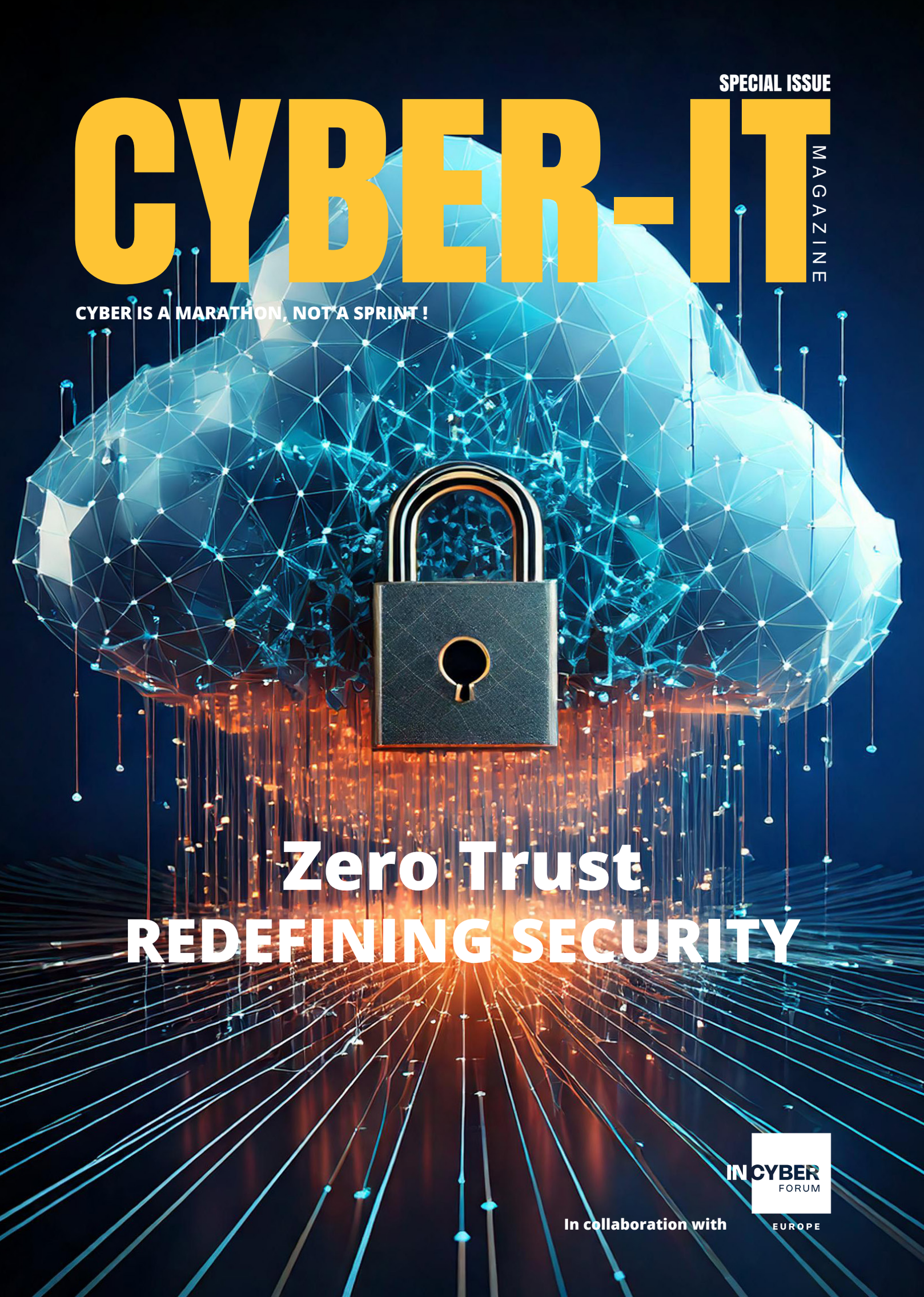
SPECIAL ISSUE

CYBER-IT MAGAZINE

CYBER IS A MARATHON, NOT A SPRINT !



Zero Trust
REDEFINING SECURITY

In collaboration with

IN CYBER FORUM EUROPE

Inquiries / Requests ?
cyberit.magazine@gmail.com

EDITO

Dear readers,

The InCyber Forum is a unique chance to step back and reflect on the issues shaping our digital world. We are grateful to the InCyber Forum's team for giving us the opportunity to connect with our readers in person and dive into the conversations that matter.

In recent years, the shift to remote work, the surge in connected devices, and the growing sophistication of cyberattacks have pushed us to rethink the way we approach security. One concept has emerged as a game-changer : Zero Trust.

It might sound complex, but it's becoming essential. Embracing a Zero Trust model means rethinking the way we secure our systems, our networks, and their users. It calls for a coordinated continuous effort from leadership, security teams, and everyday users.

In this special issue, we'll explore the many aspects of Zero Trust, starting with the origins of the concept as we know it today, and ending with a deep dive into how it's being implemented across organizations.

Zero Trust can seem like an abstract concept, but its creator, John Kindervag, developed an analogy that makes it easier to comprehend. In the following pages, we'll explore this analogy through his own explanation.

ARNAUD LEROY

CONTENTS

Zero Trust
Not as new as we think

The term “Zero Trust” was officially created in 2010 by analyst John Kindervag, and its definition was later included in the 2021 NSTAC report (National Security Telecommunications Advisory Committee), a comprehensive document produced by the U.S. National Security Telecommunications Advisory Committee.

At its core, Zero Trust is a cybersecurity strategy built on a simple but powerful principle: no user should be trusted. It assumes that a breach has either already happened or is inevitable.

As a result, no user should be granted access to sensitive data based solely on a single verification at the organization level.

Instead, every user, device, application, and transaction must be continuously verified. The Zero Trust concept appeared in 2010, when Kindervag, then at Forrester Research, challenged the dominant security model.

Back then, network security relied heavily on the idea of trust zones: anything outside the firewall was considered “untrusted,” while everything inside was deemed “safe.”

Kindervag quickly identified this blind trust as a flaw, one that attackers were all too eager to exploit.

Timeline of a concept

Defining network protection

Engineers at Digital Equipment Corporation (DEC) published the first article about firewall technology, marking the beginning of decades of thinking around segmented network security

1987

Network access control

L'IEEE Standards Association publie le protocole 802.1X pour le contrôle d'accès au réseau (NAC)

2001

1990

THE EARLY DAYS

The Jericho Forum is founded, recognizing a major shift: users and applications are moving beyond the boundaries of the corporate network. It introduces the early foundations of Zero Trust through the concept of de-perimeterisation

2010

Network segmentation

Early attempts to segment networks begin to emerge through the use of VLANs and subnets. These methods required no authentication, offered minimal restrictions, and included very limited internal security features

2010

Birth of zero trust

Analyst John Kindervag introduces the "Zero Trust model" in a Forrester Research paper. He shifts authentication and security into the data flow and suggests segmenting sessions. Still focused on network access, his model moves the perimeter inside the network

Google step in

Google's BeyondCorp initiative redefines traditional enterprise security architecture. Following the Operation Aurora attack, the company begins implementing the Zero Trust model across its entire organization

2014

Gartner & ZTNA

Gartner introduces the concepts of SASE (Secure Access Service Edge) and ZTNA (Zero Trust Network Access)

2019

2016

Zero Trust in the cloud

Zscaler introduces the first cloud-delivered Zero Trust solution, allowing organizations to eliminate external attack surfaces and reduce the risk of lateral movement

2020

NIST defines the zero trust framework

The NIST releases Special Publication 800-207 as a unified model for establishing a Zero Trust Architecture (ZTA), marking the first major shift in how Zero Trust is formally defined within network security frameworks

2021

SSE in the spotlight

According to Gartner, the security components of SASE are recognized as a new standalone market category: Security Service Edge (SSE)

2022

The US enforces zero trust

The Office of Management and Budget requires all federal agencies to adopt Zero Trust principles by 2024 marking a major policy shift in U.S. cybersecurity strategy

Source : Zscaler

UNDERSTANDING ZERO TRUST

UNDERSTANDING ZERO TRUST THROUGH A US SECRET SERVICE ANALOGY

Article based on an interview with John Kindervag, conducted by MIEL.
Interview by Kamel Mouhoubi

John Kindervag, the creator of the Zero Trust concept, sat down with Kamel Mouhoubi for an interview on MIEL's media channel. During this in-depth conversation, he drew a compelling analogy between the U.S. Secret Service and the core principles of Zero Trust. Here are the main takeaways.

When the U.S. Secret Service protects the President, they rely on three key pieces of information that we often overlook.
First, they know exactly who the President is, they are not trying to figure that out.

Second, they always know where the President is. You will never hear someone ask,
"Do you have the President with you ?" That simply does not happen.
Third, they know precisely who is allowed to access the President at any given moment.
These are the three core questions you should be asking, whether you are protecting the President, your data, or your digital assets. The principle is the same.

A powerful visual example of this concept is President Barack Obama's inauguration parade in 2009. In the top right corner of the image, you can see a perimeter guarded by agents. But those agents are not there for actual protection, they are a visible warning, a signal not to cross that line. The real security lies lower in the frame.

The vehicle represents the real security zone. It embodies the tactical core of the Zero Trust model.

To apply Zero Trust properly, you must understand the concept of a protect surface, because without it, the entire idea loses its meaning. The protect surface is the opposite of the attack surface. And it is where Zero Trust begins.

The attack surface is too vast to control. The real solution is to flip the problem, reduce it to something small, well-defined, and easy to understand. That is what we call the protect surface. In this analogy, the protect sur-

face is represented by four individuals inside the vehicle (symbolizing the President, his wife, and their two children). If those four people make it through the day unharmed, then the Secret Service has done its job.

They know exactly what and who they are supposed to protect, and that is precisely what cybersecurity should be about: understanding what truly needs protection.

In the image, you can see how the Secret Service operates close to the protect surface. They establish a tight, contained zone that isolates the President and his family from everything outside. They perform a task we often fail to do in cybersecurity: managing access to this micro-perimeter.

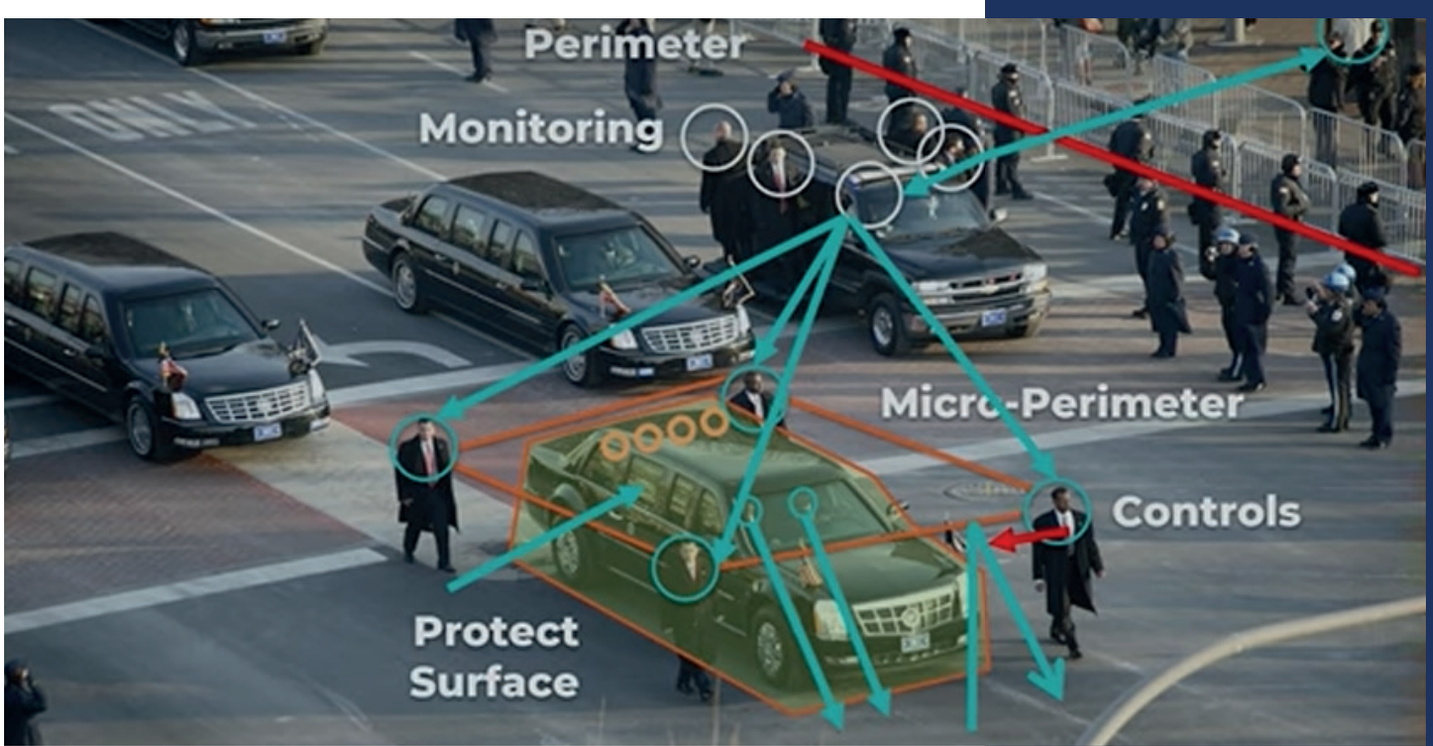
We tend to run our security checks far from what we are actually trying to protect. This creates a vulnerable in-between zone, what we commonly refer to as the internal network. It is a buffer area between the asset and the perimeter.

Zero Trust removes that buffer. There is nowhere to hide, because everything trying to access sensitive resources is fully visible. That visibility is key.

At the heart of it all is policy. Security policies are the foundation of any cybersecurity strategy, and especially of the Zero Trust model. If something bad happens, it is likely because the policy in place allowed it to.
In a Zero Trust context, a policy does one thing only: it either allows or denies access. No exceptions.

We start with a deny-all strategy. Then, we build out detailed access rules based on what an individual actually needs to do their job. If someone tries to approach the President, the agents near the vehicle will immediately stop them, that is the deny policy in action.

These agents are constantly watching and updating their rules. They gather threat intelligence information in real time by observing the crowd.
For example, the person dressed in white in the upper right corner of the image is already being monitored.
They also have the ability to adjust their policy dynamically, to allow someone to get access to the President under specific conditions, for example.
All of this translates directly into cybersecurity.



Zero Trust, mission impossible ?

Transitioning to Zero Trust is an ambitious goal and a long-term transformation journey. But it is also a real opportunity to adapt to an environment that has changed significantly over the past decade.

Understanding the concept : The Key to Successful execution

Launching a Zero Trust project requires a solid understanding of its core concepts, along with the technological components that make practical implementation possible. The goal is to tailor the vision to your organization's specific context.

Success starts with understanding the main principles of Zero Trust, principles that will guide the entire project, from technology selection to deployment strategy. The Zero Trust model states that "all users and devices should be able to access the appropriate resources, from any location, under the same security standards." It revolves around three core pillars: verification, enforcement, and assumption of breach.

1.Continuous controls
Access decisions must dynamically take into account contextual signals, such as user's identity, location, device type and its security status, etc…

2.Enforcing Least Privilege Access
Access must be granted based on the principle of least privilege. This means ensuring, based on contextual information, that a user only has the exact level of access required to perform a specific task within an application. Access can also be restricted by defining a specific time frame to perform the task.

3.Operating under the assumption that compromise is a reality
Operate under the assumption that your environment may already be compromised. The goal is to detect threats quickly, neutralize them effectively, and limit their impact as much as possible.

Identifying Expectations Around Zero Trust Implementation

The fundamental question becomes: What problems need to be solved and in what order of priority?

To achieve this, the process typically starts with non-technical **brainstorming workshops.**

The goal is to identify expectations by expressing them as high-level objectives, free from technical details or complexity.

Once the list is established, you will need to prioritize each expectation. For example, you might decide to focus first on defending against ransomware or ensuring the protection of critical data.

The possible options for addressing each requirement may involve different Zero Trust pillars, a variety of technologies per pillar, and varying levels of implementation complexity.

Expectations generally fall into two categories: strengthening security and adopting a thoughtful approach to emerging scenarios, in line with today's evolving challenges. Security naturally plays a central role, as Zero Trust is fundamentally a modern security model.

However, it is equally important to assess the business value of Zero Trust. Security should not be viewed solely through a negative or alarming lens. Instead, it should be seen as a tool for adaptation, one that helps protect resources and ensure business continuity in an increasingly complex environment.

Defining Your Maturity Level

When you begin your Zero Trust journey, **you are not starting from scratch.** You will need to evaluate your existing environment and chances are, you have already integrated tools or technologies that align with the Zero Trust model. You may also already have conditional access policies in place to protect access to certain applications, or you might be using multi-factor authentication (MFA) for some groups of employees. To assess your Zero Trust maturity level, you can refer to Microsoft's Zero Trust Maturity Model white paper. The table below provides an overview of the Identities and Devices pillars. Depending on the capabilities you have already implemented, you may fall into a **Traditional, Advanced, or Optimal** maturity level for each pillar.

This maturity assessment is a valuable first step in understanding your current position. It allows you to identify existing solutions that align with the Zero Trust approach, estimate the complexity of integrating them, and determine which solutions may need to be replaced.

Take ransomware detection, for example. If your SIEM can't effectively detect and respond to such attacks in real time, this becomes a weak point. You might consider deploying an EDR solution, ideally paired with a SIEM capable of quickly detecting compromised endpoints and isolating them to prevent lateral movement.

Or maybe rebuilding a large number of workstations in a short amount of time is too complex ? In that case, a high-performance, automated solution, ideally delivered as a cloud service, should be considered.

Starting with the Quick Wins

Quick wins offer a clear advantage: they are **motivating** for teams and deliver tangible results fast. They also help reassure stakeholders at a higher level about the feasibility and benefits of a Zero Trust initiative.

The downside ? Quick wins can sometimes create a false sense of satisfaction, giving the impression that "we completed Zero Trust", when in fact it is just the beginning. For example, rolling out Single Sign-On (SSO) for the most widely used or business-critical applications is a highly visible step that is not necessarily complex to implement. If the main concern is ransomware prevention, deploying an Endpoint Detection and Response (EDR) solution can quickly provide visibility into workstation threats and help respond accordingly.

A quick win should be seen

	Traditionnel	Avancé	Optimal
Identités	Le référentiel d'identité est on-premises Pas de SSO entre le cloud et les applications on-premises Visibilité limitée sur les risques liés à l'identité	L'identité Cloud est fédérée avec le système on-premises Les politiques d'accès conditionnel contrôlent l'accès et fournissent des actions correctives L'analyse des signaux améliore la visibilité	L'authentification sans mot de passe est activée L'utilisateur, l'appareil, l'emplacement et le comportement sont analysés en temps réel pour déterminer les risques et fournir une protection continue
Appareils	Les appareils sont joints au domaine et gérés avec des solutions telles que Group Policy Object ou Config Manager Les appareils doivent être connectés au réseau pour accéder aux données	Les appareils sont enregistrés auprès du fournisseur d'identité cloud Accès uniquement accordé aux appareils gérés et conformes dans le cloud Les stratégies DLP sont appliquées pour les appareils d'entreprise et BYO	Un EDR (Endpoint threat detection) est utilisée pour surveiller les risques liés aux appareils Le contrôle d'accès est basé sur le risque de l'appareil pour les appareils d'entreprise et BYO

Microsoft's Zero Trust Maturity Model – Assessment Overview

as a tactical milestone, a direct, measurable gain that fits into a broader, long-term strategic approach: the transition to a Zero Trust model.

Prioritizing Identity First

In the Zero Trust model, identity is the essential element, tightly linked to the device used for access. Some even argue that "identity is the new perimeter," given that many breaches now exploit identity-based vulnerabilities. Identity compromise is the main entry point for the vast majority of attacks targeting businesses and organizations.

According to the 2024 Trends in Securing Digital Identities report, 90% of organizations experienced at least one identity-related incident over the past year.

To mitigate these risks, organizations can implement passwordless authentication, which eliminates password-related vulnerabilities altogether. This type of authentication can rely on biometric traits such as a fingerprint or facial recognition, or a device-bound PIN that is never transmitted over the network. In addition to strong authentication, conditional access is a core element of the Zero Trust model. It makes real-time access decisions by evaluating the full context of each request, taking into account factors such as user identity risk, device compliance and maturity, location of the request, and other contextual signals collected across the environment.

Monitoring Security

One of the core principles of Zero Trust is the assumption of breach, the idea that, despite all protective measures, an attack may still occur and grant access to the information system.

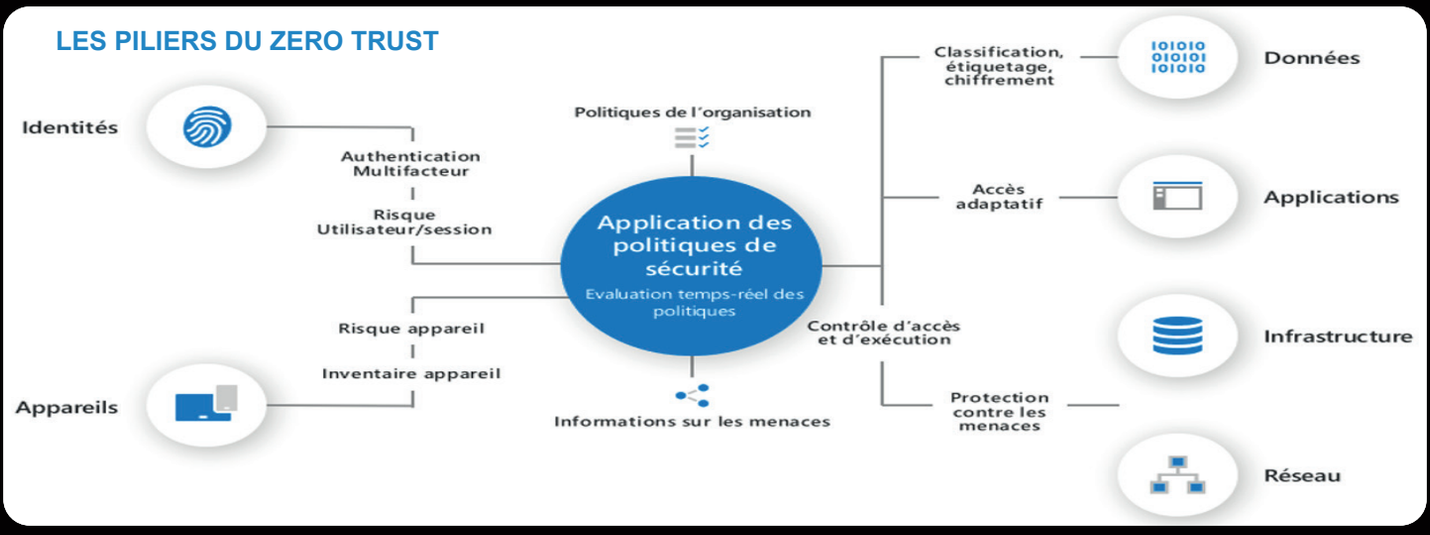
While security monitoring is not always formally listed as a pillar of Zero Trust, it is widely recognized by industry professionals as a cross-cutting component of the model. Since the identity pillar is now considered the “new perimeter” and a primary target for attackers, monitoring identity-related activity has become essential. A SIEM (Security Information and Event Management) platform consolidates signals from a wide range of sources, helping to detect weak signals, generate relevant alerts, and support investigation, without the need to navigate across multiple dashboards.

However, traditional SIEM solutions often produce false positives, which can reduce operational efficiency.

More modern, cloud-based and AI-powered solutions are far more effective at handling large volumes of signals. They help reduce false positives and offer orchestration and automated response capabilities, making them more suitable for today’s dynamic environments.

Internet as the New Corporate Network

One of the key principles of Zero Trust is to ensure consistent security, regardless of where



Source : Microsoft

the user or device is accessing an application or service. Today, most applications are accessible online, whether through SaaS providers or internal applications migrated to the cloud.

When identities are managed through Active Directory, workstations are handled via cloud-based services, applications are remotely accessible, and security systems can operate directly from the cloud, the traditional notion of a corporate network becomes obsolete.

This shift supports the growing idea that “the Internet is becoming the new corporate network.” Best practices for network security architecture, once reserved for internal applications, now also apply to cloud-hosted services, including subnet segmentation, DMZs, and network controls.

It is recommended to implement network segmentation for resources that remain hosted on-premises. For OT and IoT systems, a more precise segmentation is recommended, following a multi-level approach based on the Purdue model, developed by Theodore J. Williams.
.

Build a Roadmap

The roadmap is the final step in this initial phase of your Zero Trust project. It is the exercise that allows you to list all the topics to be addressed, organize them, and estimate the effort and time required for each one. It is important to consider your top priorities and quick wins, even if they are not explicitly included in your broader strategy and to clearly define key milestones.

Each initiative should be mapped across the six main pillars of the Zero Trust model.

These key insights are designed to help you shape your Zero Trust approach, giving you greater clarity to move forward with confidence and strengthen your organization’s security posture.

CREDITS

Editor-in-Chief: Arnaud LEROY
Graphic Design: Arnaud LEROY
English Translation: Maëva ASTORGA
Magazine Mentor: Guillaume POUPARD

April 2025