VIPRE ENDPOINT SECURITY

Cloud-udgave

NEXT GEN ENDPOINT SECURITY MADE SIMPLE

Virksomheder anvender i stigende grad clouden i tillæg til kontoret, og i takt dermed udvikler sikkerhedstruslerne sig og bliver mere og mere sofistikerede, hyppige og omkostningstunge. Cyberkriminalitet har udviklet sig til at være en indbringende forretning, hvor de traditionelle værktøjer og metoder, der anvendes til at bekæmpe cyberkriminalitet, er utilstrækkelige i en cloud-centreret it-verden. Der kommer flere og flere dag 0-trusler, trojanske heste, ransomware og malware i takt med, at onde aktører - både kriminelle og nationalstater - angriber alle organisationer, uanset størrelse.

I 2020 rapporterede det amerikanske forbundspoliti FBI en stigning på 69 % i antallet af klager over cyberkriminalitet, hvilket svarer til over 4 mia. dollar (USD)[2] Det er ofte svært for virksomheder at afgøre, om en sårbarhed blot er et irritationsmoment eller kan have en katastrofal forretningsmæssig indvirkning. Det kompliceres yderligere af den tid og de værktøjer, der kræves for at holde sig ajour med de daglige nye trusler.

Endpoint security er ofte baseret på en uorganiseret samling af værktøjer fra forskellige leverandører, hvilket giver huller i beskyttelsen. De deraf følgende kaotiske opdateringsmekanismer gør, at organisationer konstant er et skridt bagud i forhold til både angribere og angreb.

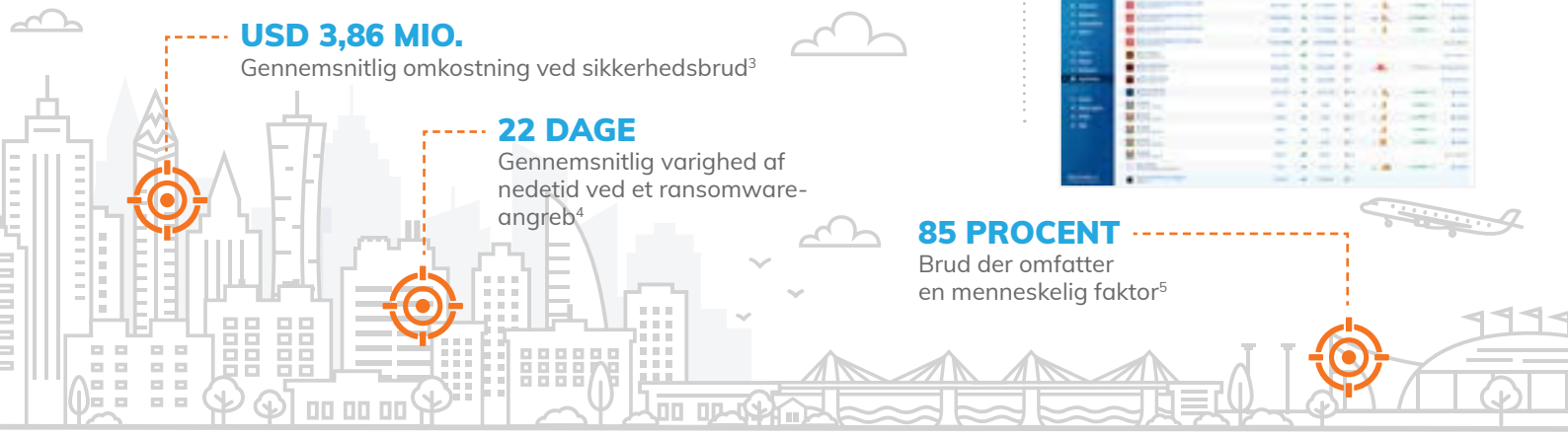
Hvad nu, hvis du kunne implementere et enkelt, omfattende værktøj, der kan modarbejde ubarmhjertige stormflod af trusler og samtidig frigør it-medarbejdernes tid, hvilket kunne resultere i en bedre overordnet produktivitet?

DE STIGENDE KONSEKVENSER AF CYBERANGREB

USD 3,86 MIO.
Gennemsnitlig omkostning ved sikkerhedsbrud[3]

22 DAGE
Gennemsnitlig varighed af nedetid ved et ransomware-angreb[4]

85 PROCENT
Brud der omfatter en menneskelig faktor[5]



USD 11 MIO.

I 2021 betalte den brasilianske fødevarevirksomhed JBS S.A: en rekordstor sum på *USD 11 mio.* i løsesum efter at have mistet godt to ugers produktivitet på grund af et ransomware-angreb.[1]

Nøglefunktioner og fordele ved VIPRE Endpoint Security Cloud

- Næste generation af antivirus blokerer selv dag 0-trusler ved hjælp af AI-adfærdsanalyse
- Scanning, rapportering og patching af programmer fra tredjeparter
- Cloud-baseret styrings- og rapporteringskonsol med pc- og mobiloptimeret adgang
- Aktiv beskyttelse qua et overskueligt og intuitivt moderne design
- Kan konfigureres og er fleksibel, så det passer til driftstilstande og produktivitetsbehov i enhver it-organisation
- Web Access Control (tilvalgsløsning) øger medarbejdernes produktivitet og reducerer samtidig virksomhedens potentielle eksponering

VIPRE kombinerer over tyve års avanceret sikkerhedsintelligens med banebrydende maskinlæring, adfærdsanalyse i realtid og et dybt, konstant lærende trusselsintelligensnetværk i et kraftfuldt værktøj for at forsvare sig mod nutidens angreb og endda morgendagens 0-day-sårbarheder.

VIPRE ENDPOINT SECURITY CLOUD: NEXT GEN ENDPOINT SECURITY MADE SIMPLE

VIPRE Endpoint Security Cloud er en kraftfuld, fuldt tilpasselig cloud-baseret platform til beskyttelse af end points, der gør det muligt for virksomheder at beskytte sig selv mod sårbarheder i Microsoft® Windows®- eller Apple® macOS®-enheder.

Forenklet, multilags sikkerhedsbeskyttelse af endpoints Beskyttelse mod angreb på filer, programmer og netværk. VIPRE Endpoint Security Cloud kombinerer flere lag af sikkerhed med netværks- og applikationsagnostisk DNS-beskyttelse uden ekstra omkostninger. Ved hjælp af effektive teknologier som signaturbaseret registrering, heuristisk analyse og adfærdsanalyse fanger VIPRE Endpoint Security Cloud proaktivt selv 0-dags-trusler. Og det bedste af det hele er, at løsningen er fleksibel og optimerer produktivitet og sikkerhed.

Systemhærdning og synliggørelse af trusler Patch- og sårbarhedsstyring hjælper med at øge synligheden af de risici, som tredjepartsapplikationer udgør i din organisation, prioriterer, hvilke svagheder og sårbarheder der skal behandles, og leverer derefter integreret patchstyring og lukker detekterede sårbarheder ned automatisk eller med et enkelt klik. Luk af for andre angreb med adgangsforebyggelse, DNS-beskyttelse og URL-blokkere. Reducer din angrebsflade, og få større synlighed med interaktive visninger af trusler.

Moderne beskyttelse med en forenklet model Endpoint Security Cloud strømliner ikke kun implementering, konfiguration og administration af sikkerhed på end points, men muliggør også fleksibel, enkel og intuitiv rapportering på alle beskyttede end points med få klik. Klare, letforståelige politikker og konfigurationsindstillinger samt intuitiv og effektiv administration kan alt sammen udføres fra en central konsol. Interaktiv synlighed hjælper med at identificere og rapportere om eventuelle kompromitterede end points sammen med en meget fleksibel mekanisme til at afhjælpning af problemer. Adgang fra hvor som helst fra en pc eller mobil enhed med en hvilken som helst browser sikrer en uovertruffen detaljeringsgrad og synlighed samt rapportering fra praktisk talt alle enheder.

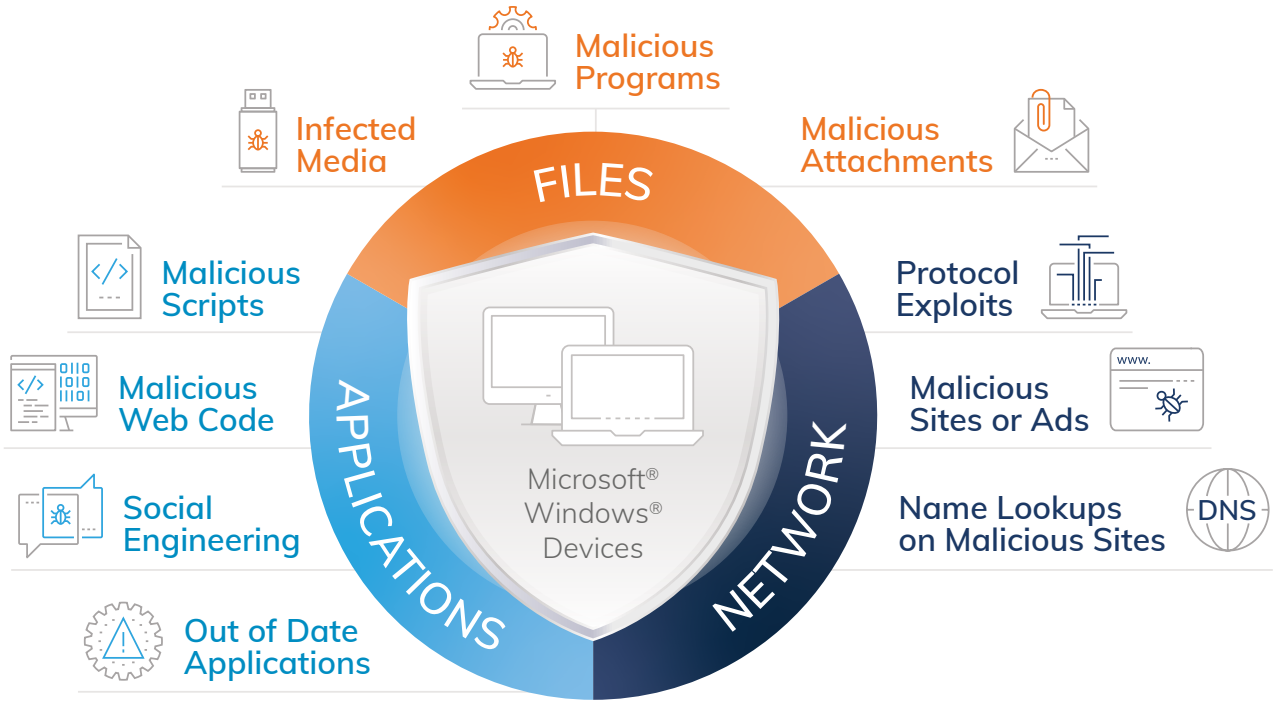
Skrivebordsvisning af centralkonsollen

Mobil visning af centralkonsollen

VIPRE Endpoint Security Cloud-funktioner

- Beskyttelse ved end points og anti-malware
- DNS-beskyttelse
- Aktiv filbeskyttelse
- Maskinlæring
- Aktiv procesbeskyttelse
- Registrering af indtrængen
- Host Intrusion Prevention System (HIPS)
- Blokering af skadelige URL'er
- E-mailbeskyttelse
- Anti-phishing
- Firewall
- Lavt CPU- og hukommelsesforbrug
- Fjernelse af tidligere installeret antivirus
- Beskyttelse mod web-eksploitering
- Patching af sårbarheder i tredjepartsprogrammer
- Webadgangskontrol (tilvalgsløsning)

ENDPOINT SECURITY-BESKYTTELSE I FLERE LAG



FILLAG

Administrerede scanninger	Automatiske og enkle manuelle dybdescanninger efter skadelige filer, med granlær administrativ kontrol og delegering
Aktiv filbeskyttelse	Aktiv beskyttelse af alle filer, der berøres i systemet
Signaturbaseret sporing	Definitionsdatabasen indeholder millioner af kendte malware-signaturer og opdateres flere gange om dagen
Emulering	Afdækker og fortolker malware-kode i et virtuelt miljø for hurtigt at spore trusler og fange avanceret malware
Eksklusioner	Nemt at identificere tilladte filer og erhvervsapplikationer

APPLIKATIONSLAG

Host Intrusion Prevention System (HIPS)	Regelbaseret system, der forhindrer skadelige processer i at udføre skadelig aktivitet
Aktiv procesbeskyttelse	Anvender maskinlæring til interaktivt at analysere procesadfærd og spore potentielt skadelig aktivitet
Patching af sårbarheder	Scan, rapporter og opdater programmer fra tredjeparter til den nyeste version

NETVÆRKSLAG

Intrusion Detection System (IDS)	Leder efter mistænkelige data i ip-frame-delen af pakken og anvender mere end 8.000 regler samt inde i selve applikationsdataene
DNS-beskyttelse	Forhindrer bruger i utilsigtet at besøge skadelige websider ved at opfange DNS-forespørgsler for kendte skadelige domæner og erstatte den normale ip-adresserespons med en omdirigering til vores DNS-sinkhole
Blokering af skadelige URL'er	Forhindrer adgang til specifikke URL'er ved at kontrollere op mod et globalt trusselsintelligensbaseret netværk, der løbende opdateres med den senest kendte liste over skadelige URL'er
Forebyggelse af webudnyttelse	Søger efter potentielt skadelig kode, der er indlejret i websider - krypteret eller ej - ved hjælp af browserudvidelser

EFTERLEV ORGANISATIONENS REGLER OG POLITIKKER MED VIPRE' WEB ACCESS CONTROL (TILVALGSLØSNING)

Øg medarbejdernes produktivitet ved at overvåge regler for anvendelse af internet med granulære sikkerhedstiltag og kontroller. Overhold medarbejderregler for at beskytte medarbejderne mod at se stødende indhold på arbejdspladsen, samt opretholde overholdelse af regler og politikker gennem detaljeret rapportering på bruger-, gruppe- og lokationsniveau.

Funktioner

- 40+ domænekategorier inklusive det mest risikofyldte indhold som hasardspil, hadefuldt indhold, dating, voksenindhold og mere
- Heuristisk filtrering, URL-tilladelse/afvisning og signaturer sikrer præcis sporing
- Løbende genindlæsning og opdatering af websitekategoriseringer

Fordele

- Giver enkel websitekategorisering og nem, forhåndsdefineret filtrering med tilpasning efter behov
- Hjælper organisationer med at overholde reglerne og giver medarbejderne sikkerhedsforanstaltninger, der sikrer, at brugerne ikke udsættes for stødende eller uhensigtsmæssigt materiale
- Vælg tidsblokke, hvor politikken skal være aktiv

"Enhver, der er bekendt med den type virus, ved, hvilken potentiel skade den kan forårsage på en organisation. Da vores medarbejder dobbeltklikkede på kryptolocker-filen, blev den straks destrueret af VIPRE."

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.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.pdfx

Efterhånden som din organisation lægger flere funktioner i clouden **er VIPRE Endpoint Security Cloud** den bedste måde ikke blot at overhale, men også at holde sig på forkant med det skiftende trusselslandskab.

LÆR MERE OM VIPRE SIKKERHEDSTJENESTER

ENDPOINT **EMAIL** **OPLÆRING** **NETVÆRK**

FOR YDERLIGERE OPLYSNINGER kan du besøge global.VIPRE.com/da, ringe på +45 70 25 22 23 eller sende en email til dk.sales@VIPRE.com.