Microsoft Security

Betere beveiliging voor MKB klanten

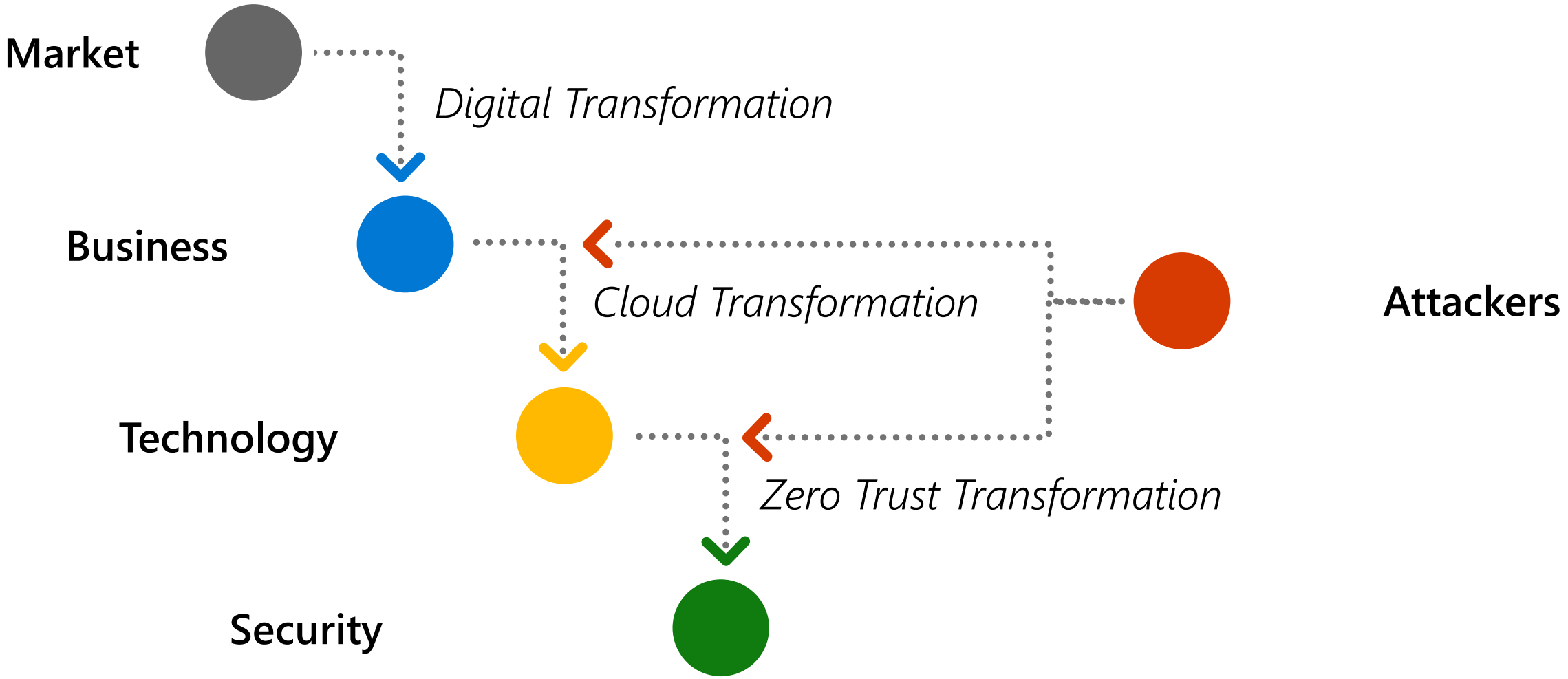
Tony Krijnen
Cloud Solution Architect @ Microsoft

Ruben Koeze
Partner Technology Strategist @ Microsoft

Agenda

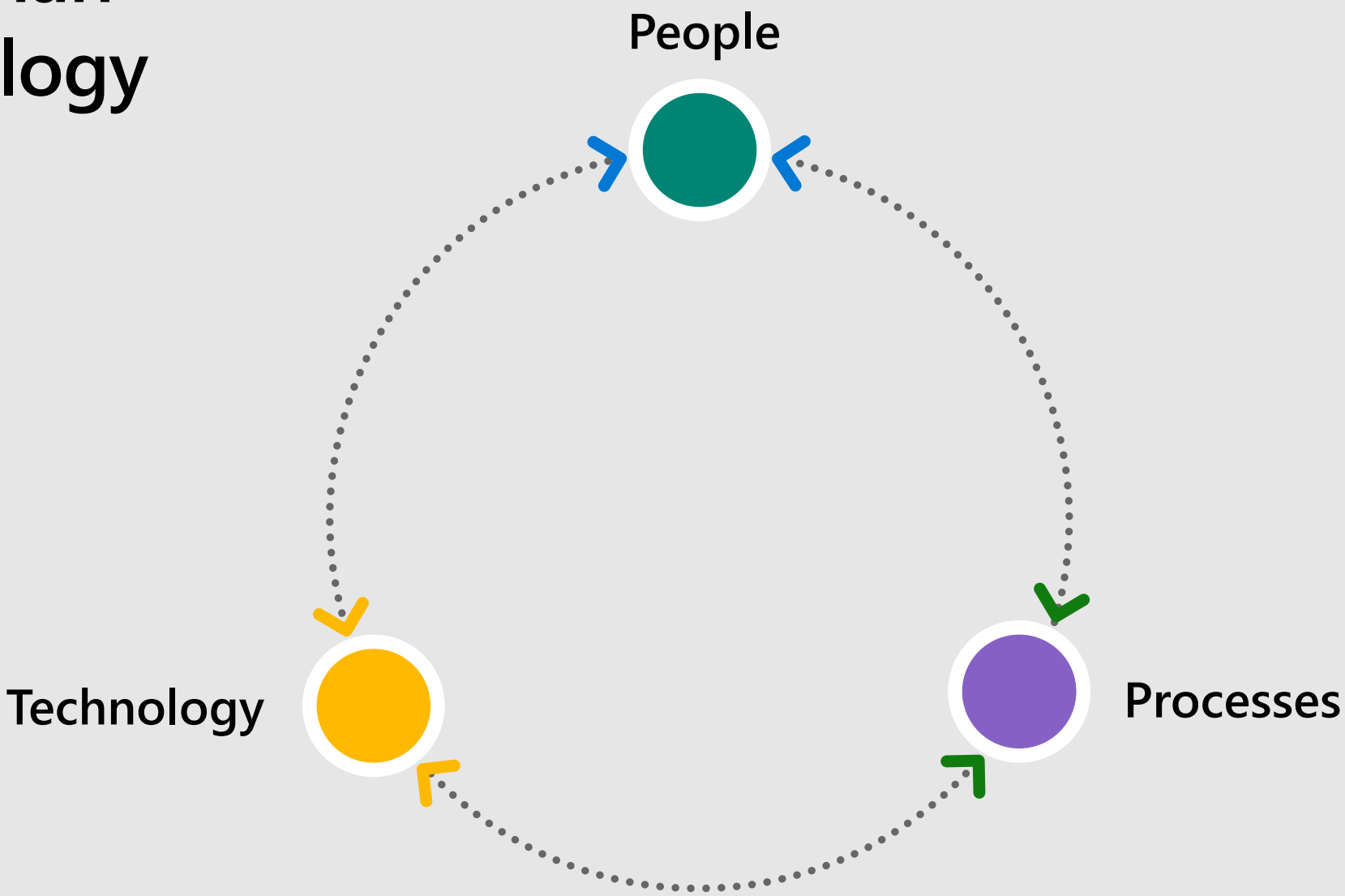
- Aanvallen vandaag de dag
- Zero Trust
- Wat te doen

The world is transforming rapidly



Technology

More than Technology



Zero Trust

Principles of Zero Trust

Instead of assuming everything behind the corporate firewall is safe, Zero Trust assumes *an open environment where trust must be validated.*

- **Assume breach** – Assume that attackers will succeed (partially or fully) and design accordingly
- **Verify explicitly** – Validate trust of users, devices, applications, and more using data/telemetry
- **Use least privileged access** – to limit the impact of any given compromise

Microsoft is actively working with NIST, The Open Group, CISA, and many others across industry to harmonize definitions, model, and architectures for Zero Trust

Zero Trust components

The Zero Trust model and controls applies *across technologies*


Identities


Endpoints

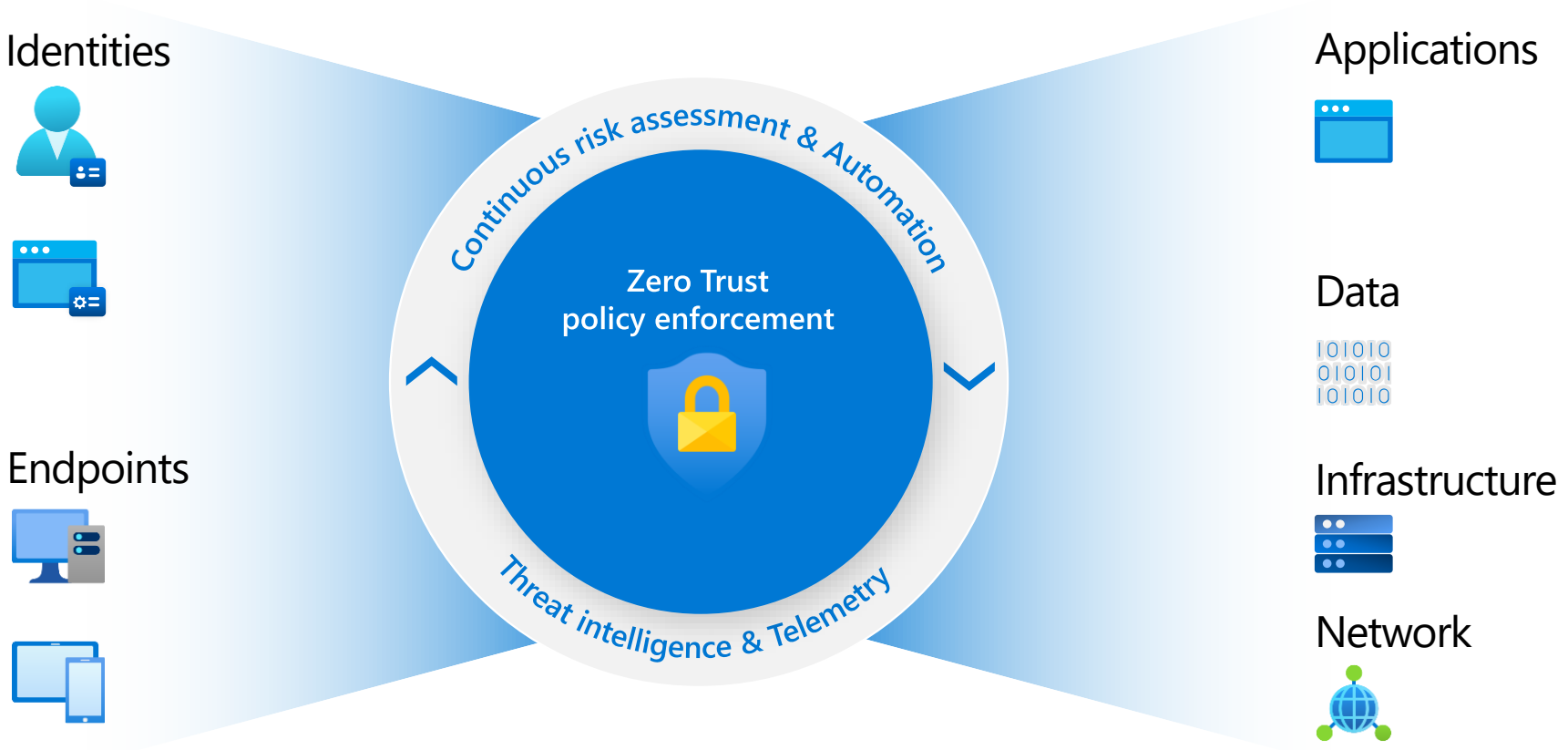

Applications


Data

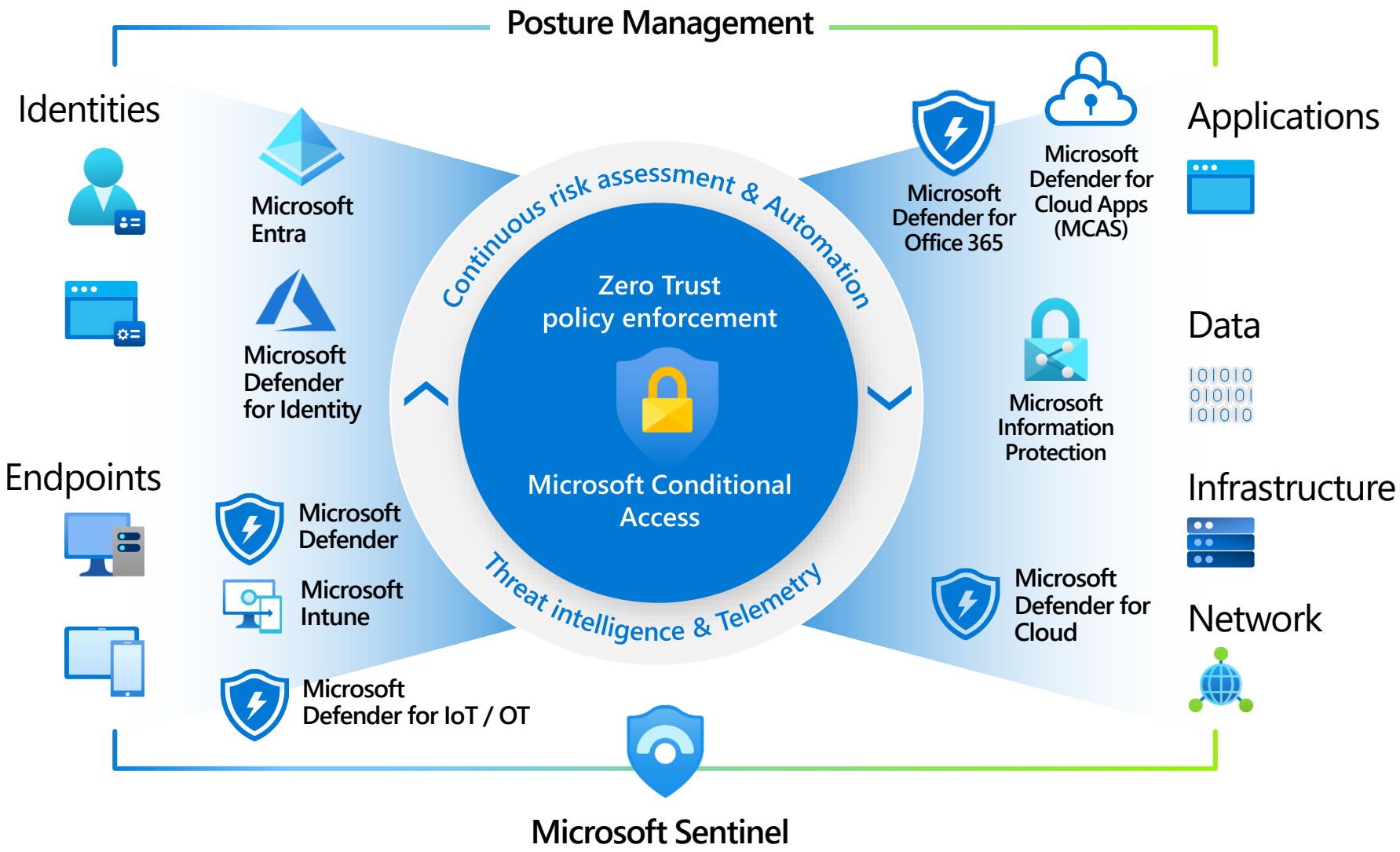

Infrastructure


Network

Zero Trust Approach from Microsoft

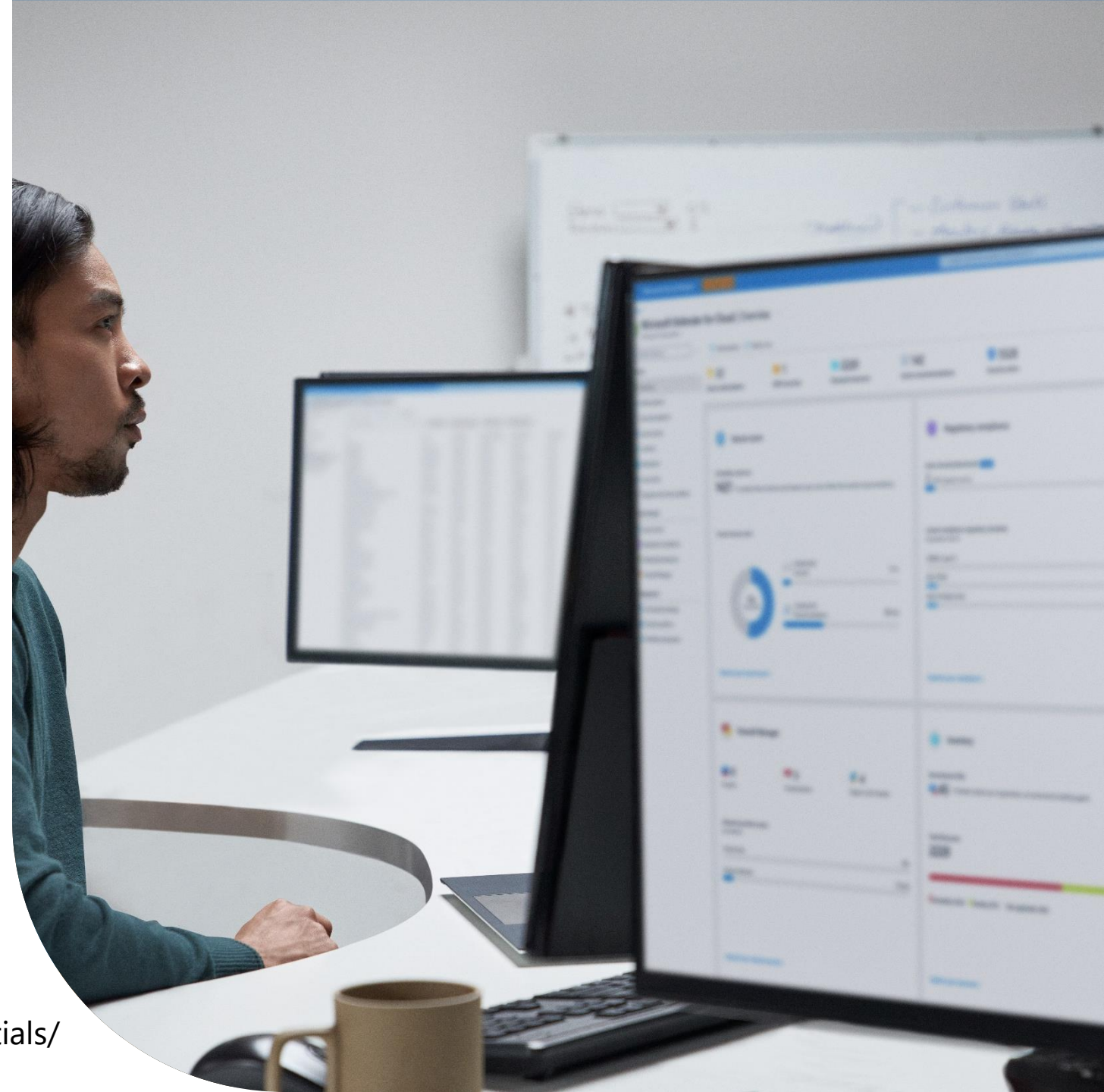


Microsoft Zero Trust Capabilities

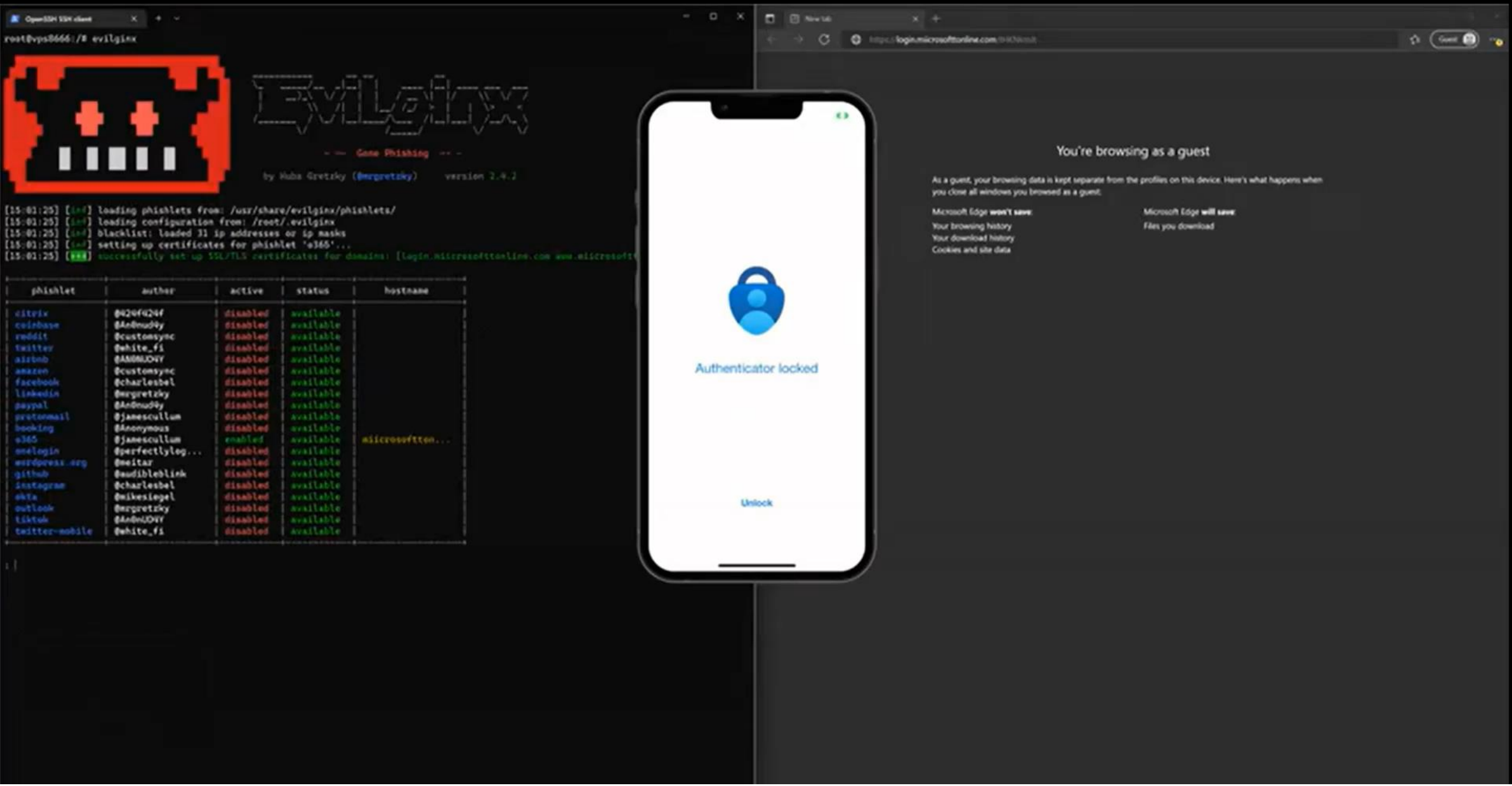


Microsoft Security

Video Phishing attack



https://janbakker.tech/
how-to-set-up-evilginx-to-phish-office-365-credentials/



Video created by Jan Bakker - https://janbakker.tech/how-to-set-up-evilginx-to-phish-office-365-credentials/

Video created by Jan Bakker - https://janbakker.tech/how-to-set-up-evilginx-to-phish-office-365-credentials/

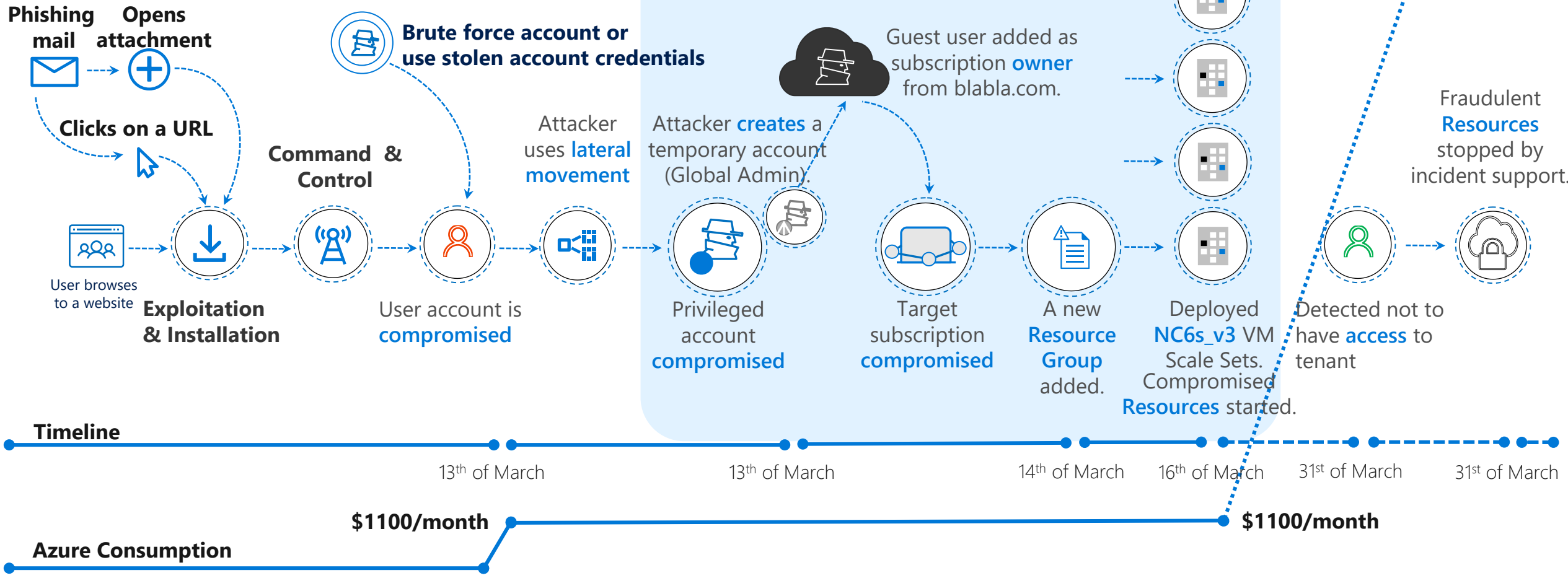
Microsoft Security

Voordat we verder gaan

Waarom je Azure subscription beveiligen en wat beveilig je eigenlijk?

Azure Fraud-case Example

Could have been avoided with better cyber-hygiene
- By enabling MFA with no session persistence
- Privilege Identity protection
- Logging / Auditing / Alerting



The 5 steps

1 Enforce MFA, FIDO2, Windows Hello

Either enforce MFA for **every** login on the Microsoft admin portals (especially the Microsoft Azure portal) and / or leverage the use of FIDO2 hardware keys or Windows Hello.

Demo

MFA

The 5 steps

1 **Enforce MFA, FIDO2, Windows Hello**

2 **Role Based Access Controls**

Limit the accounts leveraging the Role Based Access Controls so that a compromised account cannot disable the taken mitigations

The 5 steps

1 Enforce MFA, FIDO2, Windows Hello

2 Role Based Access Controls

3 Budget & Anti Fraud Alerts

Within partner center (CSP Direct) or at most Indirect Provider portals you can set alerts when the consumption nears a certain threshold. This allows you to quickly react to a possible attack.

Anti fraud alerts

Demo

Anti Fraud Alerts

The 5 steps

1. Enforce MFA, FIDO2, Windows Hello
2. Role Based Access Controls
3. Budget & Anti Fraud Alerts
4. Limit options with Azure Policies

With the master admin account (protected by a FIDO2 Key) create specific accounts (with RBAC) for specific deployment tasks and limit these accounts through Azure Policies.

Demo

Azure Policies

The 5 steps

1. Enforce MFA, FIDO2, Windows Hello
2. Role Based Access Controls
3. Budget & Anti Fraud Alerts
4. Limit options with Azure Policies
5. Secure Score

Turn on Microsoft Defender for Cloud (This is FREE for Subscription management!) and check the Secure Score for that Azure subscription. Leverage the advice to increase this.

Microsoft Defender for Cloud overview

Strengthen your cloud security posture

Secure score | Policies and compliance | Automation

Leveraging Azure Arc

Protect your multicloud and hybrid workloads

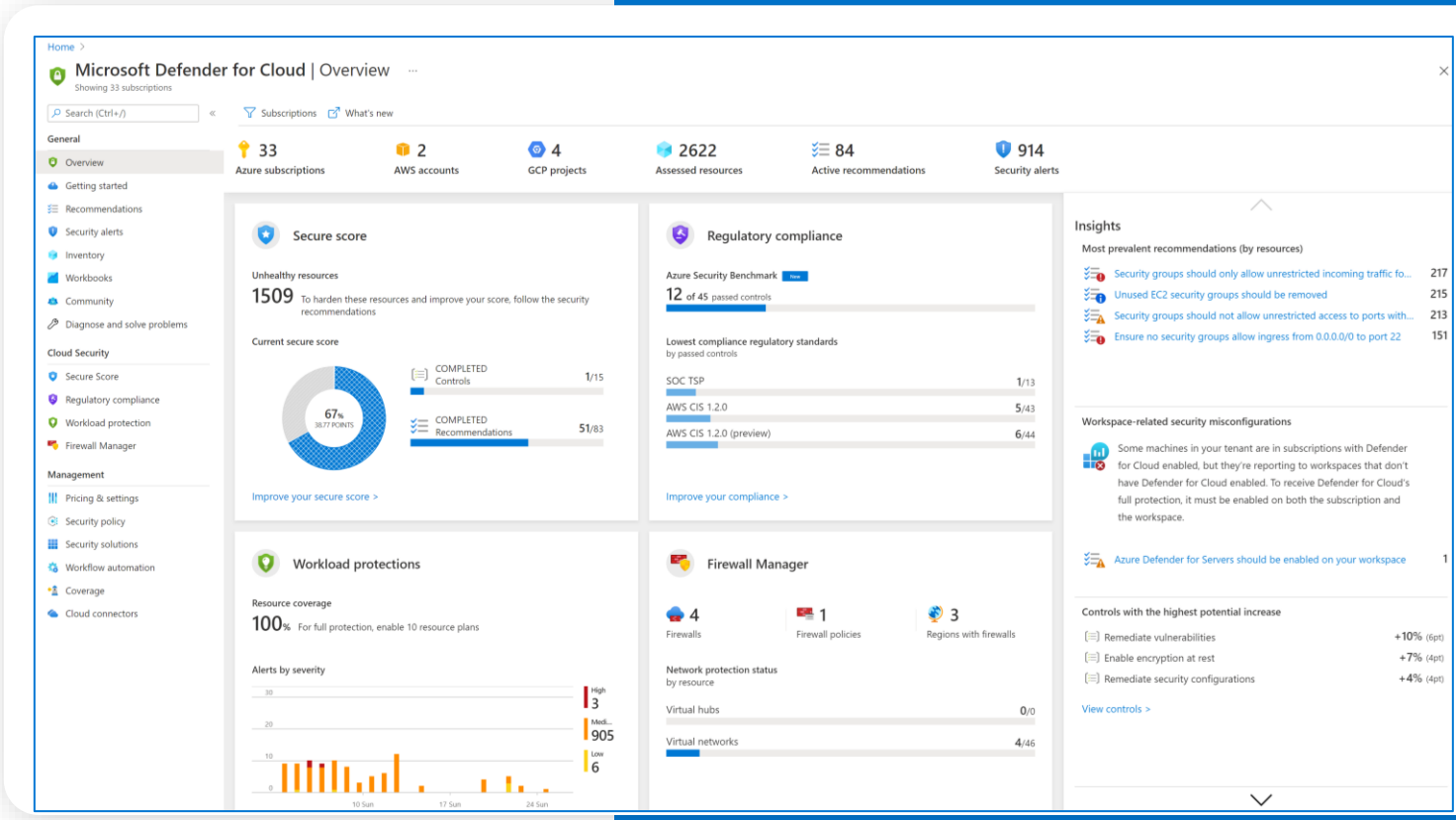
Servers | Cloud native workloads | Databases and storage

Azure service layers | IoT devices

Streamline security management

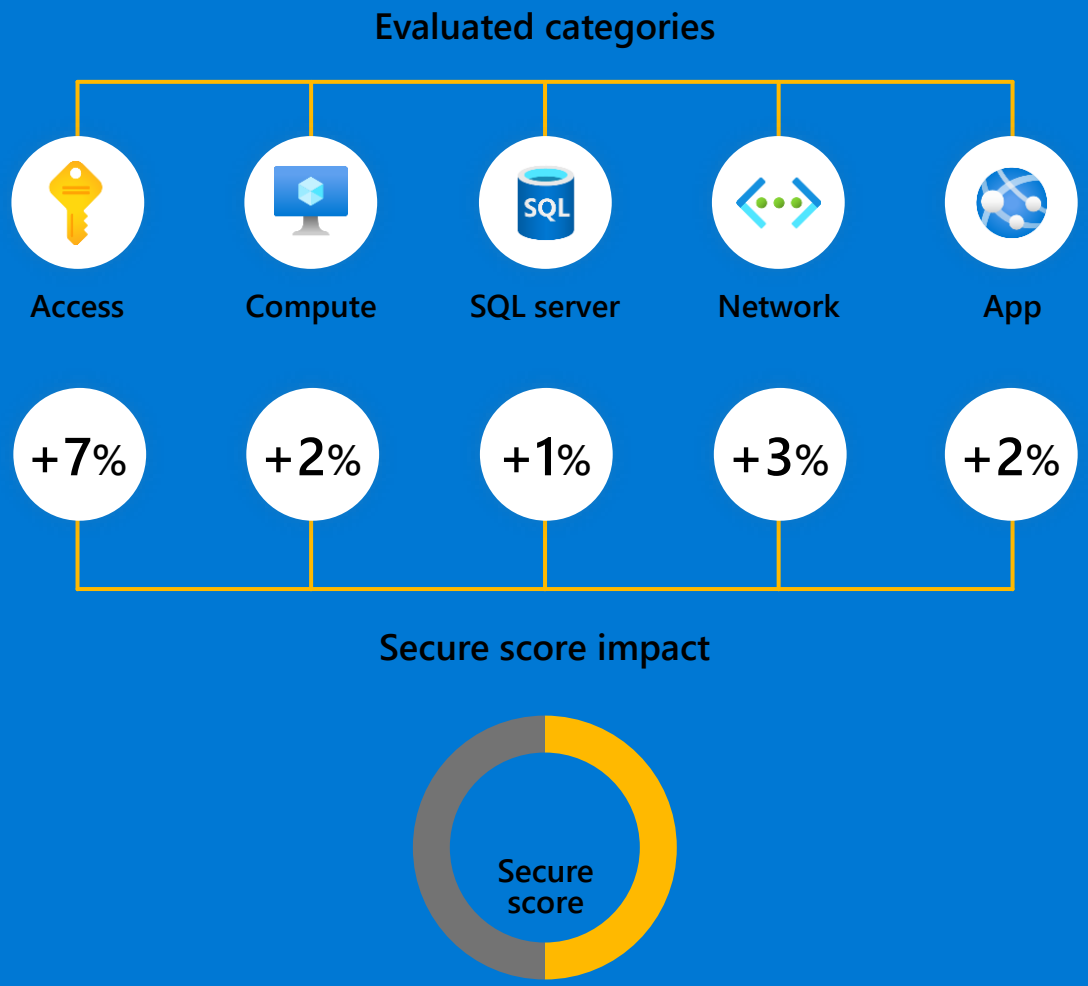
The security dashboard

- Unified resource view
- All your cloud resources in one place: Azure, AWS, on premises and other clouds
- Focused views for security posture, compliance, and workload protection
- Clear & simple view
- Identify all your security related stats at a glance
- Emphasis on visibility & clear KPIs



Security posture management with secure score

- Gain insights into the security state of your cloud workloads across Azure and AWS
- Address security vulnerabilities with prioritized recommendations
- Improve your secure score and overall security posture in minutes
- Speed up regulatory compliance
- Granular control of secure score



Demo

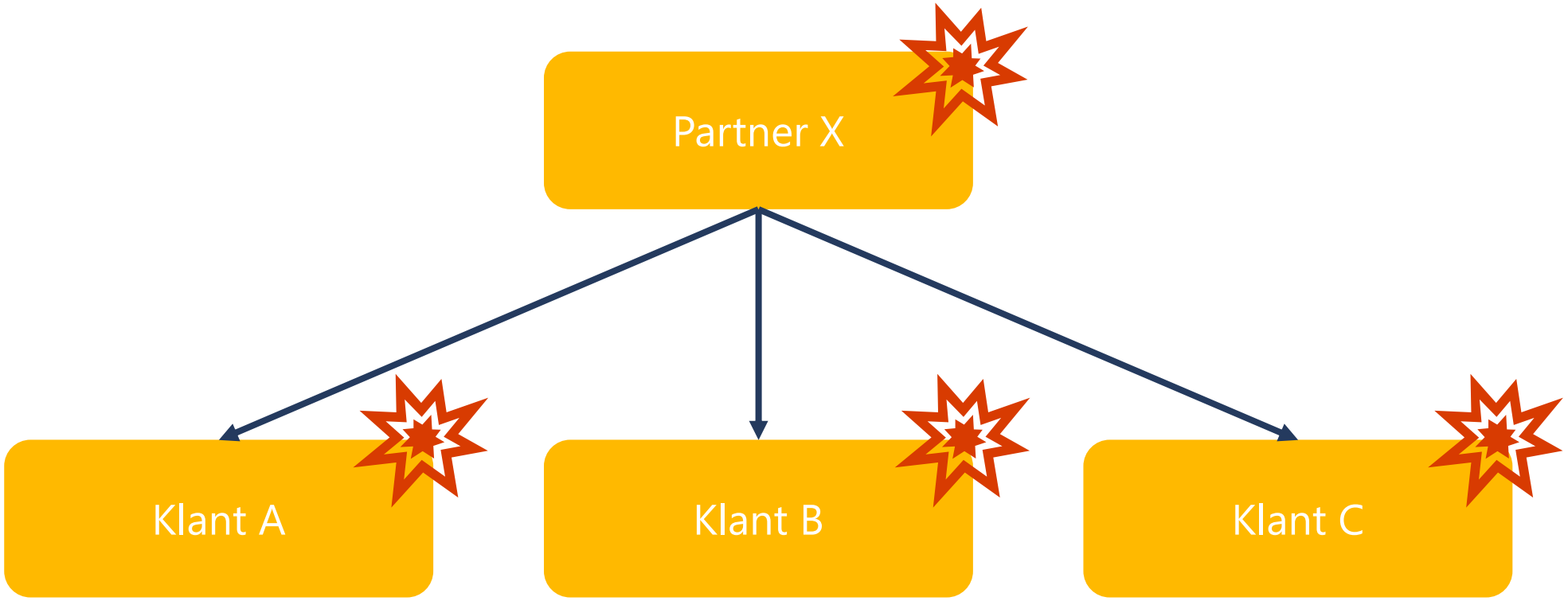
Defender for Cloud – Secure Score

Microsoft Security

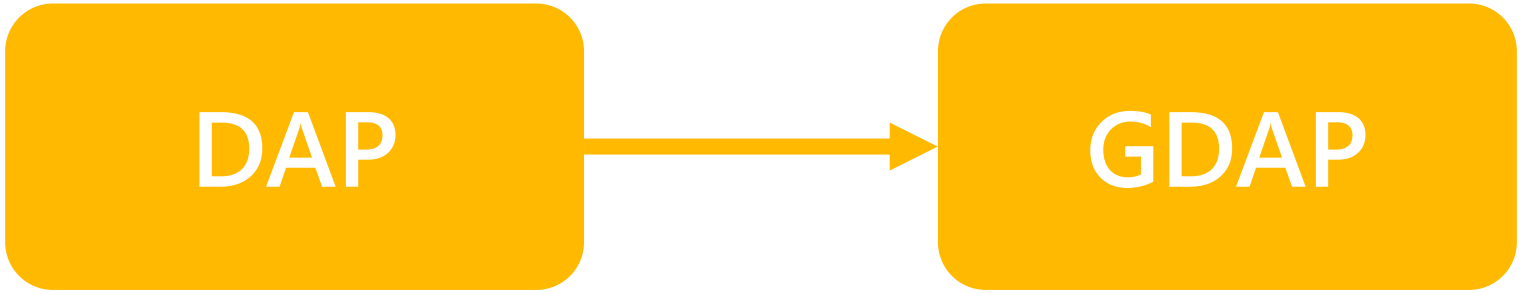
DAP & GDAP

Bonus

De oude situatie

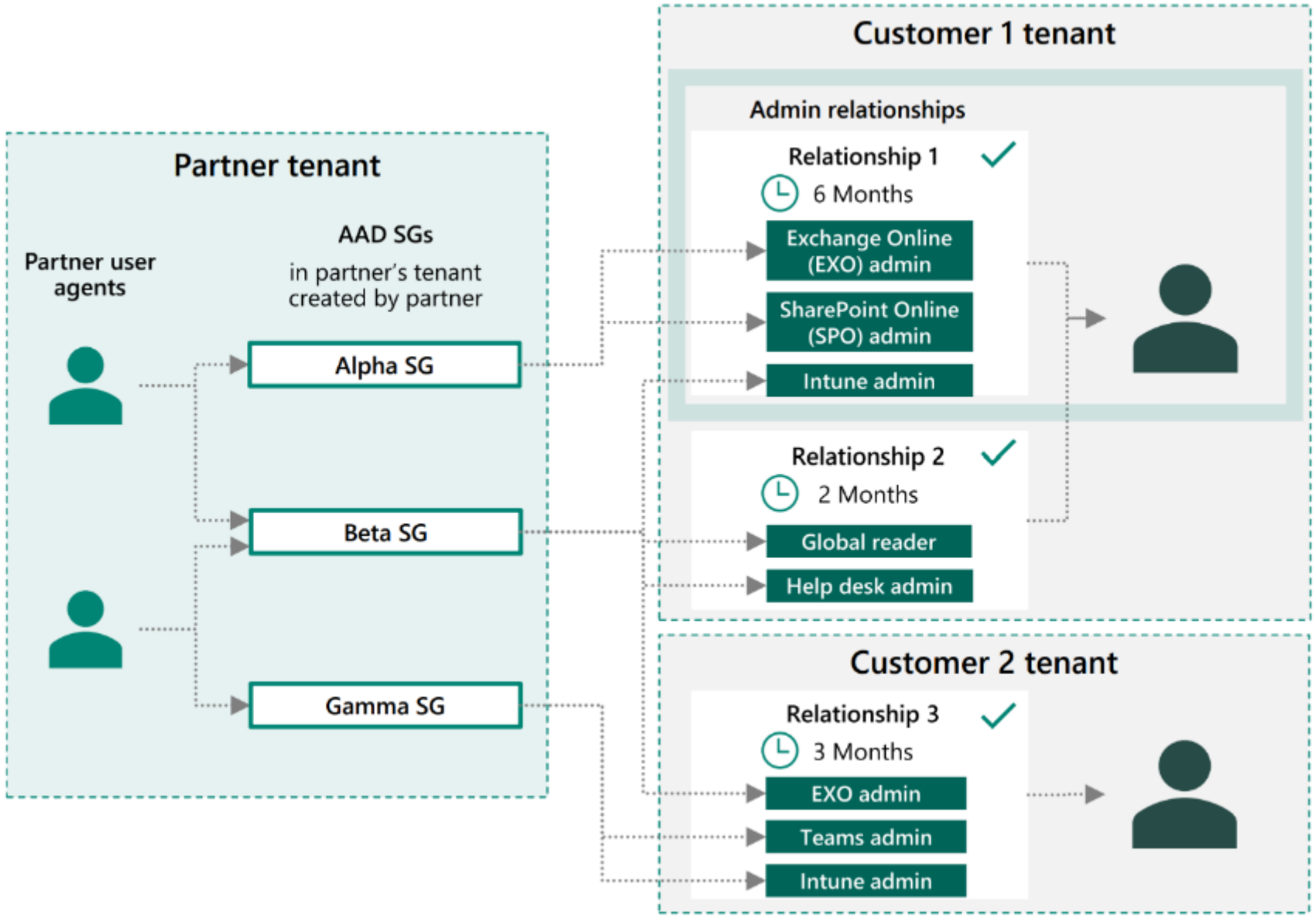


Wat gaat er veranderen?

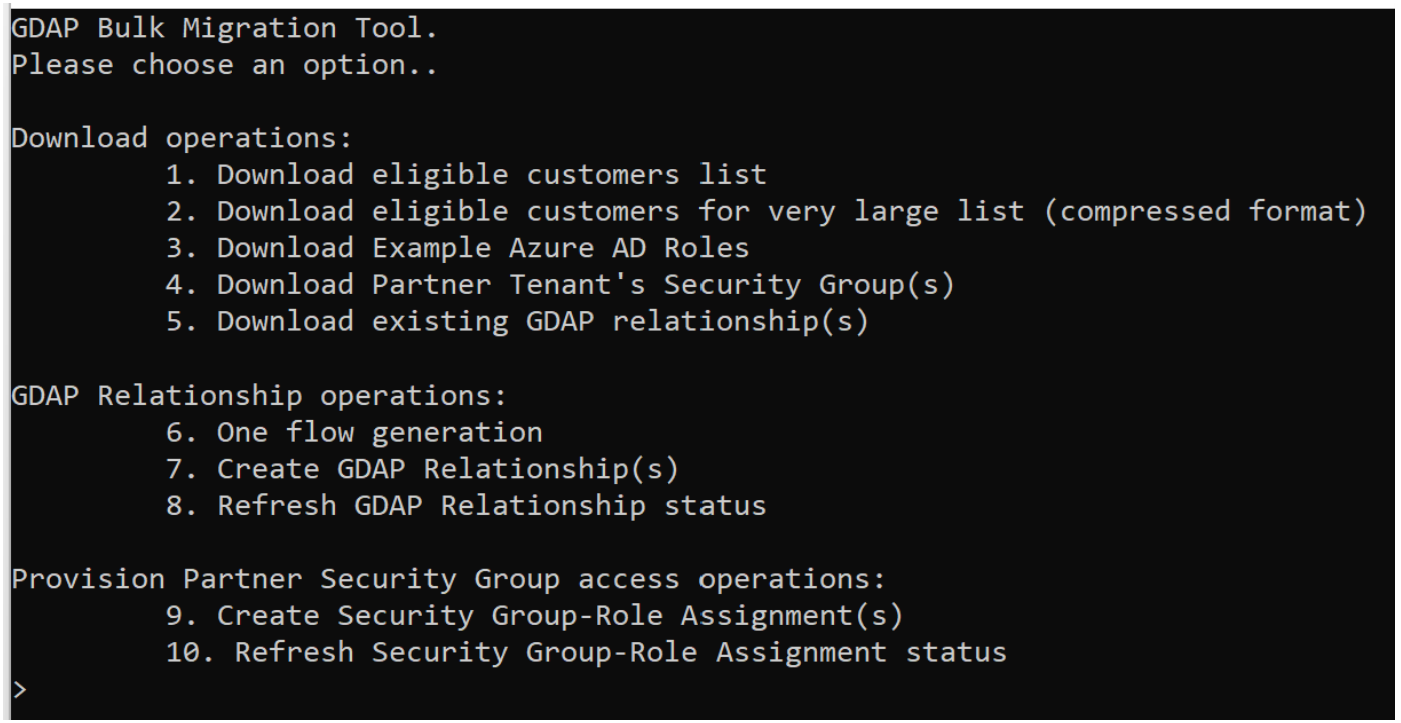


	DAP	GDAP
Level of access / roles	Global Admin + Helpdesk Agent	Custom
Relationship Timeline	Indefinite	Max 2 years
Invitation Link	Same for every customer	Custom for every customer
Security Group Assignment	☒	☑
Activity Logs	☒	☑
Access to S&C center	☒	☑
PIM support	☒	☑

Voorbeeld


Partner tenant
Partner user agents
AAD SGs
in partner's tenant created by partner
Alpha SG
Beta SG
Gamma SG
Customer 1 tenant
Admin relationships
Relationship 1
6 Months
Exchange Online (EXO) admin
SharePoint Online (SPO) admin
Intune admin
Relationship 2
2 Months
Global reader
Help desk admin
Customer 2 tenant
Relationship 3
3 Months
EXO admin
Teams admin
Intune admin

GDAP bulk migration tool



[GDAP bulk migration tool - Partner Center | Microsoft Docs]

Handson Lab

https://aka.ms/MBPLab

Microsoft Security

Thanks!