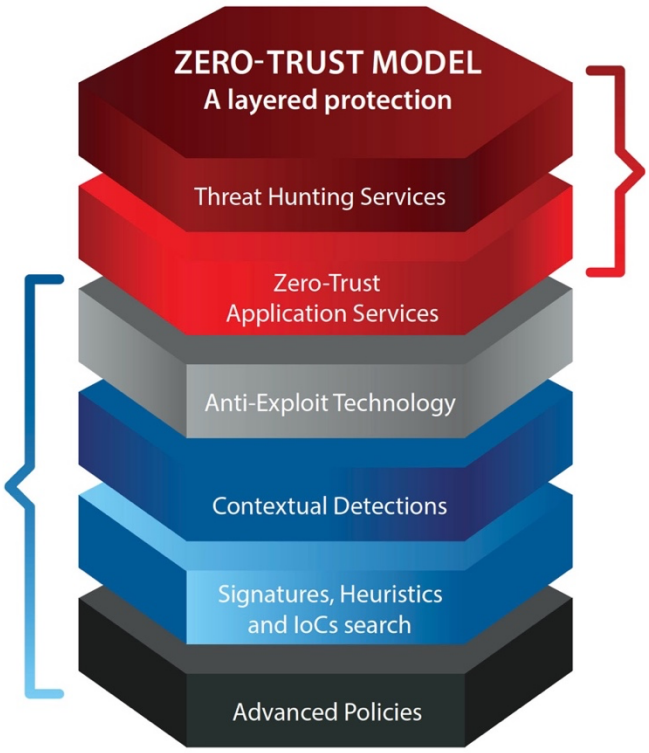
UTFORDRINGER MED MANGE LØSNINGER

Trusselbilde endrer seg hele tiden
For mange varsler – mangel på effektivitet
Komplisert installasjon og administrasjon

WatchGuard Advanced EPDR er en innovativ datasikkerhetsløsning for datamaskiner, bærbare enheter og servere, levert fra skyen. Den automatiserer forebygging, oppdagelse, innesperring og respons på enhver avansert trussel, zero day malware, ransomware, phishing, utnyttelse i minnet, samt angrep uten fil eller skadelig programvare, i og utenfor bedriftsnettverket.
I motsetning til andre løsninger, kombinerer den det bredeste spekteret av endepunktbeskyttelse teknologier (EPP) med automatisert deteksjon og respons (EDR) evner. Den har også **SOC-funksjonalitet**, administrert av WatchGuard-eksperter, som leveres med løsningen:

Zero-Trust Application Service - 100% klassifisering av applikasjoner. Alle kjørbare filer er enten godkjent eller merket som «skadelig programvare»
Threat Hunting Service - deteksjon av hackere og tidligere godkjent kode som kan benyttes i angrep.



WatchGuard

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

WatchGuard Advanced EPDR er en integrasjon mellom tradisjonell endepunktsikkerhet og EDR (deteksjon og respons) som gjør det mulig å forsvare seg mot *avanserte* datatrusler.

TRADISJONELL FOREBYGGENDE TEKNOLOGI

- Personal or managed firewall (IDS)
- Device control
- Collective Intelligence
- Deny list / Allow list
- Permanent multi-vector anti-malware & on-demand scan
- Pre-execution heuristics
- URL filtering – web browsing
- Anti-phishing
- Anti-tampering
- Automatic remediation and ability to rollback
- Recover encrypted files with shadow copies

+ AVANSERT SIKKERHETSTEKNOLOGI
Kontinuerlig monitorering med EDR
Kontinuerlig monitorering av endepunktrisiko
Skybasert maskin (KI) som lærer å klassifisere 100% av prosessene
(APTs, ransomware, rootkits, osv.)
Sandboxing in virkelige miljøer
Trusseljakt, med analyse av atferd for å detektere LotL
(Living-off-the-Land techniques)
Angrepsindikatorer blir kartlegget til MITRE ATT&CK Framework
Anti-exploit. Deteksjon og forebygging mot RDP-angrep (Remote Desktop Protocol) remediation:
Inneslutning, isolasjon og programblokkering
Undersøkelse og respons: ekstern tilgang til endepunktene
STIX 2.0 IoCs søk
Forbedrede sikkerhetspolicyer gjør endepunkter mer motstandsdyktige mot vanlige angrepsteknikker

MAKSIMAL SIKKERHET MED ENKEL OPPSETT

SOC-funksjonaliteten reduserer bemanningskostnader. Det er ingen falske varsler å administrere, ikke noe bortkastet tid på manuelle innstillinger, og intet ansvar er delegert.

Ingen administrasjonsinfrastruktur å installere, konfigurere eller vedlikeholde.

Ta kontakt for mer info!