoli nástroje ušetří vašim analytikům spoustu času.

Cortex XDR

Rozšířená detekce a reakce

Cortex XDR™ je první rozšířená platforma detekce a reakce na trhu, která zahrnuje klíčové zdroje bezpečnostních dat a pomáhá zastavovat moderní útoky. Pomocí inteligentního seskupování upozornění a skórování incidentů vám Cortex XDR pomůže odhalit reálné hrozby v šumu velkého množství přicházejících provozních informací. Zbytečně komplikované a roztříštěné bezpečnostní produkty může váš tým nahradit jednotnou platformou pro prevenci, detekci, vyšetřování a reakci.

Cortex XDR neprůstřelnou ochranou koncových bodů automaticky blokuje útoky a přesně detekuje hrozby ve vašem prostředí pomocí behaviorální analytiky. Poskytuje ucelený obrázek o každém incidentu a odhaluje kořenovou příčinu, takže můžete hrozby vyšetřovat až osmkrát rychleji než dřív. Toto jedinečné řešení zjednodušuje všechny fáze bezpečnostních operací od třídění upozornění až po cílený lov hrozeb. Pomáhá tak nahradit nedostatek vysoce zkušených bezpečnostních analytiků a výrazně šetří čas potřebný k rozpoznávání hrozeb a reakcím na ně. Úzká integrace s vynucovacími body zrychluje reakci a umožňuje zastavit ty nejzákeřnější útoky ještě předtím, než stihnou napáchat škody.

Cortex XSOAR

Rozšířená bezpečnostní koordinace, automatizace a reakce

Cortex XSOAR zvyšuje účinnost SOC nejkomplexnější platformou SOAR (bezpečnostní koordinace, automatizace a reakce) na trhu. Manažeři zodpovědní za zabezpečení můžou transformovat všechny aspekty operací jednotným přístupem ke správě incidentů, automatizaci, spolupráci v reálném čase a zpracování informací o hrozbách. Týmy můžou spravovat upozornění napříč všemi zdroji, standardizovat procesy pomocí scénářů (playbooks), jednat na základě informací o hrozbách a automatizovat reakci pro každý bezpečnostní incident. Výsledkem je o 90 % rychlejší odezva a 95% pokles počtu upozornění, která vyžadují lidskou intervenci.

Crypsis

Služby reakce na incidenty

Crypsis Group, dceřiná společnost Palo Alto Networks, je poradenská firma, která poskytováním nejkvalitnějších reakcí na incidenty, služeb správy rizik a digitálních forenzních služeb pracuje na vytváření bezpečnějšího digitálního světa. Pomáháme našim klientům s účinnou obranou před nejvážnějšími kybernetickými hrozbami. Naše schopnost globální reakce, neustálé technologické inovace a elitní odbornost na poli kybernetického zabezpečení nám umožňují udržovat si náskok před rychle se vyvíjejícími hrozbami.

Cortex XPANSE

Správa povrchů vystavených útokům

Cortex XPANSE je platforma automatizované správy povrchů vystavených útokům (ASM), která poskytuje ucelenou a přesnou inventarizaci globálních prostředků organizace, které jsou přístupné z internetu, a chybných konfigurací. Pomáhá tak průběžně odhalovat, vyhodnocovat a omezovat povrchy vystavené útokům zvenčí, upozorňovat na rizikovou komunikaci, vyhodnocovat rizika na straně dodavatelů a posuzovat zabezpečení při nákupech a slučování společností.