WHITEPAPER

Sådan får du:
Enkel og effektiv sikkerhed – allerede i browseren

paloalto NETWORKS

conscia

Sådan får du:
Enkel og effektiv sikkerhed – allerede i browseren

Langt de fleste virksomheder har sat cybersikkerhed højt på dagsordenen hos både direktion og bestyrelse. Men disciplinen gøres ofte mere kompleks, besværlig og kostbar, end den behøver at være.

I dette whitepaper ser vi på en løsning fra Palo Alto Networks, som rykker avanceret og effektiv sikkerhedsteknologi direkte ind i browseren. Samtidig tilbyder den en enkel og effektiv metode til både at sikre virksomheders digitale aktiver og minimere risikoen for ødelæggende angreb.

På trods af dét, ligner og fungerer løsningen Prisma Access Browser i nærmest enhver henseende som en helt almindelig Chrome-browser.

Vigtigst er, at den er hurtig at konfigurere, implementere og administrere. Den kan også løfte hovedparten af de opgaver, du hidtil formentlig har løst med omkostningstunge, besværlige og ofte langsomme VDI-løsninger (Virtual Desktop Infrastructure).

Dette whitepaper giver indsigt i, hvordan Prisma Access Browser kan styrke din virksomheds sikkerhedsinfrastruktur, lette administrationen og reducere omkostninger – alt sammen uden at trække på tålmodigheden hos hverken jeres interne eller eksterne brugere.

God læselyst!

Sådan løser du flere sikkerheds-udfordringer på samme tid

Der er mange prioriteter at tage hensyn til i sikkerhedsarbejdet. Først og fremmest vil man gerne beskytte kritisk infrastruktur og følsomme data. Men det er også en prioritet at sikre, at dine brugere har optimale muligheder for at løse opgaver enkelt, hurtigt og problemfrit – uanset hvor de befinder sig, eller hvilken enhed, de anvender.

Det er en helt relevant overvejelse at gøre sig: mange organisationer har vitterlig konkrete udfordringer med at balancere kravene til høj sikkerhed mod behovet for produktivitet og smidige skift mellem talrige systemer og cloudservices.

Her kommer Prisma Access Browser ind i billedet:

Browseren adresserer både risikoen for datalækager, udfordringen med ineffektiv og tidsrøvende adgangskontrol samt høje omkostninger til sikkerhedsinfrastruktur. Samtidig bliver du i stand til at implementere og løbende tilrette sikkerhedspolicies, så forretning, data og medarbejdere beskyttes bedre.

Grænsefladen er identisk med en helt almindelig Chrome-browser og giver brugerne nem adgang til at tilgå onlineressourcer som fx Microsoft eller ERP-system præcis som de plejer.

Men bag kulisserne leverer browseren et robust sikkerhedslag baseret på Zero Trust-principper – synkroniseret med virksomhedens Active Directory – der kun giver brugere adgang til de ressourcer og data i virksomheden, som de er autoriserede til. Ligeledes trækker den på kontinuerlig scanning af links for blandt andet at minimere risiko for phishing.

Udvidede sikkerhedsfeatures med Prisma Access Browser

Ved at udvide Zero Trust til browseren Prisma Access Browser, integreres Zero Trust Network Access hvilket transformerer traditionel sikkerhed ved ikke at antage nogen iboende tillid til brugere eller enheder. Disse ZTNA 2.0-funktioner muliggør granulær og identitetsbaseret adgangskontrol direkte i browseren, hvilket forbedrer sikkerheden og minimerer eksponeringen for trusler.

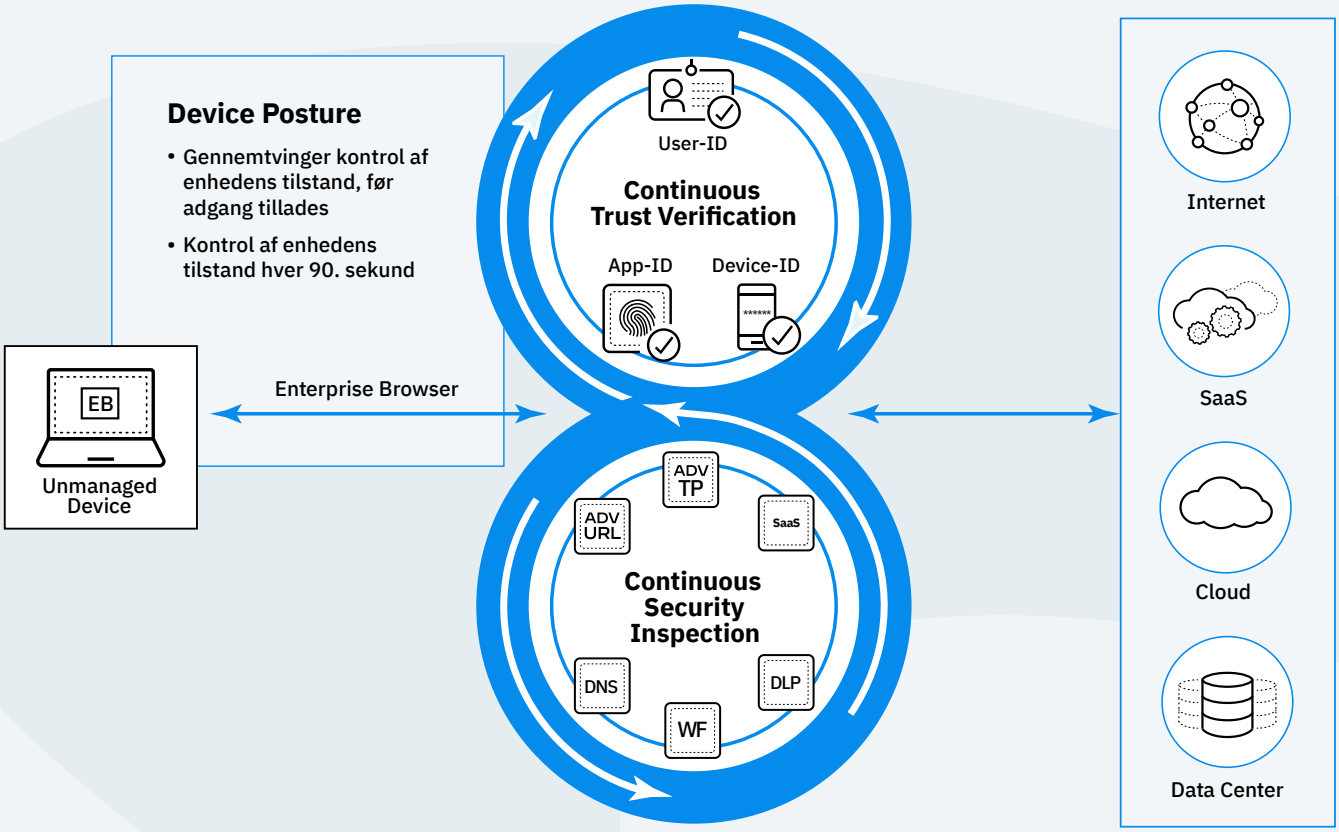
Det er med til at sikre, at virksomheden markant reducerer risikoen for datalækager og cyberangreb, samtidig med at produktiviteten blandt medarbejderne bibeholdes.

Prisma Access Browser bruger Prisma Access Continuous Trust Verification til at levere finjusteret, mindst privilegeret adgang, dyb og kontinuerlig sikkerhedsinspektion samt Prisma Access Continuous Security Inspection til at tilbyde et komplet spektrum af sikkerhedstjenester, herunder avanceret trusselsforebyggelse, avanceret URL-filtrering, DNS-sikkerhed, sandboxing og mere.

Opret en sikker arbejdsplads på enhver enhed; Prisma Access Browser skaber et sikkert miljø for webbrowsing ved at beskytte browserens aktiver, runtime og overflade mod sårbarheder og angreb. Denne omfattende beskyttelse sikrer, at alle onlineaktiviteter og data i browseren er isoleret fra webbaserede trusler og trusler fra kompromitterede enheder.

Zero Trust – Prisma Access Browser vs. Forbrugerbrowser	
Forbrugerbrowser	**Prisma Access Browser**
Ingen kontrol af enhedens tilstand, hvilket øger risikoen for kompromitterede enheder og følsomme oplysninger.	Gennemfører streng kontrol af enhedens tilstand, før adgang gives, ved brug af kontinuerlig tillidsverifikation og sikkerhedsinspektioner for at sikre overholdelse og minimere risici.
Undlader at bekræfte brugerens identitet for handlinger, hvilket øger sårbarheden over for identitetsbaserede angreb.	Integrerer just-in-time MFA og giver et ekstra sikkerhedslag for ultrasensitive handlinger.

Prisma Access Browser muliggør kontinuerlig tillidsverifikation og sikkerhedsinspektion for ikke-administrerede enheder.



Sikker arbejdsplads – Prisma Access Browser vs. Forbrugerbrowsere	
Forbrugerbrowser	**Prisma Access Browser**
Browseraktiver	
Ikke alle browseraktiver er krypterede, og de, der er, kan nemt omgås.	Et ekstra krypteringslag beskytter alle browseraktiver med en betroet krypteringskæde, der er uafhængig af operativsystemet.
Trusselsaktører kan spoofe operativsystemet for at dekryptere browseraktiver.	Implementerer sikkerhedsforanstaltninger specielt designet til at modvirke spoofingforsøg og forhindre uautoriseret adgang til krypterede browseraktiver.
Browser runtime	
Mangler beskyttelse mod endpoint-malware, der målretter browseren.	Indbygget beskyttelse mod keyloggere og forsvar mod screen scrapers.
Kan ikke afbøde risici fra interne forsøg på at manipulere browserens hukommelse.	Implementerer kontroller for at beskytte browser-hukommelse mod manipulation og sikre integriteten af runtime-operationer.
Overafhængighed af endpoint-certifikater gør browseren sårbar over for potentielle angreb på certifikater.	Forbedrer sikkerheden ved at beskytte mod manipulation af enhedscertifikater, hvilket reducerer risikoen på certifikatniveau.
Browserens overfladeområde	
Komponenter er sårbare over for angreb.	Tillader deaktivering eller kontrol af sårbare browserkomponenter på ubeskyttede websites og mindsker eksponering for kendte sårbarheder.
Inkluderer kun minimale sikkerhedskontroller mod ondsindede udvidelser.	Giver fuld kontrol over installerede udvidelser og deres tilladelser, og sikrer, at udvidelser, der kan få adgang til følsomme oplysninger, bliver korrekt administreret og kontrolleret.

Nemt at implementere og tilpasse sikkerhedspolicies

En af de mest bemærkelsesværdige egenskaber ved Prisma Access Browser er løsningens evne til at automatisere sikkerhedsforanstaltninger, især når det gælder beskyttelse af følsomme data – også kaldet Data Loss Prevention (DLP). Som administrator kan du nemt konfigurere og håndholde policies, der fx slører persondata, gør det umuligt at tage skærmbilleder eller begrænser videresendelse af fortrolig information såsom datasæt knyttet til din virksomheds kunder eller til jeres produktudvikling.

Hermed minimerer du i betydelig grad risikoen for, at følsomme oplysninger distribueres uden for virksomheden. Eksempelvis kan data som CPR-numre eller finansielle oplysninger automatisk maskeres i realtid, hvis de forsøges delt uden for godkendte kanaler.

Denne funktionalitet gør tillige op med en relativt ny og stadig mere påtrængende udfordring. Nemlig at brugere ad vanvare potentielt kommer til at eksponere følsomme data for omverdenen, når de lader fortrolige datasæt eller interne rapporter bearbejde ved hjælp af en ekstern, generativ AI som fx ChatGPT. Her kan ingen med sikkerhed vide, om de samme data ”genbruges” i et svar på et spørgsmål, andre brugere uden for virksomheden måtte stille.

Synlighed	Compliance dashboard	Detaljerede logs	Risikominimering
• Kortlæg GenAI-apps i brug – både godkendte og uofficielle (shadow AI). • Identificer udvidelser, der anvender GenAI.	• Overvåg brug af GenAI og politikker i henhold til regler og lovgivning. • Identificer compliance-regler og potentielle forstyrrelser. • Eksporter en compliancerapport	• Detaljerede logs • Gennemgå alle Gen-AI-prompt og svar. • Efter prompt-type: indgående, udgående. • Efter brugerrejse: kopieret ind, kopieret ud, indtastet, delt skærm.	• Beskyt mod ondsindede prompts og jailbreak-forsøg.

Omfattende indsigt og trends: uofficielle GenAI-apps, de 10 mest aktive brugere, der interagerer med AI, mest anvendte GenAI baseret på dataeksponering.

Prisma Access Browser gør det således muligt at håndhæve sikkerhedspolitikker konsistent på tværs af alle medarbejdere uanset hvilke enheder de arbejder fra – eller om de befinder sig inden for virksomhedens netværk eller arbejder hjemmefra.

Dette reducerer alt andet lige risikoen for både internt eller eksternt funderede databrud og gør det muligt at opretholde selv strenge compliance-krav uden at påvirke brugernes arbejdsgange negativt.

Reducér omkostninger og afhængighed af VDI-løsninger

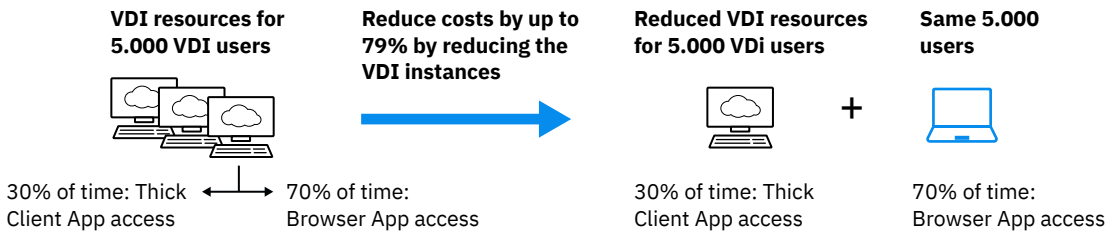
Traditionelle VDI-løsninger (Virtual Desktop Infrastructure) har længe været det primære værktøj, når man ville give brugerne sikker fjernadgang til virksomhedsressourcer. Disse løsninger er dog ofte forbundet med høje omkostninger, kompleks opsætning og administration samt ofte også lange svartider.

Prisma Access Browser eliminerer disse udfordringer ved at tilbyde en løsning, der knytter systemadgange og datakontrol til en sikker og let konfigurérbar enterprise-browser – som ydermere trækker på hver enkelt brugers lokale systemressourcer. Det forøger ydeevnen i betydelig grad og minimerer udfordringen med lange svartider.

Eksempler på VDI Reduktion
Prisma Access Browser reducerer i høj grad afhængigheden af VDI-ressourcer ved at flytte almindelige browsingaktiviteter til virksomhedens browser. Eksempler inkluderer:

- Ressourceoptimering: Prisma Access Browser mindsker behovet for VDI-ressourcer betydeligt, da alle almindelige browsingaktiviteter overføres til virksomhedens browser. Fx hvis en typisk VDI-bruger tidligere brugte 70 % af deres tid på browseren og 30 % på tunge klienter, vil VDI-ressourcer kun være nødvendige til 30 % af denne brugers arbejde.

Med Prisma Access Browser kan organisationen minimere sine VDI implementering

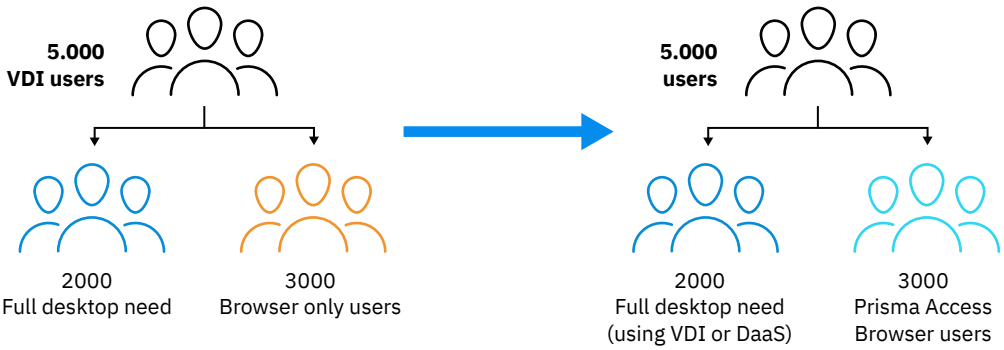


Segmenterede brugergrupper: Ikke alle brugere har behov for fuld desktopadgang eller adgang til tunge klientapplikationer. Ved at kategorisere brugere i grupper som enten browser-only eller fuld desktop kan organisationer effektivisere VDI-udrulninger og dermed reducere omkostningerne ved større VDI-implementeringer.

Erfaringer fra nogle af de første Prisma Access Browser-kunder viser, at man på koncernniveau kan reducere VDI-omkostninger med op mod 60 % og samtidig give brugerne en bedre og mere smidig oplevelse. Primært fordi kun kritiske applikationer forbliver på VDI, mens resten håndteres i browserregi.

Hertil kommer afledte – men sværere kvantificérbare – gevinster i form af en mere strømlinet infrastruktur, fordi man bliver i stand til at mindske behovet for løbende investeringer i og vedligehold af VDI-relateret hardware.

Med Prisma Access Browser kan organisationen minimere sine VDI implementeringer



Sikkerhed med brugervenlighed i centrum

En af de mest centrale fordele ved Prisma Access Browser er dens evne til at levere en problemfri oplevelse for brugerne. Browseren fungerer som enhver anden browser, men med avancerede sikkerhedsforanstaltninger, der kører i baggrunden. Det betyder, at medarbejdere kan udføre deres arbejde uden forstyrrelser eller behov for hyppige skift mellem forskellige systemer.

Det gør det lettere for medarbejderne at tage løsningen til sig, fordi den ikke kræver ændringer i daglige arbejdsgange. Vel at mærke samtidig med administratorer lettere kan sikre, at data håndteres i overensstemmelse med både interne politikker og regulative krav fx GDPR.

Som administrator får du med Prisma Access Browser adgang til et centraliseret dashboard, hvor du kan definere, administrere og distribuere alle sikkerhedspolitikker ud til de forskellige brugergrupper i virksomheden. Det reducerer den tid og de ressourcer, der normalt kræves for at vedligeholde et komplekst IT-miljø, og gør det samtidig lettere at tilpasse og strømline sikkerhedsniveauet på tværs af organisationen.

Dertil kan du direkte i browseren definere hvilke applikationer, der må eller ikke må hentes ned. Dette minimerer i betydeligt omfang udfordringen med, at medarbejderne downloader og anvender ikke sanktionerede og potentielt usikre applikationer i virksomhedsregi – såkaldt ”shadowware.”

The Depth and Breadth of Prisma Access Browser

Secure Environment		Last-Mile Data and Identity Controls		User-First Workspace	
Device isolation	Advanced URL filtering	>1K data classifiers	Watermarks	Private app access	
Keylogger protection	Multilayered anti-phising	ML, OCR, EDM, IDM	Screenshot/sharing control	SSH/RDP support	
Screen scrapers protection	Advanced malware prevention	Regulation profiles	Camera/mic control	Sync across devices	Quick offboarding
Trusted certificate store	Advanced threat protection	Directional-based DLP	Login restrictions	App acceleration	User privacy
Network security and isolation	Extension visibility and protection	Any control on any app	Tenant restrictions	Extension management	Productivity suite
Device posture	Audit trails	File protection	Password manager	Automated DEM	Integrated apps
Browser hardening	User timeline	Clipboard control	Step-up MFA	Enterprise branding	Deploy in minutes
Anti-tampering	Session recording	Typing guard	Passkeys	Internet Explorer mode	Zero infra changes
Attack surface reduction	Threat hunting and forensics	Data masking	Admin approval	Secure AI assistant	
Browser isolation	Shadow IT	Printing control	Just-in-time	SSO integration	

Cross-platform intergrations: SIEM | SOAR | IdP | ZTNA | EDR | Threat intel | Asset management

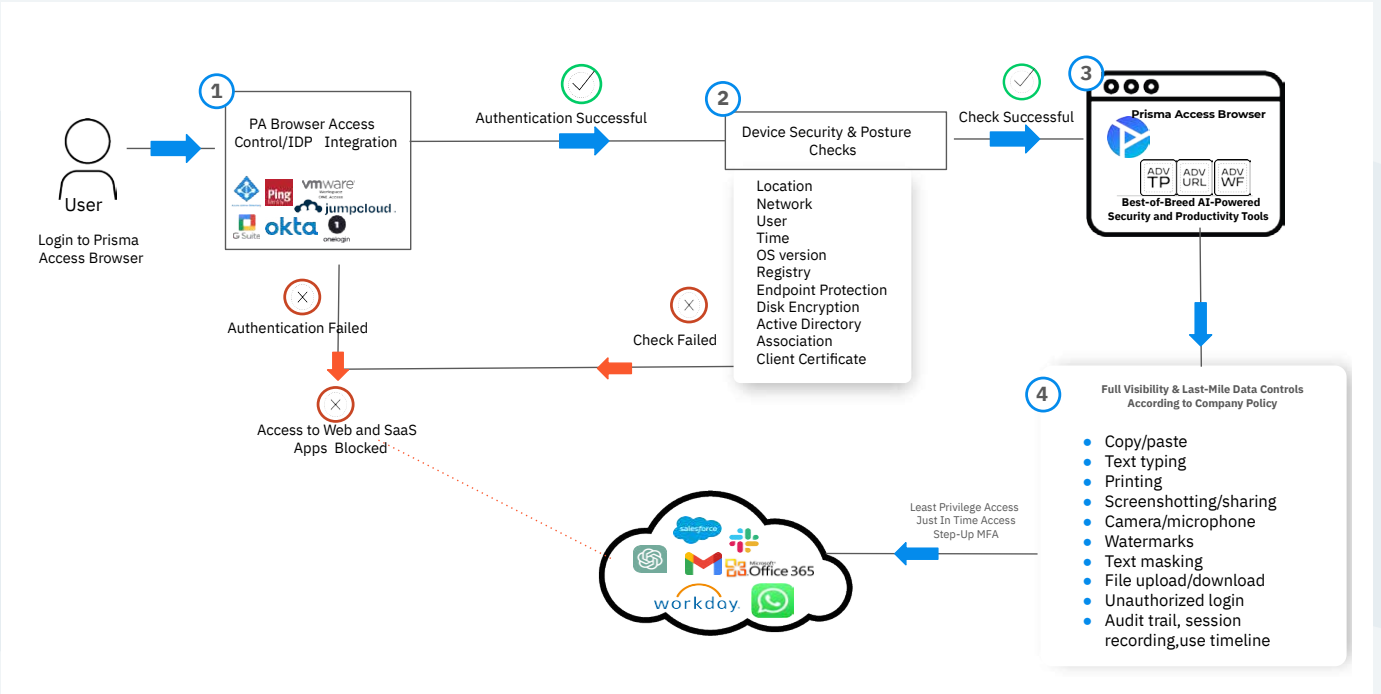
Granulær adgangskontrol og effektiv governance

En vigtig pointe ved Prisma Access Browser er, at løsningen giver virksomheder mulighed for at implementere granulær adgangskontrol, hvor man udelukkende giver brugerne adgang til de ressourcer, de har brug for. Det er særligt vigtigt for organisationer med strenge compliance-krav, hvor det er essentielt at minimere risikoen for uautoriseret adgang til følsomme informationer.

Hermed bliver det nemt for blandt andet forsknings- og udviklingstunge virksomheder at begrænse adgang til specifikke datafiler baseret på brugernes roller og deres geografiske placeringer. Det sikrer, at man hele tiden har overblik over og kontrol med de pågældende datasæt og systemer – og samtidig sikrer, at forskningsansatte har nem og uhindret adgang til de pågældende ressourcer.

Tilsvarende kan browserens adgangskontrolfunktioner tildele specifikke rettigheder baseret på brugerens rolle, afdeling eller – som nævnt – geografiske placering. For eksempel kan en ekstern konsulent få adgang til præcis det begrænsede antal applikationer, der gør det muligt at løse en specifik opgave, mens interne medarbejdere har mere omfattende rettigheder. Denne fleksibilitet giver organisationer mulighed for at opretholde en høj grad af sikkerhed uden at påvirke produktiviteten negativt.

How Prisma Access Browser works



Investér i en fremtidssikret sikkerhedsinfrastruktur

Sigtet med Prisma Access Browser er, som nævnt, dels at imødekomme en række sikkerhedsudfordringer og samtidig minimere behovet for både tidskrævende administration og investeringer i hardware til drift af bl.a. VDI.

Kombineret med løbende opdateringer og integration med Palo Alto Networks øvrige sikkerhedsportefølje kan virksomheder være sikre på, at deres sikkerhedsinfrastruktur altid er opdateret og klar til at håndtere nye trusler.

Integrationen med Palo Alto Networks' avancerede Precision AI trusselsintelligens gør det muligt for virksomheder at reagere proaktivt på nye typer angreb. Det bliver fx lettere at reagere hurtigt og i mange tilfælde automatisk, når nye trusler – såsom en omfattende bølge af phishing-angreb – rammer.

Drevet af Palo Alto Networks Precision AI™

HVER DAG

7,6 PB+ trusseldata indsamlet fra 70.000+ kunder.
Træner kontinuerligt **4.400+ ML-modeller** for præcis og omfattende beskyttelse.

~2,3M
Nye og unikke angreb identificeret.

237K
Nye og unikke ondsindede filer forhindret.

112M
Ondsindede URL'er blokeret.
76 % opdaget 24 timer før andre leverandører.

~11,3
milliarder angreb blokeret.

35
millioner nye filer analyseret.

32
milliarder nye URL'er analyseret.

- **Beskyt følsomme data direkte, hvor de tilgås**

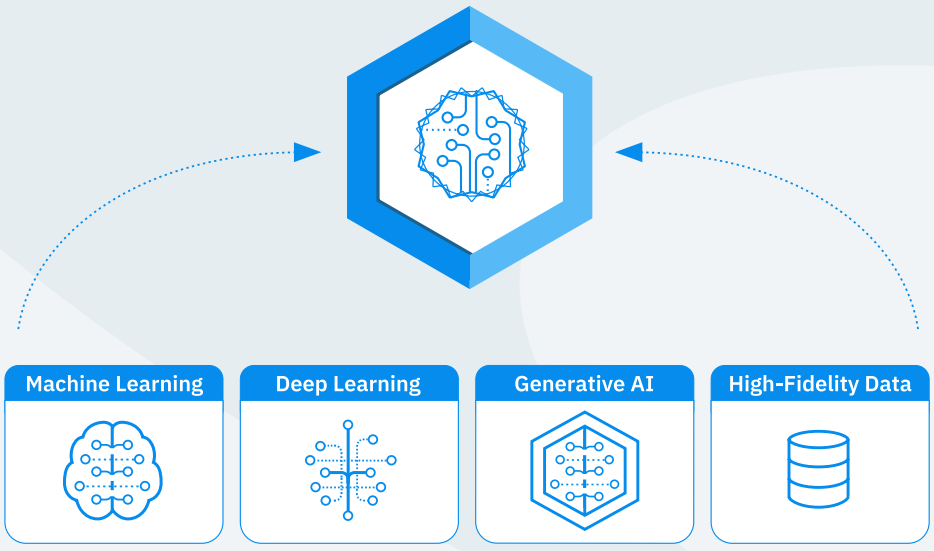
  Prisma Access Browser integrerer browserbaseret datatabsforebyggelse for at beskytte følsomme oplysninger i browsermiljøet. Denne funktion forhindrer proaktivt uautoriseret deling, overførsel eller lækage af følsomme data og sikrer overholdelse af lovkrav og virksomhedens datapolitikker.

Databeskyttelse - Prisma Access Browser vs. Forbrugerbrowsere	
Forbrugerbrowser	**Prisma Access Browser**
Ingen mulighed for at maskere følsomme data.	Maskerer følsomme data dynamisk baseret på indhold og kontekst, hvilket sikrer, at fortrolige oplysninger forbliver beskyttede.
Sårbar over for dataeksfiltrering gennem skærmbilleder, deling, kopiering/indsætning og print.	Blokerer for skærmbilleder, deling via samarbejdsværktøjer, kopiering/indsætning og print med konfigurerbare vandmærker på følsomme skærme for at forhindre uautoriseret optagelse.
Minimal kontrol over filbevægelser, hvilket kan føre til uautoriserede dataoverførsler.	Håndterer filoverførsler med kryptering til downloads fra virksomhedsapps og blokerer uploads til personlige drev. Begrænser desuden fil down- og uploads baseret på indhold og kilde, hvilket sikrer, at filer kun bevæger sig inden for godkendte kanaler.

- **Udnyt AI-drevne sikkerhedstjenester**

  Precision AI™ fra Palo Alto Networks er det proprietære AI-system, der hjælper sikkerhedsteams med at opnå pålidelige resultater ved at bruge omfattende data og sikkerhedsspecifikke modeller til at automatisere detektion, forebyggelse og afhjælpning med branchens førende nøjagtighed.

  Precision AI intregrerer de bedste AI-egenskaber, herunder maskinlæring, dyb læring, generativ AI og mere.



- **Machine Learning**
  Machine learning giver mulighed for præcist og automatisk at forudsige, forebygge og afhjælpe sikkerhedsproblemer ved at bruge konkrete data som input til at forudsige nye situationer.

- **Deep learning**
  Deep learning hjælper med at opbygge forudsigende modeller til at identificere og opdage sikkerhedsproblemer i realtid ved at lære fra store mængder sikkerhedsdata.

- **Generative AI**
  GenAI giver værktøjerne evnerne til at "tale menneskesprog" så store mængder trusselsintelligens kan blive opsummeret og leveret igennem copilots.

- **Forbedret nøjagtighed med høj-præcisionsdata**
  Modeller trænes kontinuerligt på risikodata fra 70.000 kunder og AI-drevne trusler for at identificere avancerede, undvigende og hidtil usete trusler.

- **Trusselsdetektion og forebyggelse i realtid**
  Analyserer netværkstrafik i realtid og stopper straks kendte, ukendte og stærkt undvigende trusler for at forhindre "patient nul."

- **Konsistent levering overalt**
  Leverer omfattende og realtidsbeskyttelse konsekvent via en robust global infrastruktur.

  Dette skaber en ekstra sikkerhedsbarriere, der beskytter virksomhedens data mod både eksterne trusler og mod interne lækager – hvad enten de er tilsigtede eller resultat af uforsigtighed.

Drag konkret fordel af et strategisk partnerskab

Når du vælger at implementere **Prisma Access Browser,** vælger du ikke blot en teknologi, men en løsning understøttet af ekspertise fra to førende aktører: Palo Alto Networks og deres stærke og holistiske tilgang til sikker teknisk infrastruktur og Conscia, der stiller dyb forståelse for disse løsninger kombineret med sikkerhedsudfordringer til rådighed.

Conscia leverer i den forbindelse ikke kun teknisk implementering af **Palo Alto Networks'** løsningsportefølje, men arbejder sammen med din organisation for at sikre, at løsningen tilpasses din virksomheds unikke forretningsbehov. Hvad enten du køber ind på hele porteføljen eller udvalgte elementer såsom **Prisma Access Browser.**

Kontakt os, og hør mere om, hvordan vi kan hjælpe dig med at øge sammenhængen og effektiviteten af din virksomheds sikkerhedsinfrastruktur

Kontakt

Kristian von Staffeldt
Security Evangelist
Conscia Danmark

kvs@conscia.com
+45 61332373

conscia.com/dk

conscia