HP WOLF ENTERPRISE SECURITY

ZERO TRUST MED HP WOLF ENTERPRISE SECURITY[1]

BECAUSE CLICK HAPPENS

Zero Trust-konceptet blev udviklet for et årti siden, og er siden udviklet til at indgå i moderne virksomheders IT-sikkerhedsarkitektur. Her får du en oversigt over Zero Trust og hvordan HP anvender konceptet at skabe maksimal end-point-security for hardware.

INDHOLDSFORTEGNELSE

BAGGRUND

Zero Trust et afgørende værktøj i den konstante kamp mod cybertrusler. Princippet i Zero Trust er, som ordet antyder at tage intet for pålydende og at kontrollere alt.

HP Wolf benytter Zero Trust på alle bruger- og enhedsidentiteter, firmware- og softwarekonfiguration samt omfattende kontekstuelle oplysninger for at træffe sikkerheds- og adgangsbeslutninger - på driftsmæssig effektiv vis.

HP WOLF ENTERPRISE SECURITY[1]

ZERO TRUST DIREKTE VED KILDEN

Når de fleste angreb starter på slutbruger-pc 'er, er det vigtigt at få Zero Trustprincippet ind i disse end points.
HP's tilgang til Zero Trust er baseret på et koncept om, at sikkerhedsfunktioner skal implementeres så tæt på angrebskilden som muligt. På samme måde som små bølger er meget tættere på deres kilde, er det at begrænse en trussel ved oprindelsespunktet langt bedre end at vente til skaden har vokset sig stor ved at rulle hen over hele organisationen.

Jo hurtigere vi kan begrænse angribernes bevægelsesfrihed, jo mindre skade kan de gøre.

Det er veldokumenteret, at de fleste angribere kommer ind ved at udnytte brugeradfærd. Det mest almindelige er at snyde folk til at klikke på dårlige links til websteder eller lokke dem til at åbne vedhæftede filer, som indeholder malware.

På denne måde bliver organisationens største trussel mod IT-angreb organisationens egne medarbejdere – de ved det bare ikke. Undervisning af medarbejderne kan hjælpe, men da fjenden kun behøver at komme ind én gang, er undervisning ikke nok til at fjerne hele risikoen.

HP´s tilgang til udfordringen er enkel: Vi anvender Zero Trust på alle potentielt risikofyldte aktiviteter på medarbejdernes computere. Vi fokuserer på de handlinger, som har den højeste risiko:

- Åbning af vedhæftede filer (Office dokumenter og PDF-filer)
- Webbrowsing og klik på links i chatklienter chat clients
- Åbning af filer på USB-enheder

HP Sure Click Enterprise,[2] flagskibet i porteføljen af HP's Wolf Enterprise Security og det primære element i vores Zero Trust-strategi, anvender Zero Trust-principper til endpoint-sikkerhed for at stoppe selv trusler, som ikke kan registreres. Ved hjælp af hardware-forstærket isolation på forsvarsniveau og inddæmningsteknologi hjælper HP Sure Click Enterprise organisationer med at være på forkant med nye trusler, som ellers ville slippe forbi andre typer forsvar.

HP Sure Click Enterprise placerer hver eneste brugeropgave (f.eks. åbning af en vedhæftet fil) i en isoleret mikrovirtuel maskine (mikro- VM). Dette forhindrer malware i at slippe ud af den opgave, som det ankom i. Dermed forhindres inficering af brugerens computer eller andet på netværket. Og når denne proces er gennemført, ødelægges mikro-VM'en sammen med malwaren.

Det bedste af det hele er, at brugerens produktivitet ikke påvirkes, da brugeren ikke skal gøre noget anderledes for at opnå effekten af trusselsinddæmning med Sure Click Enterprise og ikke behøver at være underlagt restriktive politikker og arbejdsprocesser.

HP tager Zero Trust-konceptet et skridt videre ved at benytte avancerede sikkerhedsfunktioner, som er bygget ind i alt moderne pc-hardware. HP Sure Click Enterprise bruger den hjælp, der er i sikkerhedshardware i nye Intel- og AMD CPU'er, til at skabe mikro-VM'er og etablere mikrosegmentering i hver enkelt opgave. Software til endpoint-sikkerhed, der mangler hardware-forstærkning, er altid modtagelig over for at blive angrebet via operativsystemet eller den underliggende infrastruktur. HP anvender derfor Zero Trust på den samlede IT-stack og skaber derved forebyggelse af trusler, som er langt sværere at underminere.

HP Wolf Security anvender Zero Trust-principper for at levere dybdegående forsvar på tværs af hele HP Wolf Security-porteføljen der forbedrer tolerancen, begrænser eksponeringen og minimerer skaderne af cyberangreb.

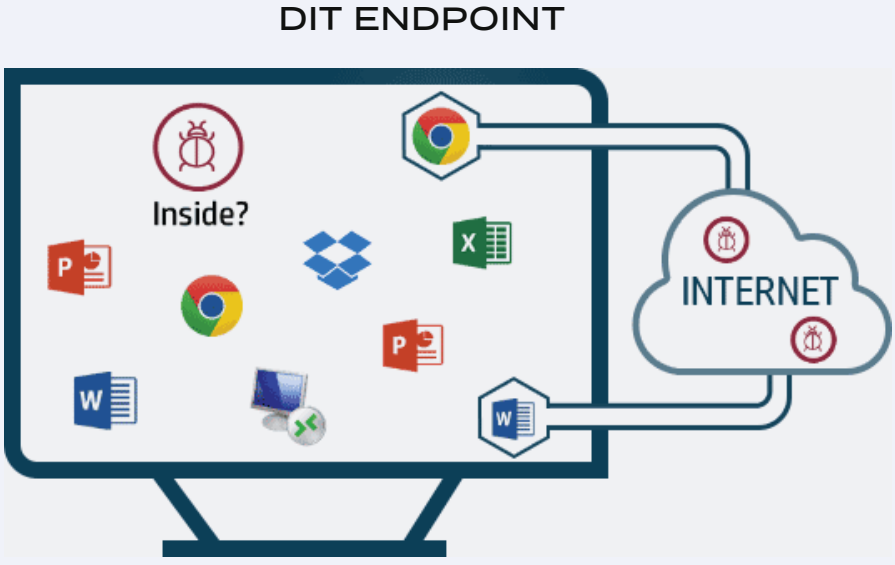
ZERO TRUST INVERTERET

BESKYTTELSE AF VÆRDIFULDE PROGRAMMER OG DATA MED HP SURE ACCESS ENTERPRISE[3]

Det primære element i Zero Trust-princippet er at ikke at stole på dataanmodninger fra ikkegodkendte brugere eller enheder. Men HP går et skridt længere og beskytter desuden også aktivt alle aktivt godkendte enheder og data.

Et godt eksempel en IT-administrator, som arbejder hjemmefra via en VPN til datacenteret og superbrugerens login-oplysninger. En sådan IT-administrator er det perfekte mål for IT-kriminelle. For kan de finde en måde at installere malware i IT-administratorens laptop får de adgang til alle login-oplysninger på administratorniveau og kan dermed tilgå forretningskritiske data samt skabe sig et platform for yderligere inficering eller destruktion af virksomhedens datamiljø.

HP Sure Access Enterprise beskytter mod denne type angrebsstrategier via HP's programisolationsfunktion. Her placeres IT-administrationsaktiviteter som i eksemplet i et sikkert og hardwareassisteret virtuelt område, som ikke kan påvirkes af andre processer på computeren. Så selv om en angriber finder en vej ind og udnytter IT-administratorens pc, kan angriberen ikke få adgang til følsomme oplysninger og logins. Og lige som med Sure Click Enterprise opnås der beskyttelse, uden at det påvirker brugerens produktivitet.



Programisolation sikrer værdifuld beskyttelse af programmer i resten af miljøet.

HP WOLF ENTERPRISE SECURITY[1]

EN UNIK ADGANG TIL ZERO TRUST FOR ENDPOINT

Da både Sure Click Enterprise og Sure Access Enterprise begge er lige effektive til at bekæmpe zero day-angreb og ikke behøver at blive tilpasset ud fra brugen af programmer, kræver hverken Sure Click Enterprise eller Sure Access Enterprise konstante opdateringer for at være på omgangshøjde med angribernes strategier.

HP's Zero Trust-trusselsforebyggelse reducerer i stort omfang presset på sikkerhedschefer og fjerner det meste malware, inden det kan inficere en eneste enhed. Det giver færre advarsler, mindre tid på genopretning og rensning enheder og højere brugerproduktivitet. Det betyder også, at der skal bruges mindre tid og færre penge på registrering og genetablering, simpelthen fordi der opstår langt færre sikkerhedshændelser.

EFFEKTIVITET	NYTTEVIRKNING
Ægte beskyttelse, ikke kun registrering	Zero trust direkte ved kilden
Simple politikker, der skal administreres	Hardwareassistance: Benytter sikkerhedsfunktionerne i alle moderne CPU'er
Få falske positiver	Trusselsinddæmning og programisolation i ét
Nem integration med sikkerhedsprocesser	Samme effektivitet i forhold til både zero day og udbredt udnyttelse
	Fanger trusseloplysninger i realtid

RESUME

ZERO TRUST TIL HYBRIDT ARBEJDE OG HYBRID CLOUD

Zero Trust er ikke et nyt koncept, men det er ekstremt relevant for nutidens hybride arbejdspladser hvor en stor del af medarbejderne enten arbejder hjemmefra eller på farten.

HP's tilgang til Zero Trust anvender trusselsforebyggelse ved kilden. Når forsvaret føjes til endpointet, behøver man ikke bekymre sig, når brugere arbejder via fjernadgang eller fra hjemmekontoret. Man behøver heller forholde sig til, om de data brugerne tilgår befinder sig i virksomhedens datacenter eller i clouden. For de IT-kriminelle bliver stoppet direkte på brugerens computer. En effektiv strategi og løsning som er nem at skalere og reducerer omkostningerne til risikoadministration i IT-afdelingen. Og som samtidig reducerer timeforbruget til fejlfinding, rensning og genoprettelse af brugerne hardware-enheder.

Få flere oplysninger på:
hp.com/wolfenterprisesecurity

[1] HP Wolf Enterprise Security kræver Windows 10. HP Sure Click Enterprise understøtter Microsoft Internet Explorer-, Edge-, Google Chrome-, Chromium og Firefox-browsere og isolerer vedhæftede filer fra Microsoft Office (Word, Excel, PowerPoint) og PDF-filer, når Microsoft Office eller Adobe Acrobat er installeret. HP Protected App understøtter på nuværende tidspunkt RDP-sessioner, Citrix® ICA-sessioner og en Chromium-baseret browser.

[2] HP Sure Click Enterprise kræver Windows 10 og understøttelse af Microsoft Internet Explorer, Edge, Google Chrome, Chromium eller Firefox. Understøttede vedhæftede filtyper omfatter Microsoft Office-filer (Word, Excel, PowerPoint) og PDF-filer, når Microsoft Office eller Adobe Acrobat er installeret.

[3] HP Sure Access Enterprise kræver Windows 10 Pro eller Enterprise.

Tilmeld dig for at få opdateringer: hp.com/go/getupdated

c07713613, juni 2021