



Sikkerhetstjenester fra Data Equipment

Tekniske spesifikasjoner

**MANAGED
ENDPOINT
PROTECTION**



Managed Endpoint Protection stopper kjente og ukjente skadevarer, sårbarheter og utpressingsvirus. Tjenesten koordinerer beskyttelsesmekanismer på Windows, Mac, Linux og Android med hendelser i nettverket og i skyen.

Tjenesten krever ingen signaturer.

Klienten krever veldig lite ressurser, så brukere vil ikke merke at programvaren er installert. Managed Endpoint Protection gir beskyttelse både online og offline.

Intellisec tjenesten



Kontinuerlig sikkerhet

Managed Endpoint Protection vil ta ansvar for å ha deres retningslinjer konfigurert og oppdatert til enhver tid, dette ved å kombinere «best-practice» anbefalinger fra sikkerhetsbransjen med erfaring fra våre konsulenter og vårt operasjonssenter. Intellisec vil fortløpende oppdatere software og sørge for at dere som kunde alltid er oppe og går på siste anbefalt versjon.



Enkel igangsettelse med assistanse fra Intellisec eksperter

Intellisec bistår med en utfyllende installasjonsguide for å kunne automatisere installasjonsprosessen av Managed Endpoint Protection. I tillegg vil våre eksperter være tilgjengelig dersom det dukker opp spørsmål underveis.



Alarm og hendelseshåndtering av vårt operasjonssenter

Vårt operasjonssenter vil håndtere alle alarmer og hendelser som oppdages av Managed Endpoint Protection, hvor de vil analysere dataene for å avdekke rotårsak for en alarm eller hendelse. Dersom man ser det nødvendig, vil du som kunde bli kontaktet for anbefalte handlinger som bør bli utført på et endepunkt. Som et eksempel, operasjonssenteret kan anbefale å isolere eller re-installere et endepunkt, hvis endepunktet er utsatt for et sikkerhetsbrudd.

Stop skadevare og løsepengerangrep

Managed Endpoint Protection hindrer oppstart av skadelige kjørbare filer, DLLs, og Office makroer med flere metoder for beskyttelse, noe som vil redusere angrepsoverflaten og samtidig øke nøyaktigheten for skadevarebeskyttelsen.

Denne tilnærmingen hindrer både kjente og ukjente skadevarer fra å infisere endepunkter ved å kombinere følgende:

Lokal analyse via maskinlæring (ML): Managed Endpoint Protection undersøker hundrevis av karakteristikk på en fil uten å være avhengig av tidligere kunnskap om trusselen og utfører umiddelbare handlinger før trusselen er i gang satt.

WildFire® inspeksjon og analyse: Managed Endpoint Protection benytter seg av WildFire® for inspeksjon av ukjente filer. WildFire® kombinerer fordelene med flere uavhengige teknikker – inkludert statisk, dynamisk og dedikert maskinvareanalyse – for å gi en høy nøyaktighet og unngå motstandsdyktig trusselidentifikasjon.

Skanning av latent skadevare: Managed Endpoint Protection utfører planlagte eller på-forespørsel skanning av skadelige kjørbare filer, DLLs, og Office makroer for å så rette disse opp uten at skadelig filer blir åpnet.



Blokkere «utnyttelse» (exploits) og «filløse» angrep

Istedenfor å sette søkelys på individuelle angrepet vil Managed Endpoint Protection blokkere «utnyttelse» teknikkene som benyttes i et angrep. Ved å gjøre dette i hver fase i et «utnyttelseforsøk» nedbrytes angrepets livssyklus og trusselen blir ineffektiv.

Managed Endpoint Protection bruker flere metoder for å forhindre «utnyttelse» (exploits):

Pre-exploit protection blokkerer rekognosering og sårbarhet profilerings-teknikker før oppstart av «utnyttelseangrepet», effektiv forhindring av angrep.

Technique-based exploit prevention arbeider for å hindre kjente og zeroday «utnyttelse», uten noen forkunnskap om trusselen, ved å blokkere ferdighetene angriperne benytter til å manipulere legitime applikasjoner.

Kernel exploit prevention forhindrer «utnyttelsesangrep» å utnytte sårbarheter i operativsystemets kernel for å opprette prosesser med eskalerte administrasjonsrettigheter. Managed Endpoint Protection forhindrer også injeksjonsteknikker brukt til å kjøre skadelig kode i operativsystemets kernel, som de som ble brukt i WannaCry og NotPetya angrepene.

Utnytt oppførselsbasert beskyttelse

Sofistikerte angrep som utnytter flere legitime applikasjoner og prosesser for skadelige operasjoner har blitt mer og mer vanlig i dag. Disse er vanskelig å avdekke, og de krever synlighet for å korrelere skadelig oppførsel. For at oppførselsbasert beskyttelse skal være effektivt, inkludert identifisering av skadelig aktivitet som oppstår innen legitime prosesser, er det kritisk å forstå alt som foregår på endepunktene.

Managed Endpoint Protection påtar seg oppførselsbasert beskyttelse på følgende måter:

Behavioral Threat Protection oppdager og stopper angrep aktivt ved å overvåke skadelige sekvenser av hendelser på tvers av prosesser og terminering av angrep når det er oppdaget.

Granular Child Process Protection forhindrer script-basert og “filløse” angrep som brukes til å levere skadevare ved å blokkere gjenkjente prosesser fra «launching child processes», vanligvis brukt for å forbigå tradisjonell sikkerhet.

Behavior Based Ransomware Protection forsvarer deg mot krypteringsbasert oppførsel forbundet med løsepengeangrep ved å analysere og stoppe løsepengeaktivitet før datatap inntreffer.



firmapost@dataequipment.no
dataequipment.no