
ZERO TRUST
AS A SERVICE
MANAGED PREVENTION
on2IT
ZERO TRUST INNOVATORS

ON2IT
ZERO TRUST INNOVATORS

Weet jij bij een cyberaanval direct wat er aan de hand is?

Datadiefstal en cyberaanvallen zijn helaas een harde realiteit. Hoe hard je ook inzet op preventie, de risico's zijn nooit 100% uit te sluiten. Maar hoe kun je je het beste wapenen, en hoe zorg jij ervoor dat je, in het geval van een inbreuk, binnen 30 minuten volledig op de hoogte bent? Weet jij direct wat er is gebeurd, welke gegevens het betrof en hoe de aanval is gepareerd?


ZERO TRUST
THE ONLY
PREVENTION
STRATEGY

Blijf voortdurend ontwikkelende hacking techniques voor

Deze nieuwe, snelle en digitale wereld vraagt om een efficiënte en betrouwbare aanpak van IT-security. Binnen het klassieke cybersecurity model is een grens getrokken tussen ‘de onveilige buitenwereld’ en het ‘vertrouwde’ eigen netwerk. Firewalls moeten ongewenst verkeer tegenhouden en eenmaal binnen het netwerk beschouwt men alle verkeer als vertrouwd.

Het gebruik van mobiele devices, webapplicaties en de toegang van klanten, leveranciers of patiënten tot het netwerk, maakt een totaal ander IT-security concept noodzakelijk: Zero Trust. Zero Trust is een effectieve strategie om ervoor te zorgen dat je security toekomstbestendig is en niet afhankelijk is van specifieke software of hardware.

Het is eenvoudig om de methode vorm te geven op een manier die voor jou het beste werkt, ongeacht waar je gegevens opslaat.

Alles op basis van Zero Trust

Kort gezegd, nemen wij het hele securityproces uit handen zodat jij je kunt richten op dat wat écht belangrijk is: je bedrijf managen en groei realiseren. Wij bieden onze Managed Security Services aan vanuit een eigen, hypermodern SOC, waar we werken met een combinatie van de beste technologische oplossingen en een team van deskundige securityspecialisten.

We laten ons bij onze dienstverlening leiden door de Zero Trust principes. Hiermee onderscheiden we ons ook direct van de concurrentie. Onze aanpak is uniek in de markt en maakt dat we in binnen- en buitenland zijn uitgegroeid tot een toonaangevende partij.

Wie en wat kun je nog vertrouwen?

De IT-wereld is voortdurend in beweging, en ook de manier waarop we naar cybersecurity kijken, is de afgelopen jaren sterk veranderd.

In 2009 introduceerde toenmalig Forrester-analist, nu ON2IT Senior VP Cybersecurity Strategy, John Kindervag zijn Zero Trust securitystrategie in de Verenigde Staten. Kort daarna droeg ON2IT als eerste diezelfde filosofie uit in Europa.

Met Zero Trust Security kun je de impact van het aangevallen gebied in het hele netwerk effectief beperken. Verdeel het netwerk in verschillende segmenten (protect surfaces) en pas security maatregelen toe die in overeenstemming zijn met de gevoeligheid van de data binnen elk segment.

Zorg er ook voor dat de segmenten van elkaar gescheiden zijn, zodat een eventueel security incident alleen gevolgen heeft voor dat ene segment en niet voor het hele netwerk.

Wij waren een van de eersten om de Zero Trust filosofie voor het beveiligen van IT-netwerken te omarmen, en we dragen actief bij aan de verdere ontwikkeling.

Wat is Zero Trust?

De Zero Trust aanpak kent ‘never trust, always verify’ als leidraad. Vooraf is er geen aanname over de mate van betrouwbaarheid; of het nu gaat om gebruikers, hosts of datasets. Daarnaast is toegang tot data gelimiteerd op een need-to-know basis.

Op basis van inzicht in data en verkeersstromen is het netwerk – en de beveiliging ervan – ‘van binnen naar buiten’ ingericht en wordt alle verkeer binnen het netwerk geïnspecteerd en gelogd.

Zero Trust is gebaseerd op vier principes:

- Definieer bedrijfsresultaten
- Het netwerk wordt van binnen naar buiten ontworpen
- Bepaal wie of wat toegang nodig heeft
- Al het dataverkeer wordt geïnspecteerd en gelogd

Zero Trust: een strategie

Zero Trust is een strategisch initiatief dat succesvolle data inbreuken voorkomt door de noodzaak van digitaal vertrouwen in jouw organisatie weg te nemen. Geworteld in het principe ‘never trust, always verify’, is Zero Trust ontworpen als een strategie die resoneert met de hoogste niveaus van elke organisatie, maar die tactisch wordt ingezet met behulp van off-the-shelf technologie.

Zero Trust strategie is losgekoppeld van technologie. Terwijl technologieën in de loop der tijd verbeteren en veranderen, blijft de strategie hetzelfde.

De belangrijkste voordelen van Zero Trust:

- Minimale blootstelling aan cyberthreats
- Lagere operationele kosten
- Grotere continuïteit voor cruciale bedrijfsprocessen
- Betere en kosteneffectieve compliance
- Toekomstbestendige architectuur

De beste service met de beste mensen

Wij bieden onze Managed Security Services aan vanuit ons managed Security Operations Center (mSOC™).

ON2IT's managed security bied je 24/7 toegang tot onze ervaren security engineers en ons AUXO™-platform, welke beiden gebruik maken van best practices en goed gedocumenteerde procedures. Onze security services breiden jouw eigen IT-afdeling uit, waardoor je inzicht krijgt in en controle over de status van je netwerkbeveiliging.


HOW TO
OPERATIONALIZE
ZERO TRUST

Wat ons mSOC™ doet

Het ON2IT mSOC™ kan je complete IT-security verzorgen op een manier die vandaag de dag voor veel organisaties intern moeilijk is te realiseren. Het blijkt vaak lastig om de juiste mensen te vinden en te behouden – de 'war for talent' woedt immers nog steeds – en budgetten zijn vaak niet toereikend. Ons mSOC™ biedt 24/7 managed detection and response van wereldklasse, aangevuld met een unieke reeks preventie- en compliance services, allemaal gebundeld als Zero Trust as a Service.

Preventie beheren
- Zero Trust Cybersecurity Controls / Management
- Zelflerend Security Operations Center
- Zero Trust Policy Validator
- Cybersecurity Improvement Advisories
- ROE™ Automated Rules of Engagement
- Tegenmaatregelen

Alarmering
- Cybersecurity Monitoring
- Ervaren Cybersecurity Analysts
- Reveal AI-based Threat Hunting
- EventFlow2.0 Zero Trust Contextual Verrijking van 100% van de Security Events
- Geautomatiseerde resolutie van 99.999% van de Security Events
- Assistentie en begeleiding bij Incident Response

Compliance en Verbetering
- Zero Trust Strategy Implementation
- Registratie van High-Value Asset
- Best Practice Violation Alerts
- Zero Trust Fitness
- Protect Surface Management en Dashboard
- Zero Trust Maturity Dashboard
- Compliance, Incident en Service Rapportages

Wij zijn jouw security geweten

Zelfs als je organisatie beschikt over een grote, eigen IT-afdeling, biedt het uitbesteden van het SOC uitgebreide security voordelen die je zelf vaak moeilijk in huis kunt halen. Wanneer je je security overlaat aan het ON2IT mSOC™, profiteer je van de professionele expertise van meerdere specialisten met verschillende achtergronden op het gebied van informatiebeveiliging. ON2IT is 's werelds eerste managed cybersecurity bedrijf dat cybersecurity op basis van de Zero Trust-strategie van John Kindervag als een managed service kan leveren.

Waarom met ON2IT werken?

Onze managed services bieden:

- Evaluatie van 99,999 procent van alle security events verminderd automatisch valse meldingen;
- Reveal AI-based threat hunting;
- Zelflerende SOC door middel van gecodificeerde evaluatie door SOC-analisten;
- 24/7 eyes on glass;
- Hoogopgeleide ervaren SOC-analisten;
- Incident response en rapid response mogelijkheden;
- Security Improvement Advisories

Cybersecurity Incident Response

Het Cybersecurity Incident Response Team (CIRT) van ON2IT is voorbereid op alle soorten cybersecurity incidenten dankzij adequate en efficiënte procedures, checklists en trainingen.

Het CIRT richt zich op de dagelijkse afhandeling van incidenten en het reageren op P1-incidenten. In het geval van een groot incident escaleert het CIRT naar een Major Incident Response Team (MIRT).

Onze teams zijn getraind om te werken met vastgestelde protocollen en checklists om de data integriteit tijdens en na een incident te handhaven.

AUXO™: het centrum van onze dienstverlening

Het ON2IT mSOC™ werkt vanuit ons in-house ontwikkelde Security Orchestration, Automation and Response (SOAR) Platform: het geautomatiseerde centrum van onze Managed Security Services.

Wij bieden onze Zero Trust as a Service klanten de uitgebreide versie van ons SOAR-platform: AUXO™. AUXO™ geeft klanten toegang tot de essentiële Zero Trust bouwstenen, inclusief het vijf-stappen model, in een uitgebreid, betaalbaar en eenvoudig te consumeren service aanbod.

Wij hebben het platform ontwikkeld omdat wij de voorkeur geven aan flexibiliteit, onafhankelijkheid, automatisering en innovatie boven de technische beperkingen van handmatige controles.

Hierdoor kunnen jij en wij meer tijd besteden aan belangrijke zaken en innovaties. Dankzij dit platform kan onze mSOCTM optimaal presteren. Bovendien verbetert het systeem met elke SOC-actie.

Automatisering is volgens ons niet alleen wenselijk, maar absoluut noodzakelijk om handmatige controles – en bijgevolg de kans op menselijke fouten – tot een minimum te beperken. Het is ook de enige manier om de steeds groter wordende datastromen snel en goed te kunnen controleren. Automatisering levert uiteraard tijdwinst op en vertaalt zich in een ongekende betrouwbaarheid.

Met ons platform monitoren we jouw IT-security, detecteren en onderzoeken we threats en geven we je aanbevelingen om individuele incidenten op te lossen en je infrastructuur sterker te maken. Ook kunnen we automatisch policies aanpassen en verbeteringen aanbrengen zodat je continu profiteert van de best mogelijke preventie.


mSOC™
AUXO™

De best mogelijke preventie met een optimale visibility

AUXO™ integreert Zero Trust-expertise van wereldklasse, technologieën, ontwerp- en implementatie services in onze managed security operations centers. Dankzij verregaande automatisering zorgen we voor de best mogelijke preventie, en onze orchestratie zorgt voor optimale zichtbaarheid en controle.

Securityoverzicht per protect surface
Door een verregaande segmentatie in functionele domeinen bieden we inzicht in de securitystatus per segment, applicatie of datatype. Zo vallen abnormaliteiten direct op en weten we bij een infectie meteen waar het probleem zit – en kunnen we dus sneller reageren.

Rules of Engagement
In onze Rules of Engagement staat beschreven welke geautomatiseerde acties het platform onderneemt zonder tussenkomst van menselijk handelen. Dit gebeurt op basis van best practices en ingestelde parameters. De best practices zijn beschreven in zogenaamde playbooks. Hierdoor kunnen we een antwoord bieden op een mogelijke aanval. De playbooks worden continu geüpdatet met nieuwe bevindingen en ervaringen. Dit betekent dat het systeem steeds beter wordt, en dat elk incident onze preventie verder versterkt.

Indicators of Good
Vaak zoeken securityspecialisten uitsluitend naar zogenaamde Indicators of Compromise (IoC's): aanwijzingen waarmee de aanwezigheid van een specifieke dreiging, zoals een bepaald malware-exemplaar, binnen het netwerk kan worden vastgesteld. Omdat je bij dreigingen die je niet kent ook niet weet wat je zoekt, hebben wij voor een omgekeerde aanpak gekozen, en gaan we eerst op zoek naar de Indicators of Good. Wij kijken bij het filteren van verkeer naar wat wel is toegestaan. Welke applicaties zijn akkoord, welke gebruikers enz. Dit maakt dat we uiteindelijk veel minder data hoeven te inspecteren, en daarmee zijn we sneller en vinden we ook sneller abnormaliteiten.


ZERO TRUST
DEFINE YOUR
PROTECT SURFACES

Hoe te beginnen met Zero Trust

Het ON2IT Readiness Assessment behandelt op transparante wijze de readiness requirements op de drie afzonderlijke organisatorische niveaus van cybersecurity.

De assessment bepaalt het doel van elk niveau, evenals of jouw bedrijf klaar is voor de benodigde services, en wat de relevante Critical Success Factors zijn. Op basis van de resultaten kunnen CISO's het gat dichten tussen de huidige en gewenste situatie en kan er een implementatie- en verbeterplan ontwikkeld worden.

Het assessment – met vragen op basis van 12 jaar Zero Trust ervaring – levert inzicht in en controle op alle drie deze niveaus en doet dit in klare taal aan de hand van relevante en meetbare maatregelen.

Na een initiële Zero Trust Readiness Assessment, wanneer je weet waar je staat, kun de Zero Trust Scoping tool inzetten om te bepalen welke onderdelen van je netwerk de eerste kandidaten zijn voor Zero Trust segmentatie.

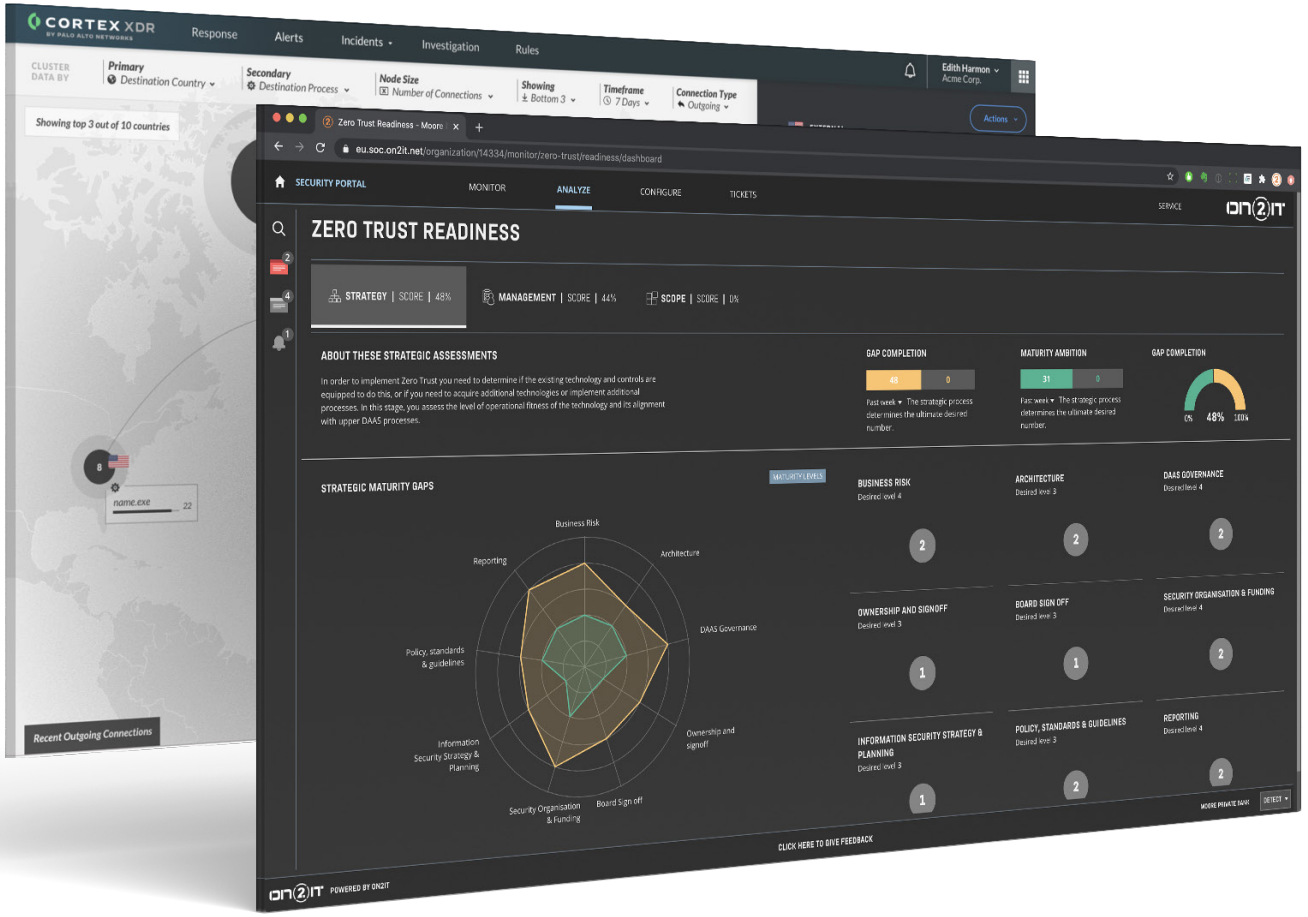
Gedetailleerde micro-segment dashboards bieden drill- downs tot het individuele control niveau en de operationele status hiervan, inclusief scoping en second line risk assessment. Aan de hand hiervan bepalen wij je Zero Trust Fitness™ Score.

Never trust, always verify

De Zero Trust aanpak kent 'never trust, always verify' als leidraad. Vooraf is er geen aanname over de mate van betrouwbaarheid; of het nu gaat om gebruikers, hosts of datasets. Daarnaast is toegang tot data gelimiteerd op een need-to-know basis.

Op basis van inzicht in data en verkeersstromen is het netwerk – en de beveiliging ervan – 'van binnen naar buiten' ingericht en wordt alle verkeer binnen het netwerk geïnspecteerd en gelogd.

Gecombineerd met de vergaande segmentatie van netwerk, applicaties, gebruikers, datasets en 'kroonjuwelen' biedt de Zero Trust strategie de best mogelijke en meest efficiënte IT-security die je je kunt wensen.


CORTEX XDR
Response
Alerts
Incidents
Investigation
Rules
Showing top 3 out of 10 countries
Recent Outgoing Connections
Zero Trust Readiness - Moore
eu.soc.on2it.net/organization/14334/monitor/zero-trust/readiness/dashboard
SECURITY PORTAL
MONITOR
ANALYZE
CONFIGURE
TICKETS
ZERO TRUST READINESS
STRATEGY | SCORE | 48%
MANAGEMENT | SCORE | 44%
SCOPE | SCORE | 0%
ABOUT THESE STRATEGIC ASSESSMENTS
GAP COMPLETION
MATURITY AMBITION
STRATEGIC MATURITY GAPS
Business Risk
Architecture
DAAS Governance
Ownership and signoff
Board Sign off
Security Organisation & Funding
Information Security Strategy & Planning
Policy, standards & guidelines
Reporting
BUSINESS RISK
ARCHITECTURE
DAAS GOVERNANCE
OWNERSHIP AND SIGNOFF
BOARD SIGN OFF
SECURITY ORGANISATION & FUNDING
INFORMATION SECURITY STRATEGY & PLANNING
POLICY, STANDARDS & GUIDELINES
REPORTING
CLICK HERE TO GIVE FEEDBACK
POWERED BY ON2IT

Meer weten?
Wil je meer weten over onze Managed Security Services, neem dan contact met ons op via (+31) 088-2266200.

ON2IT
ZERO TRUST INNOVATORS

Hogeweg 35 / 5301 LJ Zaltbommel / Algemeen 088-2266200

ZERO TRUST INNOVATORS

www.on2it.net