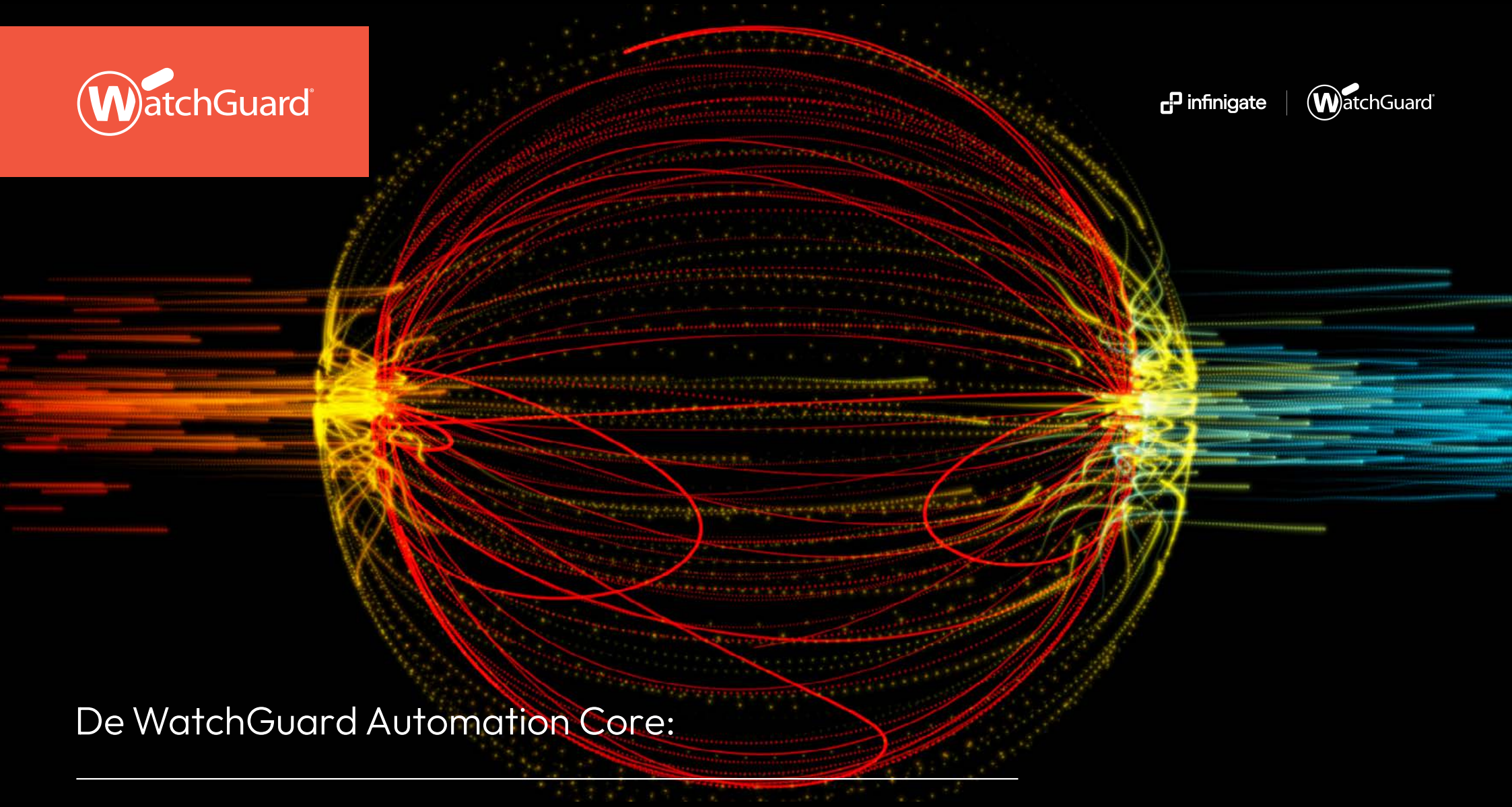
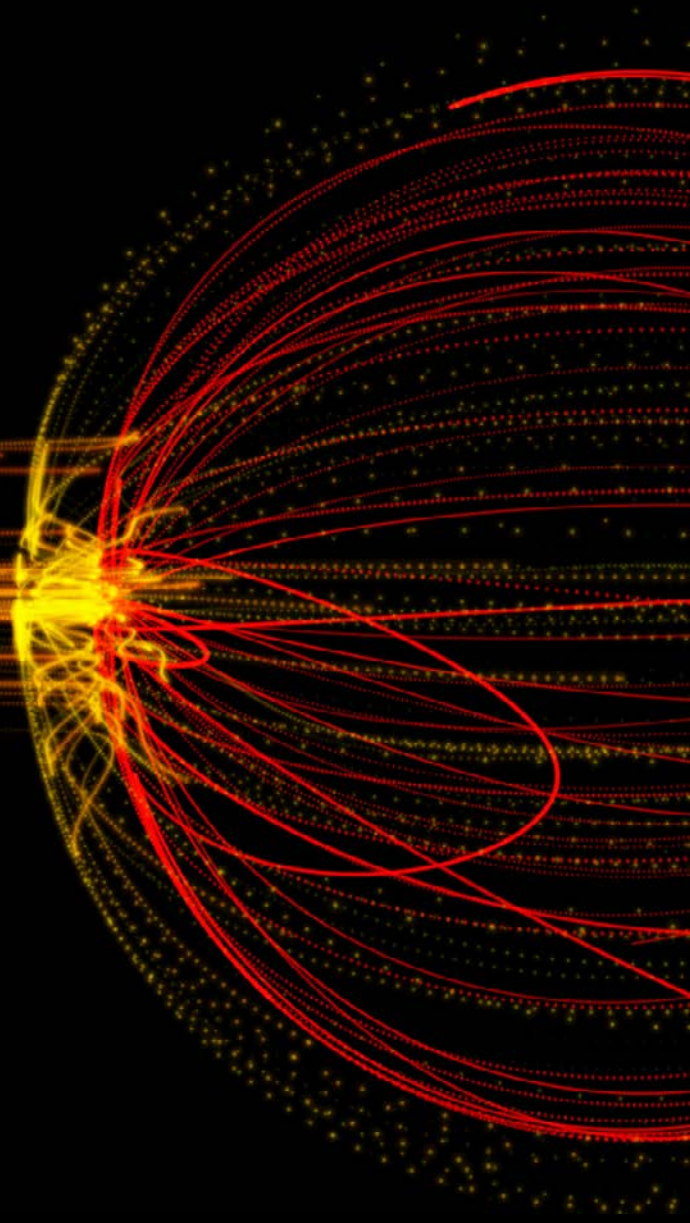


De WatchGuard Automation Core:

Een intelligente, autonome en uitbreidbare omgeving bouwen

Inhoudsopgave



FIREWALLS

De nieuwe omgeving

Firewalls zijn al sinds de begindagen van het web van fundamenteel belang voor de bescherming van endpoints en netwerken. Het belang van hun rol is er niet minder op geworden. De moderne next-generation firewall bevindt zich in het hart van een bedrijf en voert kritieke netwerk- en beveiligingsfuncties uit. Firewalls combineren veel beveiligings-controles op één plaats, waardoor uw efficiënte beveiliging toeneemt en gelaagde beveiliging haalbaar wordt voor sommige organisaties die het anders niet zouden kunnen implementeren. Als toegangspoort tot uw computeromgeving is een firewall een kritische schildwacht, die elke bit en byte beoordeelt wanneer deze uw netwerk binnenkomt en verlaat. Helaas is het juist deze beveiligingscomponent die ons zo vertrouwd is geworden, dat zijn rol vaak als vanzelfsprekend wordt beschouwd.

Geen enkel ander soort beveiliging heeft meer inzicht in en controle over uw beveiligingsstrategie dan de firewall. Maar naarmate meer zakelijk verkeer buiten het netwerk plaatsvindt, moet de rol van de firewall veranderen en ontwikkelen als onderdeel van een groter, uniform beveiligings-platform.

DE NOODZAAK

Voor een uniform beveiligingsplatform

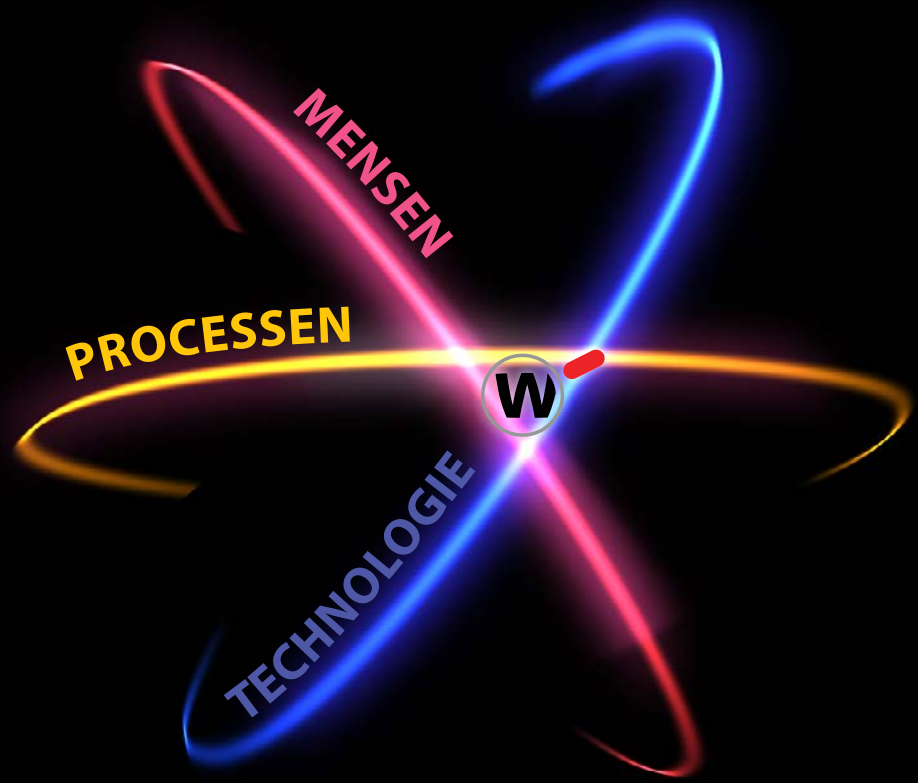
Nu de grenzen van de IT-omgeving steeds minder tastbaar worden, moeten bedrijven de beveiligingsmogelijkheden van hun netwerk kunnen uitbreiden voor zowel gebruikers als apparatuur, ongeacht waar deze zich bevinden. Werknemers, uitzendkrachten, bezoekers en hun apparaten komen regelmatig uw netwerk binnen en verlaten het weer wanneer zij hun activiteiten buiten uw bedrijf uitvoeren. In het huidige agressieve bedreigingslandschap kan echter één geïnfecteerd endpoint of gestolen wachtwoord de deuren openen voor een aanvaller. Om uw computeromgeving in de komende tijd te beveiligen is meer nodig dan een gesloten deur. Er moet goed worden nagedacht over waar uw kwetsbare punten liggen om die vervolgens aan te pakken.

Een Unified Security Platform (USP) zorgt voor een grotere mate van coördinatie tussen uw mensen, processen en technologie, met als voor-deel een betere en efficiënte beveiliging.

Mensen. Mensen vormen de zwakste schakel als het gaat om kwets- baarheid van uw netwerk en beveiliging. Vanzelfsprekend leren we gebruikers zich bewust te zijn van bedreigingen en zoiets als het verbeteren van wachtwoorden is feitelijk een no-brainer. Maar vertrouwen op de consequente toepassing van al deze regels alleen, is sterk af te raden. Een uniform beveiligingsplatform kan helpen om naleving van deze regels af te dwingen. Het kan ook bijdragen aan het beveiligings-bewustzijn onder uw personeel en u meer inzicht geven in de gebruikers die het grootste risico vormen.

Processen. Hoewel het voorkomen van cyberaanvallen het uiteindelijke doel is, zou elk bedrijf een plan klaar moeten hebben om snel te kunnen reageren op een cyberaanval. Door informatie over bedreigingen en reactiemogelijkheden op één platform te consolideren, maakt een uniform beveiligingsplatform het mogelijk bedreigingen te identificeren, te prioriteren en te beperken, waar ze ook opduiken.

Technologie. Effectieve, gelaagde beveiliging, is alleen mogelijk als die lagen niet geïsoleerd worden ingezet. Wanneer elke laag met de andere kan ‚praten', krijgt u beter beeld van die bedreigingen in een bredere context. Een uniform beveiligingsplatform brengt al deze technologieën naadloos samen, zodat uw team bedreigingen snel kan identificeren, prioriteren en beperken.



BESCHERMING VAN UW SNEL GROEIENDE IT DOOR

Hiërarchische automatisering

Meer dan ooit hebben IT-managers behoefte aan beveiliging met een hoge mate van autonomie en automatisering om tijdverspilling tegen te gaan, netwerkprestaties te optimaliseren en de hoogste beveiliging tegen cyberaanvallen te bieden. Automatisering is de sleutel tot het leveren van een effectief Unified Security Platform dat uw team in staat stelt meer te doen met minder mensen. Verregaande automatisering stelt technologieleveranciers in staat geavanceerdere technieken in te zetten die aansluiten op de soms complexe netwerkarchitecturen van vandaag de dag. Hierdoor is het mogelijk om meer bescherming te bieden tegen de nieuwste bedreigingen, iets wat teams met beperkte middelen maar al te vaak over het hoofd zien.

Voor sommige bedrijven zal het automatiseren van handmatige zich herhalende taken met betrekking tot het beheer en onderhoud van de IT-omgeving, belangrijke inzichten opleveren in vergelijking met de manier waarop hun team vandaag werkt. Een ander bedrijf zal onmiddellijk profiteren van de geautomatiseerde inzet in de Cloud en de nauwe integratie met de services die het al in gebruik heeft.

Automatiserings hiërarchie

Op het hoogste automatiserings-niveau kan een Unified Security Platform vrijwel geheel autonoom opereren wat IT-teams aanzienlijke voordelen biedt, zoals bijvoorbeeld:

- Snelle detectie en adequaat anticiperen
- Belangrijke kostenbesparing
- Sterk verbeterd inzicht en duidelijk overzicht

NIVEAU 1 **MANAGEMENT & ZICHTBAARHEID**	HANDTEKENING & SOFTWARE UPDATES	KANT-EN-KLARE RAPPORTEN & DASHBOARDS		VEILIGE FIREWALL DEFAULTS
NIVEAU 2 **OPERATIONEEL**	CLOUD DEPLOYMENT	LICENTIE MANAGEMENT	FACTUUR & SUPPORT TICKET VERWERKING	API & WEB SERVICE INTEGRATIE
NIVEAU 3 **RESPONSIEVE BEVEILIGING**	GEDRAGS- EN STATISTISCHE MODELLERING	SANERING	BEDREIGING CORRELATIE	ENDPOINT ISOLATIE
NIVEAU 4 **VOORSPELLENDE BEVEILIGING**	AI-AANGEDREVEN PREVENTIE, DETECTIE, TRIAGE EN HERSTEL			

NIVEAU 1

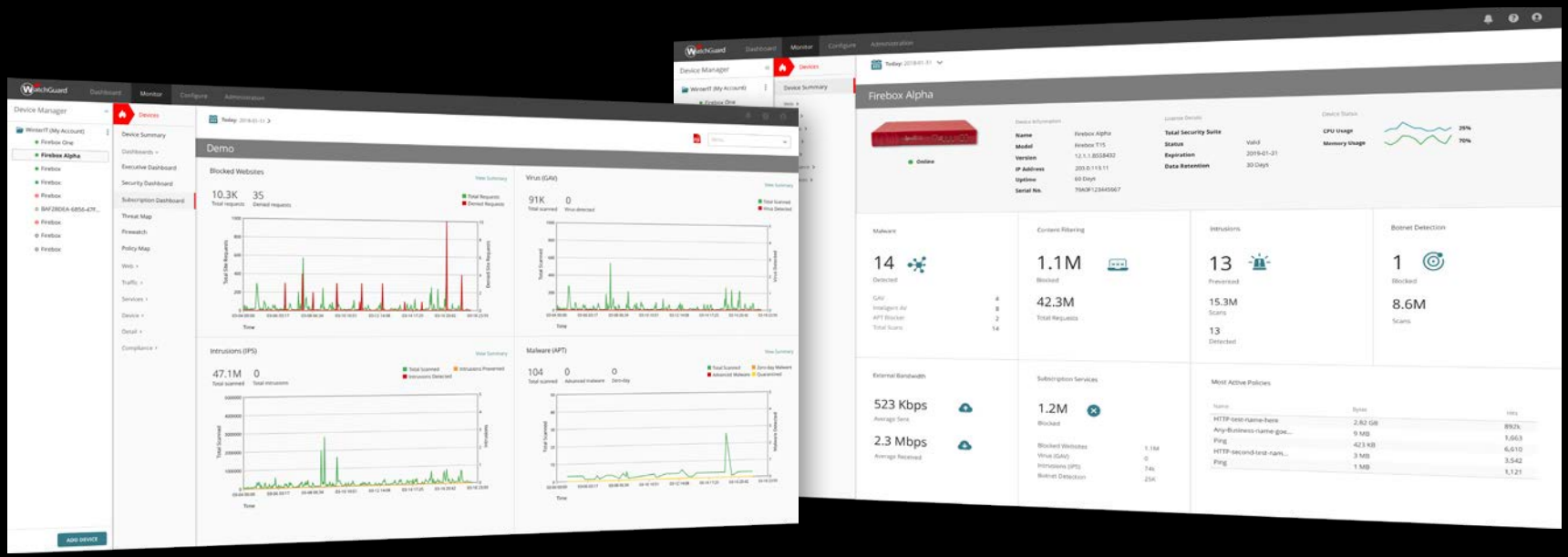
Management & visibility

Hoe kan ik frequente, herhalende en foutgevoelige handmatige taken tot een minimum beperken?

99% van de inbraken op het netwerk is te wijten aan een verkeerd geconfigureerde firewall.2 Met WatchGuard Cloud maakt u„ één set-up, herhaald gebruik“ die frequente, foutgevoelige handmatige taken vervangt, door geautomatiseerde processen.

BESPAAR TIJD MET:

- **Security als een standaard.**
  Zorg ervoor dat nieuwe apparatuur optimaal geconfigureerd en beveiligd is.
- **Geautomatiseerde updates.**
  Regelmatig geplande updates van software en signatures houden uw omgeving beschermd tegen de nieuwste bekende bedreigingen
- **Rapporten en dashboards.**
  Rapporten met real-time gegevens en bruikbare, vereenvoudigde overzichten van het hele netwerk maken het ontdekken van problemen en het aantonen van compliance eenvoudig, terwijl er significant veel tijd wordt bespaard aan manuren in vergelijking met een handmatige samenstelling.



2. https://www.gartner.com/en/documents/3215918

NIVEAU 2

Operationele automatisering

Hoe kan ik ons beveiligingsaanbod efficiënter inzetten en ondersteunen?

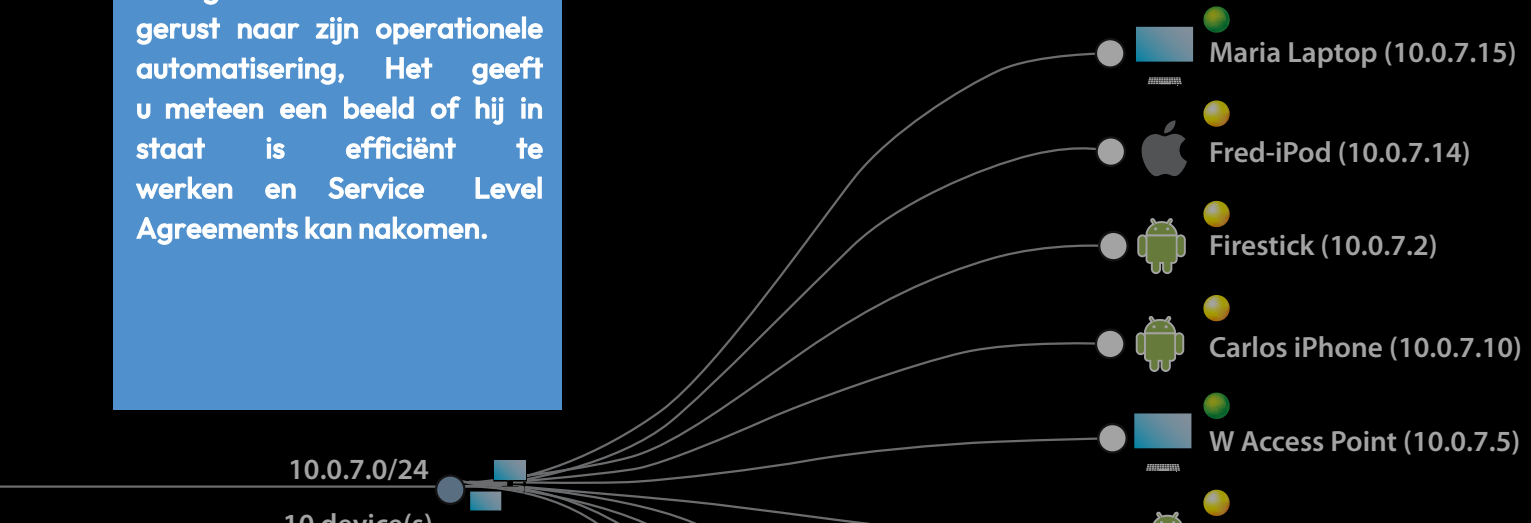
Het installeren van nieuwe apparatuur op een externe locatie kan kostbaar en tijdrovend zijn. Operationele automatisering maakt gebruik van de kracht van de Cloud om de implementatie, het beheer en de ondersteuning te vergemakkelijken. IT-Service providers kunnen licentiebeheer van zowel software als apparatuur beheren.

BESPAAR TIJD MET:

- **Zero-touch implementatie.**
  Apparatuur wordt vooraf geconfigureerd vanuit de Cloud. Er hoeft geen IT-medewerker naar de locatie waar de apparatuur geïnstalleerd wordt.
- **API en web service integratie.**
  Integreert met belangrijke webapplicaties.
- **Gestroomlijnd beheer van softwarelicenties.**
  Naadloze integratie van processen met Professional Services Automation (PSA)-tools.
- **Geïntegreerd beheer van supporttickets.**
  Nauw geïntegreerde tools voor bewaking en beheer op afstand (RMM) voor een snellere reactie op ondersteuningsverzoeken.

TIP

Vraag een Service Provider gerust naar zijn operationele automatisering, Het geeft u meteen een beeld of hij in staat is efficiënt te werken en Service Level Agreements kan nakomen.



NIVEAU 3

Responsive security automatisering

Hoe blijf ik op de hoogte van de laatste bedreigingen zodat ik snel kan reageren?

Tijdig reageren op bedreigingen kan het verschil betekenen tussen een snelle oplossing en een ernstig beveiligingsincident. Het gemiddelde bedrijf besteedt honderden manuren per week aan het opschonen, repareren en/of patchen van netwerken, applicaties en apparatuur.[3] Slechts 39% van de bedrijven zegt effectief te zijn in het detecteren van bedreigingen.[4] Automatisering van securityprocessen zorgt ervoor dat u tijdig kunt ingrijpen en de bedreiging in korte tijd kun elimineren, zonder dat u daar een omvangrijk IT-team voor nodig heeft.

BESPAAR TIJD MET:

- **Geavanceerde detectie.**
  Door de verschillende incidenten aan elkaar te koppelen, worden patronen eenvoudig zichtbaar. Potentiële bedreigingen kunnen verder worden onderzocht in een geïntegreerde sandbox-omgeving.
- **Samengestelde scores.**
  Door een bedreiging een bepaalde score te geven, wordt de informatie veel betrouwbaarder.
- **Geautomatiseerde respons.**
  Automatisch ingrijpen om de bedreiging te elimineren wanneer een schadelijk bestand of proces wordt geïdentificeerd
- **Endpoint controle.**
  Direct isoleren van geïnfecteerde Endpoints totdat deze weer in orde kunnen worden gebracht.

3. https://go.juniper.net/assets/pdfs/OSI/2000683-001-EN.pdf
4. https://go.juniper.net/assets/pdfs/OSI/2000683-001-EN.pdf

NIVEAU 4

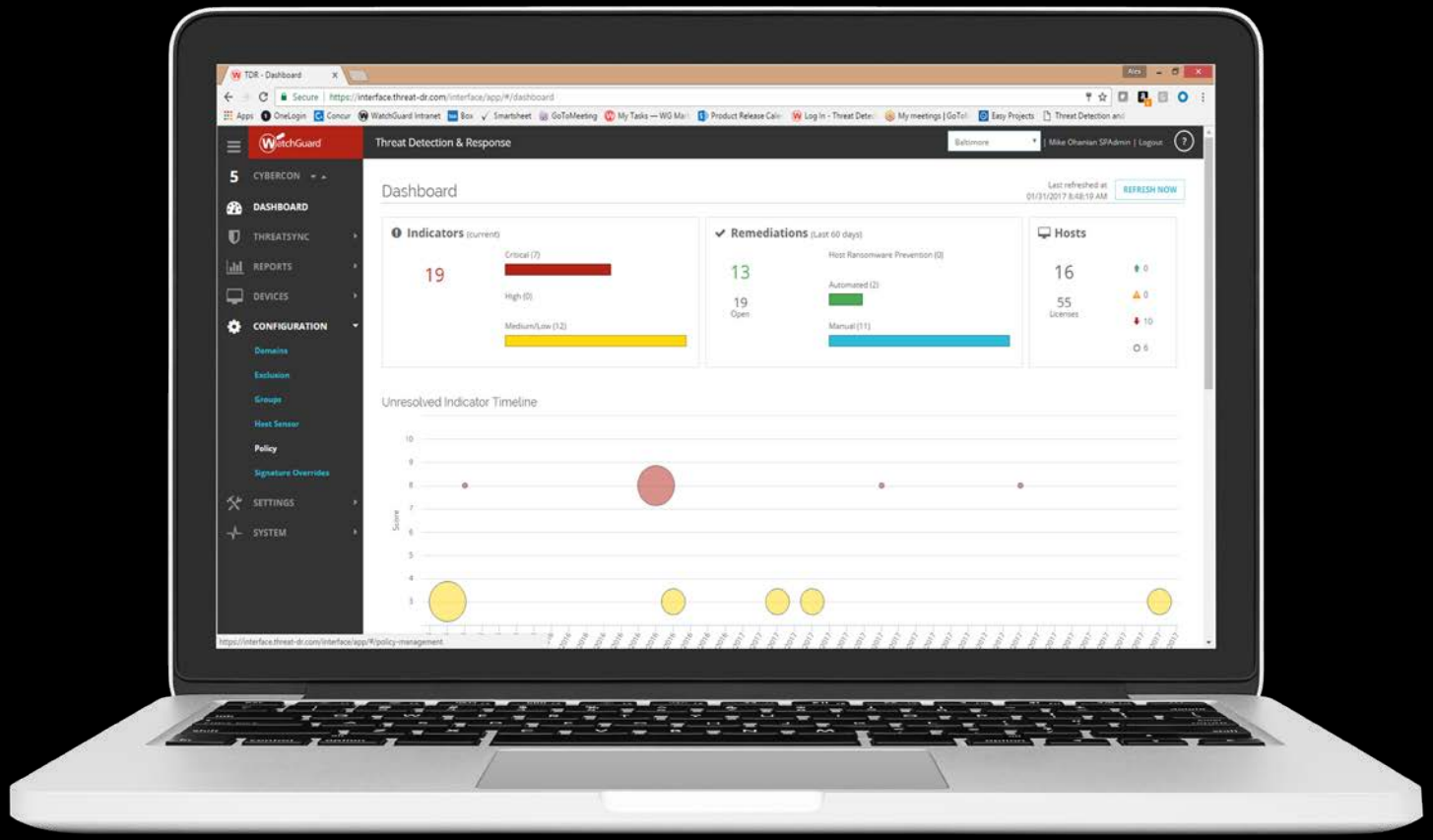
Predictive security automatisering

Hoe kan ik geavanceerde bedreigingen blokkeren zonder een team van beveiligingsexperts in te huren?

Voorkomen dat een aanval uw omgeving binnendringt, is de beste manier om uw organisatie veilig te houden. WatchGuard Cloud maakt het eenvoudig om geavanceerde technieken, zoals kunstmatige intelligentie (AI)-technologie, in te zetten om continu nieuwe bedreigingen te voorspellen en zich ertegen te verdedigen.

BESPAAR TIJD MET:

- **Voorkom inbraken.**
  Door het voorkomen van inbraken op het netwerk, kan uw IT-team haar tijd besteden aan het nog verder optimaliseren van uw IT omgeving in plaats van het oplossen van de schade die is aangericht vanwege die inbraak.

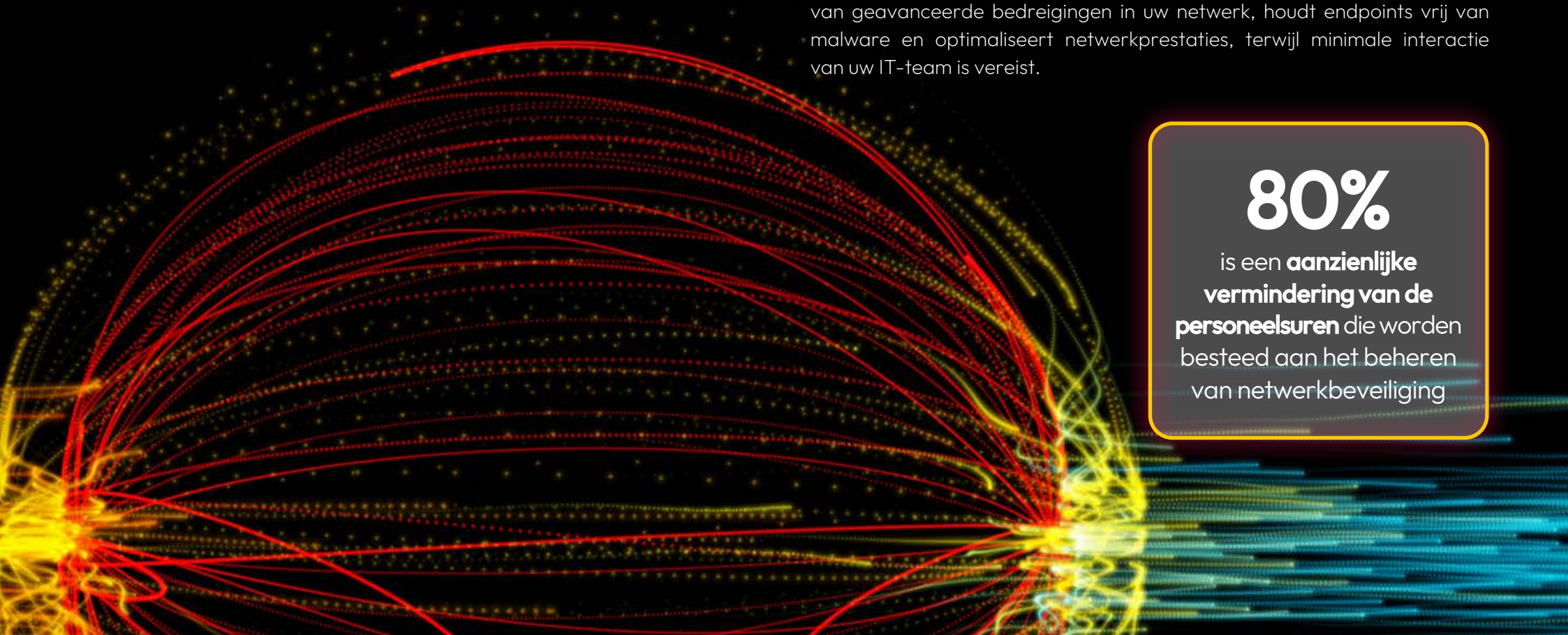


DE WATCHGUARD

Automation core

Automatisering is het hart van het WatchGuard's Unified Security Platform. Het versnelt processen, elimineert bedreigingen en stelt IT-teams in staat om meer te doen met minder mensen. Gedefinieerd als de WatchGuard Automation Core, is ons wijze van automatisering uniek en veelzijdig en richt zich op alle vier automatiseringsniveaus. Het is aangetoond dat door het automatiseren van processen de hoeveelheid uren die door uw IT- team in netwerkbeveiligingsbeheer wordt gestoken met maar liefst 80% kan worden verminderd in vergelijking met traditionele netwerkbeveiligingsoplossingen.

WatchGuard's Automation Core creëert een zero-touch feedbackloop voor beveiliging zonder menselijke tussenkomst en maakt centraal beveiligingsbeheer eenvoudig te implementeren. Deze oplossing maakt het mogelijk uw beveiliging naadloos uit te breiden naar elke computeromgeving binnen uw bedrijf, of dat nu een hoofd- of bijkantoor is. WatchGuard's Automation Core creëert een intelligente, autonome omgeving die zich uitstrekt van het LAN tot aan de Cloud en uiteindelijk tot het endpoint, waardoor een continu, geïntegreerde bescherming gegarandeerd is. Een Automation Core zorgt voor veilige gebruikerstoegang tot essentiële bronnen, blokkeert het binnendringen van geavanceerde bedreigingen in uw netwerk, houdt endpoints vrij van malware en optimaliseert netwerkprestaties, terwijl minimale interactie van uw IT-team is vereist.



80%

is een **aanzienlijke vermindering van de personeelsuren** die worden besteed aan het beheren van netwerkbeveiliging

ONDERDELEN VAN

De watchguard automation core

NIVEAU 1 **MANAGEMENT & ZICHTBAARHEID**	**Watchguard firebox.** Het Firebox-platform biedt standaardinstellingen voor de firewall en kant-en-klare dashboards en rapporten, waardoor uw team snel aan de slag kan en er tegelijkertijd voor kan zorgen dat de apparatuur veilig is geconfigureerd.
	Watchguard cloud. WatchGuard Cloud biedt realtime gegevens en bruikbare, begrijpbare inzichten vanuit uw hele netwerk. Het beheren van de Firebox systeemtaken en het genereren van rapporten is eenvoudig met onze kant-en-klare rapport-templates.
NIVEAU 2 **OPERATIONEEL**	**Rapiddeploy.** Configureer uw Firebox vooraf vanuit de Cloud. Geen noodzaak om IT-personeel ter plaatse te hebben.
	Watchguard firebox. Nauwe integratie en de beschikbaarheid van API's voor toonaangevende PSA- en RMM-tools, zorgen voor eenvoudiger licentiebeheer en een snellere reactie op ondersteuningsverzoeken.
	Authpoint mfa. WatchGuard's AuthPoint service bevat geautomatiseerd token-management en AD en LDAP synchronisatie functies die de uitrol van tokens eenvoudiger maakt.
NIVEAU 3 **RESPONSIEVE BEVEILIGING**	**Threatsync, apt blocker and dnswatch.** WatchGuard herkent verdacht DNS-gedrag en blokkeert gebruikers op voorhand om verbinding te maken met risicovolle websites. Vervolgens voegen we informatie van netwerk- en endpoints samen om de bedreiging te beoordelen. Indien nodig gebruiken we sandboxing voor een diepere inspectie. En zonder dat u een vinger hoeft uit te steken, automatiseert onze oplossing hersteltaken, om een bedreiging binnen enkele seconden te elimineren. Deze geautomatiseerde processen beschermen uw gebruikers en gegevens, ongeacht of ze zich op locatie bevinden of buiten de deur zijn.
NIVEAU 4 **VOORSPELLENDE BEVEILIGING**	**Intelligentav.** Onze AI-aangedreven antivirus is de enige firewalloplossing die belangrijke bedreigingen blokkeert, 33 maanden voordat ze uit het niets verschijnen, waardoor WatchGuard het enige firewallplatform is met voorspellende bescherming op niveau 4!

DE WATCHGUARD AUTOMATION CORE

Biedt voordelen

Doeltreffende beveiliging

- De gemiddelde Firebox blokkeerde in 2019 meer dan 2.100 malware varianten, waarvan bijna 40% werd geclassificeerd als 'zero day', dat wil zeggen volledig niet te detecteren op basis van bestaande signatures. Elk apparaat blokkeerde gemiddeld nog eens 240 netwerkaanvallen.

Bij NSS Labs testen bleek WatchGuard één van slechts 2 firewall platformen die NUL gemiste bedreigingen liet noteren. WatchGuard heeft drie jaar achtereen de „Recommended rating" behaald.

Uitbreidbaarheid

- Bescherm uw gebruikers tegen phishing en ransomware.
- Isoleer endpoints en herstel deze, waar ze zich ook ter wereld bevinden.
- Controleer toegang naar bedrijfsmiddelen, accounts en informatie met de geïntegreerde multi-factor authenticatie tools, SSO voor centrale toegang naar Cloud-hosted applicaties en interne bronnen via RDP en SSH.
- Bewaak de 'policies' voor zowel gebruikers als apparatuur wanneer ze het netwerk binnenkomen of verlaten.

Optimale bezetting it-afdeling

- Meer dan 12.000 implementaties zijn opgeleverd waarbij gebruik werd gemaakt van onze Cloud-implementatieservice. Slechts 1/100e van de tijd en kosten werd besteed aan de set-up en configuratie van standaard apparatuur.

Meer dan 100 dashboards en ingebouwde rapporten geven u optimaal inzicht waarbij u honderden uren bespaart ten opzichte van andere monitorsystemen.

Bespaar tijd en geld

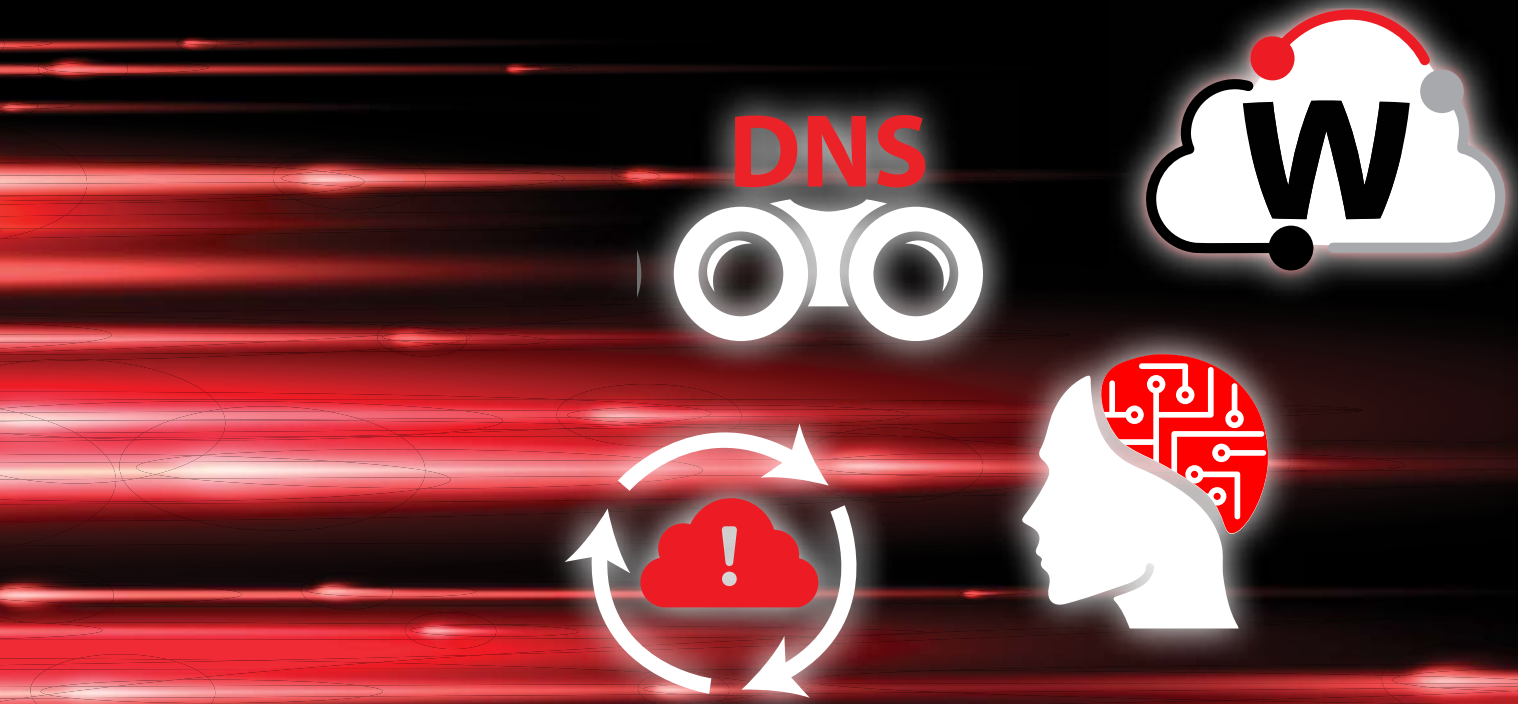
- Met behulp van AI voorspelt het Firebox-platform bedreigingen tot 33 maanden voordat ze uit het niets verschijnen.
- Mochten aanvallen hun weg vinden naar het netwerk, dan maakt de Automation Core het mogelijk om verdacht gedrag vroegtijdig te signaleren en bedreigingen binnen enkelen minuten automatisch te elimineren.

WATCHGUARD LEVERT OPLOSSINGEN VOOR

Het volledige spectrum

Met WatchGurad Cloud-, DNSWatch-, ThreatSync- en IntelligentAV-producten kunnen IT-teams zich concentreren op de beveiliging terwijl ze hun capaciteit over het hele spectrum inzetten waar een IT-team verantwoordelijkheden voor heeft.

De Automation Core zorgt voor een uniform beveiligingsplatform binnen elke omgeving waarin uw bedrijf actief is, waarbij WatchGuard superieure bescherming biedt tegen de nieuwste bedreigingen.



DE WATCHGUARD

Unified security platform™

NETWORK SECURITY

WatchGuard Network Security-oplossingen zijn eenvoudig te implementeren, te gebruiken en te beheren. Onze unieke benadering van netwerk-beveiliging richt zich op het bieden van de beste beveiliging op bedrijfsniveau voor elke organisatie, ongeacht omvang of technische expertise.

SECURE WI-FI

WatchGuard's Secure Wi-Fi Solution, is een unieke oplossing en ontworpen om een veilig, beschermd kanaal voor Wi-Fi omgevingen te bieden. Doordat de administratie eenvoudig blijft, zijn de beheerskosten laag. Met uitgebreide mogelijkheden en inzicht in bedrijfsanalyses, beschikt het bedrijf over alle informatie om efficiënt te werken.

MULTI-FACTORAUTHENTICATION

WatchGuard AuthPoint® is de juiste oplossing om de wachtwoord-gedreven beveiligingskloof te dichten met multi-factor authenticatie op een eenvoudig te gebruiken Cloud platform. WatchGuard's unieke benadering voegt het „mobiele telefoon DNA" toe als een identificerende factor om ervoor te zorgen dat alleen de juiste persoon toegang krijgt tot gevoelige netwerken en Cloud applicaties.

ENDPOINT SECURITY

WatchGuard Endpoint Security beschermt tegen huidige en toekomstige cyberaanvallen. Het parade-paardje van het bedrijf, Panda Adaptive Defense 360, dat werkt op basis van kunstmatige intelligentie, verbetert onmiddellijk het beveiligingsniveau bij organisaties. Het combineert mogelijkheden voor endpoint protection (EPP) en detectie en respons (EDR) met zero-trust-toepassing en threat hunting services.