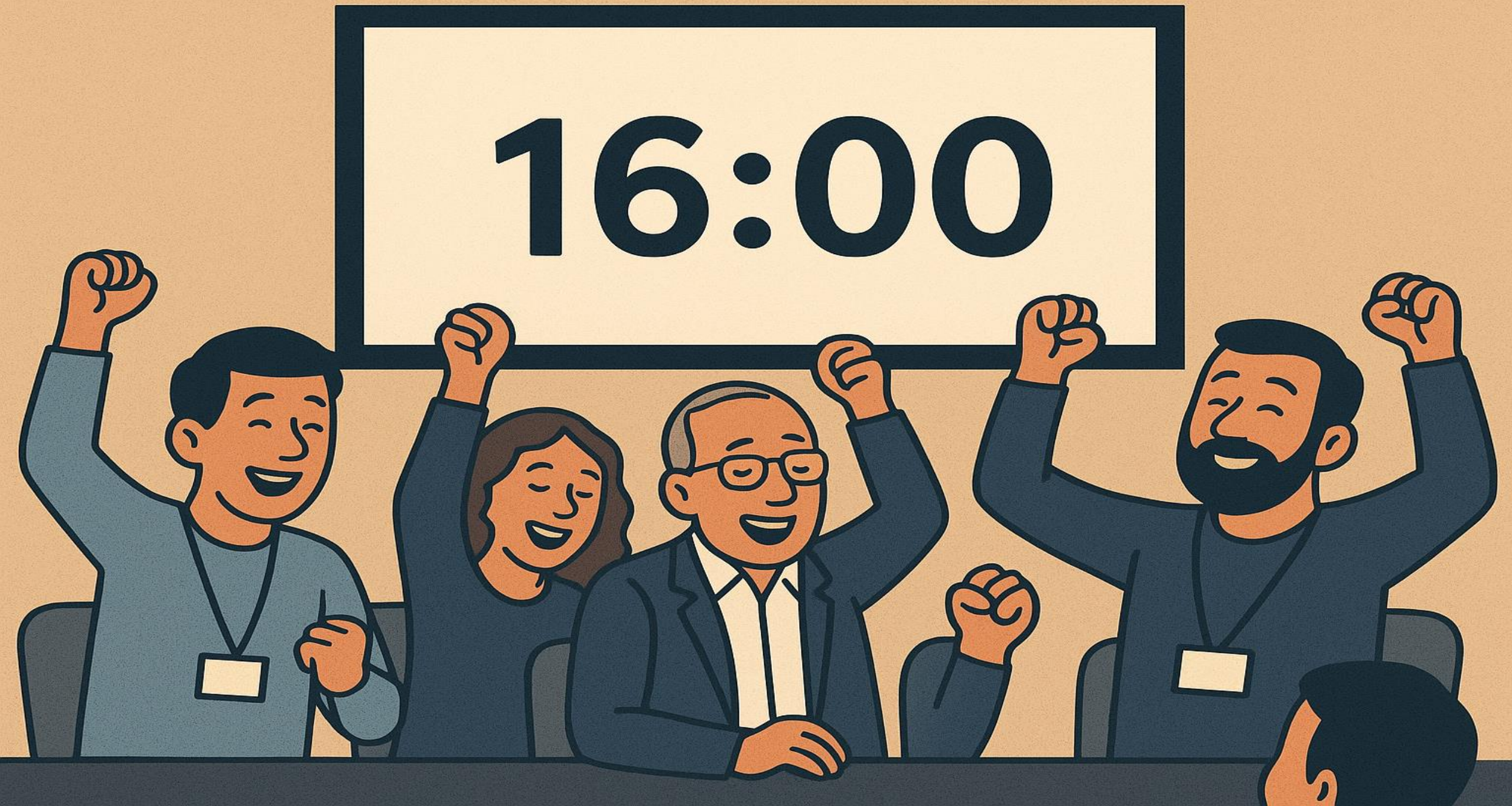
Workplace Ninja

User Group Finland

Zero Trust in Real Life
From Framework to Field Experience


15:15


16:00

“Kysyin kollegalta, miten hän selviää kriiseistä meidän Zero Trust -toteutuksessa.
Hän sanoi: *‘Helppoa: ensin panikoin… ja sitten teen PowerShell-skriptatun workaroundin, jota kadun kolme päivää myöhemmin.’”*

About us

Morten Nilsen

Principle Consultant, twoday

Focus:

Enterprise Security & Compliance

Hobbies:

Keeping my Norwegian wife and kids happy

Contact

morten.b.nilsen@twoday.com

Kent Agerlund

Principle Consultant twoday &
Microsoft Regional Director

Focus:

Enterprise Security & Compliance

Hobbies:

Life

Contact

Kent.Agerlund@twoday.com

Agenda

Workplace Ninja

Helsinki 2025

Zero Trust in Real Life

Introduction

Homework
Your key to success

Zero trust

Zero trust assessment

Closing and Next step

Attendees
All goes hmmm now I understand the session

Attendees
Wondering by now if they should take notes……don't

Attendees
Asking questions and are curious

Attendees
At this time, you can see yourself in these scenarios, and you still have questions

Attendees
I'm ready for a demo

Attendees
Cool stuff, I'm confident I can present this overview to management

Intro Outcome:
- Zero trust is also YOUR responsibility
- It's a teamwork
- Hackers love when you don't take responsibility

Assessment outcome:
- Zero Trust overview
- Zero Trust roadmap
- You own the plan

Session outcome:
- You can perform a Zero Trust GAP analysis
- You know how to engage management and other team members
- You successfully take the first steps

Introduction

Your Zero Trust Homework (starts tomorrow)

1. Run the Zero Trust Assessment Tool

Install → run → open the HTML

Look at the red and orange items

Don't argue the about findings — start the conversations

2. Show the report to someone outside your silo

Entra Admin → show it to Intune Admin

Intune admin → show it to the Security admins

Security admin → show it to Purview Admin

Purwin Admin → show it to hmmm you don't exist

3. Take a step back and *think strategically*

Get a sponsor

Create a roadmap

Where are the quick wins?

Understand what is most important for your organization

Read, share and discuss the Microsoft Digital Defense Report 2025

4. Pick ONE fix each - and help each other deliver it

Examples:

Fix one dangerous device configuration gap

Move one ASR rule from Audit to Block

Clean up one unused admin role assignment

The fairy tale

Yes, every vendor claims to have solved Zero Trust.

Yes, the marketing slides all look the same.

No, none of them tell you *how the hell to actually implement it*.

.. But the reality is

Token theft from phishing is everywhere.

Device trust is often implicit

Data is leaking because people paste confidential content into ChatGPT.

And attackers don’t care about your slide deck maturity model!

The real problems we encounter in the field

Identity is a mess:

- "Yes, we have MFA… but not if you are on our location"

Device posture:

- "Yes, we require compliance… but only for our pilot devices in IT."

Data maturity:

- "We have data classification… but it's in a PDF saved on SharePoint."

Zero Trust "silos"

Policy Optimization
- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Microsoft Defender for Cloud
Secure Score & Exposure score
Compliance Manager

Identities
- Human
- Non-human

Strong authentication

Microsoft Entra ID
ID Protection
Workload ID

Entra ID Governance

Defender for Identity

Request enhancement

Zero Trust Policies
- Evaluation
- Enforcement

Microsoft Entra
Conditional Access

Classify, label, encrypt

Data
- Emails & documents
- Structured data

Defender for Office 365
Microsoft Purview
Microsoft Priva

Network
- Public
- Private

Azure Networking

Entra Internet Access
Entra Private Access

Adaptive Access

Apps
- SaaS
- On-premises

Defender for Cloud Apps

Endpoints
- Corporate
- Personal

Device compliance

Risk assessment

Intune
Device Management

Defender for Endpoint
Extended Endpoint Detection and Response (XDR)

Defender for APIs

Runtime control

Infrastructure
- Serverless
- Containers
- IaaS
- Paas
- Internal Sites

Microsoft Entra
Permissions Management

Defender for Cloud
Azure Arc

Threat Protection
- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Microsoft Defender
- Defender for Endpoint
- Defender for Office 365
- Defender for Identity
- Defender for Cloud Apps
- Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

"Real" Zero Trust

Policy Optimization
- Governance
- Compliance
- Security Posture Assessment
- Productivity Optimization

Microsoft Defender for Cloud
Secure Score & Exposure score
Compliance Manager

Identities
- Human
- Non-human

Microsoft Entra ID
ID Protection
Workload ID

Entra ID Governance

Defender for Identity

Strong authentication

Request enhancement

Zero Trust Policies
- Evaluation
- Enforcement

Microsoft Entra
Conditional Access

Network
- Public
- Private

Azure Networking

Entra Internet Access
Entra Private Access

Classify, label, encrypt

Data
- Emails & documents
- Structured data

Defender for Office 365

Microsoft Purview

Microsoft Priva

Adaptive Access

Apps
- SaaS
- On-premises

Defender for Cloud Apps

Endpoints
- Corporate
- Personal

Intune
Device Management

Defender for Endpoint
Extended Endpoint Detection and Response (XDR)

Device compliance

Risk assessment

Defender for APIs

Runtime control

Infrastructure
- Serverless
- Containers
- IaaS
- Paas
- Internal Sites

Microsoft Entra
Permissions Management

Defender for Cloud
Azure Arc

Threat Protection
- Continuous Assessment
- Threat Intelligence
- Forensics
- Response Automation

Microsoft Defender
Defender for Endpoint | Defender for Office 365 | Defender for Identity | Defender for Cloud Apps | Defender for Cloud

Microsoft Sentinel
- Security Information and Event Management (SIEM)
- Security Orchestration, Automation, and Response (SOAR)

Your attackers don’t care about your Org Chart

- “Not my department” thinking = misconfigurations and blind spots
- Zero Trust requires shared telemetry across Identity, Device, and Data

“Zero Trust dies the moment we say: *‘That’s not my job.’*”

From fancy PowerPoint to field experience

A solution?
The *New* Microsoft Zero Trust Assessment Tool

- It scans your tenant using Graph with read-only permissions.
- It produces a beautiful HTML report with actionable findings.
- It tells you what's broken before attackers tell you.

Demo

How It Works

Here's a quick summary of the steps for you to run the tool. Check our documentation for full details.

First, you install the ZeroTrustAssessment PowerShell module.

```
Install-Module ZeroTrustAssessment -Scope CurrentUser
```

Then, you connect to Microsoft Graph and to Azure by signing into your tenant.

```
Connect-ZtAssessment
```

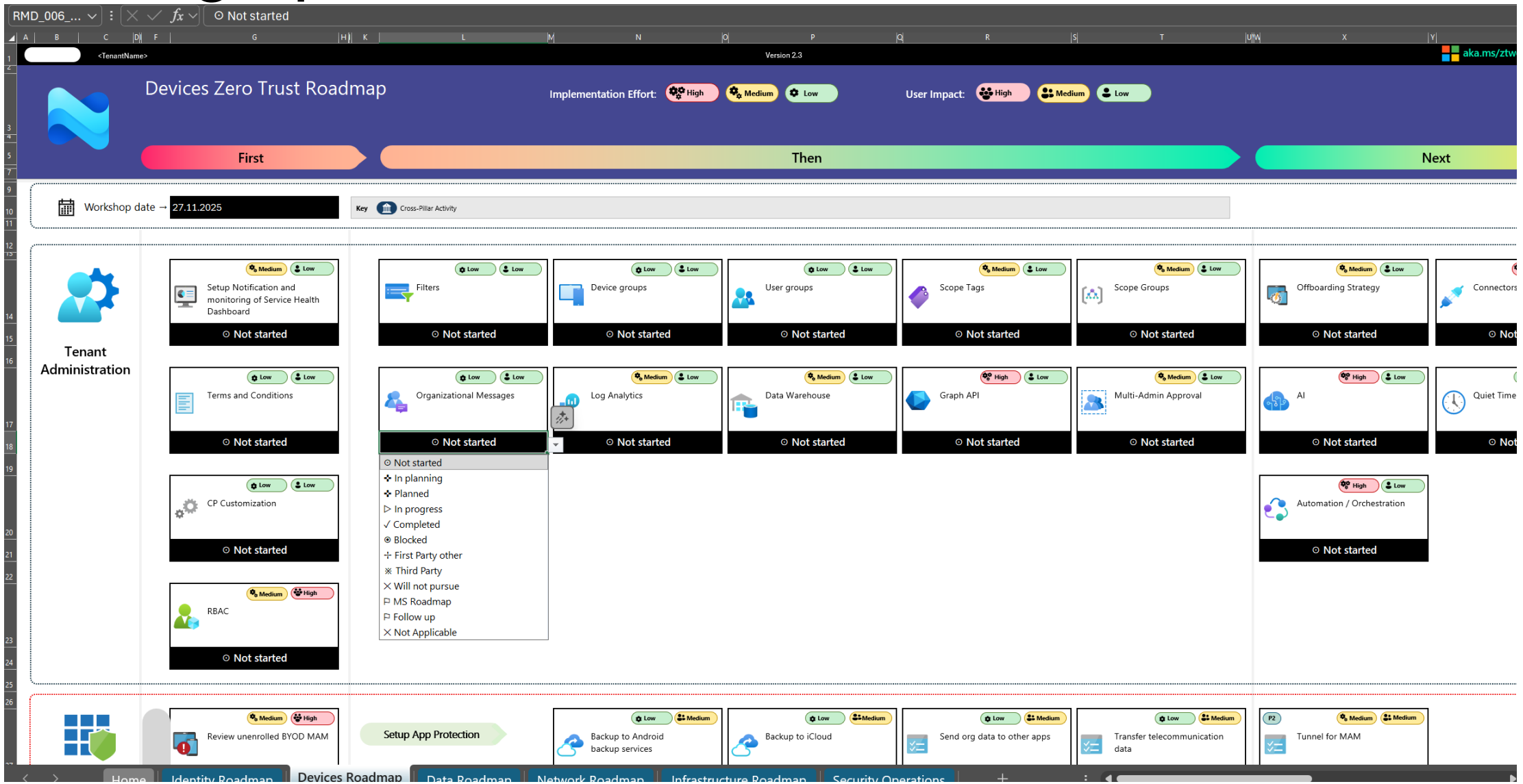
After that, you run a single command to kick off the data gathering. Depending on the size of your tenant, this might take several hours.

```
Invoke-ZtAssessment
```

After the assessment is complete, the tool will display the assessment results report. A sample report of the assessment can be viewed at aka.ms/zerotrust/demo.

The tool uses read-only permissions to download the tenant configuration, and it runs the analysis locally on your computer. We recommend you treat the data and artifacts it creates as highly sensitive organization security data.

Getting operational

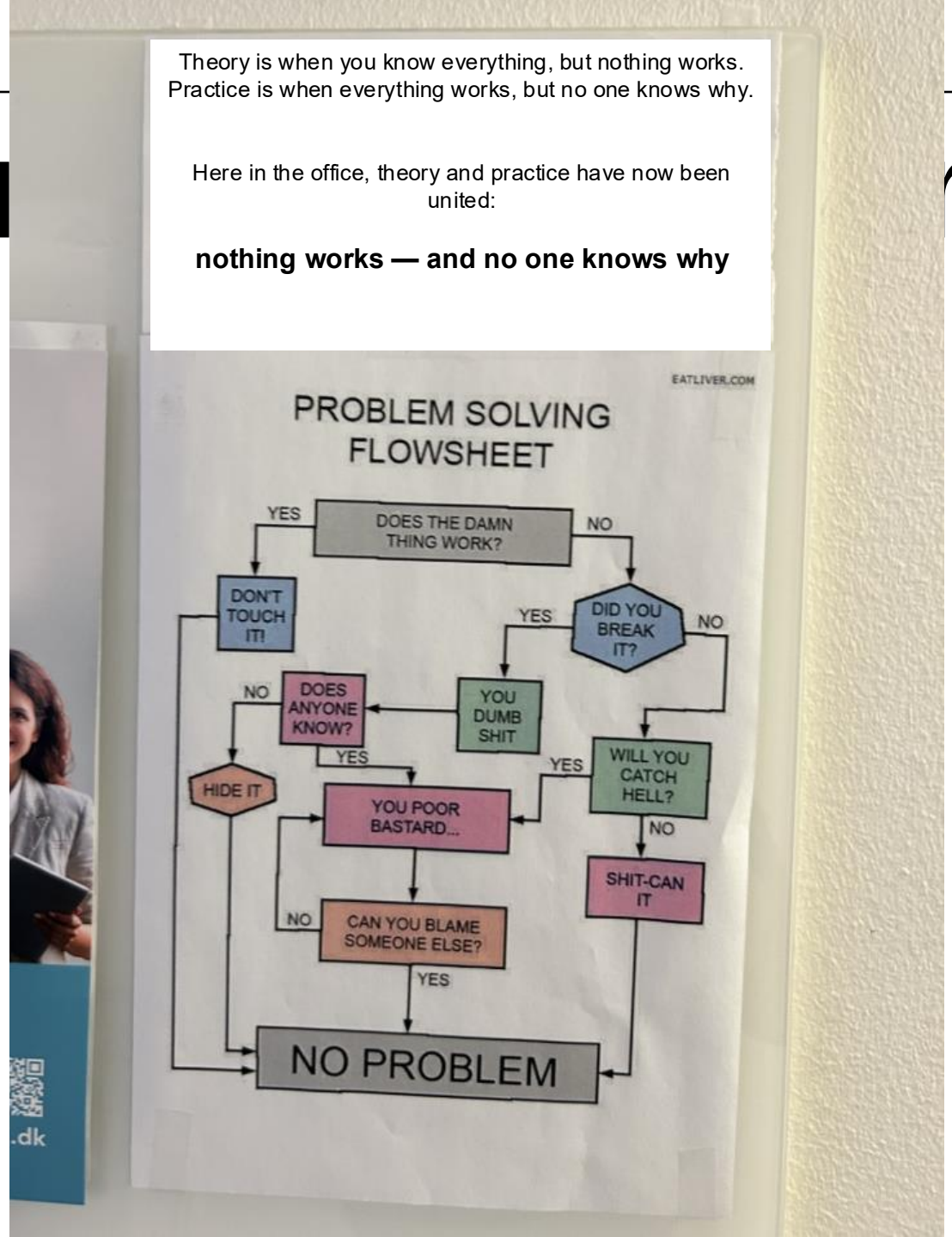


The MVP of Security

- Identity is the ~~new~~ (primary) perimeter
- Conditional Access can protect against phishing, token theft, risky sign-ins, password spray etc.
- The key to Zero Trust

We need to do better!

How ou re doing Cond today



Personas

Personas illustrate key challenges and requirement from the users' perspectives

Personas have common:

- Goals
- Behaviors
- Security Needs
- Resource Access Needs

Personas	Description	Definition
Global	All users in an organization	All Users
Admins	Internal users with privileged roles	(user.extensionAttribute1 -eq "Admin")
ExternalAdmins	External users with privileged roles	(user.extensionAttribute1 -eq "ExternalAdmin")
Internals	Internal employees	(user.extensionAttribute1 -eq "Internal")
Externals	External employees and contractors	(user.extensionAttribute1 -eq “External")
Guests	B2B users	(user.userType -eq "Guest")
ServiceAccounts	User accounts for services	(user.extensionAttribute1 -eq "ServiceAccount")

Naming convention

Format:
CA###-Persona-Type-App-Platform-Control-OptionalDescription

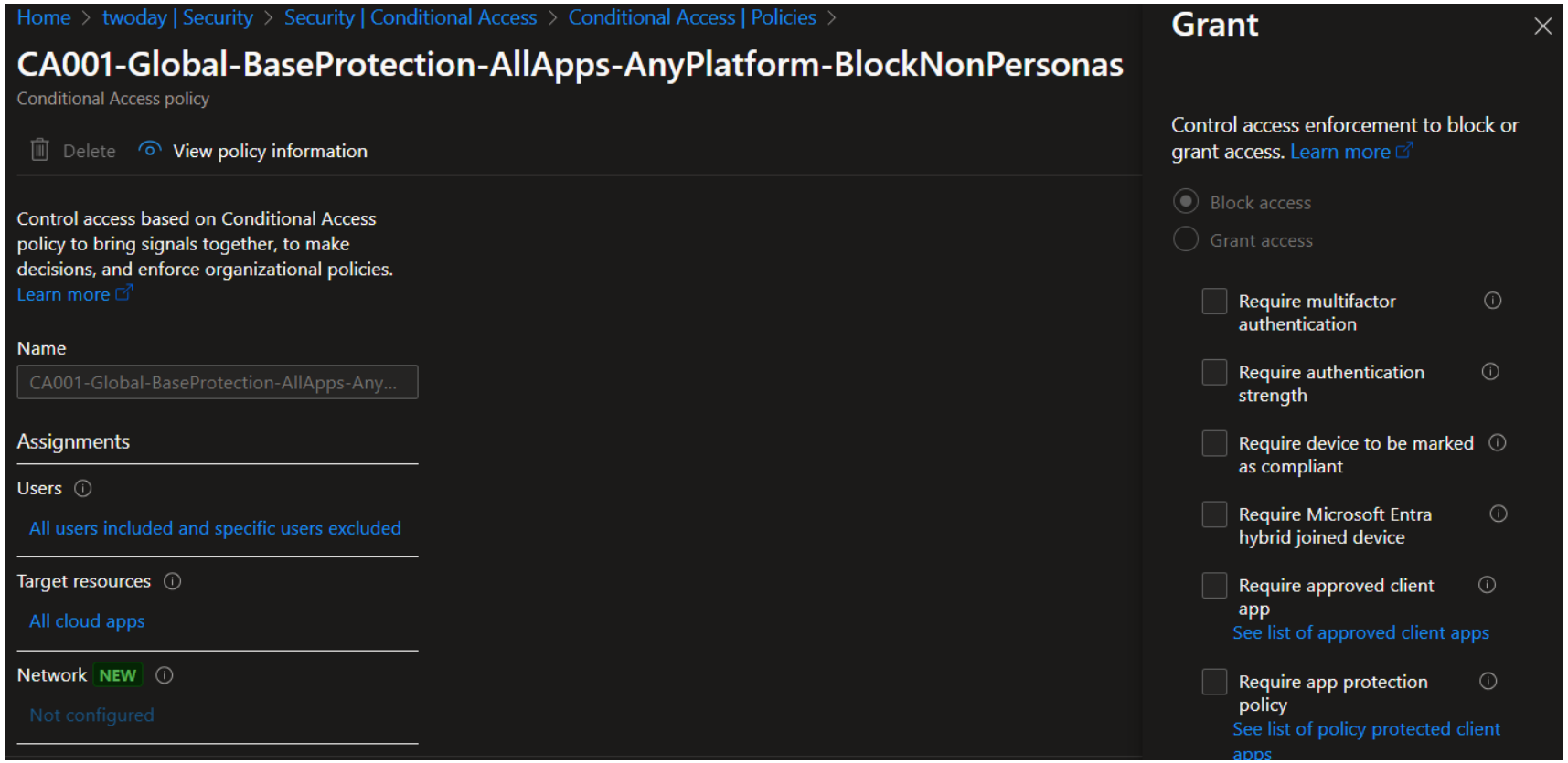
Examples:

CA100-Admins-BaseProtection-AllApps-AnyPlatform-CompliantandMFA
CA201-Internals-BaseProtection-AllApps-AnyPlatform-MFA
CA302-Guests-DataProtection-AllApps-AnyPlatform-NonPersistantBrowser

Persona	Range
Global	CA001–CA099
Admins	CA100–CA199
ExternalAdmins	CA200–CA299
Internals	CA300–CA399
Guests	CA400–CA499
ServiceAccounts	CA500–CA599

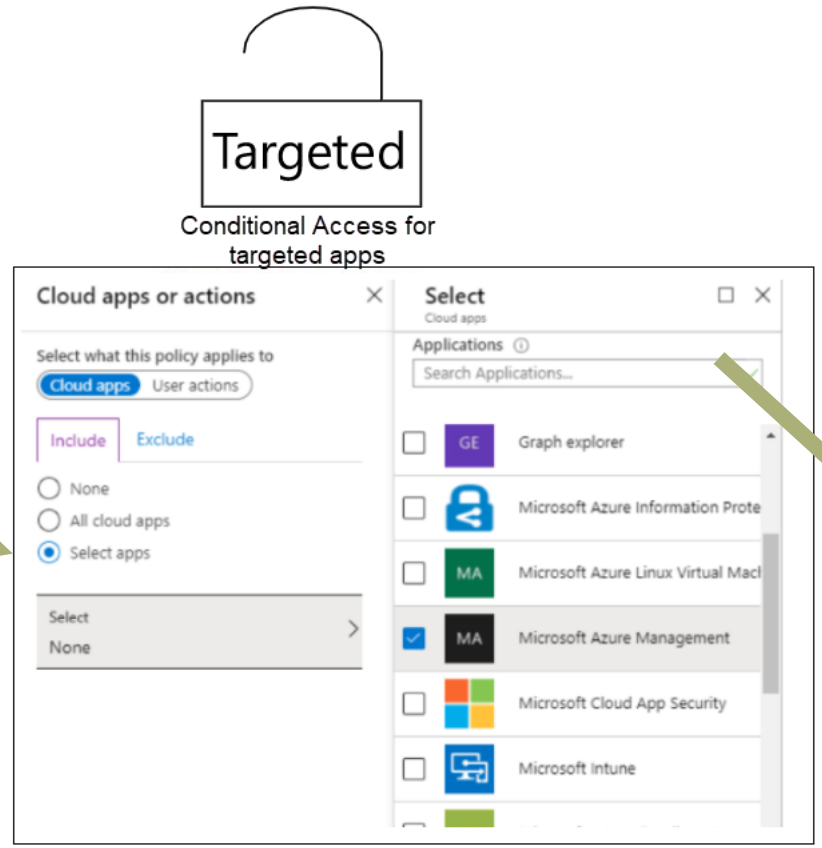
Blocking non personas

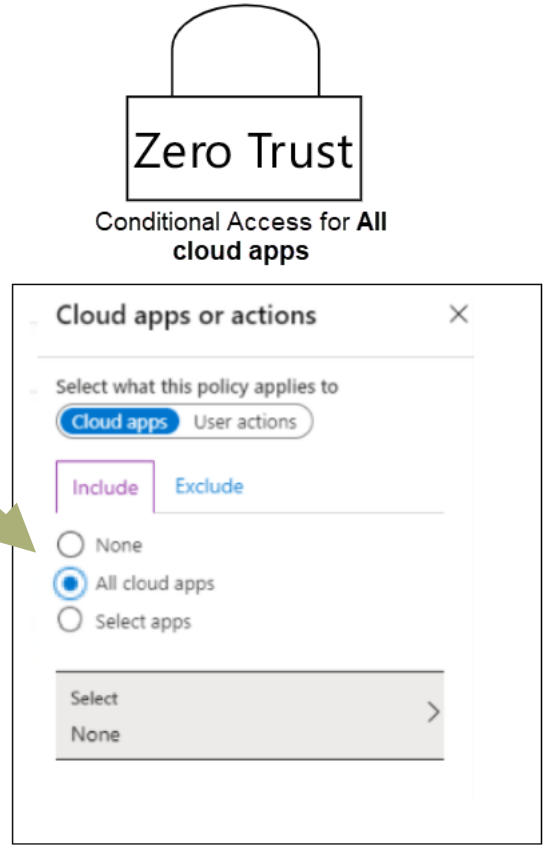
- If a user has not yet been categorized with a persona, they will be blocked from getting access



Targeted

- Applies to a specific scenario, for example Kent accessing **Outlook** from **his office location** on **his Windows device**

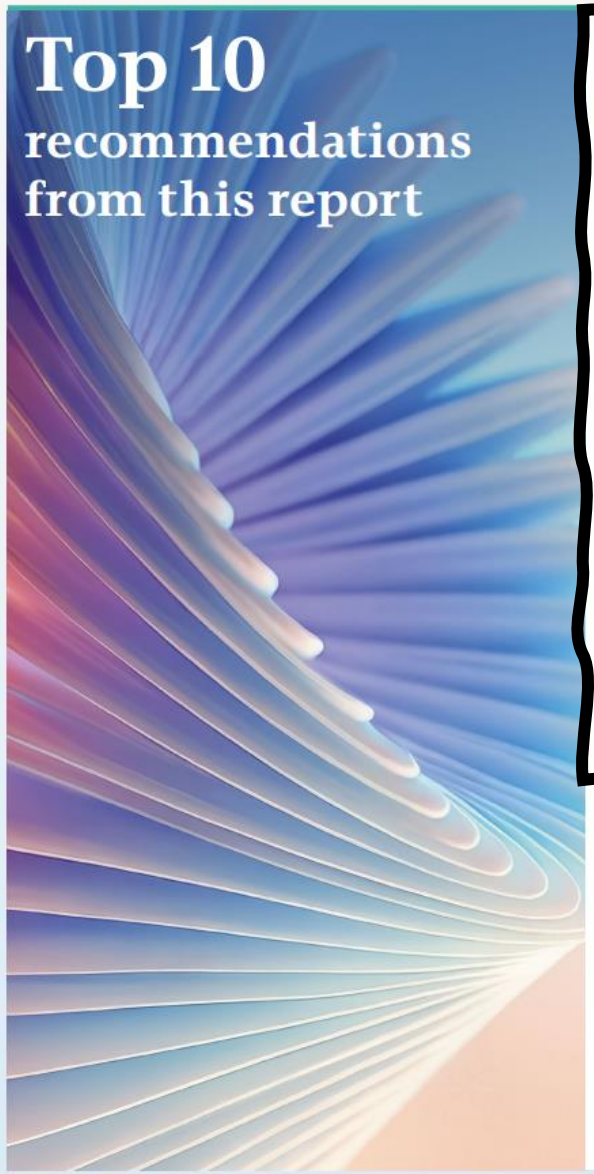




Zero Trust

- Applies to a specific persona accessing **all apps** from **any** location on **any** device

Top 10 recommendations from this report



1. Manage cyber risk at the boardroom level

Treat cybersecurity as a business risk on par with financial or legal challenges. It is important that corporate boards and CEOs understand the security weaknesses of their organization. Track and report metrics like multifactor authentication (MFA) coverage, patch latency, incident counts, and incident response time to develop a comprehensive understanding of both your organization's potential vulnerabilities and its preparedness in the event of a cybersecurity incident.

2. Prioritize protecting identities

Since identity is the top attack vector, enforce phishing-resistant multifactor authentication across all accounts, including administrative accounts.

3. Invest in people, not just tools

Cybersecurity is a whole-of-organization effort. Find ways to upskill your workforce and consider making security part of performance reviews. Culture and readiness—not just technology—are primary factors in both an organization's defenses and its resilience.

4. Defend your perimeter

A third of attackers use crude tactics as the easy path into an organization's exposed footprint, often looking beyond what you deploy to the vendors and supply chain you trust, including perimeter web-facing assets (18%), external remote services (12%), and supply chains (3%). Knowing the full scope of your perimeter, auditing the accesses you grant to trusted partners, and patching any exposed attack surface forces attackers to work harder to be successful.

5. Know your weaknesses and pre-plan for breach

Combine knowledge of the organization's exposure footprint with organizational risk awareness to develop a proactive plan for responding to future breach. Tie security controls to business risks in terms the board can understand. Since a breach is a matter of when, not if, develop, test, and practice your incident response (IR) plan—including specific scenarios for ransomware attacks, which remain one of the most disruptive and costly threats to operations. How fast can you isolate a system or revoke credentials?

6. Map and monitor cloud assets

Since the cloud is now a primary target for adversaries, conduct an inventory on every cloud workload, application programming interface (API), and identity within the organization, and monitor for rogue virtual machines, misconfigurations, and unauthorized access. At the same time, work proactively to enforce app governance, conditional access policies, and continuous token monitoring.

7. Build and train for resiliency

If breaches are all but inevitable, resilience and recovery become key. Backups must be tested, isolated, and restorable, and organizations should have clean rebuild procedures for identity systems and cloud environments.

8. Participate in intelligence sharing

Cyber defense is a team, not individual, sport. By sharing and receiving real-time threat data with peers, industry groups, and government, we can make it harder for cyber adversaries to achieve their goals.

9. Prepare for regulatory changes

It's more important than ever for organizations to align with emerging laws like the European Union (EU) Cyber Resilience Act or United States (US) critical infrastructure mandates, which may require reporting cyber incidents within a certain timeframe or Secure by Design practices. These regulations reinforce the importance of timely incident reporting and stronger internal oversight of an organization's cybersecurity practices.

10. Start AI and quantum risk planning now

Stay ahead of emerging technologies. Understand both the benefits and risks of AI use within an organization and adjust your risk planning, attack surface exposure, and threat models appropriately. Prepare for a post-quantum cryptography (PQC) world by taking the time to inventory where encryption is used and create a plan to upgrade to modern standards as they evolve.

Key takeaways

What every leader needs to know about today's threat landscape

1. Phishing-resistant MFA is the gold standard for security

No matter how much the cyber threat landscape changes, multifactor authentication (MFA) still blocks over 99% of unauthorized access attempts, making it the single most important security measure an organization can implement. Phishing-resistance provides an even more secure solution.

Read more on p23

2. Adversaries are targeting identities that enable access to data

Government organizations, information technology (IT) companies, and research and academic institutions were the most impacted by cyber threats this year. Among other data they hold that might interest adversaries, these organizations store vast amounts of personally identifiable information (PII), whose theft enables future attacks. Accessing organizational data has become a primary objective for threat actors. Government, NGO, and academic entities using legacy systems or operating with small IT teams and limited incident response capabilities should prioritize securing data and identity-facing assets.

Read more on p17

3. Adversaries are using diverse—but well-known—initial access routes

Incident response investigations found that 28% of breaches were initiated through phishing or social engineering, 18% were via unpatched web assets, and 12% leveraged exposed remote services. Not only are adversaries heavily leveraging the ClickFix social engineering method to deliver malware this year, but threat actors are incorporating exploits for known vulnerabilities faster than ever.

Read more on p13

4. Most attacks are for money, not espionage

More than half of cyberattacks with known motives had financial objectives such as extortion or ransom, while only 4% were motivated solely by espionage.

Read more on p11

5. Data exfiltration is the norm

Regardless of adversary motivations, accessing organizational data is now a primary goal for attacks. In the past year, we observed data collection in 80% of reactive engagements.

Read more on p29

6. Workload identities are under threat

As organizations implement phishing-resistant MFA and conditional access policies, adversaries are pivoting to targeting identities and elevated privileges granted to service-to-service workloads like apps, services, and scripts that access cloud resources because service-based workloads are often implemented with elevated privileges but weak security controls.

Read more on p17

7. Adversaries are conducting destructive attacks in the cloud

We have seen an 87% increase in campaigns aimed at disrupting Azure cloud customer environments through destructive actions such as ransomware or mass deletion. Additionally, over 40% of ransomware attacks now involve hybrid components.

Read more on p41

8. Adversaries are already using AI as a multiplier

Adversaries have begun implementing AI across a range of malicious activities, including for automated vulnerability discovery or phishing campaigns, malware or deepfake generation, data analysis, and to craft highly convincing fraudulent messages.

Read more on p52

9. Using AI can be both a benefit and a vulnerability

AI is driving rapid, substantial change. While it offers many benefits for organizations, particularly in cyber defense, AI can be attacked as well. As organizations implement the strengths of AI, they should also manage the weaknesses and potential exposure of sensitive data by protecting against threats like prompt injection, malicious tool invocation, and training data poisoning.

Read more on p52

10. Quantum computing could challenge cybersecurity

Quantum computing has vast economic potential, but if used by malicious actors, it could threaten the encryption of sensitive data.

Read more on p57

Your Zero Trust Homework (starts tomorrow)

1. Run the Zero Trust Assessment Tool

Install → run → open the HTML

Look at the red and orange items

Don't argue the about findings — start the conversations

2. Show the report to someone outside your silo

Entra Admin → show it to Intune Admin

Intune admin → show it to the Security admins

Purview admin → show it to Intune Admin

3. Take a step back and *think strategically*

Get a sponsor

Create a roadmap

Where are the quick wins?

Understand what is most important for your organization

Read, share and discuss the Microsoft Digital Defense Report 2025

4. Pick ONE fix each - and help each other deliver it

Examples:

Fix one dangerous device configuration gap

Move one ASR rule from Audit to Block

Clean up one unused admin role assignment

THANK YOU ALL AND
A SPECIAL THANKS TO OUR SPONSORS!

PATCH MY PC

Microsoft

PLENTICS

Metropolia

twoday

NETOX

DELL

Workplace Ninja
User Group Finland

intel

Thank you!