

VIPRE kombinerar över tjugo års avancerad säkerhetsintelligens med banbrytande maskininlärning, beteendeanalys i realtid och ett djupt, ständigt lärande hotunderrättelsenätverk till ett kraftfullt verktyg för att försvara sig mot dagens attacker och även morgondagens nolldagssårbarheter.

VIPRE ENDPOINT SECURITY CLOUD: NÄSTA GENERATIONENS ENDPOINT SECURITY PÅ ETT ENKELT SÄTT

VIPRE Endpoint Security Cloud är en kraftfull, helt anpassningsbar molnbaserad skyddsplattform för slutpunkter som gör det möjligt för företag att skydda sig mot sårbarheter i Microsoft® Windows® eller Apple® macOS®-slutpunktsenheter.

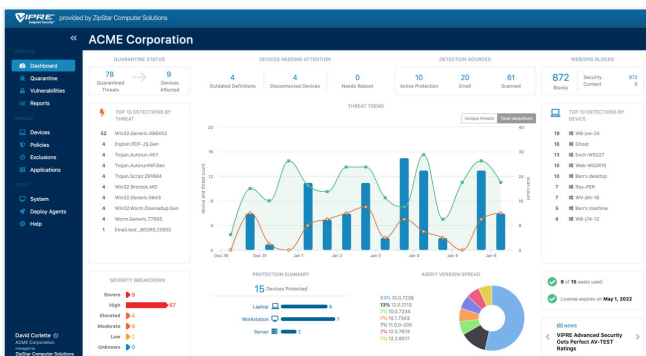
Förenklad Endpoint Security-skydd i flera lager Skyddar mot attacker mot fil-, program- och nätverkslager. VIPRE Endpoint Security Cloud kombinerar flera säkerhetslager med nätverks- och programagnostiskt DNS-skydd utan extra kostnad. Genom kraftfull teknik som signaturbaserad detektering, heuristisk analys och beteendeanalys, fångar VIPRE Endpoint Security Cloud proaktivt upp även noll dagarshot. Det bästa av allt är att lösningen är flexibel och optimerar produktivitet och säkerhet.

Systemhärdning och hotsynlighet Patch- och sårbarhetshantering bidrar till att öka synligheten för de risker som utgörs av tredjepartsprogram inom din organisation, prioriterar vilka svagheter och sårbarheter som ska åtgärdas och levererar sedan inbäddad patchhantering för att hindra upptäckta sårbarheter automatiskt eller med ett enkelt klick. Hindra andra attacker med intrångsskydd, DNS-skydd och webbadressblockerare. Minska din attackyta och få synlighet med interaktiva visningar av hot.

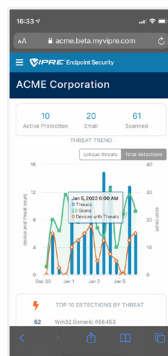
Modernt skydd i en förenklad modell VIPRE Endpoint Security Cloud effektiviserar inte bara distributionen, konfigurationen och hanteringen av slutpunktssäkerhet utan möjliggör även flexibel, okomplicerad och intuitiv rapportering på alla skyddade slutpunkter med några enkla klick. Tydliga, lättförståeliga policyer och konfigurationsinställningar, tillsammans med intuitiv och effektiv administration, kan alla utföras från en central konsol. Interaktiv synlighet hjälper till att identifiera och rapportera om eventuella komprometterade slutpunkter, tillsammans med en mycket flexibel mekanism för hantering av problem. Få åtkomst varifrån som helst på en PC- eller mobilenhet, med vilken webbläsare som helst för att säkerställa oöverträffad detaljrikedom och synlighet, tillsammans med rapportering, från praktiskt taget vilken enhet som helst.

VIPRE Endpoint Security Cloud-funktioner

- ✓ Slutpunktsskydd och skydd mot utpressningsprogram
- ✓ DNS-skydd
- ✓ Aktivt filskydd
- ✓ Maskininlärning
- ✓ Aktivt processskydd
- ✓ Intrångsskyddssystem
- ✓ Hostintrångsskyddssystem
- ✓ Blockerare av skadlig webbadress
- ✓ E-postskydd
- ✓ Anitnätfske
- ✓ Brandvägg
- ✓ Låg CPU- och minnesanvändning
- ✓ Borttagning av tidigare installerat antivirusprogram
- ✓ Skydd mot webbexploatering
- ✓ Sårbarhetspatchning för program från tredje part
- ✓ Webbåtkomstkontroll (tillägg)

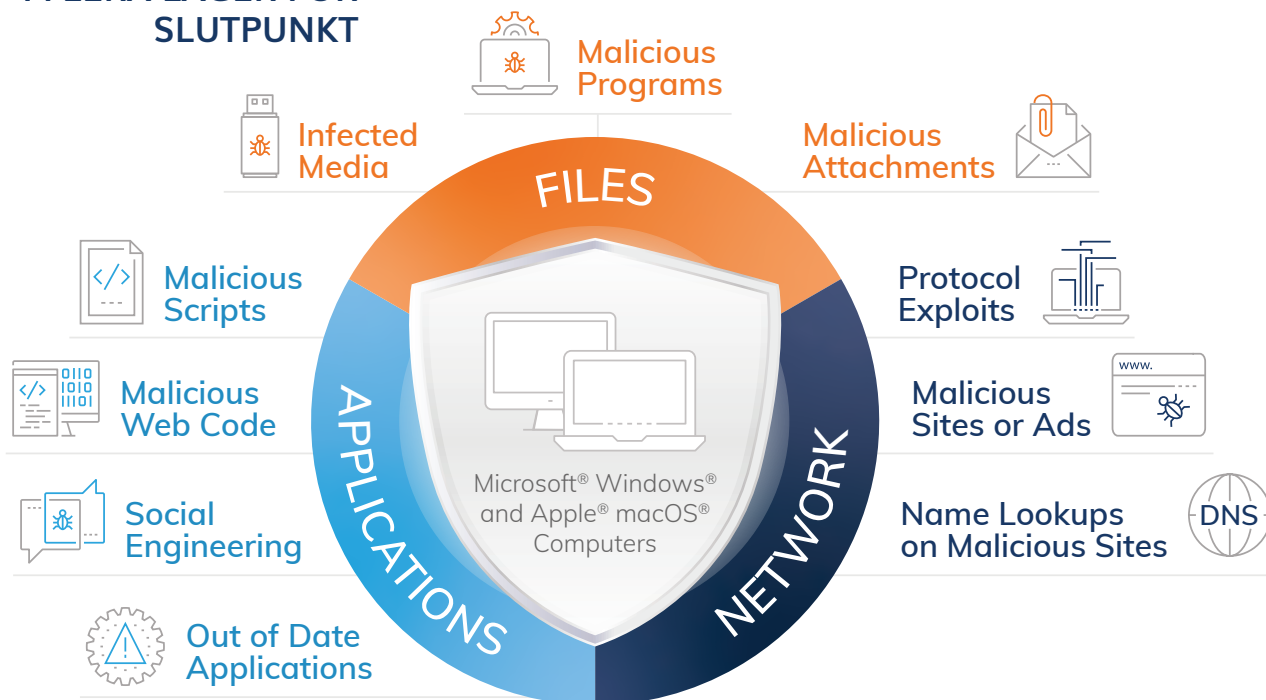


Skrivbordsvy på central konsol



Mobilvy på central konsol

SÄKERHETSSKYDD I FLERA LAGER FÖR SLUTPUNKT



FILLAGER

Hanterade skanningar	Automatisk och enkel manuell djupsökning efter skadliga filer, med detaljerad administrativ styrning och delegering
Aktivt filskydd	Interaktivt skydd av varje fil som berörs av systemet
Signaturbaserad detektering	Definitionsdatatabas som innehåller miljontals kända skadliga signaturer som uppdateras flera gånger om dagen
Emulering	Nystar upp och tolkar skadlig kod i en virtuell miljö för att snabbt upptäcka hot och fånga upp avancerad skadlig kod
Uteslutningar	Identifiera enkelt tillåtna filer och affärsprogram

PROGRAMLAGER

Hostinetrångsskyddssystem (HIPS)	Regelbaserat system som förhindrar skadliga processer från att utföra skadlig aktivitet
Aktivt processskydd	Utnyttjar maskininlärning för att interaktivt analysera processbeteende och detektera potentiellt skadlig aktivitet
Sårbarhetspatchning	Skanna, rapportera och uppdatera program från tredje part till senaste version

NÄTVERKSLAGER

Intrångsskyddssystem (IDS)	Letar efter misstänkta data i IP-ramdelen av paketet och utnyttjar fler än 8 000 regler, samt i själva programdatan
DNS-skydd	Förhindra användare från att av misstag besöka skadliga webbplatser genom att fånga upp DNS-frågor för de kända skadliga domänerna och ersätta det normala IP-adresssvaret med en omdirigering till vårt DNS-sinkhole
Blockering av skadlig webbadress	Förhindrar åtkomst till specifika webbadresser genom att kontrollera mot ett globalt hotunderrätelsenätverk som uppdateras med den senaste listan över kända skadliga webbadresser
Skydd mot webbexploatering	Letar efter potentiellt skadlig kod inbäddad på webbsidor – krypterad eller inte – med webbläsartillägg

UPPFYLL EFTERLEVNADSKRAV OCH OMSORGSPLIKT MED VIPRE:S WEB ACCESS CONTROL (TILLÄGG)

Öka de anställdas produktivitet genom att övervaka internetanvändningspolicyer med noggranna säkerhetsåtgärder och kontroller. Uppfyll arbetsgivarens omsorgsplikt för att skydda anställda från att se stötande innehåll på arbetsplatsen, samt upprätthålla HR-efterlevnad genom detaljerad rapportering på användar-, grupp- och platsnivå.

Funktioner

- Fler än 40 domänkategorier inklusive det mest riskfyllda innehållet som spel, hat, dejting, innehåll för vuxna med mera
- Heuristisk filtrering, tillåt/neka webbadress och signaturer säkerställer korrekt detektering
- Ständigt uppdaterade webbplatskategoriseringar

Fördelar

- Tillhandahåller enkel webbplatskategorisering och enkel fördefinierad filtrering, med anpassning efter behov
- Hjälper organisationer att efterleva krav och regler och tillhandahåller skyddsåtgärder för anställda som säkerställer att användarna inte utsätts för stötande eller olämpligt material
- Välj tidsblock under vilka policyn ska tillämpas

"Alla som är bekanta med den typen av virus förstår den potentiella skada det kan orsaka en organisation. När vår anställda dubbelklickade på cryptocker-filen förintade VIPRE den direkt."

Matt Bauer, McKernan Packaging Clearing House

- 1 <https://www.nytimes.com/2021/06/02/business/jbs-beef-cyberattack.html>
- 2 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report_Feb_Jul2021.pdf
- 3 IBM 2020: <https://www.ibm.com/security/data-breach>
- 4 Statista 2021: <https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/>
- 5 Verizon 2021: <https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf>

Eftersom din organisation utökar fler funktioner till molnet, är **VIPRE Endpoint Security Cloud** det bästa sättet för att inte bara komma före utan också ligga kvar steget före det föränderliga hotlandskapet.

TA REDA PÅ MER
OM VIPRE
SECURITY SERVICES



SLUTPUNKT



E-POST



UTBILDNING



NÄTVERK

FÖR MER INFORMATION gå in på www.global.vipre.com/sv/
ring +46 8-5000 94 20 eller skicka ett e-postmeddelande till
sales@VIPRE.com.

