
ZERO TRUST
AS A SERVICE
MANAGED PREVENTION
on2it
ZERO TRUST INNOVATORS

ON2IT
ZERO TRUST INNOVATORS

Can you inform your CEO within minutes of a data breach?

Data theft and cyberattacks are a harsh reality. No matter how much you focus on prevention, the risks can never be eliminated. But what is the best way to defend yourself? And how do you ensure that, in the event of a data breach, you know everything you need to know within 30 minutes? Do you know immediately what happened, which data was impacted and how the attack was stopped?


ZERO TRUST
THE ONLY
PREVENTION
STRATEGY

A strategy for constantly evolving hacking techniques

This new, fast, digital world requires an efficient and reliable approach to IT security. The classic cybersecurity model draws a line between 'the unsafe outside world' and the 'familiar' own network. Firewalls must keep out undesirable traffic and, once inside the network, all traffic is regarded as trustworthy.

The exploded use of mobile devices, web applications and network access by employees working at home, customers, suppliers or patients requires an entirely different IT security concept: Zero Trust. Zero Trust is an effective strategy to ensure your security is future proof and not dependent on specific software or hardware. It is easy to shape the method that works best for you, regardless of where you store your data.

Authentic Zero Trust

We take the entire security process off your hands so that you can focus on what matters: managing your business and achieving growth. We supply our Managed Security Services from our state-of-the-art SOC, where we work with a combination of the best technological solutions and a team of expert security specialists. Our services are guided by the Zero Trust principles. This sets us apart. Our unique approach in the market has made us a leading player.

Who and what can you trust these days?

The IT world is constantly changing. How we look at cybersecurity has also changed dramatically over the past few years.

In 2009, Forrester analyst John Kindervag introduced his Zero Trust security strategy in the United States. Shortly after, ON2IT was the first company in Europe to cultivate the same philosophy.

Zero Trust Security enables you effectively to reduce the impact of the attacked area in the entire network. Divide the network into different segments and apply protection measures consistent with the sensitivity of the data within each segment.

Make sure you also have segments that are separate from each other, so any security incident will impact only the one segment and not the entire network.

We were one of the first to embrace the Zero Trust philosophy of securing IT-networks, and we actively contribute to its development.

What is Zero Trust?

The Zero Trust approach uses the guiding principle of ‘never trust, always verify’. There is no assumption in advance about the degree of reliability, whether concerning users, hosts or data sets. Furthermore, access to data is limited to a need-to-know basis.

Based on insight into the data and traffic flows, the network and its protection are set up ‘from the inside out’. All traffic within the network is inspected and logged.

Zero Trust is based on four principles:

- Define business outcomes
- Design from the inside out
- Determine who or what needs access
- Inspect and log all traffic

Zero Trust: a strategy

Zero Trust is a strategic initiative that prevents successful data breaches by eliminating the need for digital trust in your organization. Rooted in the principle of ‘never trust, always verify’, Zero Trust is designed as a strategy that resonates with the highest levels of any organization yet is tactically deployed using off-the-shelf technology.

Zero Trust strategy is decoupled from technology. While technologies improve and change over time, the strategy remains the same.

The main advantages of Zero Trust:

- Minimal exposure to cyberthreats
- Lower operating costs
- Greater continuity for crucial business processes
- Better and cost-effective compliance
- Future-proof architecture

The best service with the best people

We offer our Managed Security Services from our managed Security Operations Center (mSOC™).

ON2IT's managed security gives you 24/7 access to our experienced security engineers and our AUXO™ platform, both of whom operate using best practices and well-documented procedures. Our security services extend your own IT department, giving you an understanding and control of your network security status.


HOW TO
OPERATIONALIZE
ZERO TRUST

What our mSOC™ does

The ON2IT mSOC™ gives you complete IT security in a way that is difficult for many organizations to achieve internally. It is often hard to find and retain the right people – the 'war for talent' is still raging – and budgets are often insufficient. Our mSOC™ offers world-class 24/7 managed detection and response, augmented by a unique set of prevention and compliance services, all bundled as Zero Trust as a Service.

Managing Prevention

- Zero Trust Cybersecurity Controls / Management
- Self-learning Security Operations Center
- Zero Trust Policy Validator
- Cybersecurity Improvement Advisories
- ROE™ Automated Rules of Engagement
- Countermeasures

Alerting and Alarming

- Cybersecurity Monitoring
- Experienced Cybersecurity Analysts
- Reveal AI-based Threat Hunting
- EventFlow2.0 Zero Trust Contextual Enrichment of 100% of Security Events
- Automated Resolution of 99.999% of Security Events
- Incident Response Assistance and Guidance

Compliance and Improvement

- Zero Trust Strategy Implementation
- High-Value Asset Registration
- Best Practice Violation Alerts
- Zero Trust Fitness
- Protect Surface Management and Dashboard
- Zero Trust Maturity Dashboard
- Compliance, Incident and Service Reporting

We are your security conscience

Even if your organization has its own large IT department, expanding it with our mSOC™ provides extensive security benefits that are often difficult to obtain yourself. When you entrust your security to the ON2IT mSOC™, you benefit from the professional expertise of highly qualified specialists with different backgrounds in information security. ON2IT is the world's first managed cybersecurity that can deliver cybersecurity based on John Kindervag's Zero Trust strategy as a managed service.

Why work with ON2IT?

Our managed services provide:

- Evaluation of 99.999 per cent of all your security events automatically and dramatically reduces false positives;
- Reveal AI-based threat hunting;
- Self-learning SOC through codified SOC analyst evaluation;
- 24/7 eyes on glass;
- Highly trained experienced SOC analysts;
- Incident response and rapid response capabilities;
- Security improvement Advisories.

Cybersecurity Incident Response

ON2IT's Cybersecurity Incident Response Team (CIRT) is prepared to deal with all types of cybersecurity incidents thanks to adequate and efficient procedures, checklists and training.

CIRT has a focus on day-to-day dealing with incidents and responding to P1 incidents. In case of a major incident, the CIRT escalates to a Major Incident Response Team (MIRT).

Our teams are trained to work with established protocols and checklists to maintain data integrity during and after an incident.

AUXO™: the core of our services

The ON2IT mSOC™ operates from our in-house developed Security Orchestration, Automation and Response (SOAR) Platform: the automated center for our Managed Security Services.

We provide our Zero Trust as a Service customers with the extended version of our SOAR platform: AUXO™. AUXO™ gives customers access to the essential Zero Trust building blocks, including the five-step model, in a comprehensive, affordable and easy-to-consume service offering.

We developed the platform because we prefer flexibility, independence, automation and innovation rather than the technical limitations of manual checks. This enables you and us to spend more time on key issues and innovations. This platform allows our mSOC™ to perform optimally. Plus, the system improves with every SOC action.

We believe that automation is not only desirable but necessary to minimize manual checks and limit the risk of human error. It is also the only way to control ever-increasing data flows quickly and effectively. Automation also saves time and generates unprecedented reliability.

With our platform, we monitor your IT security, detect and investigate threats and give you recommendations for solving individual incidents and strengthening your infrastructure. We can also automatically adjust policies and make security improvements so that you always benefit from the best possible prevention.


mSOC™
AUXO™

The best possible prevention with optimal visibility

AUXO™ integrates world-class Zero Trust expertise, technologies, design and implementation services into our managed security operations centers. Thanks to far-reaching automation, we provide the best possible prevention, and our orchestration ensures optimal visibility and control.

Security overview per protect surface
With far-reaching segmentation in functional domains, we provide insight into the security status per segment, application or data type. Abnormalities are immediately noticeable. In the event of an infection, we know right away where the problem lies and can respond more quickly.

Rules of Engagement
Our Rules of Engagement describe the automated actions the platform takes without human intervention. This is done based on best practices and set parameters. Best practices are explained in our playbooks. These allow us to provide an answer to a possible attack. We continuously update the playbooks with new findings and experiences. This means that the system is getting better and better and that every incident further strengthens our prevention.

Indicators of Good
Security specialists often only look for Indicators of Compromise (IoCs): indicators that make it possible to determine the presence of a specific threat within the network, such as a particular malware copy. Because you don't know what to look for in the case of unknown threats, we have opted for a reversed approach, where we first look for the Indicators of Good. When filtering traffic, we focus on what is allowed, what applications are approved, which users. This means that we need to inspect much less data in the end. This speeds up the process and allows us to detect abnormalities more quickly.


ZERO TRUST
DEFINE YOUR
PROTECT SURFACES

How to get started with Zero Trust

The ON2IT Readiness Assessment transparently addresses the readiness requirements at the three separate organizational levels of cybersecurity.

The Assessment determines each level's objective, and whether your business is ready for the required services and the relevant Critical Success Factors. Based on the results, CISOs can determine the gap between the current and the desired situation and develop an implementation and improvement plan.

With inquiries based on ten years of Zero Trust experience, the assessment provides insight and control across these levels with a common language and metrics for relevant measures.

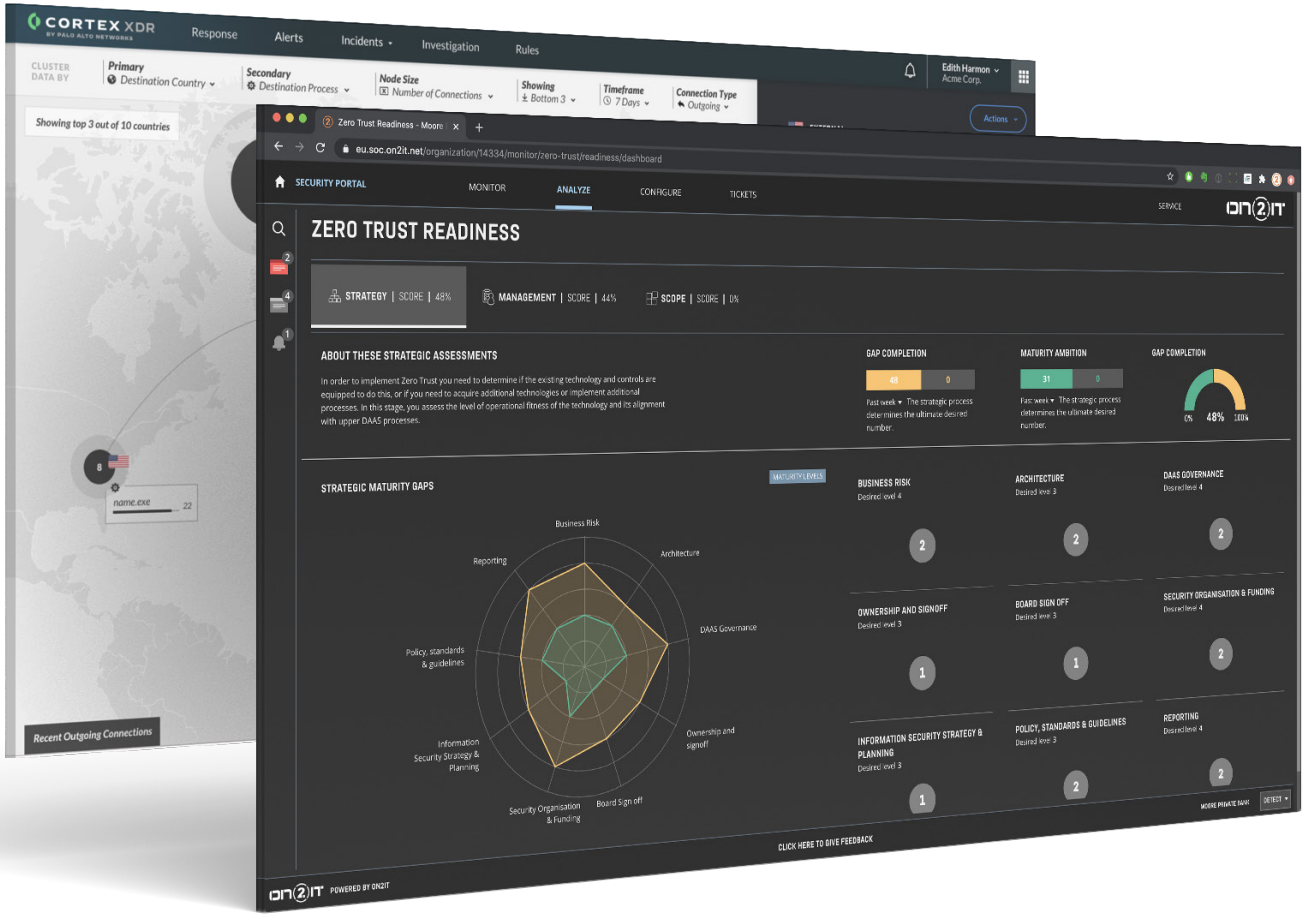
After the initial Zero Trust Readiness Assessment, you know where you stand. You can use the Zero Trust Scoping tool to determine which parts of your network are the primary candidates for Zero Trust segmentation. Detailed protect surface dashboards offer drilldowns to the individual control level and its operational status, including scoping and second-line risk assessment. We use this to determine your Zero Trust Fitness™ Score.

Never trust, always verify

The Zero Trust approach uses the guiding principle of 'never trust, always verify'. There is no assumption in advance about the degree of reliability, whether concerning users, hosts or data sets. Moreover, access to data is limited to a need-to-know basis.

Based on insight into the data and traffic flows, the network and its protection are set up 'from the inside out'.

Combined with extensive segmentation of the network, applications, users, data sets and 'crown jewels', the Zero Trust strategy provides the best possible and most efficient IT security that you could wish for.


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

More information?
For more information about our managed security services, please contact us on (214) 206-8446.

ON2IT
ZERO TRUST INNOVATORS

7300 Lone Star Drive / Suite C200 Plano, TX 75024 / (214) 206-8446

ZERO TRUST INNOVATORS

www.on2it.net