

Kjør eller åpne hva du vil – uten bekymringer!

Det finnes mange kjente sårbarheter og utdaterte programvareversjoner som kan utnyttes. Ofte er disse sårbarhetene på Internett - uten beskyttelse fra bedriftens interne sikkerhet.

Enda verre, kan ansatte *ubevisst* gjøre det mulig for hackere å finne veien inn til bedriftens endepunkter og nettverk.

Det er på tide at alle bedrifter, uansett størrelse, implementerer kraftig endepunktsikkerhet (EPP) med avansert endepunkteteksjon og respons (EPDR).



Advanced
Endpoint Protection,
Detection & Response



Advanced
Endpoint
Protection



Endpoint
Detection &
Response

3 GODE GRUNNER TIL Å VELGE WATCHGUARD

1. **Zero Trust** – EPDR er en tjeneste som klassifiserer 100 % av alt som kjører på enhetene ved å analysere *alle* mistenkelige og ukjente prosesser/applikasjoner. Den bruker spesielle KI-algoritmer i WatchGuard sin sky-plattform, og verifiseres til og med av våre sikkerhetsekspertene ved behov. Som et resultat er *alle* kjørbare filer enten godkjent eller merket som «skadelig programvare». Kunden trenger ikke foreta seg noe selv, da alt er helautomatisk.
2. **Spar tid og ressurser** - trusseljakt krever ofte et svært dyktig IT-team som må bruke mange timer *før* de oppdager trusselen, og finner en løsning. Med WatchGuard sin avanserte løsning, overvåker sikkerhetsanalytikere kundens endepunktmiljø. Den informerer om potensielle pågående angrep og kartlegger kilder. Den oppdager anomalier og relevante hendelser, og reduserer angrepsflaten.
3. **Sky-plattform** - Med WatchGuard sin skyplattform er det enkelt å distribuere, konfigurere og administrere endepunktsikkerhet. Det gir sanntid beskyttelse og kommunikasjon med endepunkter. Administrer hele porteføljen fra én skjerm!



PATCH MANAGEMENT

Slipp å huske på oppdateringer i tredjeparts applikasjoner



FULL ENCRYPTION

Løsningen – i tilfelle bærbar PC blir stjålet



DATA CONTROL

Gjør det lett å finne ut hvor personopplysninger ligger – GDPR krav