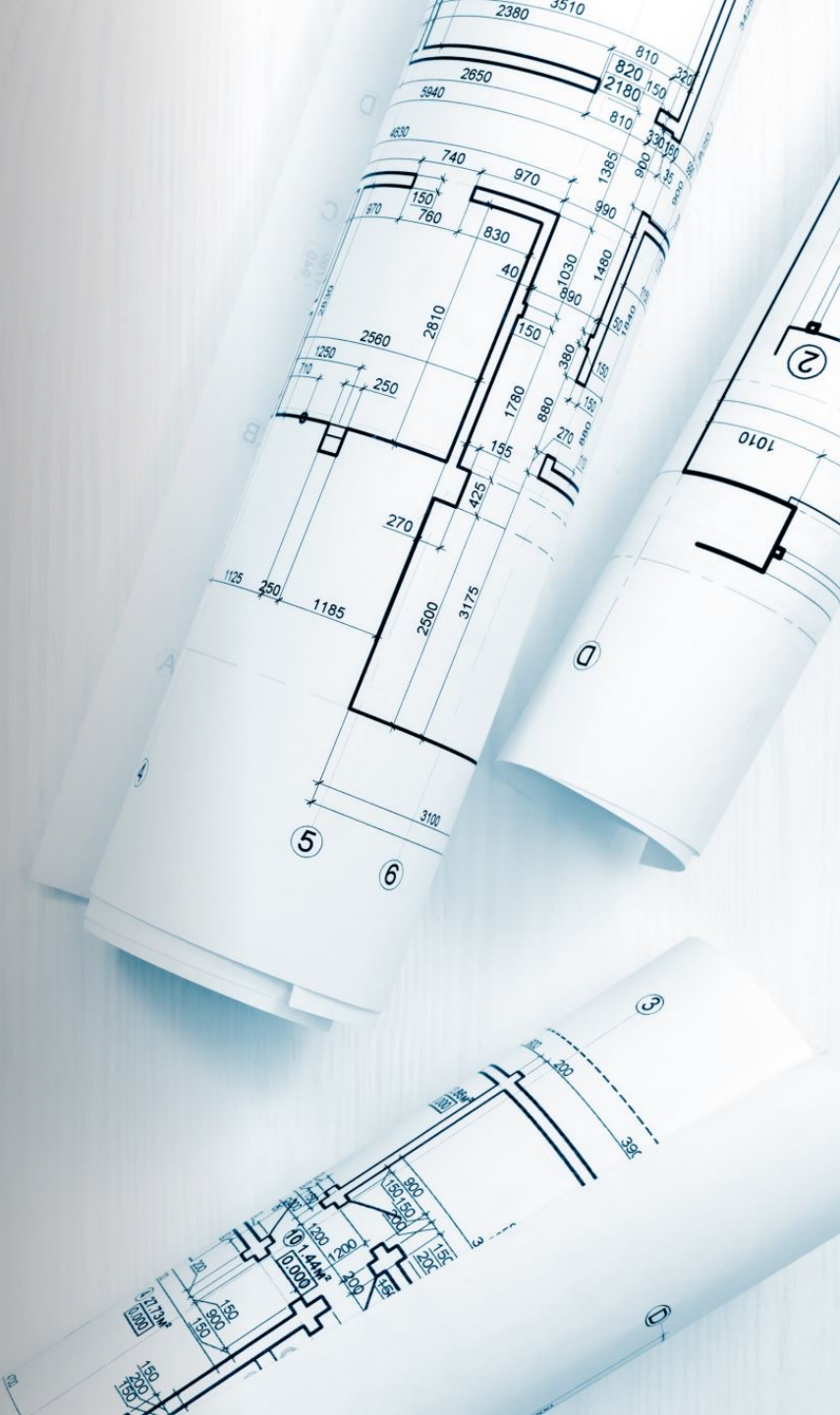
Microsoft Security
Adoption Framework

Microsoft Cybersecurity Reference Architectures (MCRA)

End to End Security Architecture following Zero Trust principles



About me

Microsoft
Sr Cloud Solution Architect

13 years of experience

The classic potato

Azure | Identity
EUC | InfoSec

alven.tech

https://twitter.com/salvestad/

Ultra runner by night

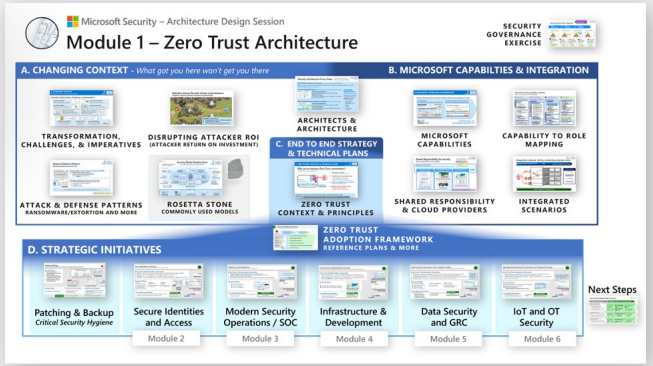
the illustration has been created by AI DALL E

Microsoft Security
Adoption Framework

Top End to End Security Challenges

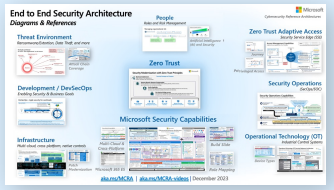
- Incomplete or network-centric architectures aren't agile & can't keep up with continuous change (security threats, technology platform, and business requirements)
- Challenges with
  - Creating integrated end to end architecture
  - Integrating security technologies
  - Planning and prioritizing security modernization initiatives

MCRA is a subset of the full Security Architecture Design Session (ADS) module 1 workshop:



Agenda

- Overview of Security Adoption Framework and End to End Cybersecurity Architecture
  - **End to End Security:** Consider the whole problem
  - **Ruthlessly Prioritize:** Identify top gaps + quick wins
  - **Get started:** Start somewhere & continuously improve
- Antipatterns and best practices
- Diagrams and references
  Applying Zero Trust principles



Security Adoption Framework

Align security to business scenarios using initiatives that progressively get closer to full 'Zero Trust'

Business Scenarios
Guiding North Star

1 - I want people to do their job securely from anywhere

2 - I want to minimize business damage from security incidents

3 - I want to identify and protect critical business assets

4 - I want to proactively meet regulatory requirements

5 - I want to have confidence in my security posture and programs

1. Strategic Framework

End to End Strategy, Architecture, and Operating Model

2. Strategic initiatives

Clearly defined architecture and implementation plans

- Security Hygiene: Backup and Patching
- Secure Identities and Access
- Modern Security Operations
- Infrastructure and Development
- Data Security & Governance, Risk, Compliance (GRC)
- OT and IoT Security

Security Adoption Framework

Reduce risk by rapidly modernizing security capabilities and practices

Microsoft

CEO

Business Leadership

CIO CISO

Technical Leadership

Architects & Technical Managers

Implementation

Securing Digital Transformation

Business and Security Integration

Security Strategy, Programs, and Epics

Architecture and Policy

Technical Planning

Implementation and Operation

Engaging Business Leaders on Security

Security Strategy and Program

CISO Workshop

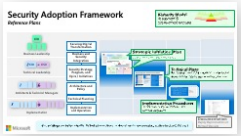
Zero Trust Architecture

Microsoft Cybersecurity Reference Architectures (MCRA)

Secure Identities and Access	Modern Security Operations (SecOps/SOC)	Infrastructure & Development Security	Data Security & Governance	IoT and OT Security

Assess current plans, configurations, and operations for Microsoft security capabilities

Includes Reference Plans



Workshops available in the Microsoft Unified catalog

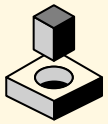
All are holistic for the 'hybrid of everything' technical estate (on-premises, multi-cloud, IoT, OT, etc.)

Common Security Antipatterns - Technical Architecture

Common mistakes that impede security effectiveness and increase organizational risk

Skipping basic maintenance

Skipping backups, disaster recovery exercises, and software updates/patching on assets



Securing cloud like on premises

Attempting to force on-prem controls and practices directly onto cloud resources

Wasting resources on legacy

Legacy system maintenance and costs draining ability to effectively secure business assets

Artisan Security

Focused on custom manual solutions instead of automation and off the shelf tooling

Disconnected security approach

Independent security teams, strategies, tech, and processes for network, identity, devices, etc.

Lack of commitment to lifecycle

Treating security controls and processes as points in time instead of an ongoing lifecycle

Best Practices

Develop and implement an **end to end technical security strategy** focused on durable capabilities and Zero Trust Principles

This workshop helps you define and rapidly improve on best practices across security including:

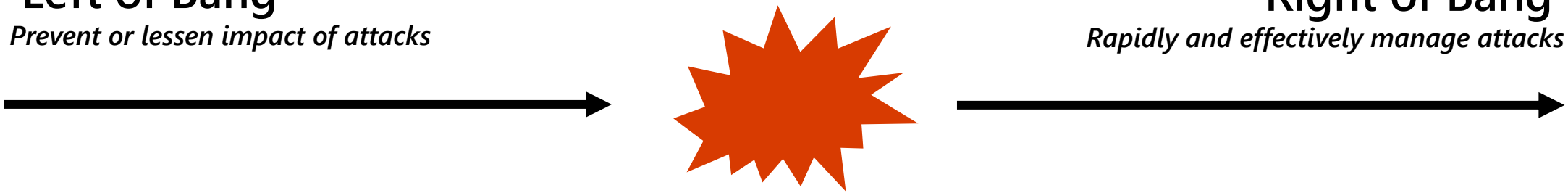
- ***Asset-centric security*** aligned to business priorities & technical estate (beyond network perimeter)
- ***Consistent principle-driven approach*** throughout security lifecycle
- ***Pragmatic prioritization*** based on attacker motivations, behavior, and return on investment
- ***Balance investments*** between innovation and rigorous application of security maintenance/hygiene
- ***'Configure before customize'*** approach that embraces automation, innovation, and continuous improvement
- ***Security is a team sport*** across security, technology, and business teams

Improving Resiliency

Enable business mission while continuously increasing security assurances

'Left of Bang'

Prevent or lessen impact of attacks



'Right of Bang'

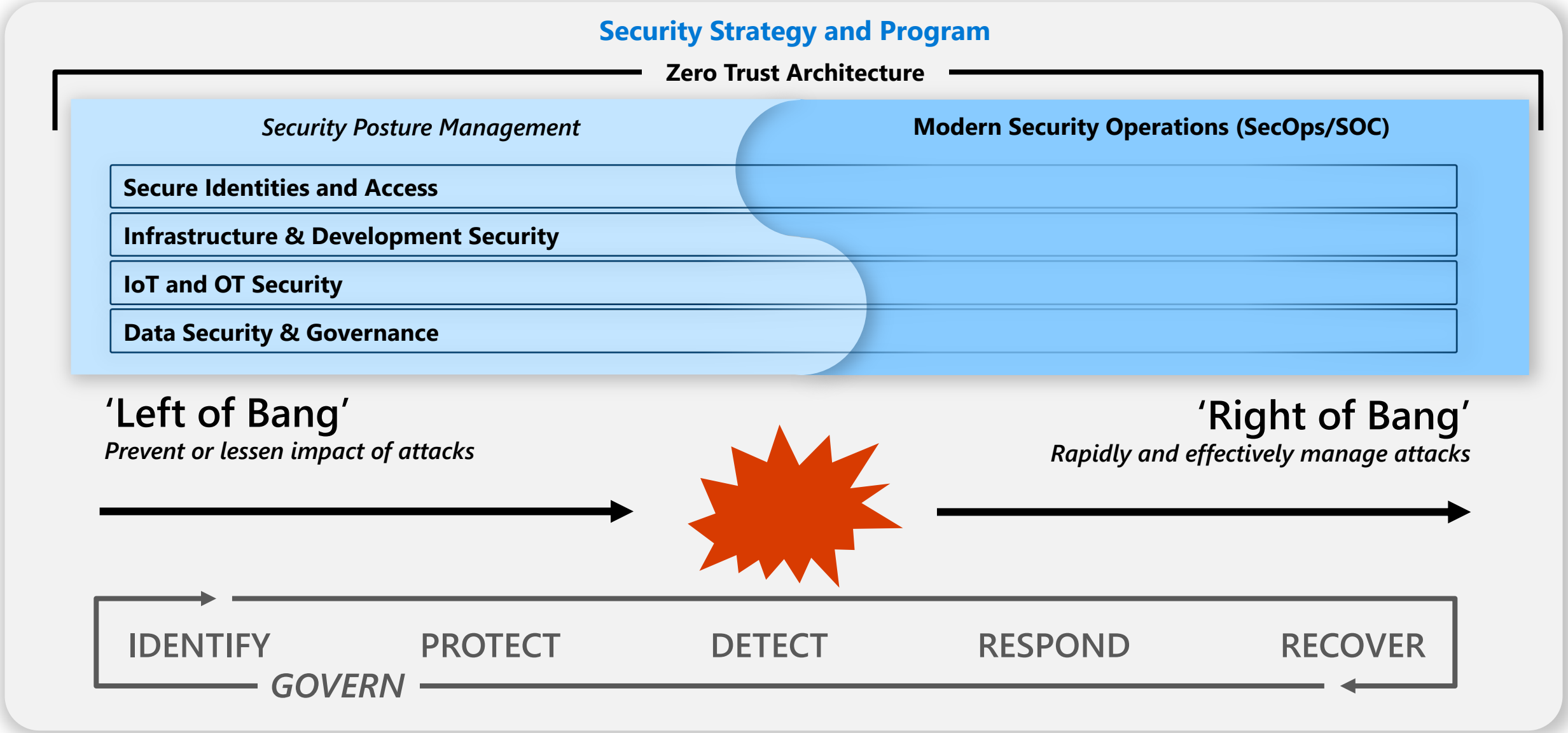
Rapidly and effectively manage attacks

The job will never be 'done' or 'perfect', but it's important to keep doing (like cleaning a house)

[NIST Cybersecurity Framework v2]

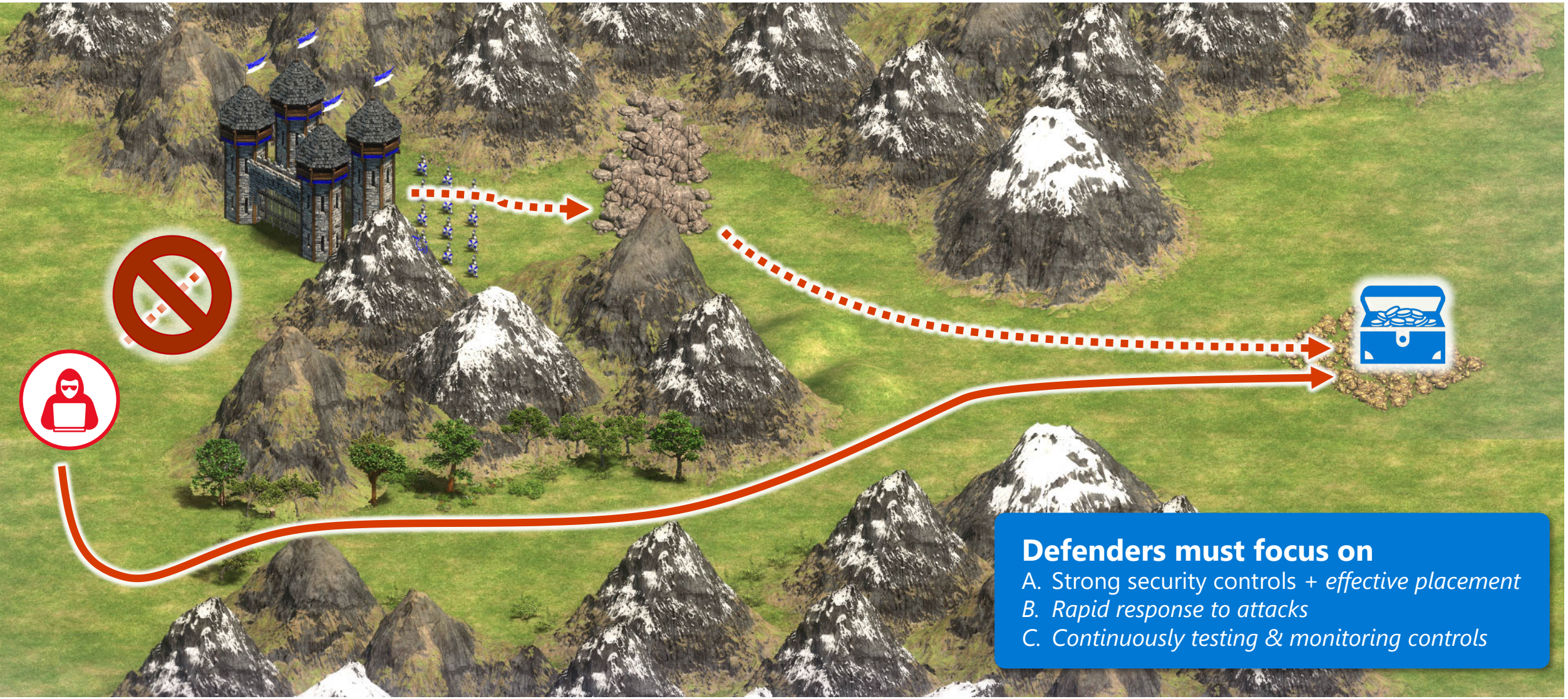
End to End Security

Enable business mission and increasing security assurances with intentional approach



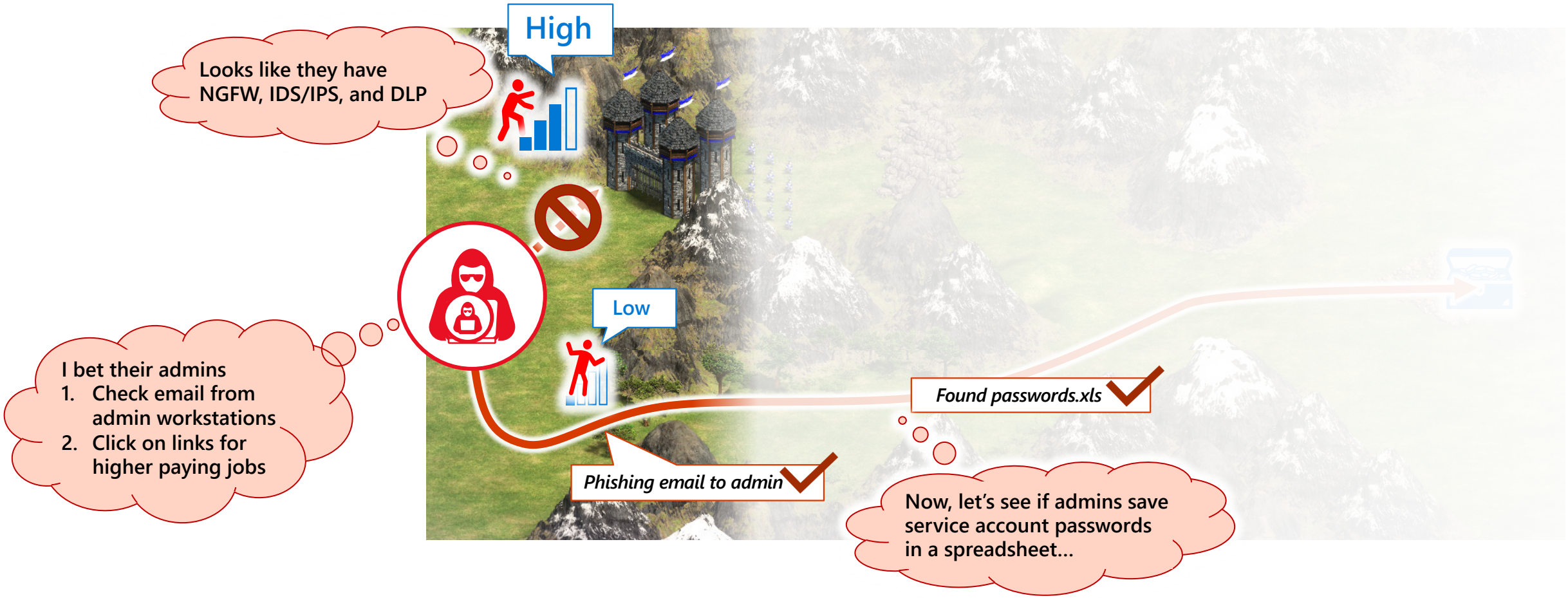
Attackers choose the path of least cost/resistance

Antipattern: Believing attackers will follow the planned path



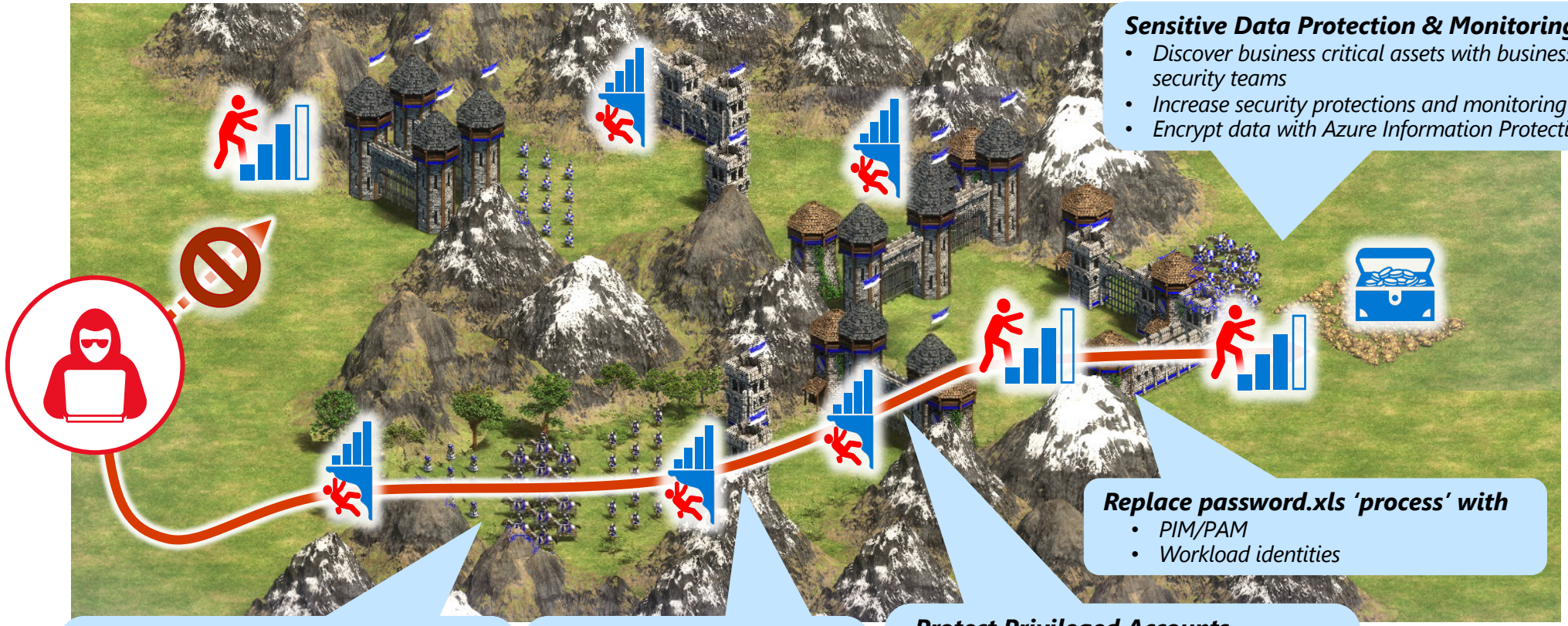
Attacker Perspective: shaped by experience & ‘fog of war’

Attackers use what they see, know, and can guess



Strategically position security investments

Raise cost and friction on attacker's easiest and highest impact paths



Sensitive Data Protection & Monitoring

- *Discover business critical assets with business, technology, and security teams*
- *Increase security protections and monitoring processes*
- *Encrypt data with Azure Information Protection*

Replace password.xls 'process' with

- *PIM/PAM*
- *Workload identities*

Modernize Security Operations

- *Add XDR for identity, endpoint (EDR), cloud apps, and other paths*
- *Train SecOps analysts on endpoints and identity authentication flows*

Rigorous Security Hygiene

- *Rapid Patching*
- *Secure Configuration*
- *Secure Operational Practices*

Protect Privileged Accounts

Require separate accounts for Admins and enforce MFA/passwordless

Privileged Access Workstations (PAWs) + enforce with Conditional Access

Security is complex and challenging

Attacks can shut all business operations down, creating board level risk

Hybrid of Everything, Everywhere, All at Once

Must secure across *everything*

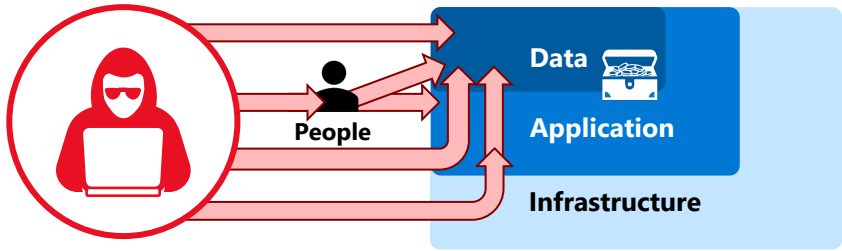
- **Brand New -** IoT, DevOps, and Cloud services, devices and products
- **Current/Aging -** 5-25 year old enterprise IT servers, products, etc.
- **Legacy/Ancient -** 30+ year old Operational Technology (OT) systems

Nothing gets retired!
Usually for fear of breaking something (& getting blamed)

'Data swamp' accumulates
managed data + unmanaged 'dark' data

Attackers have a lot of options

- *Forcing security into a holistic complex approach*



- **Regulatory Sprawl -** *200+ daily updates from 750 regulatory bodies*
- **Threats –** *Continuously changing threat landscape*
- **Security Tools –** *dozens or hundreds of tools at customers*

Goal: Zero Assumed Trust

Reduce risk by finding and removing implicit assumptions of trust

With 30+ years of backlog at most organizations, it will take a while to burn down the backlog of assumed trust

False Assumptions

of implicit or explicit trust

- Security is the opposite of productivity
- All attacks can be prevented
- Network security perimeter will keep attackers out
- Passwords are strong enough
- IT Admins are safe
- IT Infrastructure is safe
- Developers always write secure code
- The software and components we use are secure

Zero Trust Mitigation

Systematically Build & Measure Trust

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

Assume Compromise
Continuously reduce blast radius and attack surface through prevention and detection/response/recovery

Shift to Asset-Centric Security Strategy
Revisit how to do access control, security operations, infrastructure and development security, and more

Explicitly Validate Account Security
Require MFA and analyze all user sessions with behavior analytics, threat intelligence, and more

Plan and Execute Privileged Access Strategy
Establish security of accounts, workstations, and other privileged entities (aka.ms/spa)

Validate Infrastructure Integrity
Explicitly validate trust of operating systems, applications, services accounts, and more

Integrate security into development process
Security education, issue detection and mitigation, response, and more

Supply chain security
Validate the integrity of software and hardware components from open source. vendors, and others

Zero Trust Security Architecture

End to End Prioritized Execution + Continuous Improvement

1. Look End to End: *Consider the whole security problem*

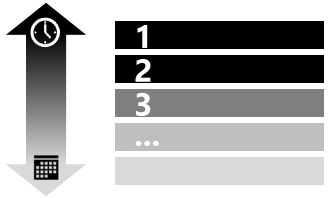
OBSERVE, ORIENT

Security is complex and challenging

Resilience required across the lifecycle

2. Ruthlessly Prioritize: *Identify top gaps + quick wins*

DECIDE



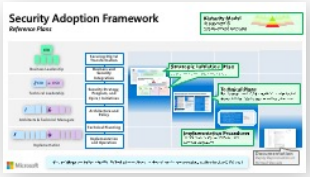
Prioritize backlog of trust assumptions

Disrupt attacker return on investment (ROI)

3. Get started: *Start somewhere and continuously improve*

ACT

Microsoft Security Adoption Framework



Leverage reference plans and architectures

End to End Security Architecture

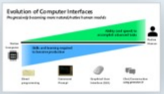
Diagrams & References

Microsoft

Cybersecurity Reference Architectures

People

Roles and Risk Management



Artificial Intelligence (AI) and Security

Threat Environment

Ransomware/Extortion, Data Theft, and more

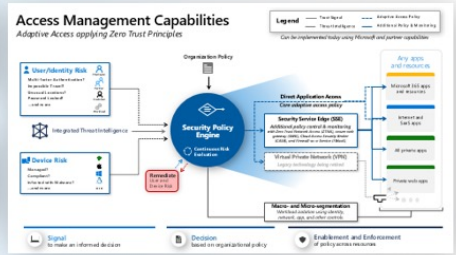
Attack Chain Coverage

Zero Trust Adaptive Access

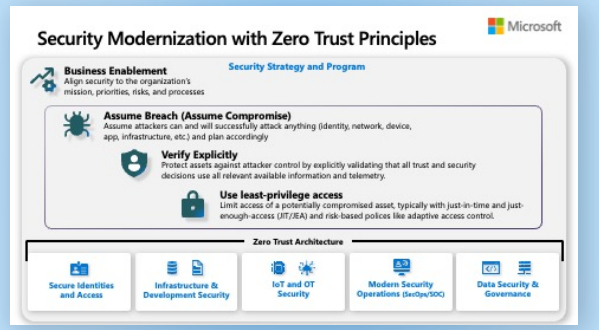
Security Service Edge (SSE)

Journey

Privileged Access

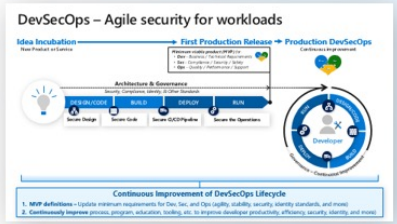


Zero Trust



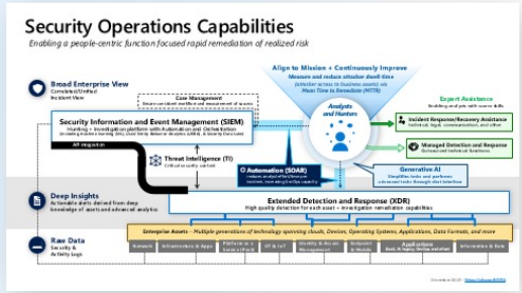
Development / DevSecOps

Enabling Security & Business Goals



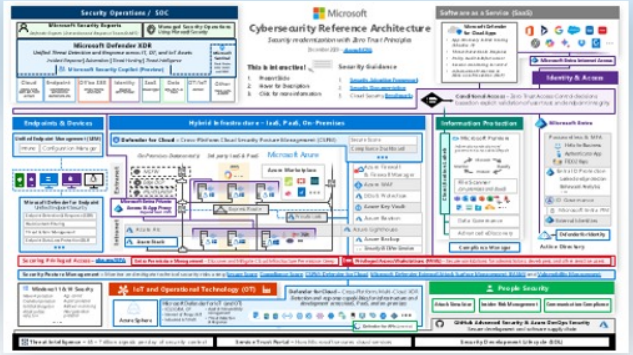
Security Operations

(SecOps/SOC)



Microsoft Security Capabilities

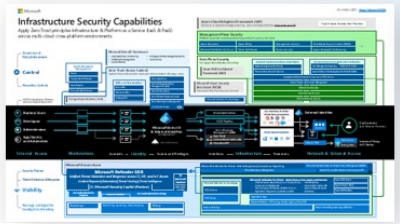
Multi-Cloud & Cross-Platform



Build Slide

Infrastructure

Multi-cloud, cross-platform, native controls



Patch Modernization

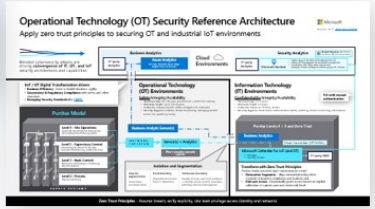
Microsoft 365 E5

Role Mapping

Operational Technology (OT)

Industrial Control Systems

Device Types



aka.ms/MCRA | aka.ms/MCRA-videos | December 2023

Security Modernization with Zero Trust Principles

Microsoft

Business Enablement

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

Security Strategy and Program

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 polices like adaptive access control.

Zero Trust Architecture

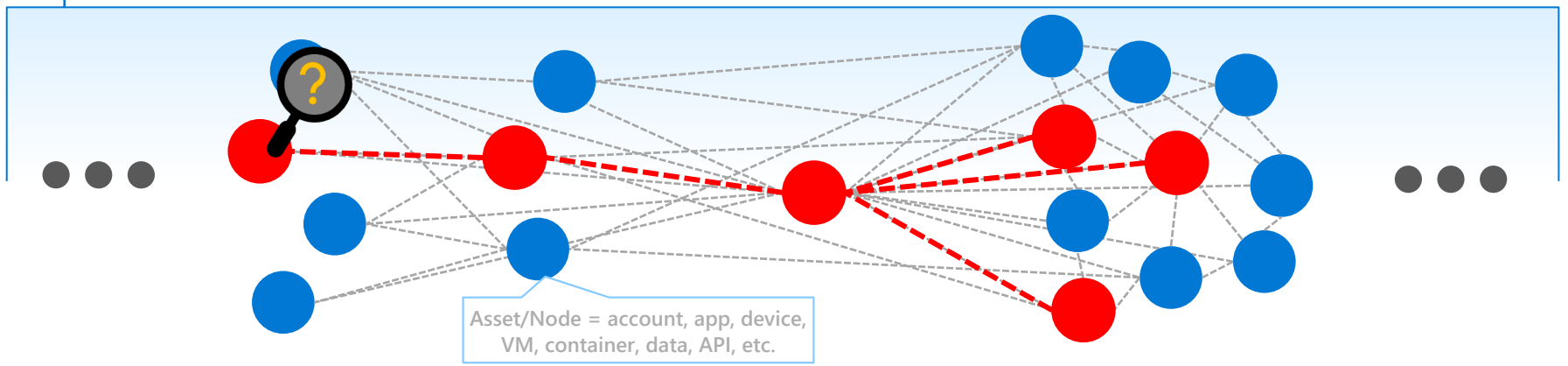
- Secure Identities and Access
- Infrastructure & Development Security
- IoT and OT Security
- Modern Security Operations (SecOps/SOC)
- Data Security & Governance

Zero Trust Principles

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

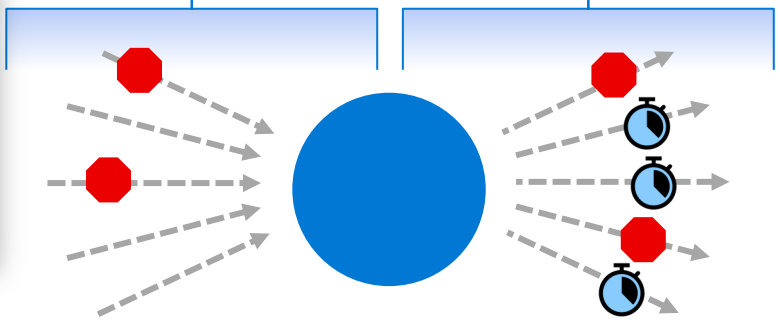
Assume Breach (Assume Compromise)
Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

→ *Transforms from ~~"defend the network"~~ to "enable secure productivity on any network"*



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

→ *Reduces "attack surface" of each asset*



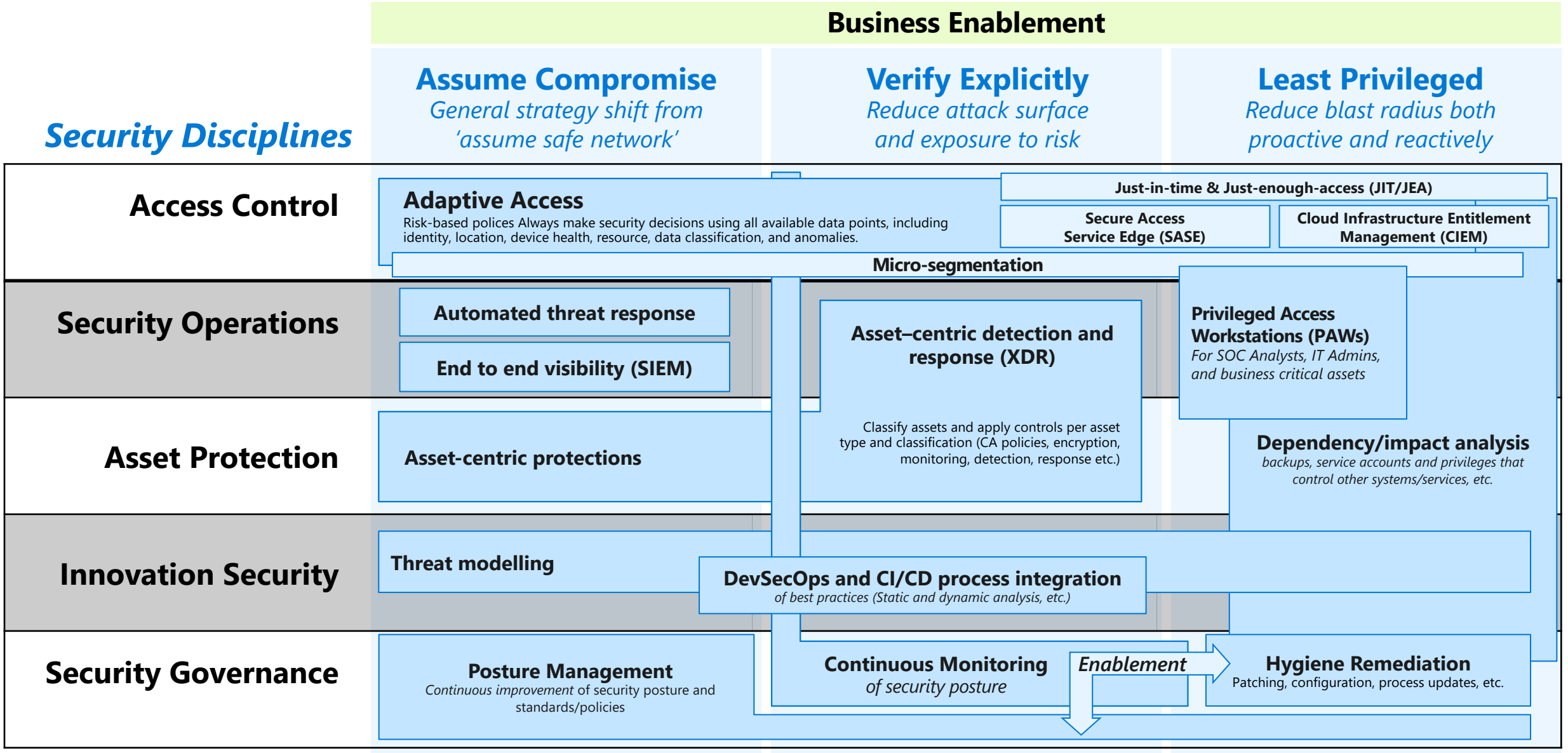
Use least privilege access
Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

→ *Reduce "blast radius" of compromises*

Apply Zero Trust principles

Key changes across security disciplines

All elements informed by threat and business intelligence, assisted by security engineering/automation



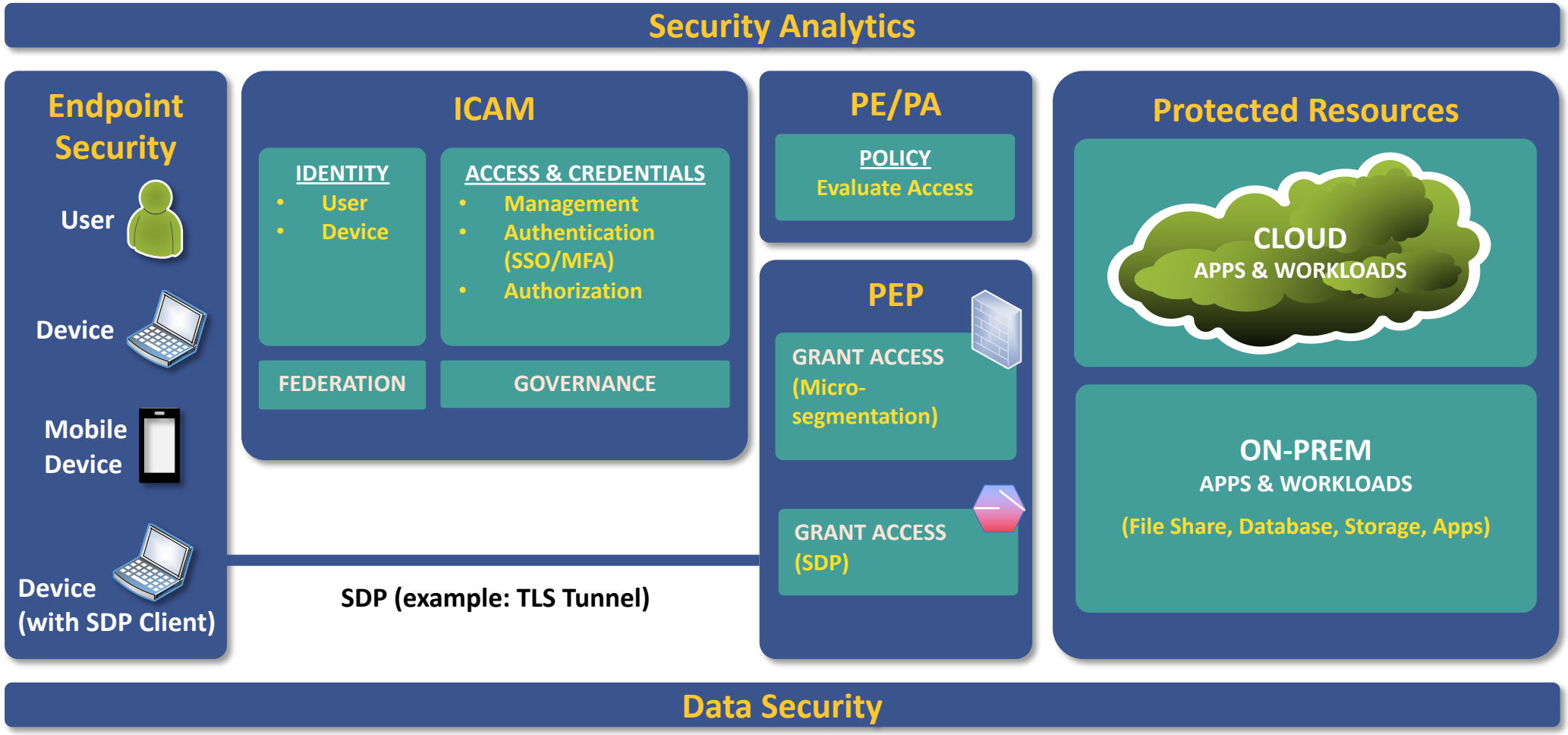
Key Industry Collaborations

The Open Group
Focused on integration with business and IT/Enterprise/Security architecture

US National Institute of Standards and Technology (NIST)
Focused on architecture and implementation with available technology

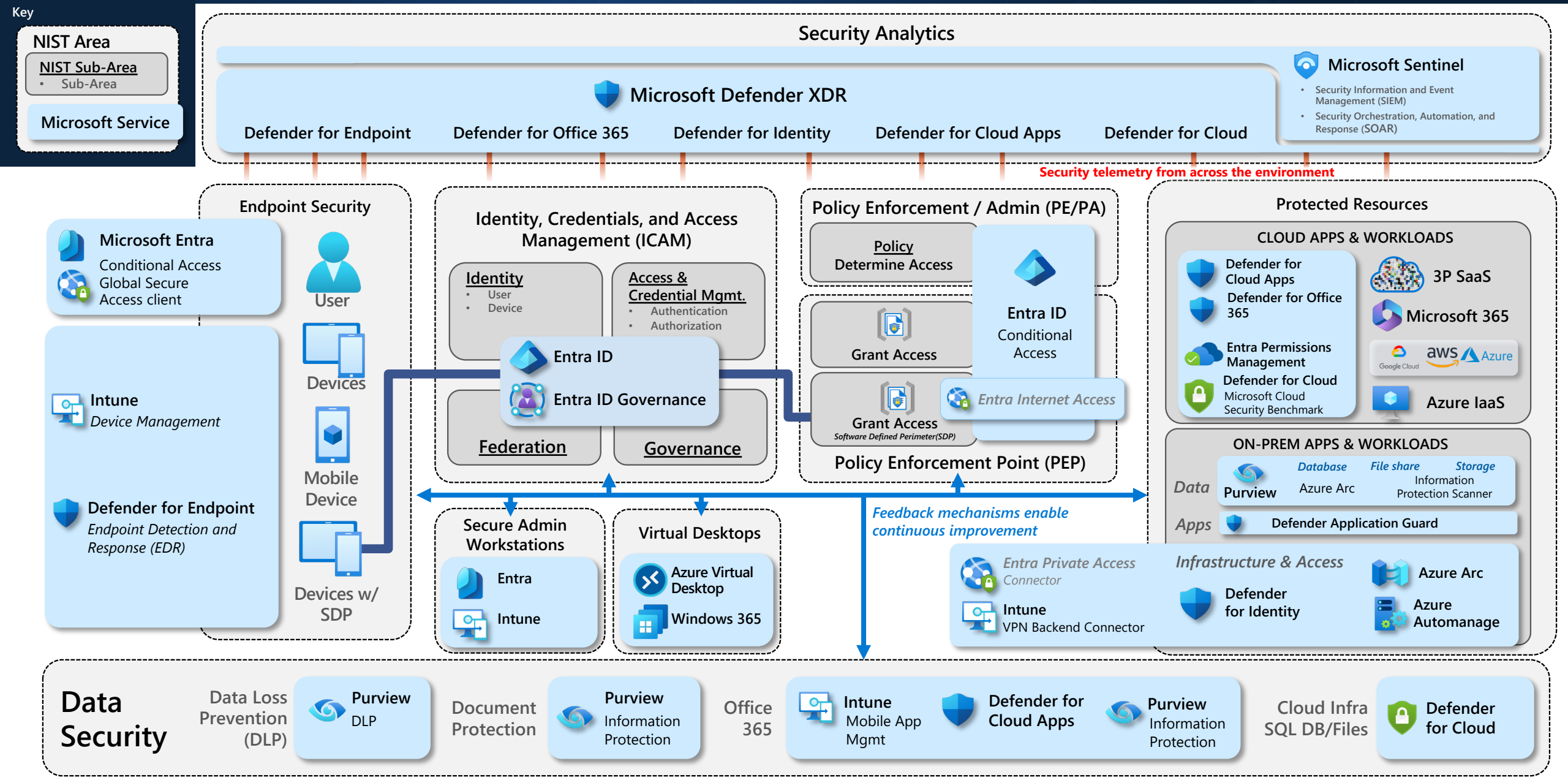
Many organizations are contributing valuable perspectives and guidance like the Cybersecurity and Infrastructure Security Agency (CISA), Cloud Security Alliance (CSA), and some technology vendors

Zero Trust Architecture (ZTA)



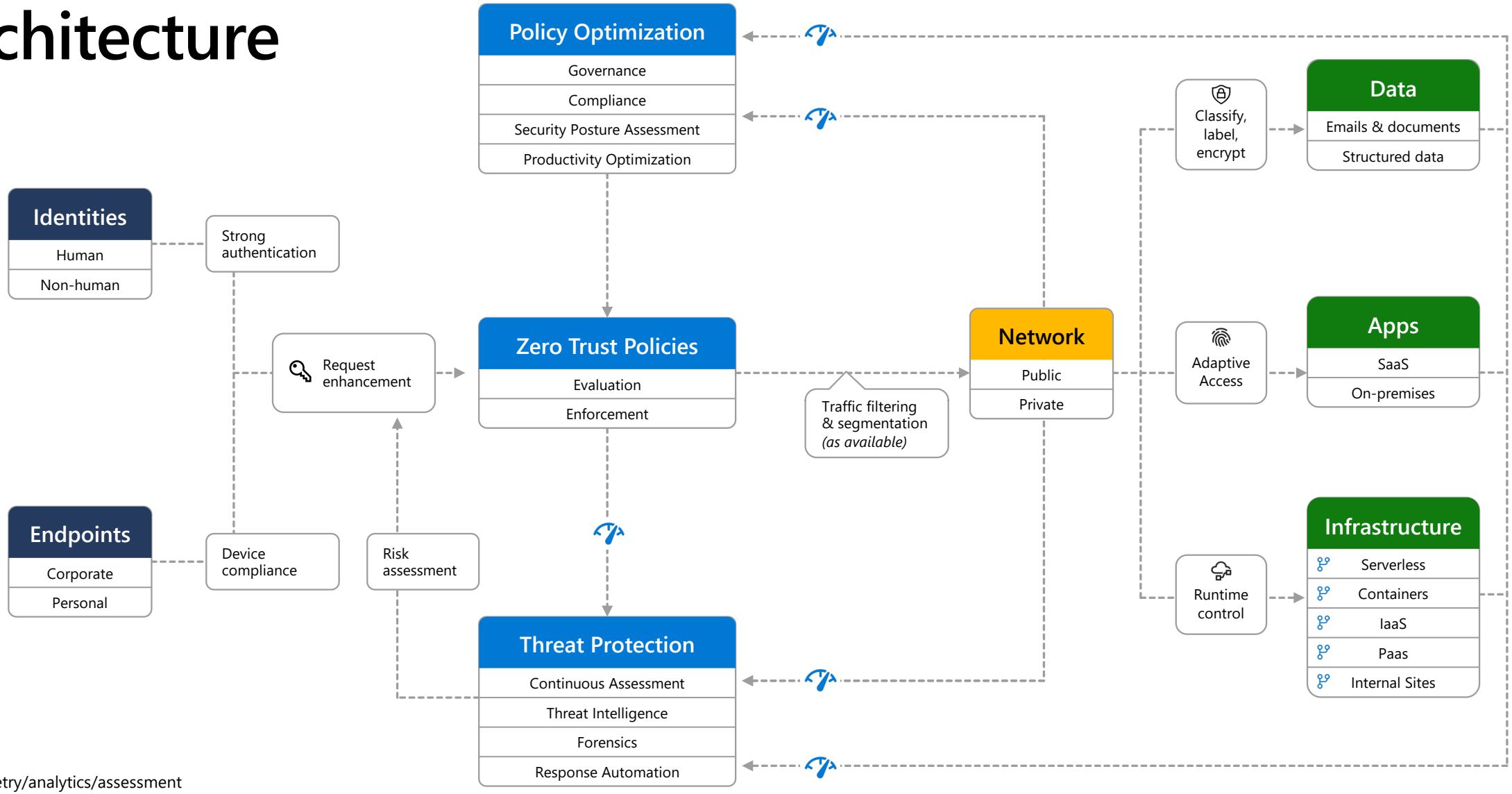
Microsoft Zero Trust Capability Mapping

Implemented in NCCoE lab (Summer 2023)



Zero Trust architecture

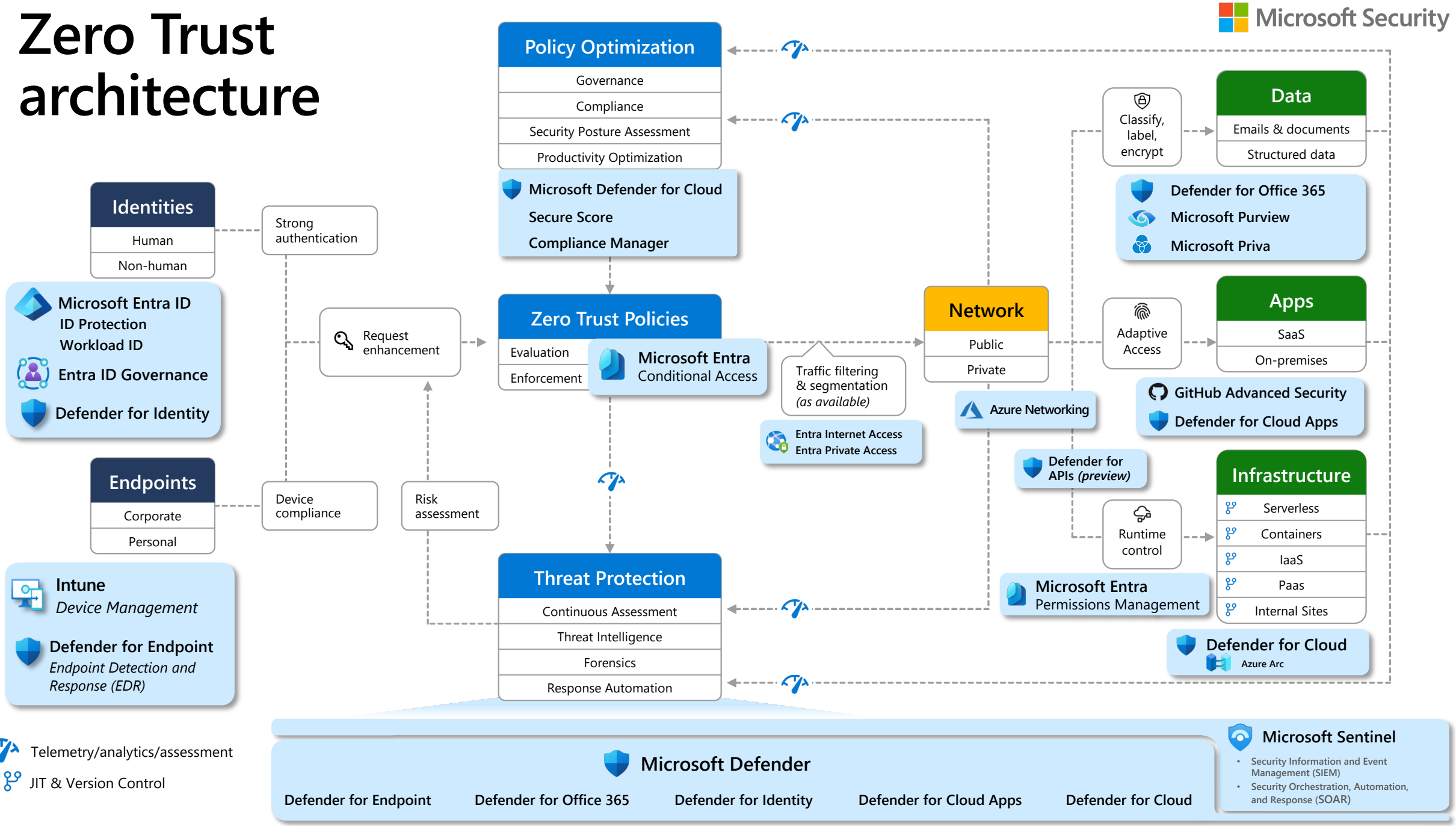
Microsoft Security



Telemetry/analytics/assessment

JIT & Version Control

Zero Trust architecture

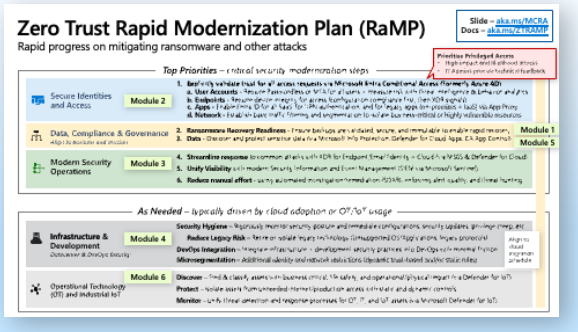


Starting the Security Adoption Framework

Multiple structured ways to accelerate end to end security transformation

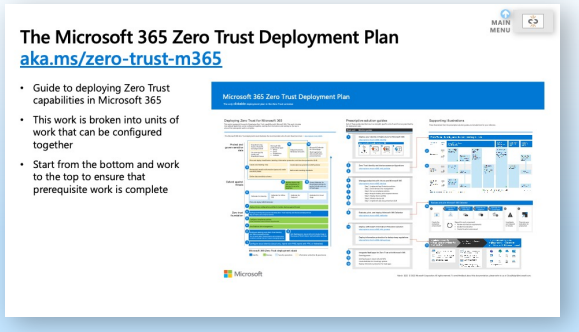
QUICK WINS

across all initiatives with Zero Trust RaMP

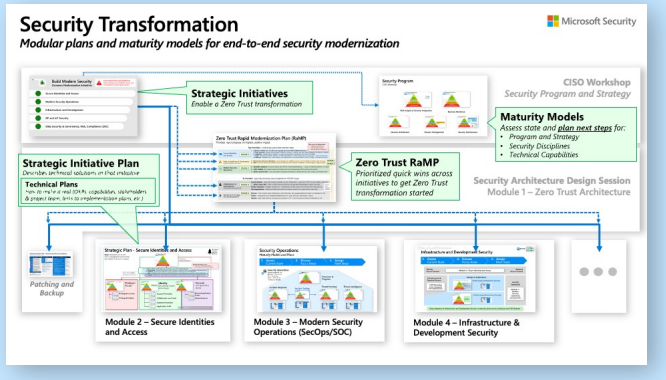


MICROSOFT 365

Implement M365 to support Zero Trust



Full Security Modernization Plans



Actionable & Complete Reference Strategy

- → ***6 Strategic Initiatives*** driving big outcomes with
  - → ***2-8 Technical Plans*** **with**
    - → Objectives & Key Results (OKRs)
    - → Project Teams and Workstreams
    - → Links to Implementation Procedures
    - → …and more

Zero Trust Rapid Modernization Plan (RaMP)

Rapid progress on mitigating ransomware and other attacks

Slide – aka.ms/MCRA
Docs – aka.ms/ZTRAMP

Prioritize Privileged Access
- High impact and likelihood attacks
- IT Admins provide technical feedback

Top Priorities – *critical security modernization steps*

Secure Identities and Access — Module 2

1. **Explicitly validate trust for all access requests via Microsoft Entra Conditional Access (Formerly Azure AD)**
   a. **User Accounts -** Require Passwordless or MFA for all users + measure risk with threat intelligence & behavior analytics
   b. **Endpoints -** Require device integrity for access (configuration compliance first, then XDR signals)
   c. **Apps -** Enable Entra ID for all SaaS, for VPN authentication, and for legacy apps (on-premises + IaaS) via App Proxy
   d. **Network -** Establish basic traffic filtering and segmentation to isolate business-critical or highly vulnerable resources

Data, Compliance & Governance — Module 1, Module 5

Align to business and mission

2. **Ransomware Recovery Readiness -** Ensure backups are validated, secure, and immutable to enable rapid recovery
3. **Data -** Discover and protect sensitive data (via Microsoft Info Protection, Defender for Cloud Apps, CA App Control)

Modern Security Operations — Module 3

4. **Streamline response** to common attacks with XDR for Endpoint/Email/Identity + Cloud (via M365 & Defender for Cloud)
5. **Unify Visibility** with modern Security Information and Event Management (SIEM via Microsoft Sentinel)
6. **Reduce manual effort -** using automated investigation/remediation (SOAR), enforcing alert quality, and threat hunting

As Needed – *typically driven by cloud adoption or OT/IoT usage*

Infrastructure & Development — Module 4

Datacenter & DevOps Security

Security Hygiene – Rigorously monitor security posture and remediate configurations, security updates, privilege creep, etc.

Reduce Legacy Risk – Retire or isolate legacy technology (Unsupported OS/Applications, legacy protocols)

DevOps Integration – Integrate infrastructure + development security practices into DevOps with minimal friction

Microsegmentation – Additional *identity and network* restrictions (dynamic trust-based and/or static rules)

Align to cloud migration schedule

Operational Technology (OT) and Industrial IoT — Module 6

Discover – Find & classify assets with business critical, life safety, and operational/physical impact (via Defender for IoT)

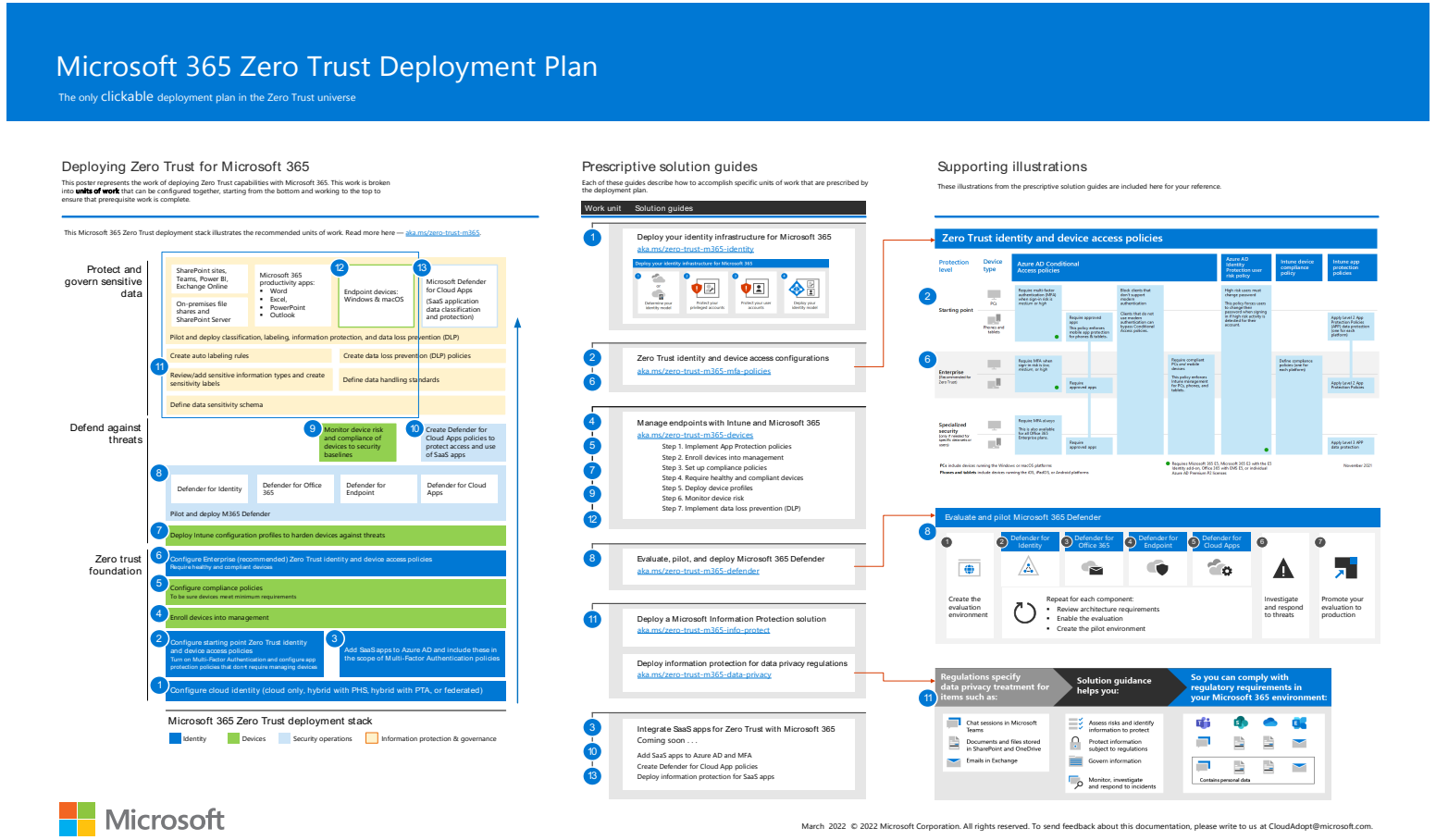
Protect – isolate assets from unneeded internet/production access with static and dynamic controls

Monitor – unify threat detection and response processes for OT, IT, and IoT assets (via Microsoft Defender for IoT)

The Microsoft 365 Zero Trust Deployment Plan

aka.ms/zero-trust-m365

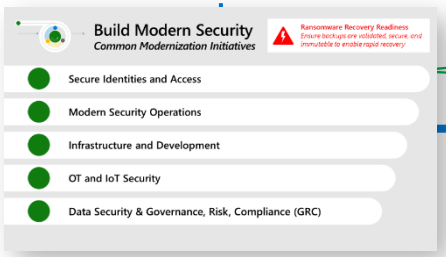
- Guide to deploying Zero Trust capabilities in Microsoft 365
- This work is broken into units of work that can be configured together
- Start from the bottom and work to the top to ensure that prerequisite work is complete



Security Transformation

Modular plans and maturity models for end-to-end security modernization

Microsoft Security



Strategic Initiatives

Enable a Zero Trust transformation

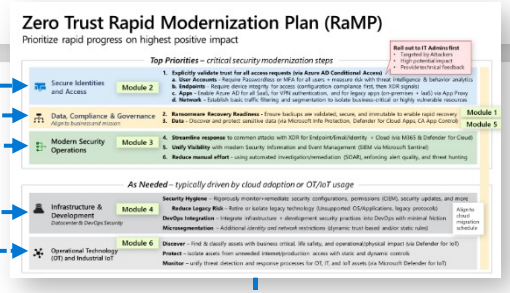
CISO Workshop

Security Program and Strategy

Maturity Models

*Assess state and **plan next steps** for:*

- *Program and Strategy*
- *Security Disciplines*
- *Technical Capabilities*



Zero Trust RaMP

Prioritized quick wins across initiatives to get Zero Trust transformation started

Strategic Initiative Plan

Describes technical solutions in that initiative

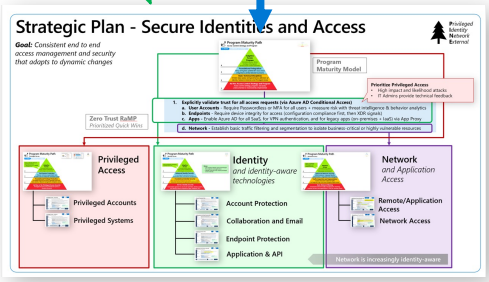
Technical Plans

How to make it real (OKRs, capabilities, stakeholders & project team, links to implementation plans, etc.)

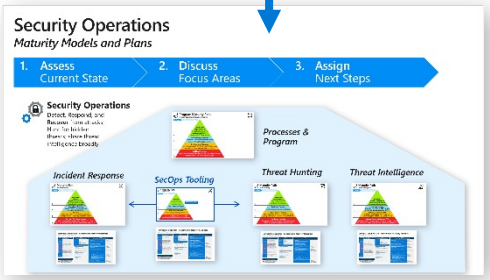
Security Architecture Design Session

Module 1 – Zero Trust Architecture

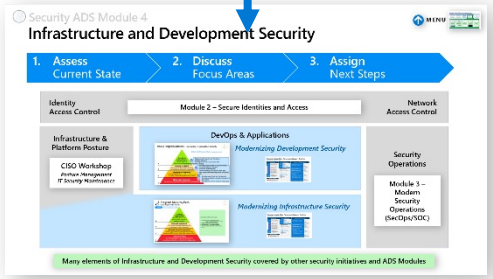
Patching and Backup



Module 2 – Secure Identities and Access



Module 3 – Modern Security Operations (SecOps/SOC)



Module 4 – Infrastructure & Development Security

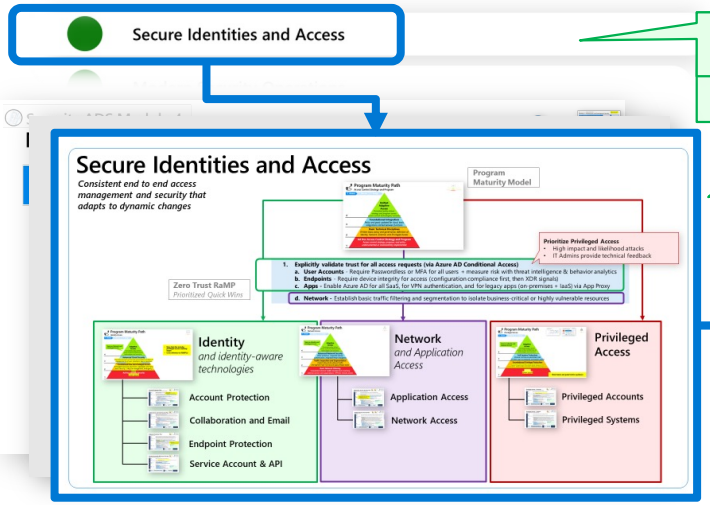
Plan Structure & Taxonomy

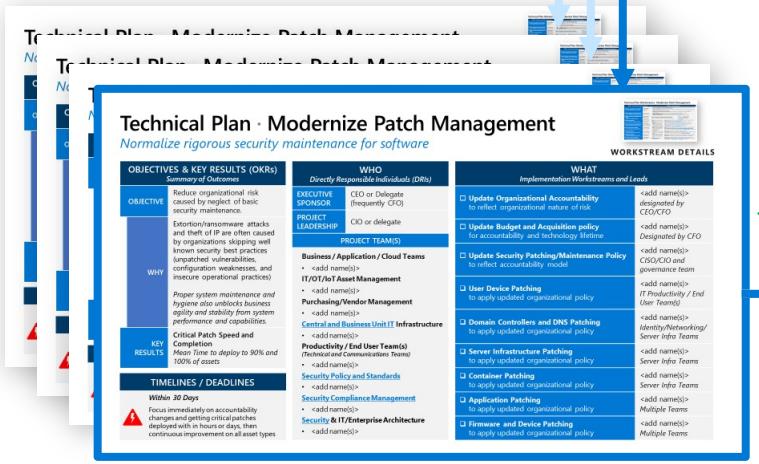
5 total

Strategic Initiative Plan

Describes technical solutions in that initiative

1 per initiative





Technical Plans

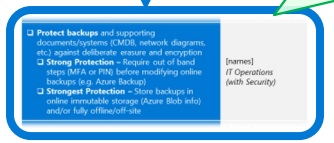
As needed per strategic initiative (1-8)

How to make it real (OKRs, capabilities, stakeholders & project team, links to implementation plans, etc.)

Implementation Procedures

Describe how to deploy/configure each technical component

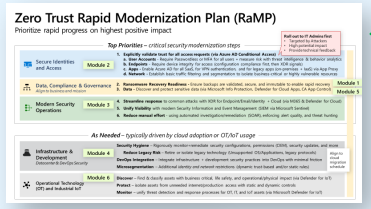
1 or more per Technical Plan



Rapid Modernization Plans (RaMPs)

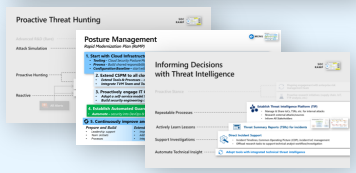
Prioritized steps for quick wins & incremental progress

As needed for complex areas



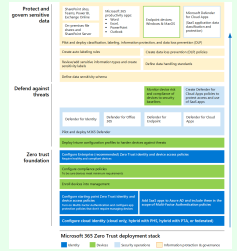
Zero Trust RaMP

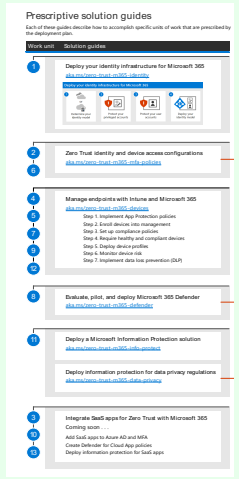
Prioritized Quick Wins across initiatives to get Zero Trust transformation started



Other RaMPs

Provide prioritized quick win guidance for selected topics





Microsoft 365 Zero Trust Deployment Plan

- *Deploy Microsoft 365 Zero Trust capabilities*
- *Grouped into work that can be configured together*

Security Resources

Microsoft

Security Adoption Framework
aka.ms/saf

Security Documentation
aka.ms/SecurityDocs

Security Strategy and Program

- CISO Workshop – aka.ms/CISOworkshop | -videos
- Cloud Adoption Framework (CAF) – aka.ms/cafsecure

- Driving Business Outcomes Using Zero Trust
  - Rapidly modernize your security posture for Zero Trust
  - Secure remote and hybrid work with Zero Trust
  - Identify and protect sensitive business data with Zero Trust
  - Meet regulatory and compliance requirements with Zero Trust

Zero Trust Architecture

- Microsoft Cybersecurity Reference Architectures (MCRA) - aka.ms/MCRA | -videos
- Ransomware and Extortion Mitigation - aka.ms/humanoperated
- Backup and restore plan to protect against ransomware - aka.ms/backup

- Zero Trust Deployment Guidance - aka.ms/ztguide | aka.ms/ztramp

Secure Identities and Access

- Securing Privileged Access (SPA) Guidance
  aka.ms/SPA
- Access Control Discipline
- Ninja Training
  - Microsoft Defender for Identity
    aka.ms/mdininja
- MCRA Video
  - Zero Trust User Access
- Microsoft Entra Documentation
  aka.ms/entradocs

Modern Security Operations (SecOps/SOC)

- Incident Response - aka.ms/IR
- CDOC Case Study - aka.ms/ITSOC
- Ninja Training
  - Microsoft 365 Defender
    aka.ms/m365dninja
  - Microsoft Defender for Office 365
    aka.ms/mdoninja
  - Microsoft Defender for Endpoint
    aka.ms/mdeninja
  - Microsoft Cloud App Security
    aka.ms/mcasninja
  - Microsoft Sentinel
- MCRA Videos
  - Security Operations
  - SecOps Integration

Infrastructure & Development Security

- Microsoft Cloud Security Benchmark (MCSB)
  aka.ms/benchmarkdocs
- Well Architected Framework (WAF)
  aka.ms/wafsecure
- Azure Security Top 10
  aka.ms/azuresecuritytop10
- Ninja Training
  - Defender for Cloud
- MCRA Video
  - Infrastructure Security
- Defender for Cloud Documentation

Data Security & Governance

- Secure data with Zero Trust
- Ninja Training
  - Microsoft Purview Information Protection
    aka.ms/MIPNinja
  - Microsoft Purview Data Loss Prevention
    aka.ms/DLPNinja
  - Insider Risk Management
- Microsoft Purview Documentation
  aka.ms/purviewdocs

IoT and OT Security

- Ninja Training
  - Defender for IoT Training
- MCRA Videos
  - MCRA Video OT & IIoT Security
- Defender for IoT Documentation
  aka.ms/D4IoTDocs

Product Capabilities
www.microsoft.com/security/business

- Security Product Documentation
  Azure | Microsoft 365

Microsoft Security Response Center (MSRC)
www.microsoft.com/en-us/msrc

Key Industry References and Resources

The Open Group

- Zero Trust Commandments - https://pubs.opengroup.org/security/zero-trust-commandments/
- Zero Trust Reference Model - https://publications.opengroup.org/security-library
- Security Principles for Architecture - https://publications.opengroup.org/security-library

US National Institute of Standards and Technology (NIST)

- Cybersecurity Framework - https://www.nist.gov/cyberframework
- Zero Trust Architecture - https://www.nist.gov/publications/zero-trust-architecture
  - NCCoE Zero Trust Project - https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
- Secure Software Development Framework (SSDF) - https://csrc.nist.gov/pubs/sp/800/218/final

Cybersecurity and Infrastructure Security Agency (CISA)

- Zero Trust Maturity Model - https://www.cisa.gov/zero-trust-maturity-model

Center for Internet Security (CIS)

- CIS Benchmarks – https://www.cisecurity.org/cis-benchmarks/

End to End Security Architecture

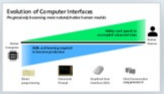
Diagrams & References

Microsoft

Cybersecurity Reference Architectures

People

Roles and Risk Management



Artificial Intelligence (AI) and Security

Threat Environment

Ransomware/Extortion, Data Theft, and more

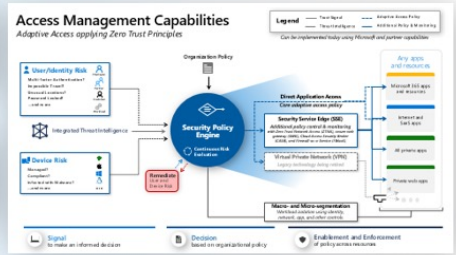
Attack Chain Coverage

Zero Trust Adaptive Access

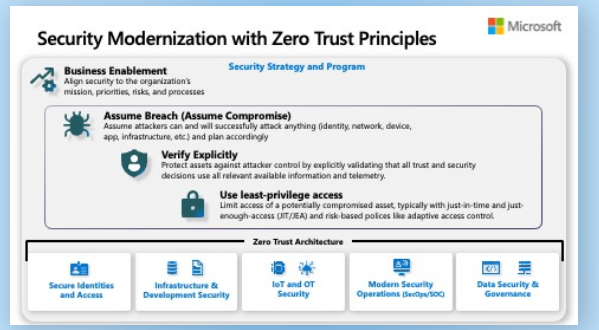
Security Service Edge (SSE)

Journey

Privileged Access

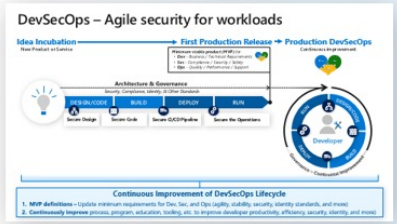


Zero Trust



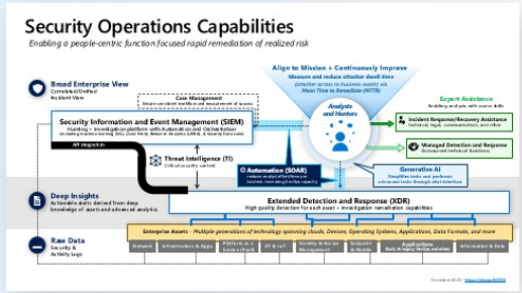
Development / DevSecOps

Enabling Security & Business Goals



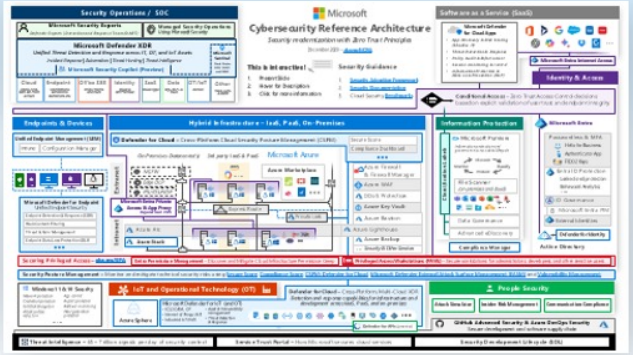
Security Operations

(SecOps/SOC)



Microsoft Security Capabilities

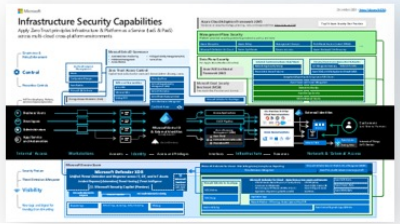
Multi-Cloud & Cross-Platform



Build Slide

Infrastructure

Multi-cloud, cross-platform, native controls



Patch Modernization

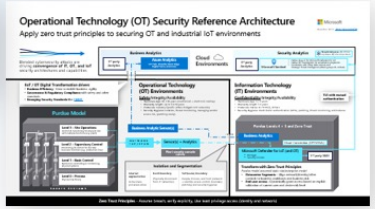
Microsoft 365 E5

Role Mapping

Operational Technology (OT)

Industrial Control Systems

Device Types



aka.ms/MCRA | aka.ms/MCRA-videos | December 2023