

Kjør eller åpne hva du vil – uten bekymringer!

Som du sikkert allerede vet, vår endepunktsikkerhets-løsning klassifiserer 100% av alt som kjører på enhetene ved å analysere alle mistenkelige og ukjente prosesser/applikasjoner. Som et resultat er alle kjørbare filer enten godkjent eller merket som «skadelig programvare».

Men, er du klar over at løsningen også har tre tilleggsmoduler?



PATCH MANAGEMENT

Log-4J, Python Tar-fil modul – tredjeparts programvare som har sårbarheter – de kan være vanskelig å ha oversikt over.

Med Patch Management kan du slippe å bekymre deg hver gang det kommer en ny sårbarhet som truer ditt IT-miljø. Patch Management oppdaterer ALLE programmene (inkl. tredjeparts) automatisk.



FULL ENCRYPTION

Hjemmekontor, firmareiser, arbeidstimer på toget - mange av oss har fått utvidet fleksibilitet i jobbsituasjonen.

Med denne fleksibiliteten øker risikoen for å bli frastjålet data. Det som fungerer, bedre enn påminnelser, bedre enn regler, bedre enn VPN, er kryptering.

GDPR og norske myndigheter anbefaler bruk av kryptering for å begrense tilgangen til enheter som kan inneholde sensitive data.



DATA CONTROL

Har bedriften din kontroll på person-identifiserbare data?

Hva skjer dersom en kunde ringer og ber deg slette alt du har av personlig opplysninger om han eller henne?

GDPR krever kontroll av private opplysninger!



ENDEPUNKTSIKKERHET



ENDPOINT PROTECTION PLUS

Effektiv skybasert sikkerhetsløsning som sentraliserer neste generasjons antivirus for alle dine Windows-, macOS- og Linux-stasjonære, bærbare datamaskiner og servere.



ENDPOINT DETECTION & RESPONSE

Legg til WatchGuard EDR på toppen av en endepunktbeskyttelse (EP) for omfattende, effektiv endepunktsikkerhet.



ENDPOINT PROTECTION, DETECTION & RESPONSE

Kombinasjonen av Endpoint Protection Plus og Detection & Response gir din bedrift dagens beste beskyttelse både mot kjente og ukjente trusler.