






Microsoft Ignite



Making end to end security real

Tamás Szivós-Aradi & Thomas Kurth

Thomas Kurth

- Working at baseVISION since 2016
 - **Founder** of baseVISION AG in 2016 
 - **CEO and Principal Security Consultant** since 2016 
 - Building first 100% Microsoft based SOC in Switzerland 
- Volunteer as Co-Organizer of Workplace Ninja Summit
 - www.wpninjas.eu



2016

2019

2020

2022

2023

2023



LinkedIn

Tamás Szivós-Aradi

- Working in security since 2004
 - Security Technical Specialist at  Microsoft
 - Technical Lead for the Security Operations Center of  Swiss Re
 - Security Architect for Endpoint Security, Identity, etc.  Swiss Re
- Guest lecturer at the Hochschule Luzern **HSLU** Lucerne University of Applied Sciences and Arts
- Volunteer for the CyberPeace Institute 
- Swiss  citizen, originally from Hungary 



2007



2008



2016



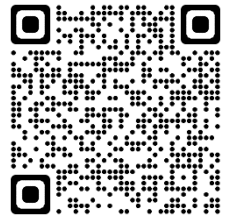
2020



2021



2023



LinkedIn

Agenda

Planning the Journey

How can you start your journey? Which key steps need to be taken?



Overview

Vision of end-to-end security.



Smart Identity Lifecycle

Identities are the core of today's infrastructure. How can we manage them efficiently?



Combat Phishing Attacks

Phishing attacks are the #1 attacks and require defense-in-depth concept including people.



Operate your XDR

Implementing products is simple, but what processes are required? Is AI the solution?

Q&A

Summary and time for questions



Overview

What does
end to end
security mean?



End to End Security

Enable business mission and increasing security assurances with intentional approach

Security Strategy and Program

Zero Trust Architecture

Security Posture Management

Modern Security Operations (SecOps/SOC)

Secure Identities and Access

Infrastructure & Development Security

IoT and OT Security

Data Security & Governance

'Left of Bang'

Prevent or lessen impact of attacks

'Right of Bang'

Rapidly and effectively manage attacks



IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

GOVERN



Security Modernization with Zero Trust Principles

Security Strategy and Program



Business Enablement

Align security to the organization's mission, priorities, risks, and processes.



Assume Breach (Assume Compromise)

Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly



Verify Explicitly

Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry.



Use least-privilege access

Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based policies like adaptive access control.

Zero Trust Architecture



Secure Identities
and Access



Infrastructure &
Development Security



IoT and OT
Security



Modern Security
Operations (SecOps/SOC)



Data Security &
Governance

Product Families Enable Modernization Initiatives

Security Strategy and Program

Zero Trust Architecture



Secure Identities
and Access



Entra



Infrastructure &
Development Security



IoT and OT
Security



Modern Security
Operations (SecOps/SOC)



Data Security &
Governance



Purview



Defender

Security Copilot (Preview)



Intune



Azure



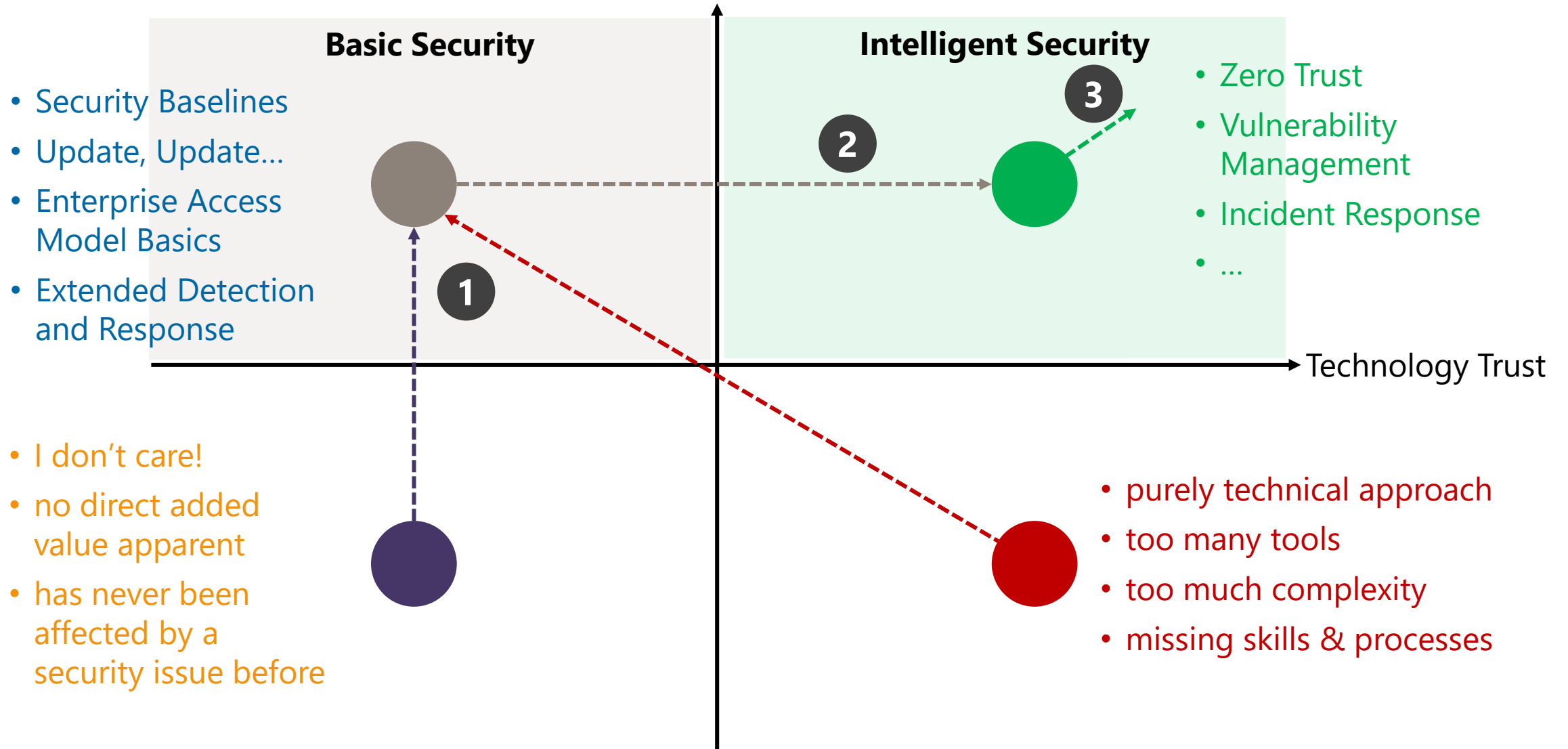
Sentinel



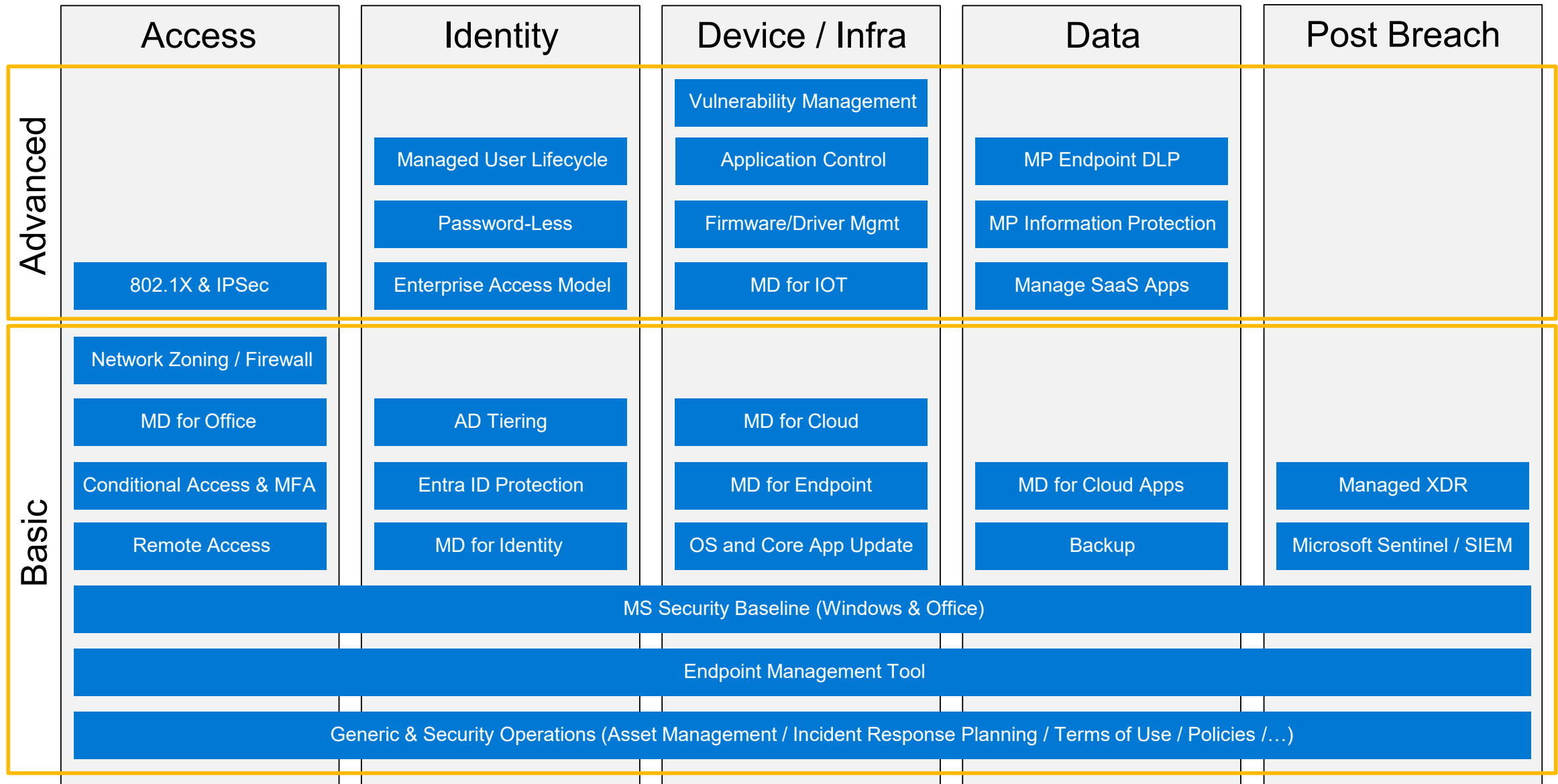
Priva

Planning the Journey

Planning the Journey - Security Maturity

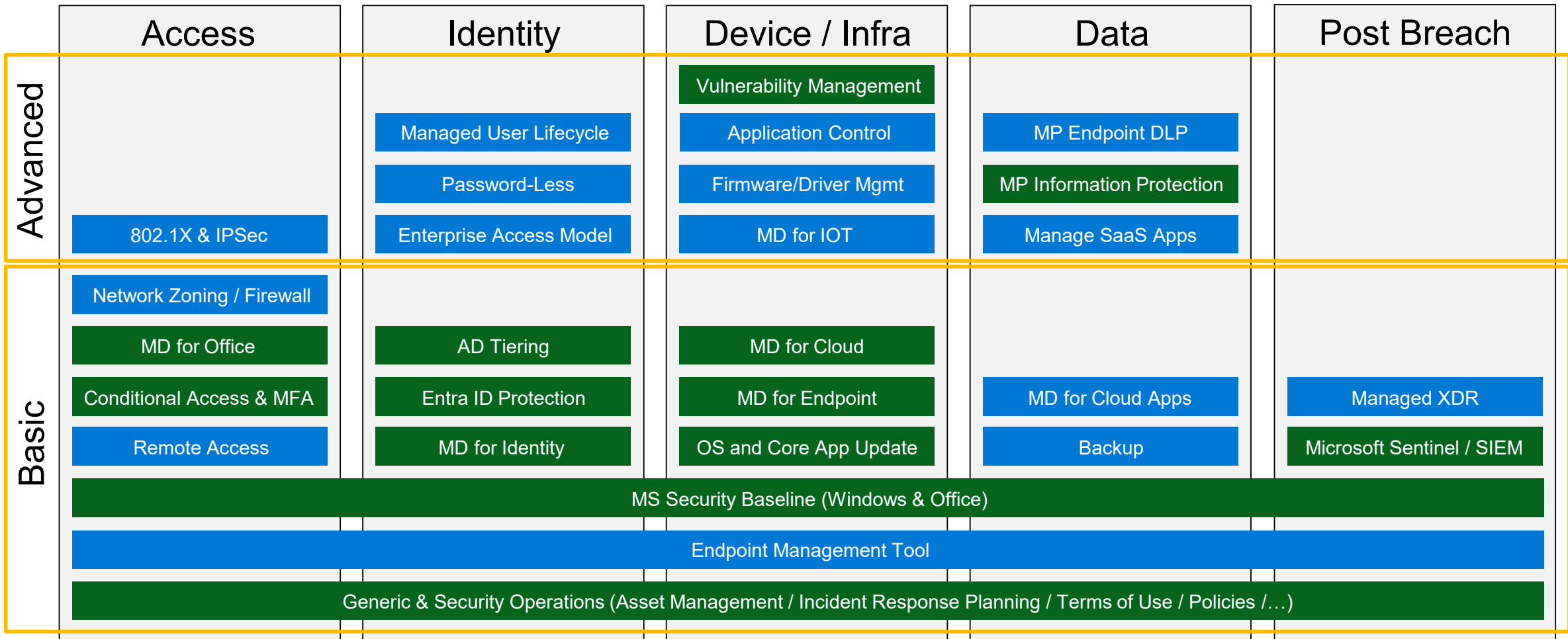


Planning the Journey - Start with a Map



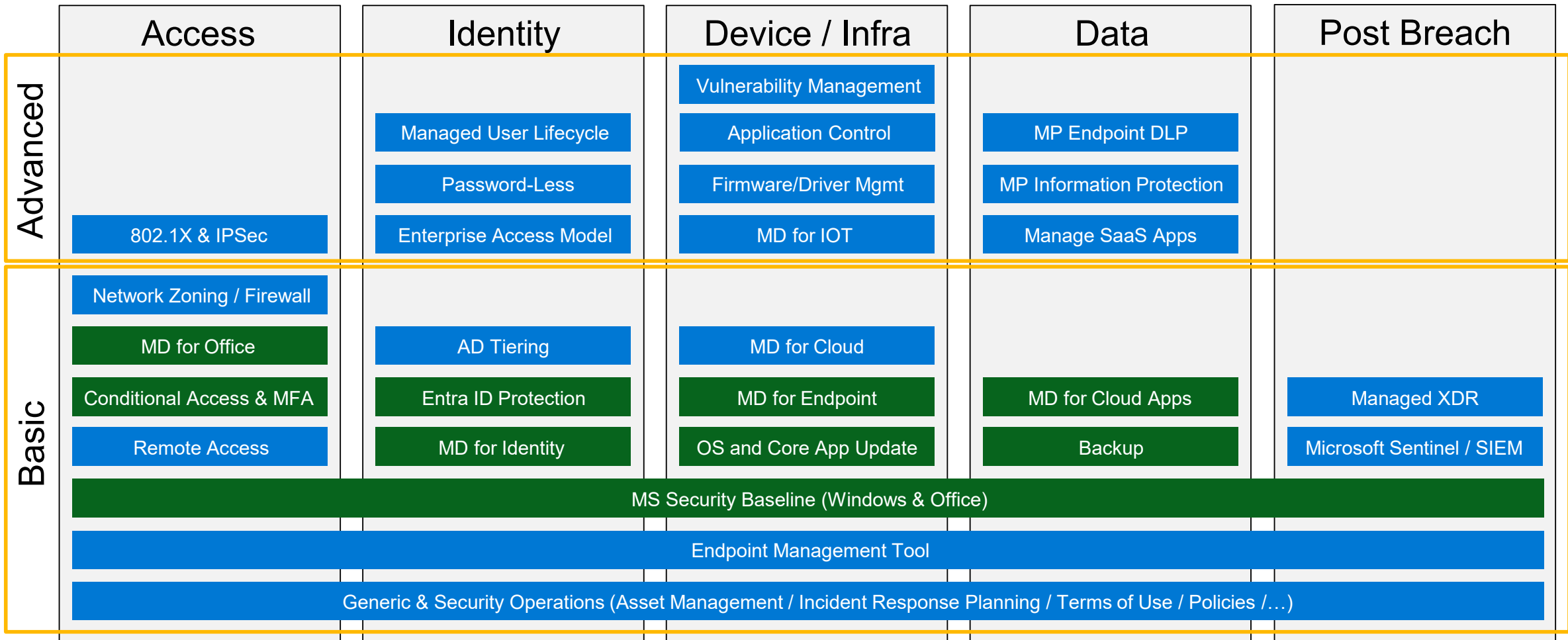
Planning the Journey - Start with a Map

- Evaluation of Xplain Cyber Incident Audit Report by BACCS(NCSC)



Planning the Journey - Start with a Map

- Microsoft Digital Defense Report: protections to mitigate 99% of ransomware attacks



Smart Identity Lifecycle

Smart Identity Lifecycle

Provisioning

- Create person in HR system
- Leverage Provisioning API to automatically create AD/EID(AAD) Users
- SCIM Provisioning to Cloud Apps
- Entra ID Connect Sync

Authentication

- Use Entra ID Lifecycle Processes with Temporary Access Pass and password-less methods
- Conditional Access with risk-based approaches

Authorization

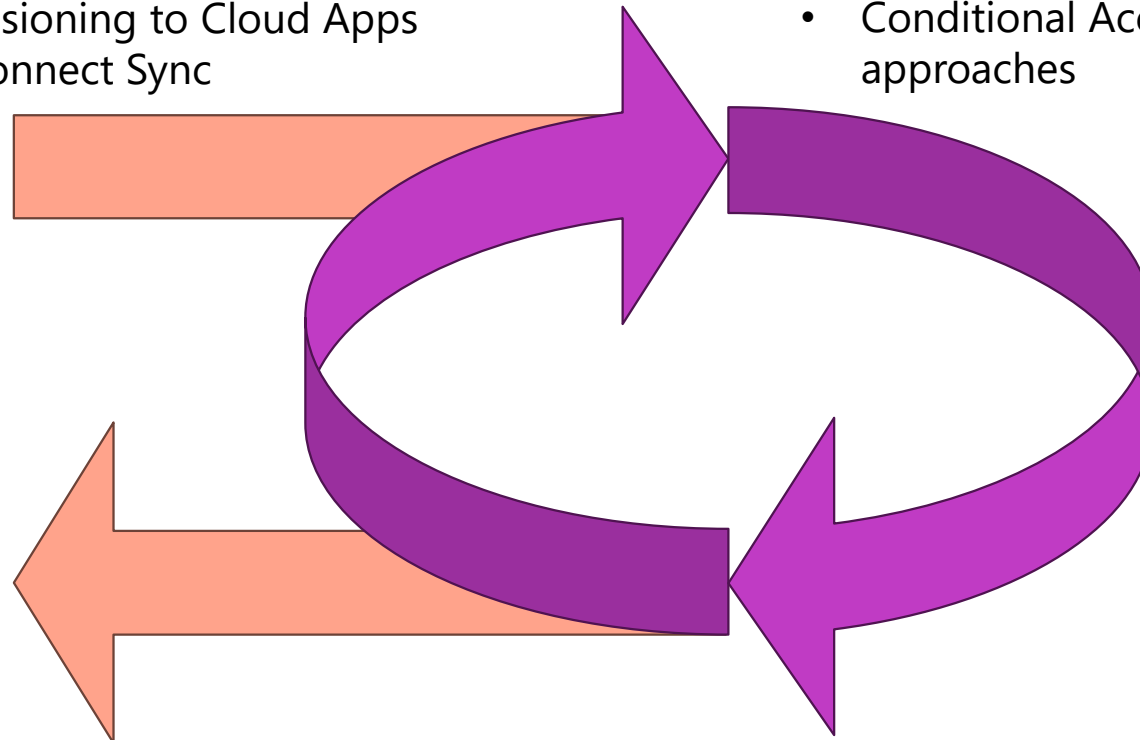
- Time-based group Assignment by Lifecycle Workflows
- Dynamic groups based on User Properties for initial permission set
- Entitlement Management Auto Assignment Policies
- Access Reviews

De-provisioning

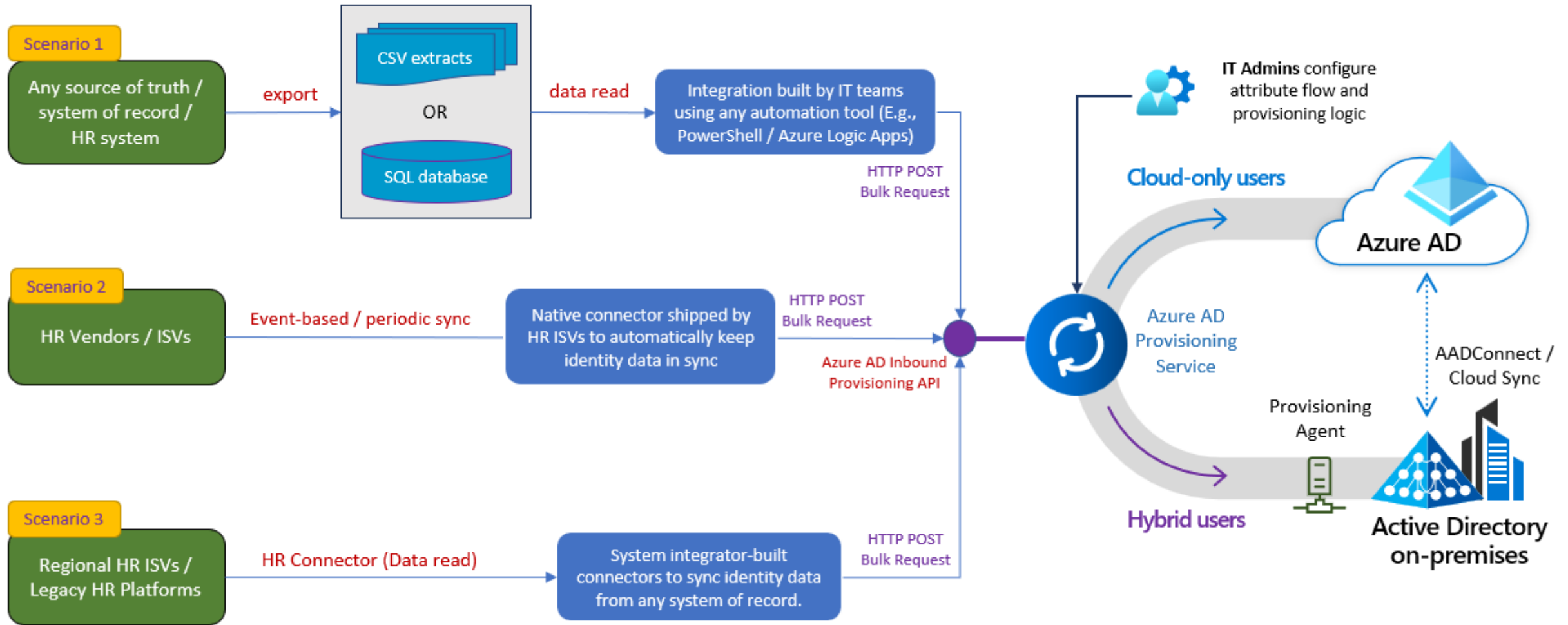
- HR based deprovisioning with Lifecycles
- Access Reviews

Self-service

- Entitlement Management Access Package
- Password Reset



Smart Identity Lifecycle - Provisioning



Smart Identity Lifecycle - Joiner/Mover/Leaver



Joiner · PRE-HIRE

For pre-hire, "X" days before employee's start date,

- Create user account (status=disabled)
- Send reminder email to manager
- Launch custom Logic Apps workflow
- Generate Temporary Access Pass (TAP)
- Send email to hiring manager with TAP

Joiner · HIRE

On the employee's start date, perform the following tasks.

- On start date
- Enable user account
- Group assignments
- Send welcome email to new hire
- Add user to Teams channel

Joiner · WELCOME

Employee's day 1 and Manager shares the temporary access pass.

- On start date
- On Day 1
- Login with temporary access pass
- Receive welcome email
- Welcome messages in Teams channel
- "Best onboarding experience ever!"

Smart Identity Lifecycle is possible with Microsoft Entra ID

Provisioning

- Create person in HR system
- Leverage Provisioning API to automatically create AD/EID(AAD) Users
- SCIM Provisioning to Cloud Apps
- Entra ID Connect Sync

Authentication

- Use Entra ID Lifecycle Processes with Temporary Access Pass and password-less methods
- Conditional Access with risk-based approaches

Authorization

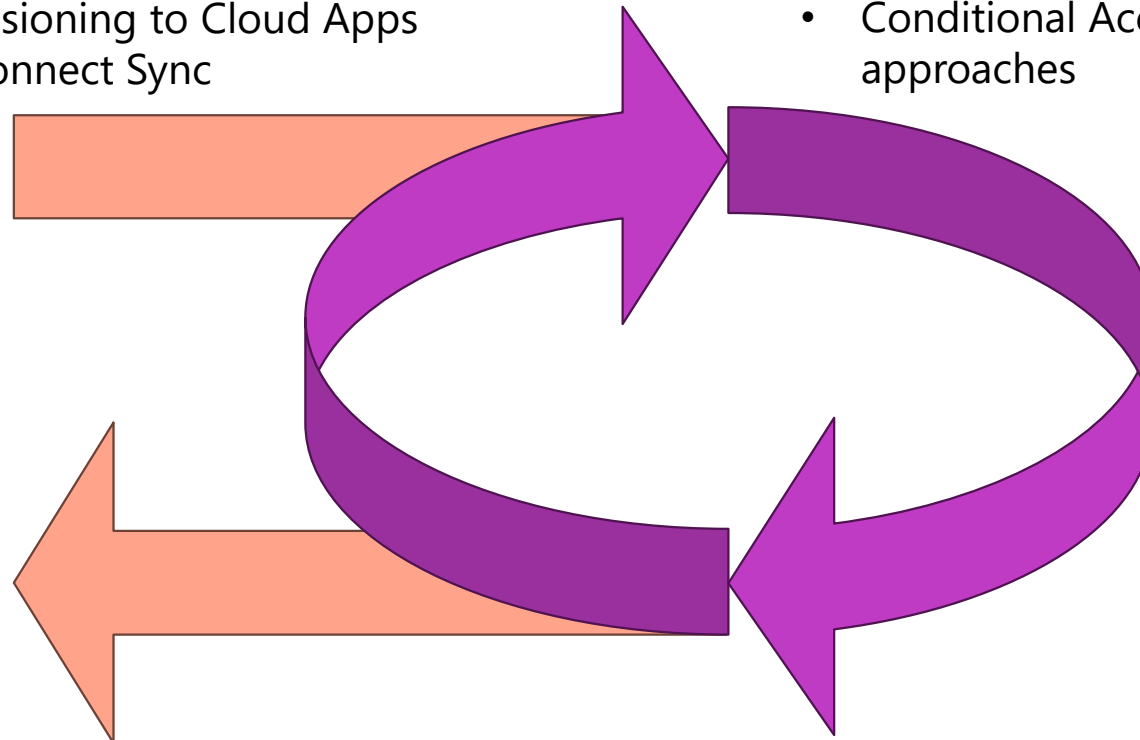
- Time-based group Assignment by Lifecycle Workflows
- Dynamic groups based on User Properties for initial permission set
- Entitlement Management Auto Assignment Policies
- Access Reviews

De-provisioning

- HR based deprovisioning with Lifecycles
- Access Reviews

Self-service

- Entitlement Management Access Package
- Password Reset



Combatting Phishing

Combat Phishing Attacks



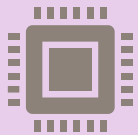
Phishing Resistant
Authentication

FIDO - Passkeys, Token and Windows Hello



Awareness

Training & Tests
SANS IT Admin



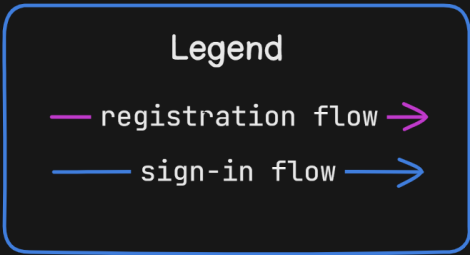
Protection

Microsoft Defender for Office (Mail & Teams)
Windows 11 - Enhanced Phishing Protection

What do we mean
by *phishing-*
resistant
authentication?

*Authentication that
relieves the user of
responsibility.*





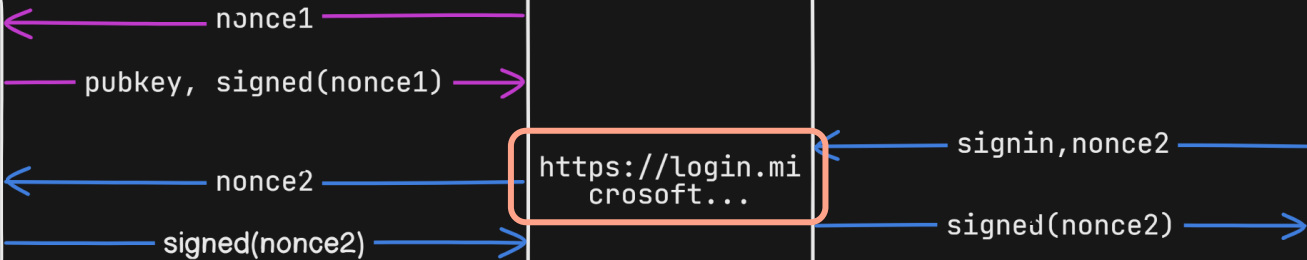
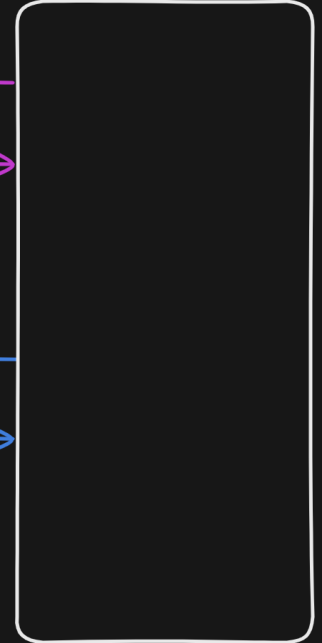
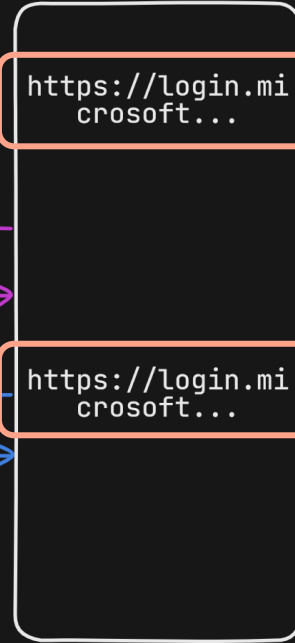
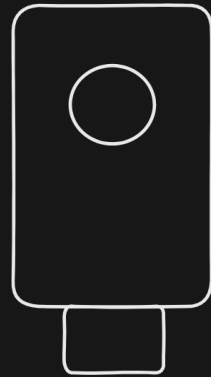
FIDO2 Authenticator

CTAP2

Client

WebAuthN

IdP

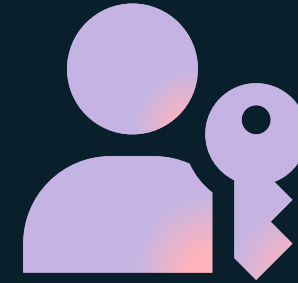
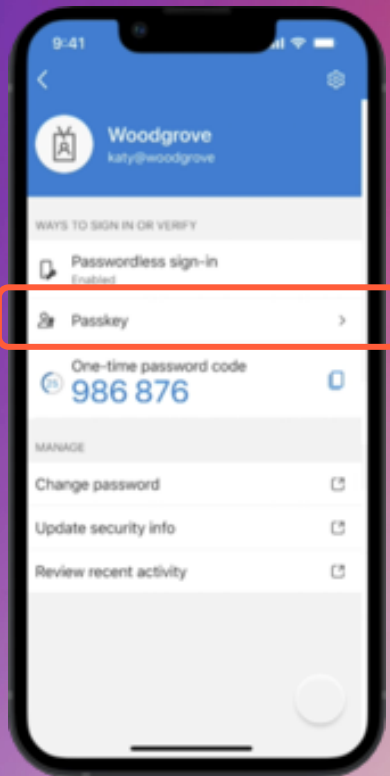


Demo

You will see:

1. Successful sign-in with a phishing-resistant authenticator
2. Phishing a sign-in with Authenticator app push-notification
3. Trying to phish a sign-in with phishing-resistant authenticator

*Coming soon
to a Microsoft
Authenticator
app near you!*



passkey

pass·key | \ 'pas-, kē \

A replacement for passwords that is a more secure, easier, and a faster method to sign in to websites and applications

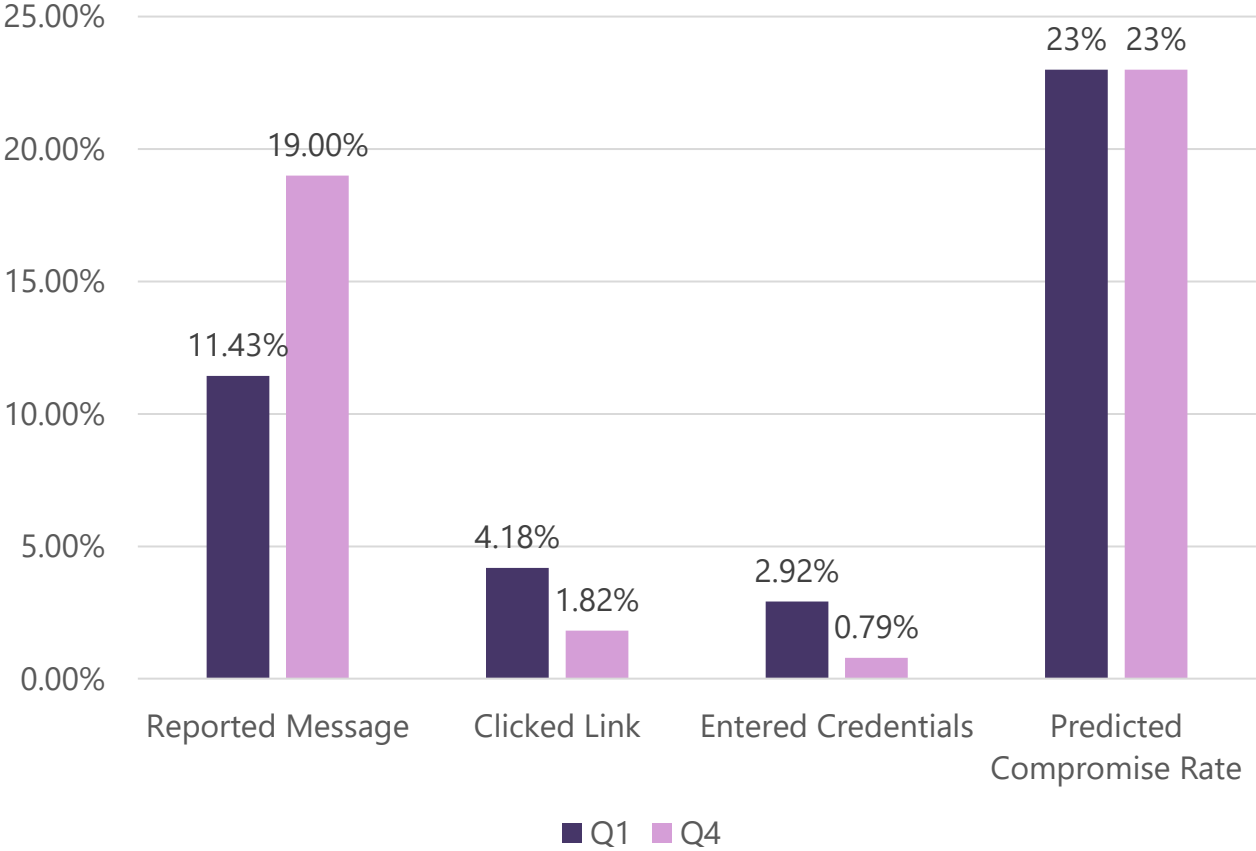
A phishing resistant, WebAuthn credential, that is usable across all your devices

A consumer-friendly and enterprise grade solution that can be synced to allow secure passwordless sign-in across a device ecosystem, or be device-bound for access on a single machine

Phishing Training

Combat Phishing Attacks - Real Example with MDO

- Impact of Awareness Campaigns



Remarks

- Reported messages almost doubled
- Clicked Links and Entered Credentials by > 50%

Demo Attack Simulation - Training Only

You will see:

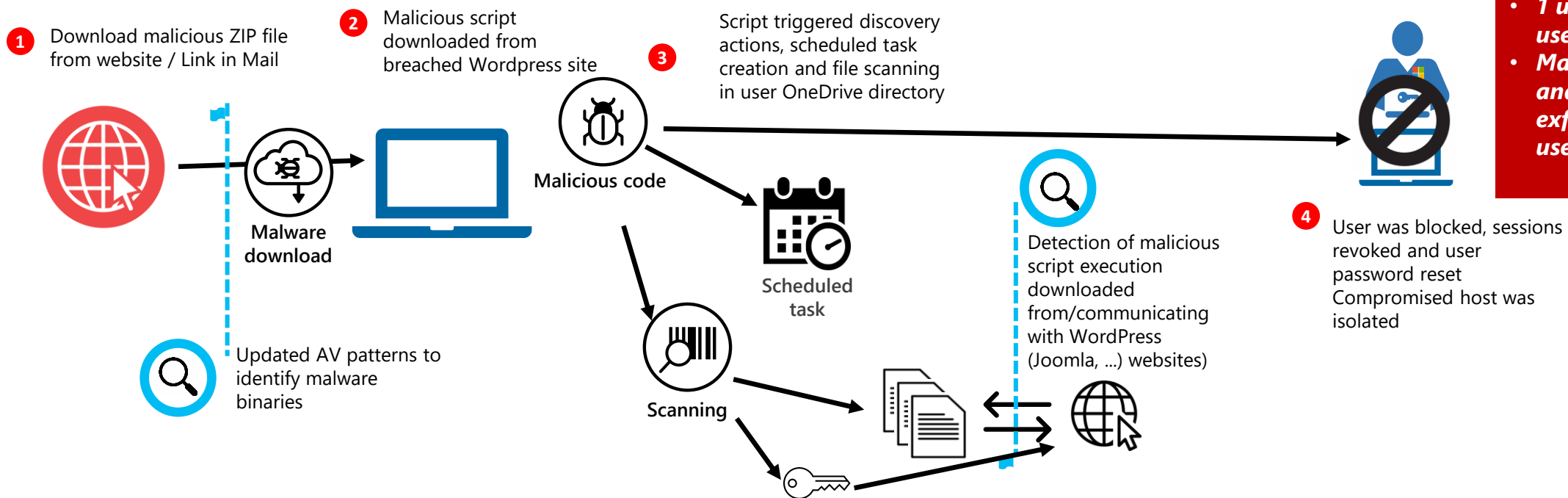
1. Flexible Assignment
2. Available Training Content

Operating your XDR Solution

Building a Security Operations Team

- Multiple roles required
 - Security Analyst
 - Security Engineer
 - Threat Intel Analyst
 - Detection Engineer
 - Incident Responder
 - Security Automation Engineers
 - ...
- Security DNA
- Security Analyst's main tasks
 - Alert Monitoring
 - Incident Analysis
 - Incident Response
 - Root Cause Analysis
 - Security Recommendation
 - Learning and Exercises

000000 (Multi-stage incident involving Execution & Discovery on one endpoint)



Impact Analysis

- 1 user involved, no other users/hosts impacted
- Malicious script read and eventually exfiltrated data from user OneDrive location

Event	Detection	Response	Lessons Learned & Next Steps
What happened exactly?	What has triggered the incident?	What response actions were taken?	<ul style="list-style-type: none"> • How can we improve for the future? • Which tasks are still open?

Operate your XDR with baseVISION MXDR Premium



Microsoft Intelligent Security Association

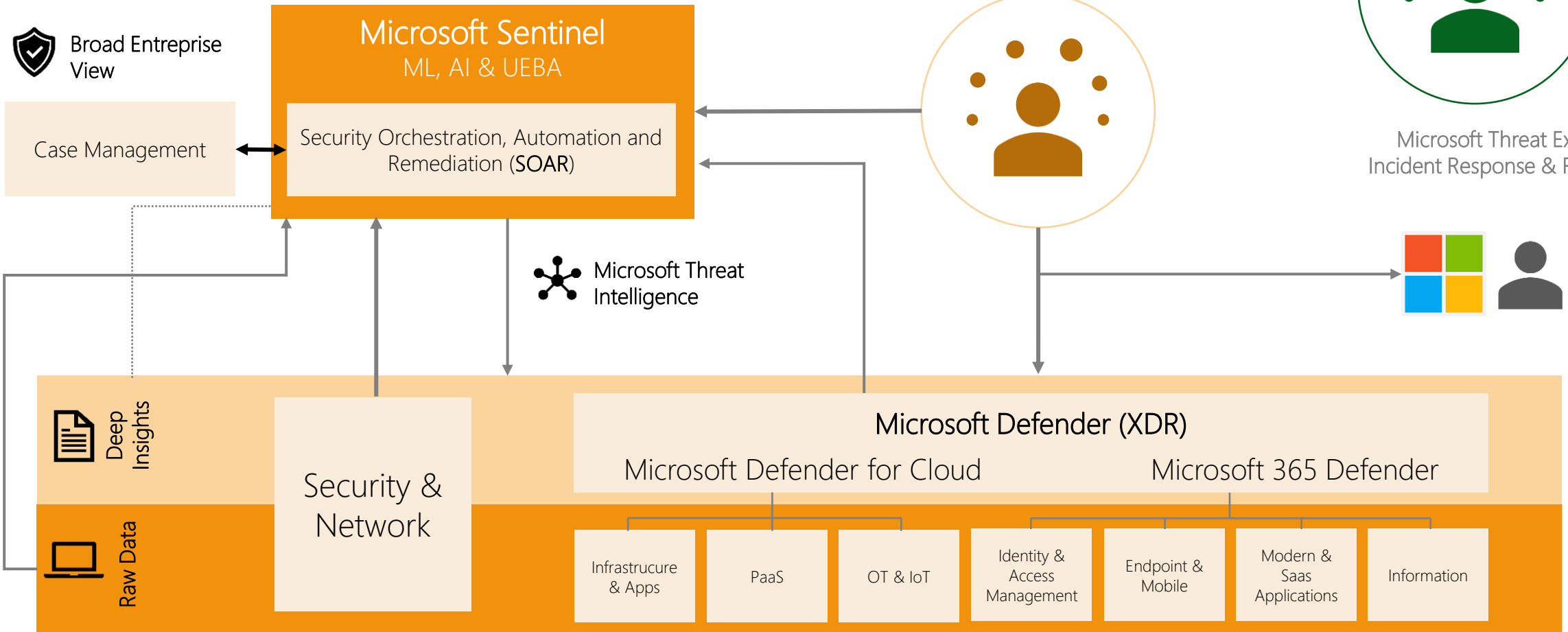


Our SOC manages the incoming Security Incidents up to 99%

Customer SPOC



Microsoft Threat Experts Incident Response & Recovery



Key Takeaways

- 1 **Focus proportionately on left-of-bang and right-of-bang**

- 2 **Start with getting basic security hygiene right and innovate continuously**

- 3 **Modernize your identity lifecycle – identities are your crown jewels**

- 4 **Enable MFA – embrace phishing-resistant methods**

- 5 **Operating an XDR is more than reacting to alerts**

Q&A

Planning the Journey

How can you start your journey? Which key steps need to be taken?



Overview

Vision of end-to-end security.

Combat Phishing Attacks

Phishing attacks are the #1 attacks and require defense-in-depth concept including people.

Smart Identity Lifecycle

Identities are the core of today's infrastructure. How can we manage them efficiently?

Operate your XDR

Implementing products is simple, but what processes are required? Is AI the solution?

Q&A

Summary and time for questions

Download Slides

