Microsoft Security

CISO Workshop

Security Program and Strategy

Your Name Here

MENU

CISO Workshop & Architecture Design Session (ADS)

Microsoft Security

What: Security workshops to accelerate modernization of security program, architecture, and technical initiatives (using Zero Trust principles).

Why: *Rapidly* increase security posture & align security to business priorities

How: Provide best practices, references, and other guidance based on real world lessons learned

- **CISO Workshop** – Strategies and Program Structure — You are Here
- **Security ADS –** Architectures and Technical Plans

Tips

- **Set a North Star and Keep Going –** A journey of incremental progress towards a clear vision
- **Mix of old & new -** Bring your experience and knowledge, but expect changes

Who should be in the CISO Workshop?

Primary Participants

- **CISO + Security Directors -** Helps modernize security strategy and program components, integrate security into larger organization
- **CIO + IT Directors –** Helps integrate security into technology program, cloud, and other initiatives
- **Enterprise + Security Architects** – and other roles with broad strategy/technology responsibilities

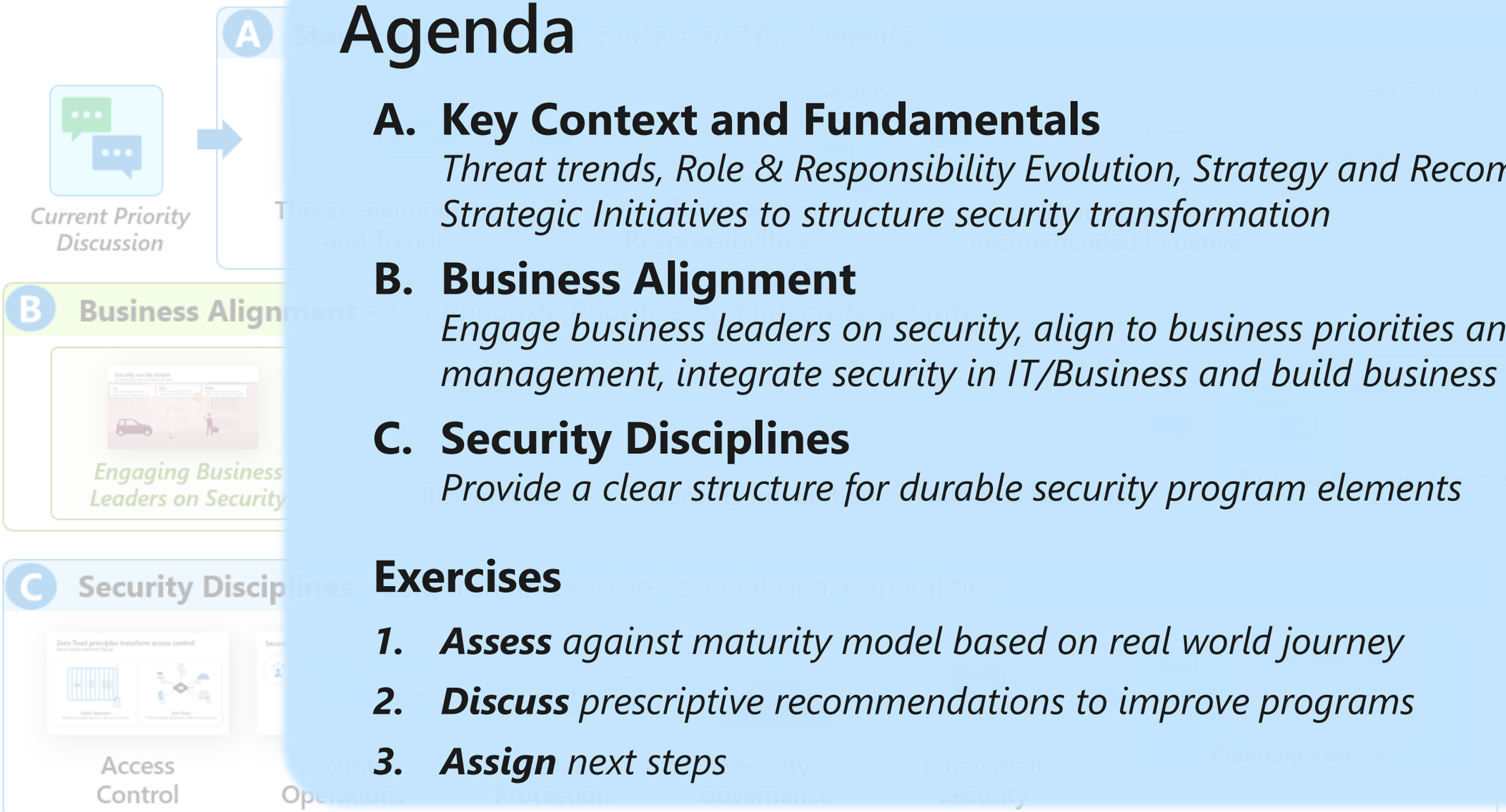
Optional Attendees

- **Business IT leads, Business initiative owners that sparked discussion –** helps integrate security into business initiatives and better understand security dependencies
- **Cloud Lead / Cloud Team (if formed) –** help integrate security into cloud initiatives and reduce unhealthy friction between teams
- *Any supporting partners and integrators chosen by those roles*

Note: This workshop is essential for people performing the functions that align with the roles above and is also useful to many other roles within an organization

CISO Workshop

End-to-end Security Program and Strategy Guidance + Integration with Digital & Cloud Transformation Teams



Agenda

A. Key Context and Fundamentals

Threat trends, Role & Responsibility Evolution, Strategy and Recommended Strategic Initiatives to structure security transformation

B. Business Alignment

Engage business leaders on security, align to business priorities and risk management, integrate security in IT/Business and build business resilience

C. Security Disciplines

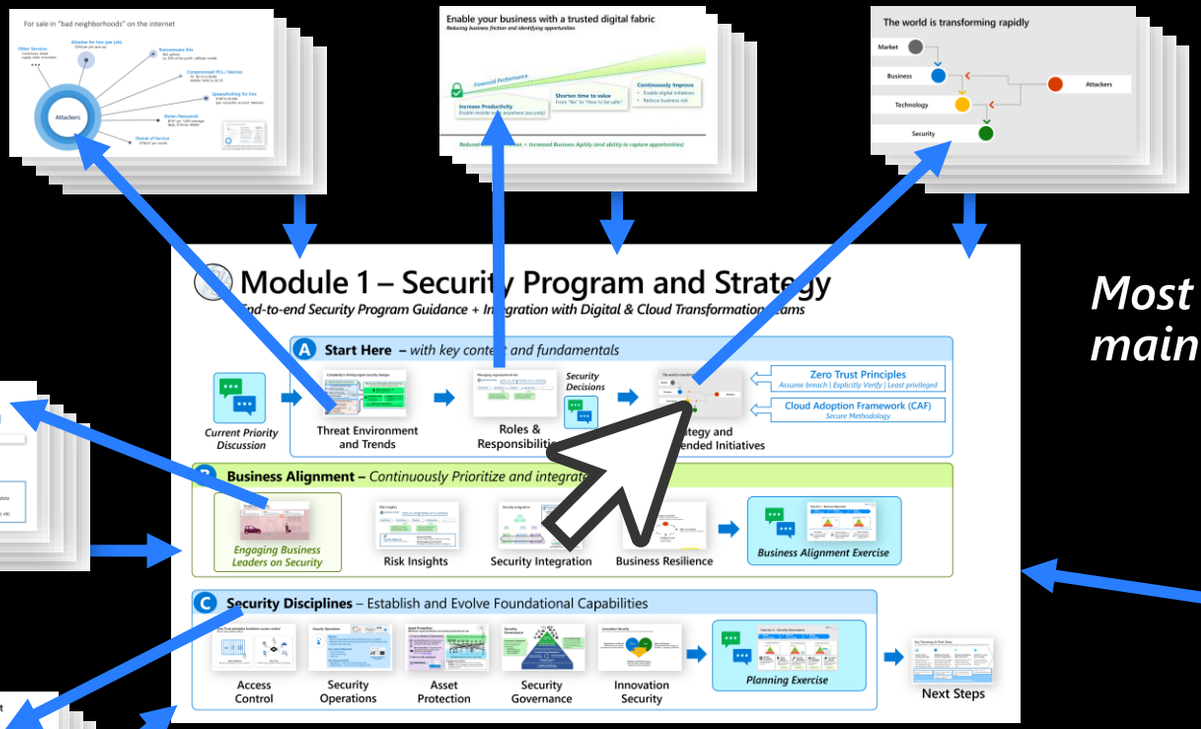
Provide a clear structure for durable security program elements

Exercises

1. ***Assess*** *against maturity model based on real world journey*
2. ***Discuss*** *prescriptive recommendations to improve programs*
3. ***Assign*** *next steps*

This presentation is interactive!

Using PowerPoint Zoom Navigation



Most sections return to the main menu after finishing

Some slides can quickly return to main menu

Jump to any section from the Main menu

Introductions

Name

Role

Expectations for today

Whiteboard – Technical Estate and Program Drivers

Current Cloud Usage

- Which workloads / business purpose?
- Which major cloud providers? (SaaS, PaaS, IaaS)

Geographic Presence

where you operate?

Compliance

& regulatory requirements

Goals and Plans

for Security and Cloud

Security Focus Areas –

What do you want to focus on?

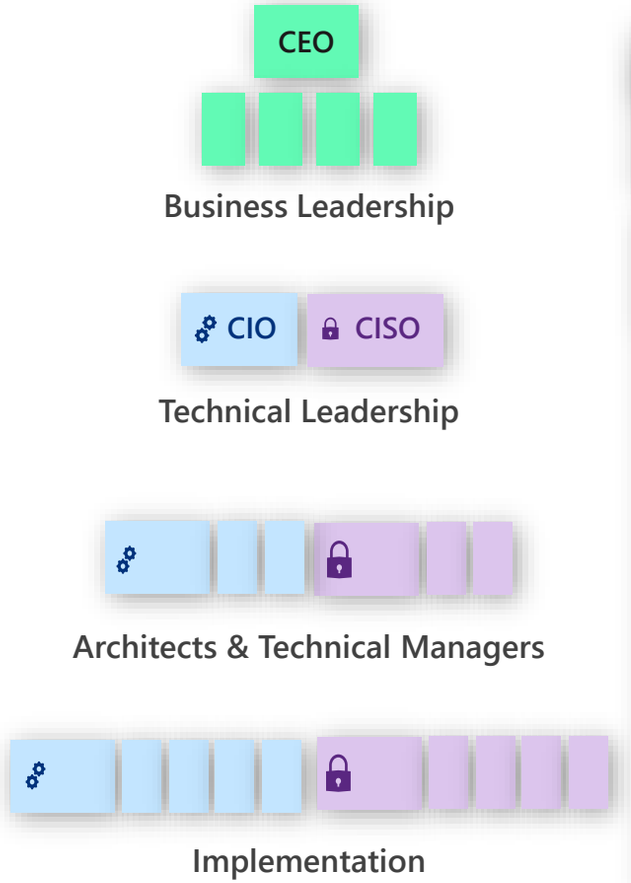
- ❑ Modern Access Control
- ❑ Modern Security Operations
- ❑ Infrastructure and Development
- ❑ OT and IoT Security
- ❑ Data Security & GRC

What's on your current priority list?

⚡	Ransomware Recovery Readiness	*Start Date / In Progress*
#	Secure Identities and Access	*Start Date / In Progress*
#	Modern Security Operations	*Start Date / In Progress*
#	Infrastructure and Development	*Start Date / In Progress*
#	Data Security & GRC	*Start Date / In Progress*
#	OT and IoT Security	*Start Date / In Progress*
#	*Other* _____	*Start Date / In Progress*

Common Security Initiatives

Mapping business outcomes to technical initiatives



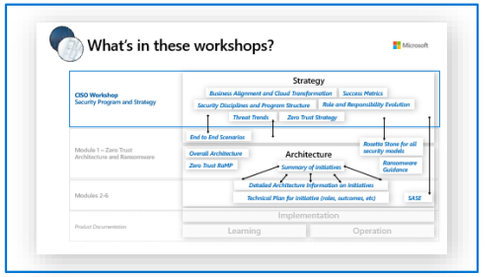
Align security to business priorities

Security Program and Strategy / Cloud Adoption Framework (CAF) - Secure Methodology

Secure hybrid work	Modernize incident response	Secure cloud migration	Find and protect critical data	Protect Industrial Control Systems
Secure Identities and Access	Modern Security Operations (SOC)	Infrastructure and Development Security	Data Security & Governance, Risk, Compliance (GRC)	IoT and OT Security

Microsoft

CISO Workshop & Architecture Design Session (ADS)



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

CISO Workshop
Security Program and Strategy

Security Architecture Design Session
Module 1 – Zero Trust Architecture

Module 2 – Secure Identities and Access

Module 3 – Modern Security Operations (SecOps/SOC)

Module 4 – Infrastructure & Development Security

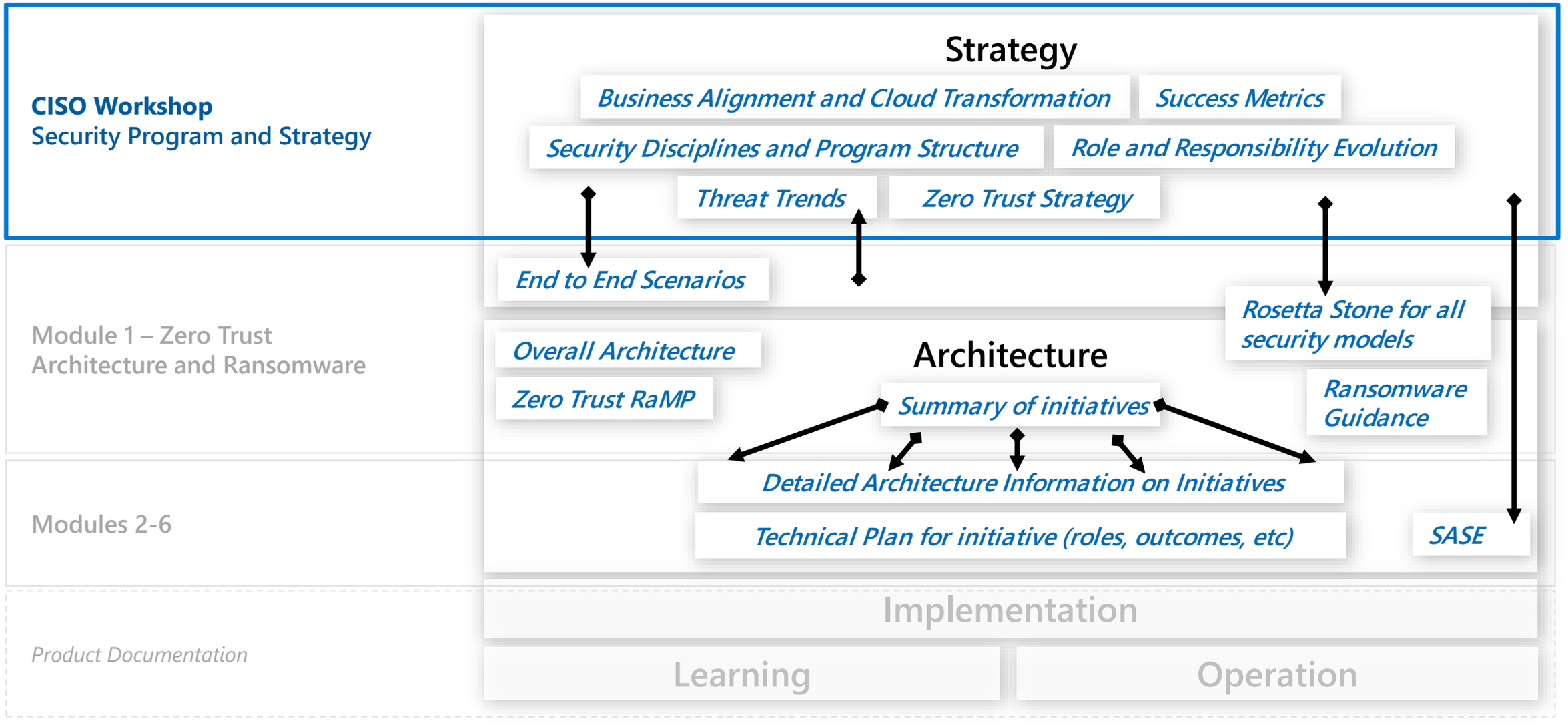
Module 5 – Data Security & Governance, Risk, Compliance (GRC)

Module 6 – IoT and OT Security

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

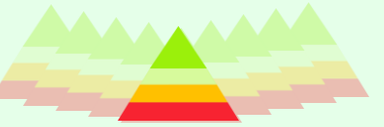
What's in these workshops?

Microsoft



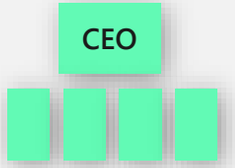
Planning for each role

Maturity Model
Assessment & Improvement exercises



Reference plans for 3 entry points

- Complete end to end security modernization
- Quick wins across all initiatives (Zero Trust RaMP)
- Microsoft 365 Zero Trust capabilities



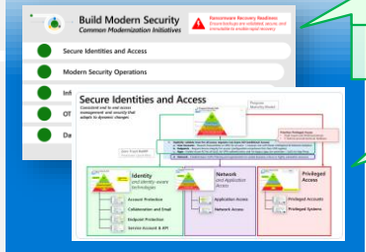
Business Leadership

Technical Leadership

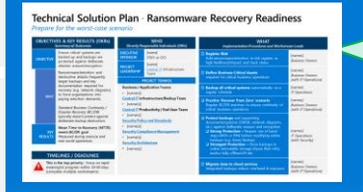
Architects & Technical Managers

Implementation

- Securing Digital Transformation
- Business and Security Integration
- Security Strategy, Programs, and Epics
- Architecture and Policy
- Technical Planning
- Implementation and Operation

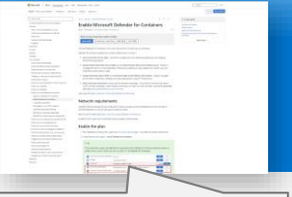


Strategic Initiative Plan
Describes technical solutions in that initiative



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

Implementation Procedures
Describe how to deploy/configure each technical component



Documentation
Step by Step Instructions on Microsoft Docs site

Microsoft

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

A security program bridges two worlds

Aligning security to business outcomes + apply Zero Trust security principles and best practices

Cloud Adoption Framework (CAF) - *Secure Methodology*

Define strategy

Plan

Ready

Adopt

Govern

Manage

Security ADS Workshop

Program Guidance

Secure

CISO Workshop

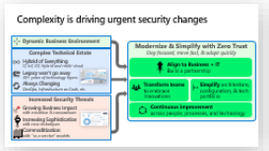
- Module 1 – Zero Trust Architecture and Ransomware
- Module 2 – Secure Identities and Access
- Module 3 – Modern Security Operations (SOC)
- Module 4 – Infrastructure & Development Security
- Module 5 – Data Security & Governance, Risk, Compliance (GRC)
- Module 6 – IoT and OT Security

CISO Workshop

End-to-end Security Program and Strategy Guidance + Integration with Digital & Cloud Transformation Teams

A Start Here – *with key context and fundamentals*

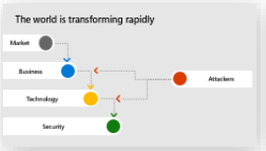
Priorities Discussion



Threat Environment and Trends

Roles & Responsibilities

Decision Makers



Strategy and Recommended Initiatives

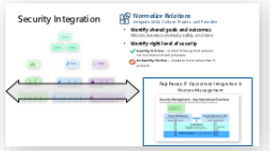
Zero Trust Principles
Assume breach | Explicitly Verify | Least privileged

Cloud Adoption Framework (CAF)
Secure Methodology

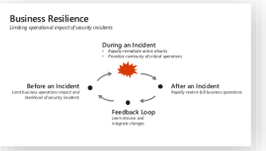
B Business Alignment – *Continuously Prioritize and integrate security*

Engaging Business Leaders on Security

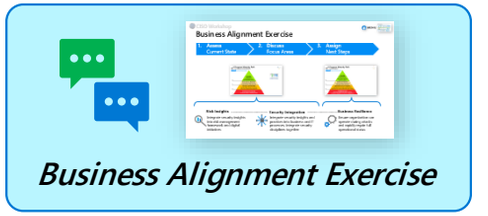
Risk Insights



Security Integration

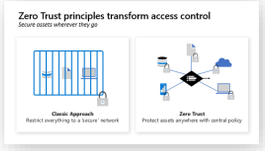


Business Resilience



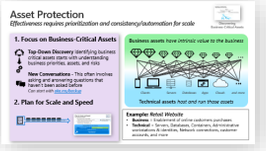
Business Alignment Exercise

C Security Disciplines – Establish and Evolve Foundational Capabilities



Access Control

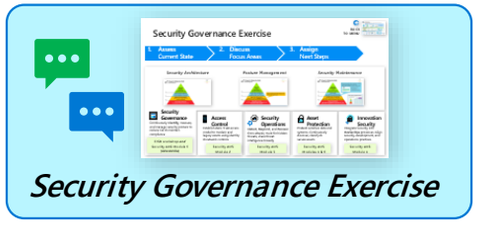
Security Operations



Asset Protection

Security Governance

Innovation Security



Security Governance Exercise

Next Steps

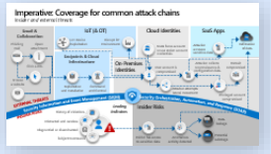
Complexity is driving urgent security changes

Dynamic Business Environment

Complex Technical Estate

Hybrid of Everything
IT, IoT, OT, Hybrid and multi-cloud

Legacy won't go away
30+ years of technology layers



Always Changing
DevOps, Infrastructure as Code, etc.

Increased Security Threats

Growing Business Impact
with extortion & ransomware

Increasing Sophistication
with new techniques

Commoditization
with "as a service" models

Modernize & Simplify with Zero Trust

Stay focused, move fast, & adapt quickly

Align to Business + IT
Build a partnership

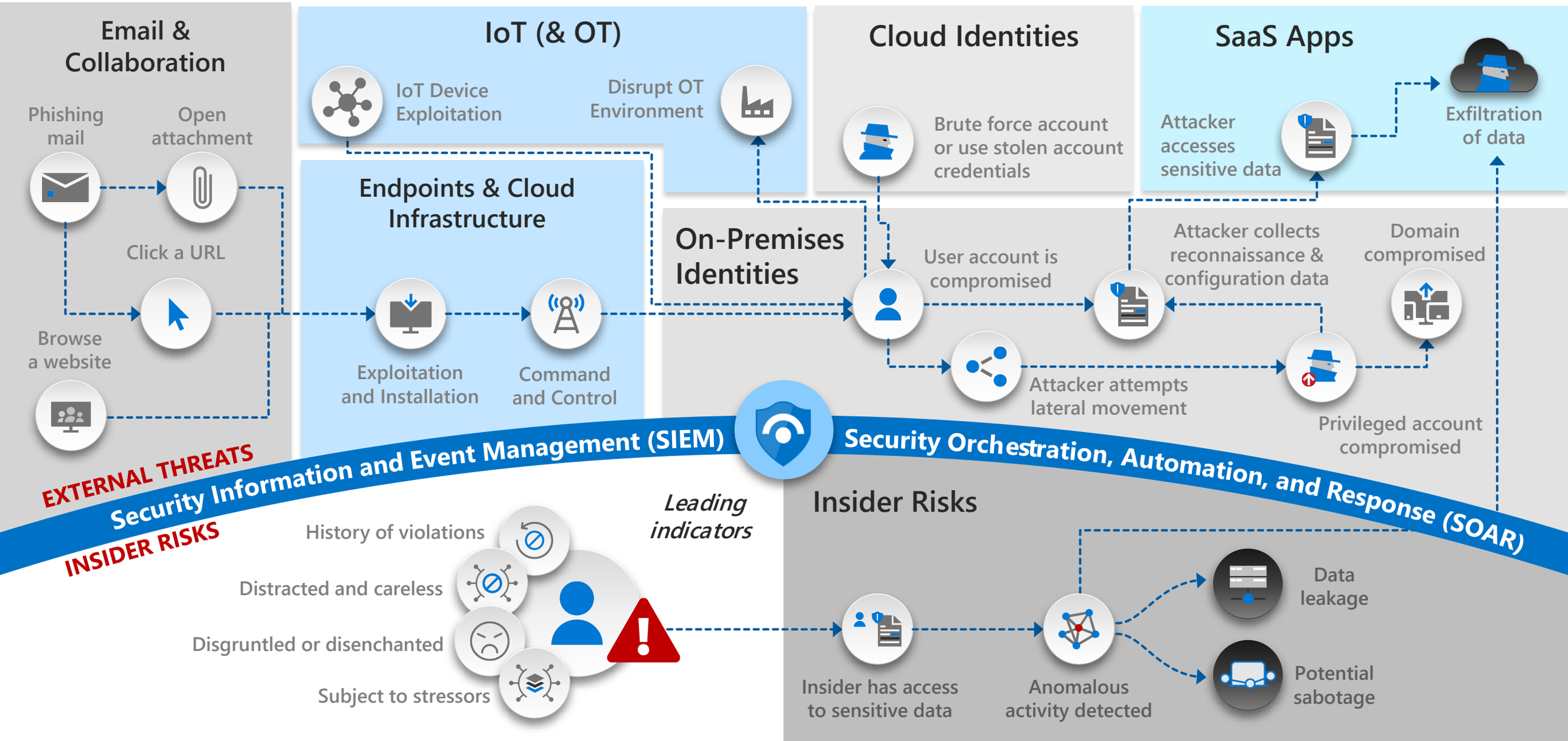
Transform teams to embrace innovations

Simplify architecture, configuration, & tech portfolio

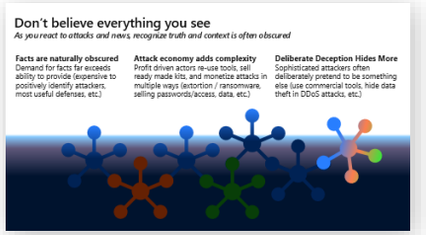
Continuous improvement across people, processes, and technology

Imperative: Coverage for common attack chains

Insider and external threats



For sale in “bad neighborhoods” on the internet



How this complicates fact validation

Attacker for hire (per job)

$250 per job (and up)

Other Services

Continuous attack
supply chain innovation

Ransomware Kits

$66 upfront
(or 30% of the profit / affiliate model)

Compromised PCs / Devices

PC: $0.13 to $0.89
Mobile: $0.82 to $2.78

Spearphishing for hire

$100 to $1,000
(per successful account takeover)

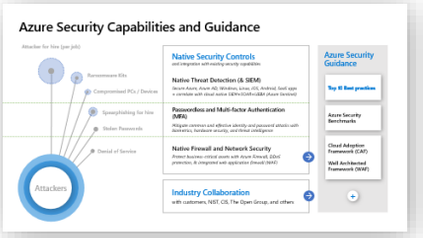
Attackers

Stolen Passwords

$0.97 per 1,000 (average)
(Bulk: $150 for 400M)

Denial of Service

$766.67 per month



How this shaped Microsoft investments

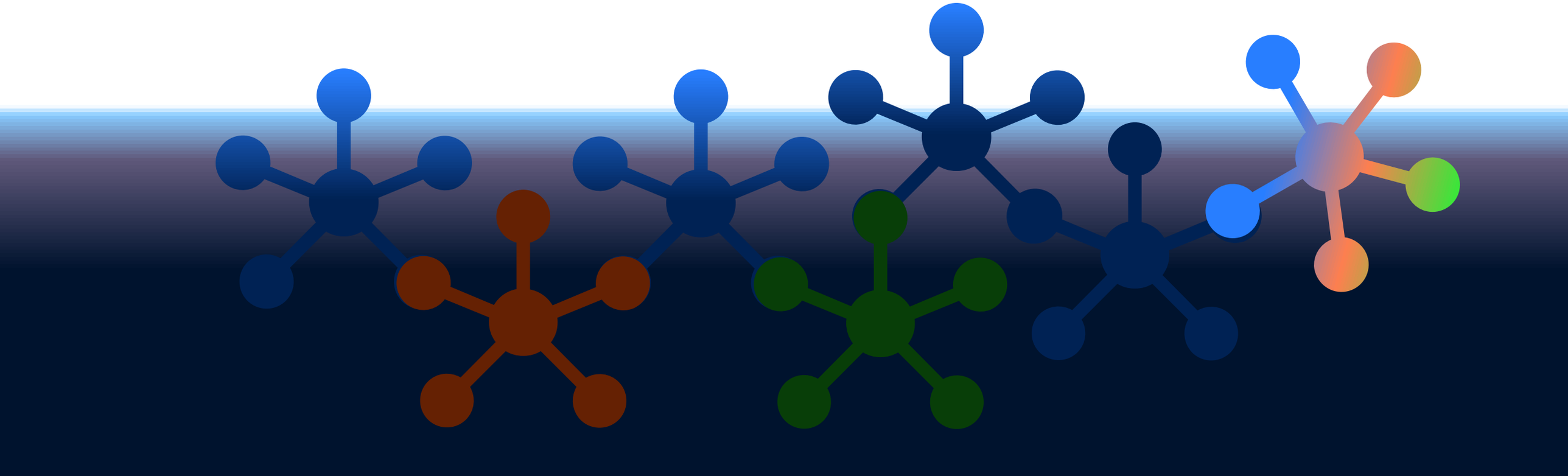
Don’t believe everything you see

As you react to attacks and news, recognize truth and context is often obscured

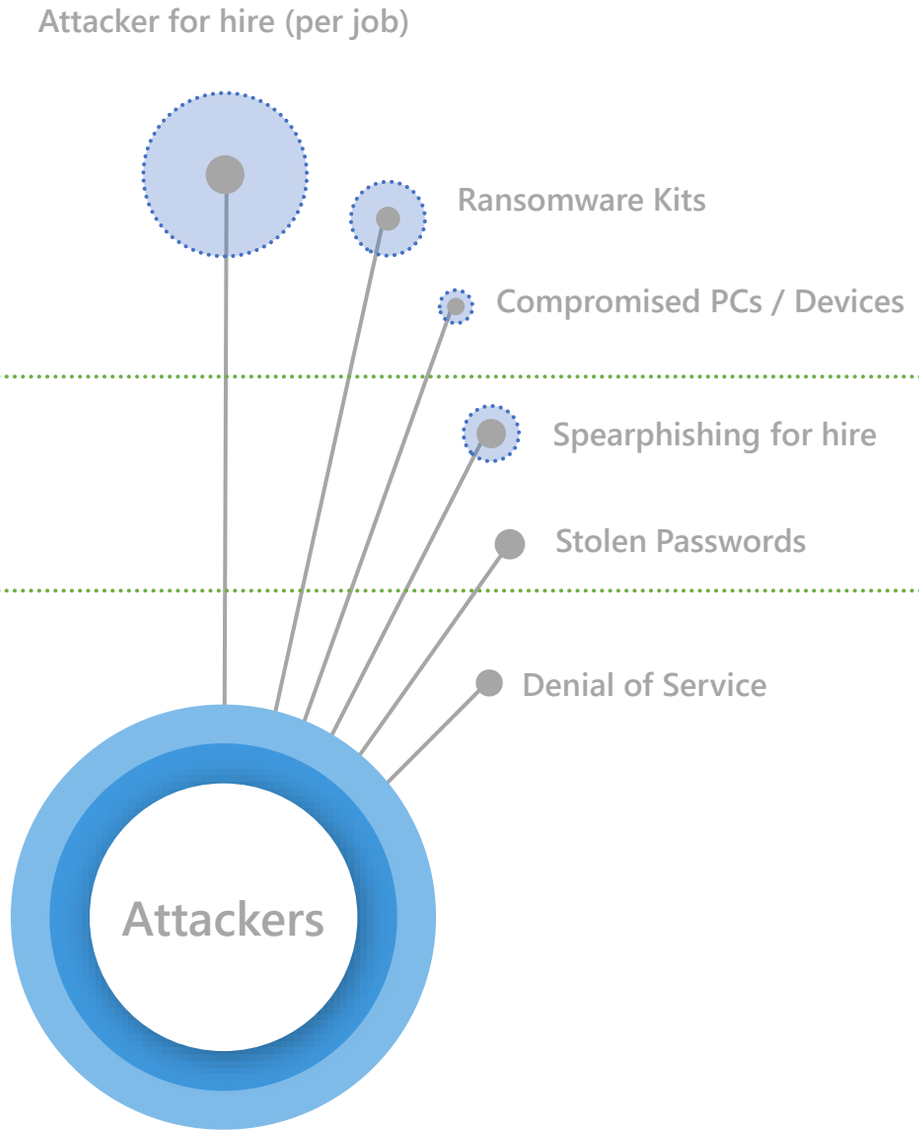
Facts are naturally obscured
Demand for facts far exceeds ability to provide (expensive to positively identify attackers, most useful defenses, etc.)

Attack economy adds complexity
Profit driven actors re-use tools, sell ready made kits, and monetize attacks in multiple ways (extortion / ransomware, selling passwords/access, data, etc.)

Deliberate Deception Hides More
Sophisticated attackers often deliberately pretend to be something else (use commercial tools, hide data theft in DDoS attacks, etc.)



Azure Security Capabilities and Guidance



Native Security Controls

and integration with existing security capabilities

Native Threat Detection (& SIEM)

Secure Azure, Azure AD, Windows, Linux, iOS, Android, SaaS apps + correlate with cloud native SIEM+SOAR+UEBA (Azure Sentinel)

Passwordless and Multi-factor Authentication (MFA)

Mitigate common and effective identity and password attacks with biometrics, hardware security, and threat intelligence

Native Firewall and Network Security

Protect business-critical assets with Azure Firewall, DDoS protection, & integrated web application firewall (WAF)

Industry Collaboration

with customers, NIST, CIS, The Open Group, and others

Azure Security Guidance

Top 10 Best practices

Azure Security Benchmarks

Cloud Adoption Framework (CAF)

Well Architected Framework (WAF)

+

Human Operated Ransomware - high impact & growing

Not another background security risk

What's different?

High Business impact

Extortion must disrupt business operations to motivate payment

Profitable for Attackers

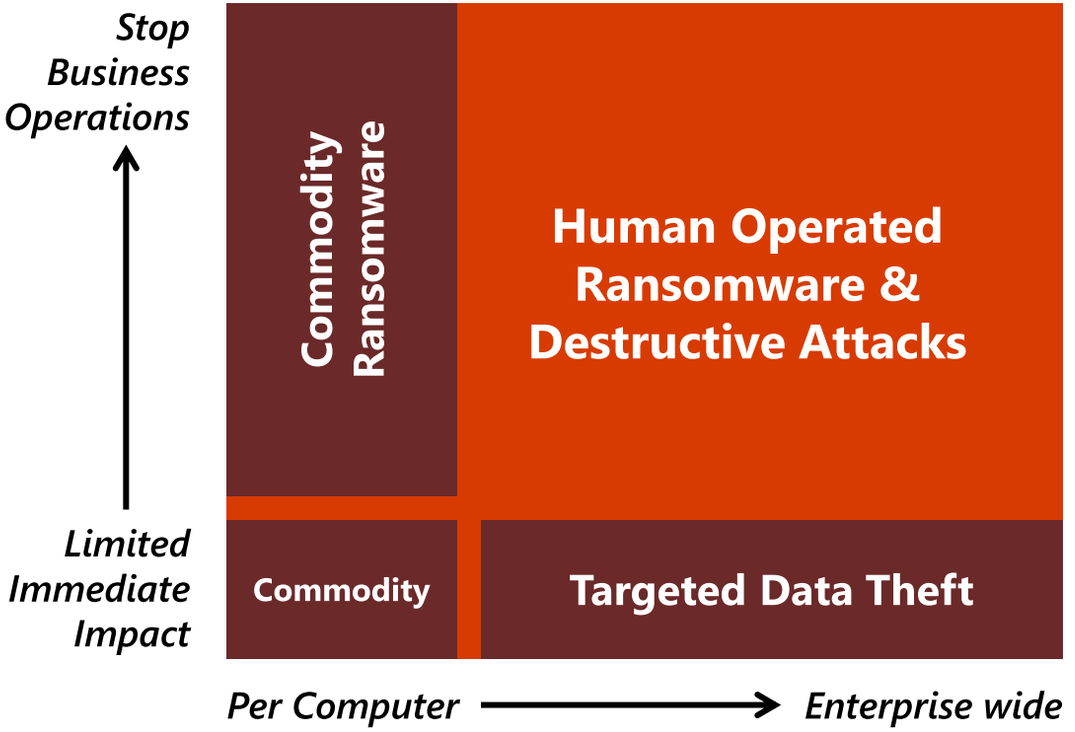
Economic incentive to continue growing

(hundreds of millions of dollars paid)

Room to Grow

Attackers can monetize security maintenance gaps at most enterprises:

- **Apply security updates** consistently to all computers
- **Securely configure all resources** using manufacturer best practices
- **Mitigate credential theft** attacks for privileged users



For more details on ransomware attacks and mitigations, see the Security ADS *Module 1 – Zero Trust Architecture and Ransomware*

2021 Microsoft Digital Defense Report contents

CHAPTER 1

Introduction

Introduction
Our 2021 focus areas

CHAPTER 2

The state of cybercrime

The cybercrime economy and services
Ransomware and extortion
Phishing and other malicious email
Malware
Malicious domains
Adversarial machine learning

CHAPTER 3

Nations state threats

Tracking nation state threats
What we're seeing
Analysis of nation state activity this year
Private sector offensive actors
Comprehensive protections required

CHAPTER 4

Supply chain, IoT, and OT security

Challenges in managing risk associated with the supplier ecosystem
How Microsoft thinks about supply chain
IoT and OT threat landscape
The 7 properties of highly secured devices
Applying a Zero Trust approach to IoT solutions
IoT at the intersection of cybersecurity and sustainability
IoT security policy considerations

CHAPTER 5

Hybrid workforce security

A Zero Trust approach for securing hybrid work
Identities
Devices/Endpoints
Applications
Network
Infrastructure
Data
People

CHAPTER 6

Disinformation

Disinformation as an emerging threat
Mitigation through media literacy
Disinformation as an enterprise disruptor
Campaign security and election integrity

CHAPTER 7

Actionable insights

Five cybersecurity paradigm shifts
Summary of report learnings
Conclusion

Contributing teams at Microsoft

Download the full report at https://aka.ms/MDDR

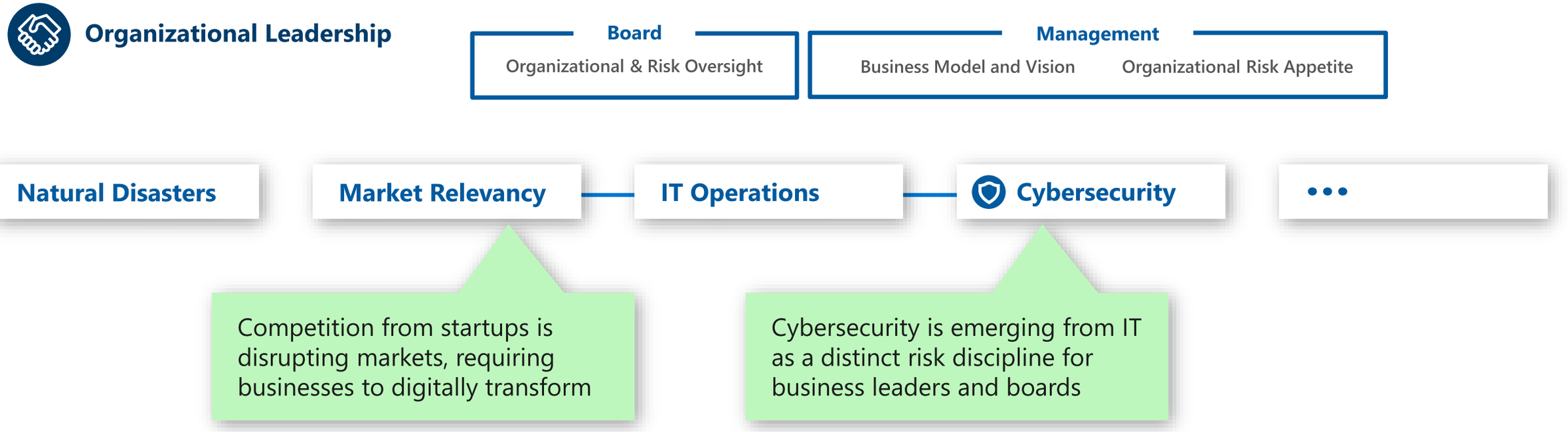
BACK
TO MENU

Review – Threat Environment and Trends

- **Security must be agile to keep up with speed of :**
  - ***Business*** *– Digital Transformation of assets and value*
  - ***Technology*** *– Cloud transformation of platforms*
  - ***Security*** *– Threats and Technical capabilities transforming*
- **Threats growing in multiple dimensions**
  - ***Business Impact*** *with extortion & ransomware*
  - ***Sophistication*** *with new techniques*
  - ***Commoditization*** *with "as a service" models*
- **Ransomware is top business impacting threat**
- **MDDR provides insights & analysis across threats**

Next Up:
1A – Strategy and Recommended Initiatives

Managing organizational risk

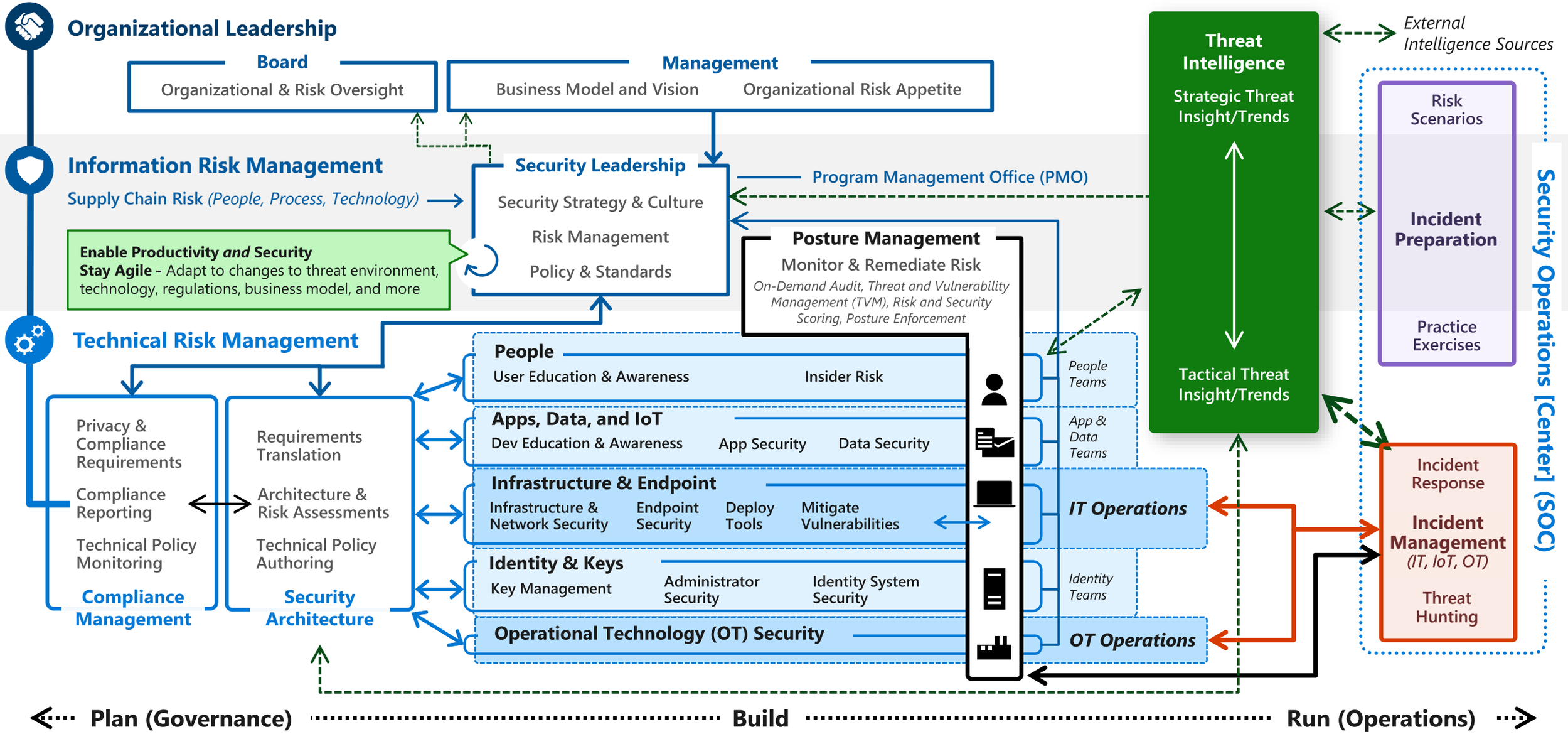


Managing Information/Cyber Risk

Security responsibilities or "jobs to be done"

December 2021 -
https://aka.ms/SecurityRoles

Microsoft



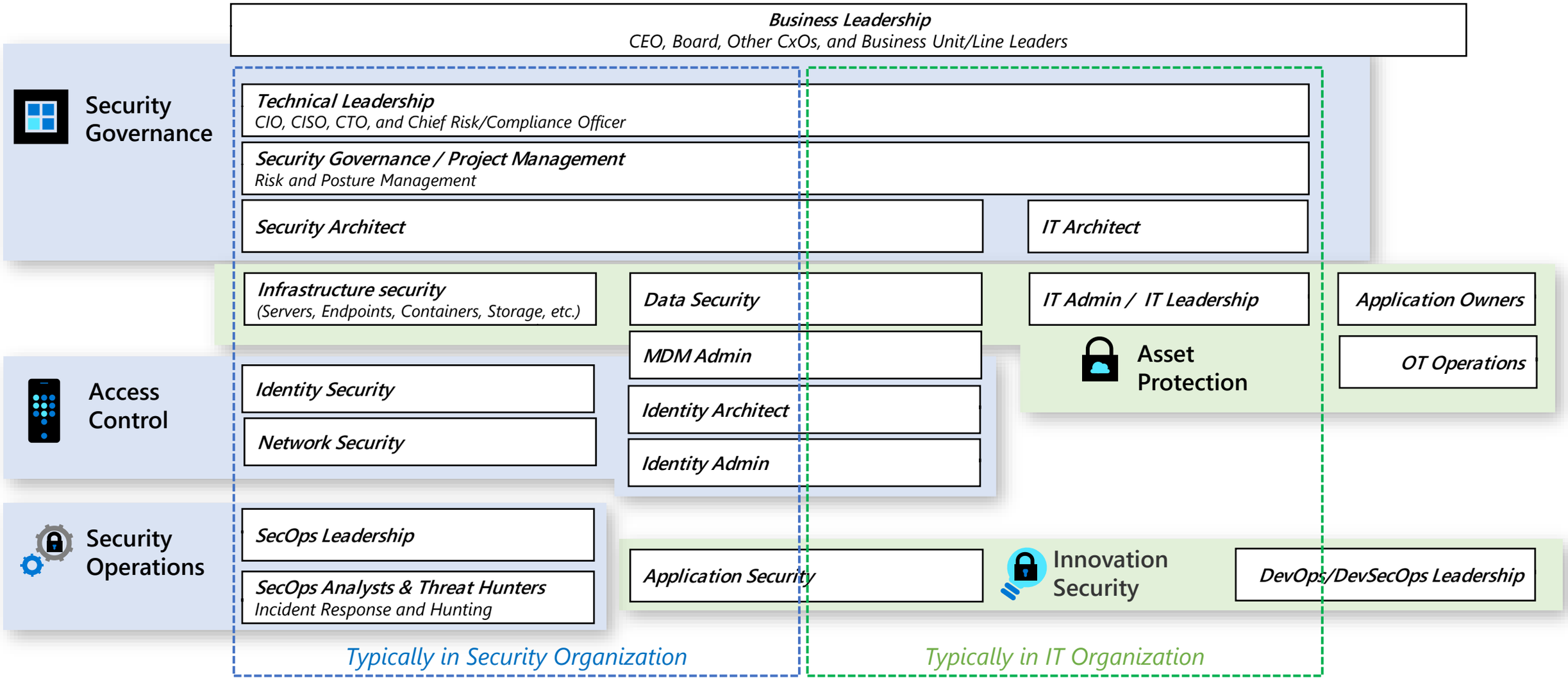
Working Together on Information/Cyber Risk

Increase collaboration across teams

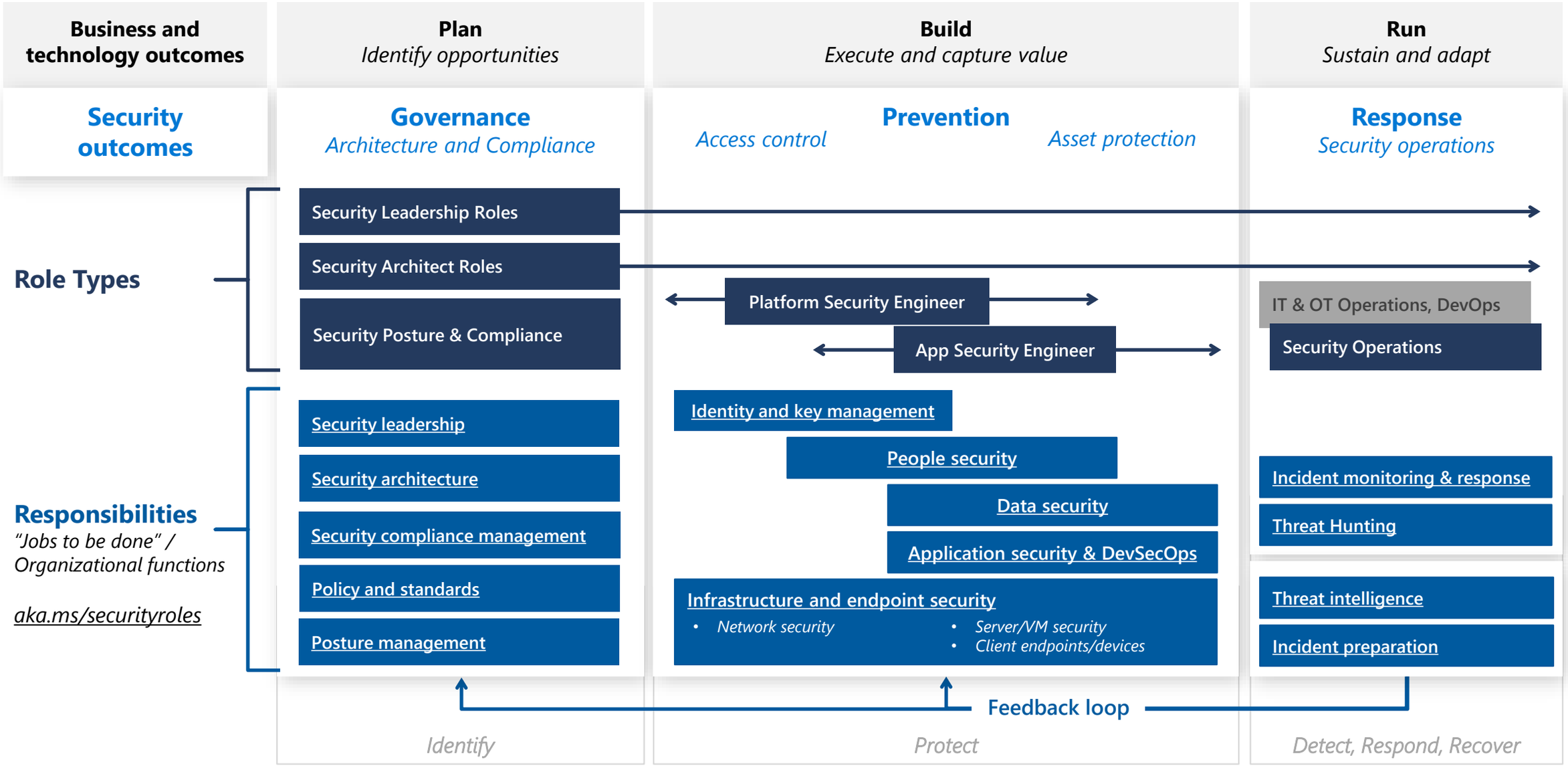
Microsoft

Mapping Roles to Disciplines

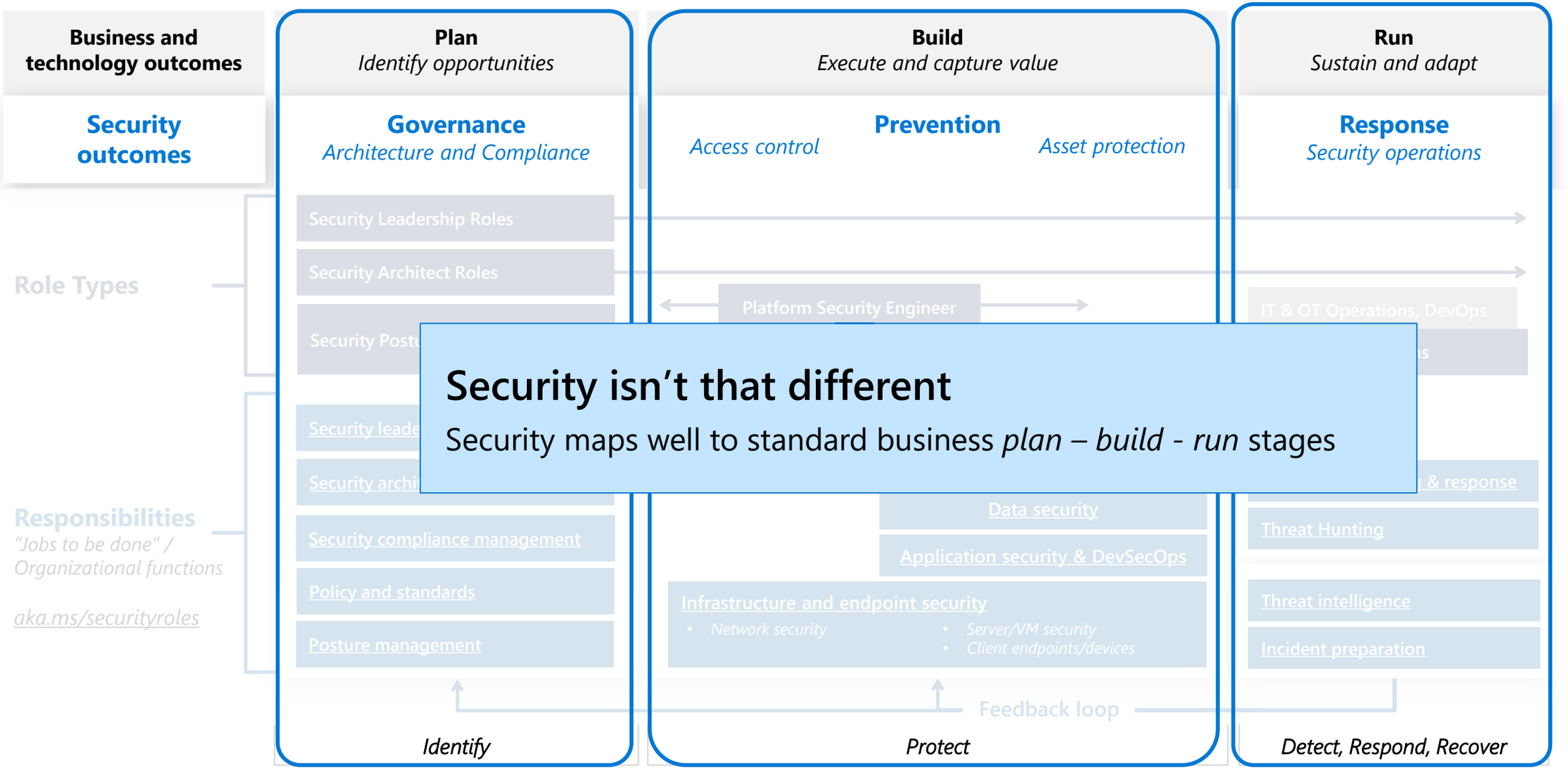
Requires collaboration between IT and Security teams



Security Roles and Responsibilities



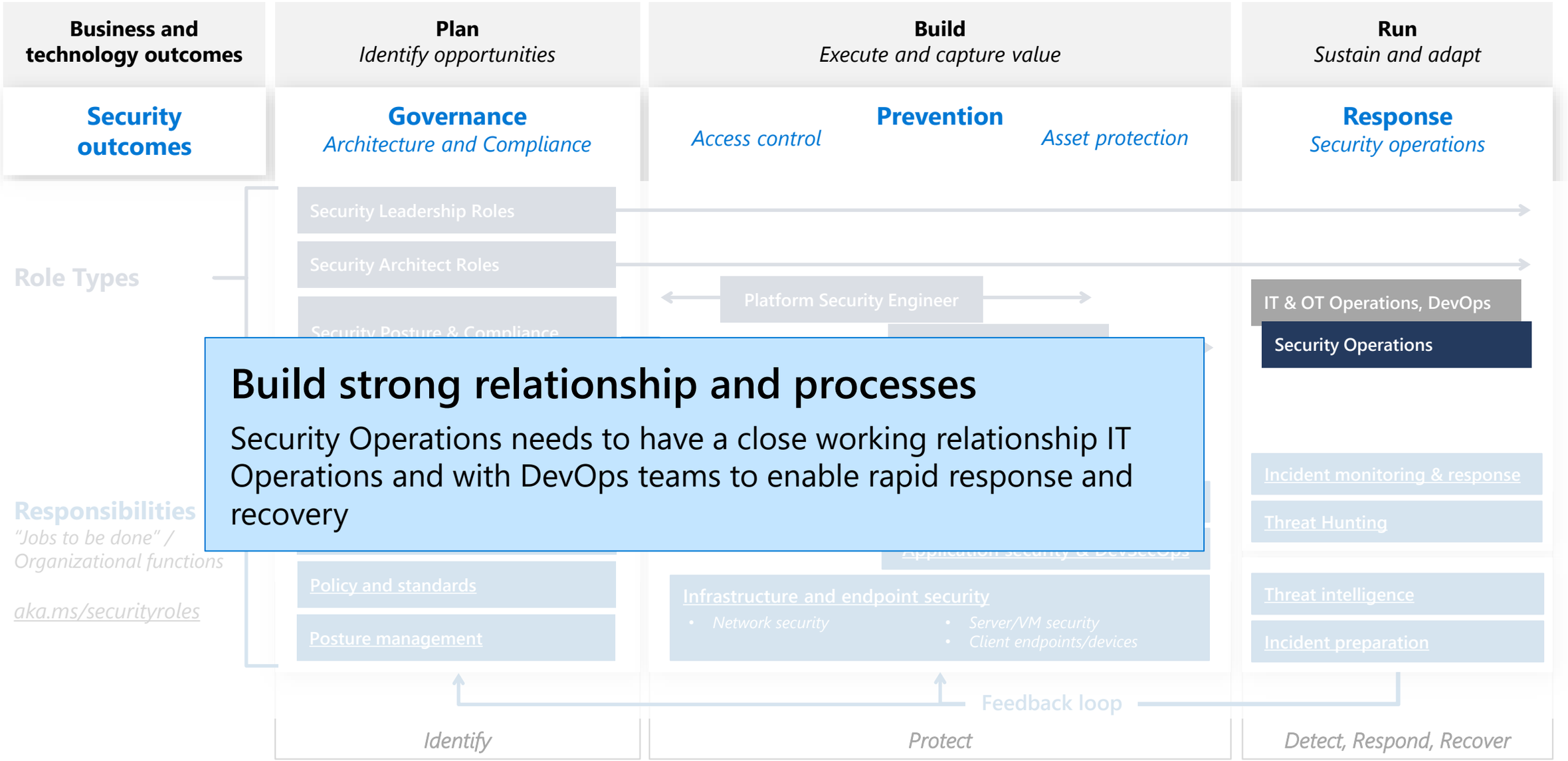
Security Roles and Responsibilities



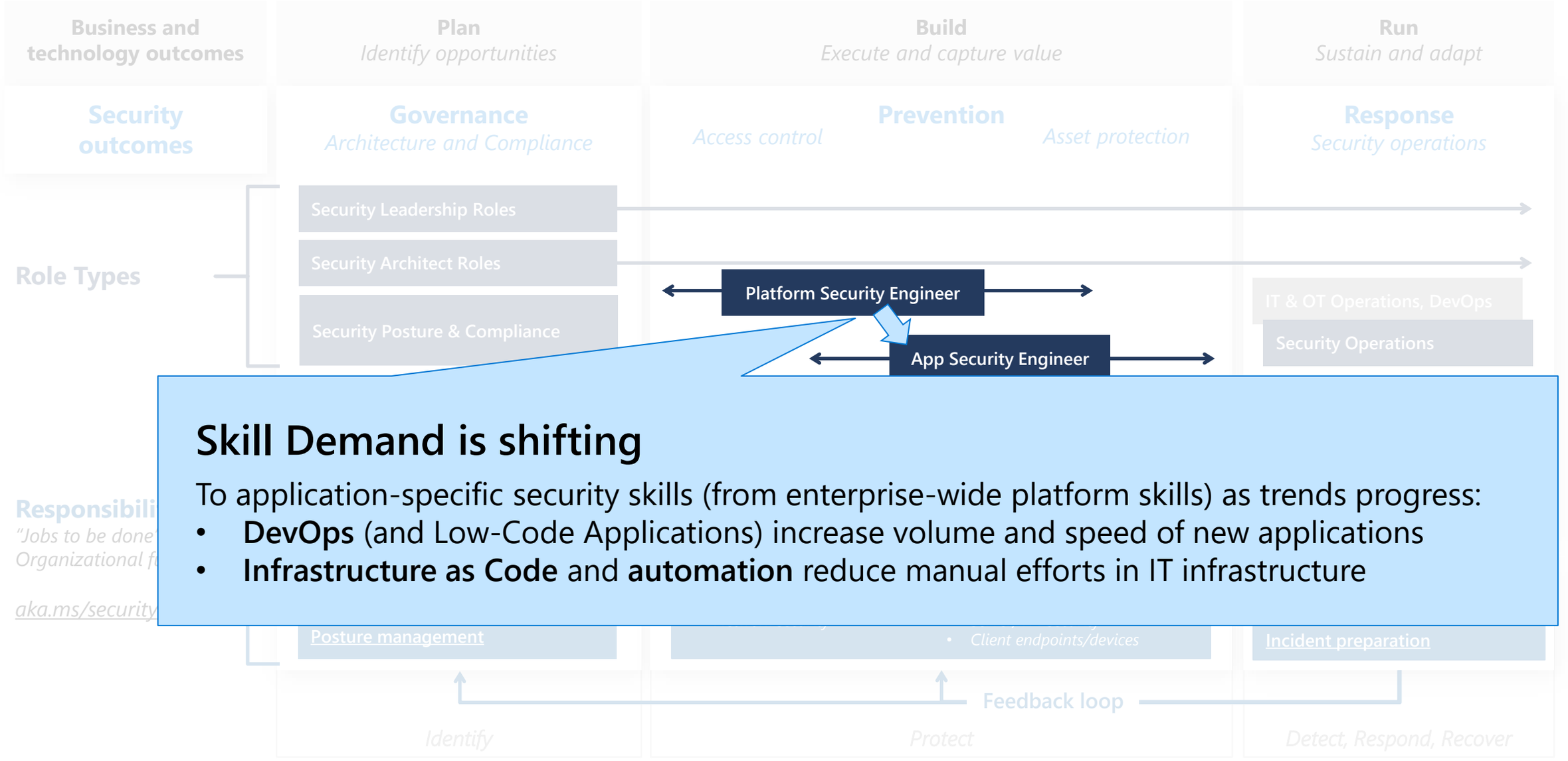
Security isn't that different

Security maps well to standard business *plan – build - run* stages

Security Roles and Responsibilities



Security Roles and Responsibilities



Skill Demand is shifting

To application-specific security skills (from enterprise-wide platform skills) as trends progress:

- **DevOps** (and Low-Code Applications) increase volume and speed of new applications
- **Infrastructure as Code** and **automation** reduce manual efforts in IT infrastructure

MENU

Exercise 1A – Business Alignment

1. **Designate** Decision Makers
2. **Publish** and Update list
3. **Socialize** and follow-up

ESTABLISH CLEAR LINES OF RESPONSIBILITY

What – Identify who is responsible for security decisions across the technical estate

Why – Consistency helps avoid confusion that can lead to

- Human and automation errors that create security risk
- Security decisions holding up projects (or security being skipped in projects)

Tips

- **Document Decisions** in Policy and Architecture to ensure consistency going forward and harmonization
- **Mix of old & new –** Some practices will be carried forward from before, but some must be changed

Who makes security decisions for the cloud?

Decision Maker	Decision Type	Additional Information
	Policy Management	*Typically GRC team + Architecture* Set direction for Decision Rights / Roles Based Access Control (RBAC), Administrator protection strategy, DevOps/DevSecOps, Security Automation (Azure Policy, integration into CI/CD and IaC, etc.), and more
	Compliance Reporting	*Typically Program Management Office* Report compliance on all assets including cloud. Work with technical teams to assess compliance status
	Posture Management	*Typically Program Management Office (PMO) & Vulnerability Management* Design processes for managing security posture –monitor status, follow up with asset owners (IT Ops, DevOps, etc.), assist with challenges in remediating risk (provide training, tooling, escalate blockers, etc.) across all assets (cloud, on prem, endpoint, mobile, identity, etc.)
	Incident Monitoring and Response	*Typically security operations team* Investigate and remediate security incidents in SIEM / XDR tooling
	Identity Security and Standards	*Typically Security Team + Identity Team Jointly* Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards
	Network Security	*Typically existing network security team* Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.
	Server, Container, & Endpoint Security	*Typically IT operations, security architects/engineers (jointly)* Monitor and remediate server security (patching, configuration, endpoint security, etc.)
	OT & IoT Security	*Typically OT operations and security architects (jointly)* Monitor OT environment for threats and vulnerabilities, plan remediation

Assign Next Steps (Part 1)

1. Designate
2. Publish
3. Socialize

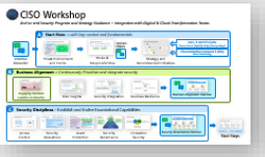
Identify who owns following up with stakeholders

#	Stakeholders	Point of Contact
1	Security Team	
2	IT Operations	
3	Cloud Teams	
4	DevOps/DevSecOps Teams	
5	*<Other Stakeholders>*	

Review – Exercise

Business Alignment

BACK TO MENU



1. **Designate**
   Decision Makers
2. **Publish**
   and Update list
3. **Socialize**
   and follow-up

Next Up:
Roles and Responsibilities Summary

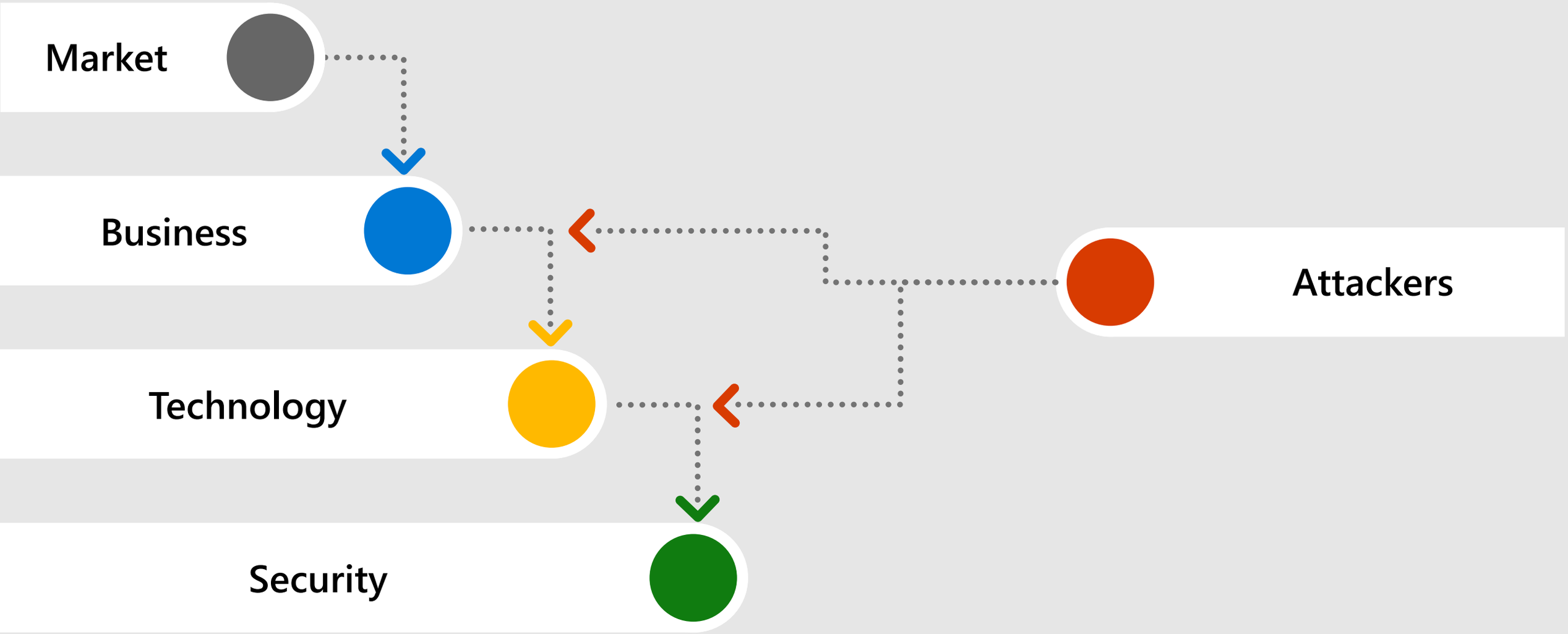
Review – Roles and Responsibilities

- Different security specialties reduce organizational risk differently
  - *Prevent, respond, govern, architect, compliance, and more*
- Security works through IT, OT, IoT, and DevOps teams
  - Must build strong relationships and processes
- Security skill demand is shifting
- Designate and publish list of security decision makers

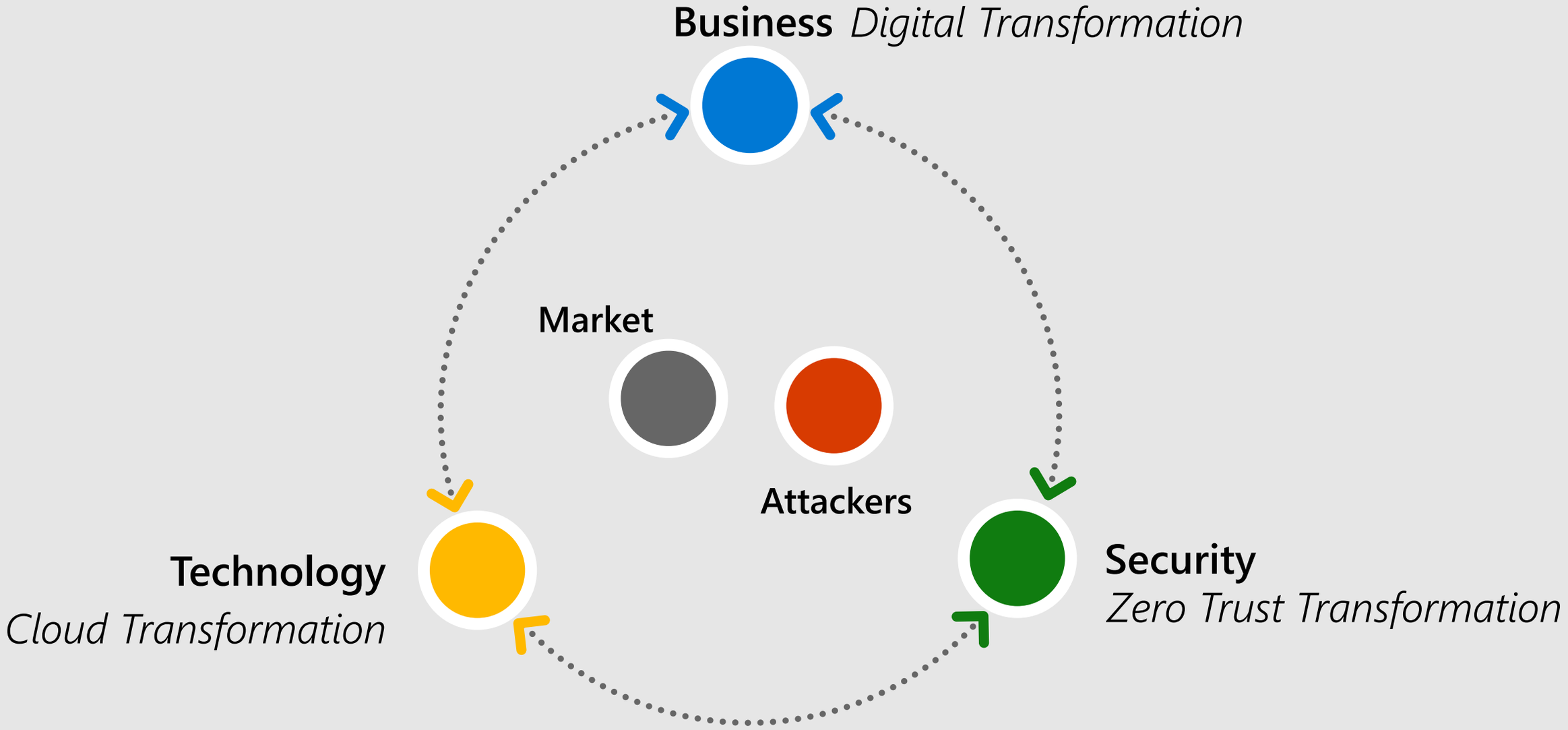
BACK TO MENU

Next Up:
1A – Strategy and Recommended Initiatives

The world is transforming rapidly



Working together



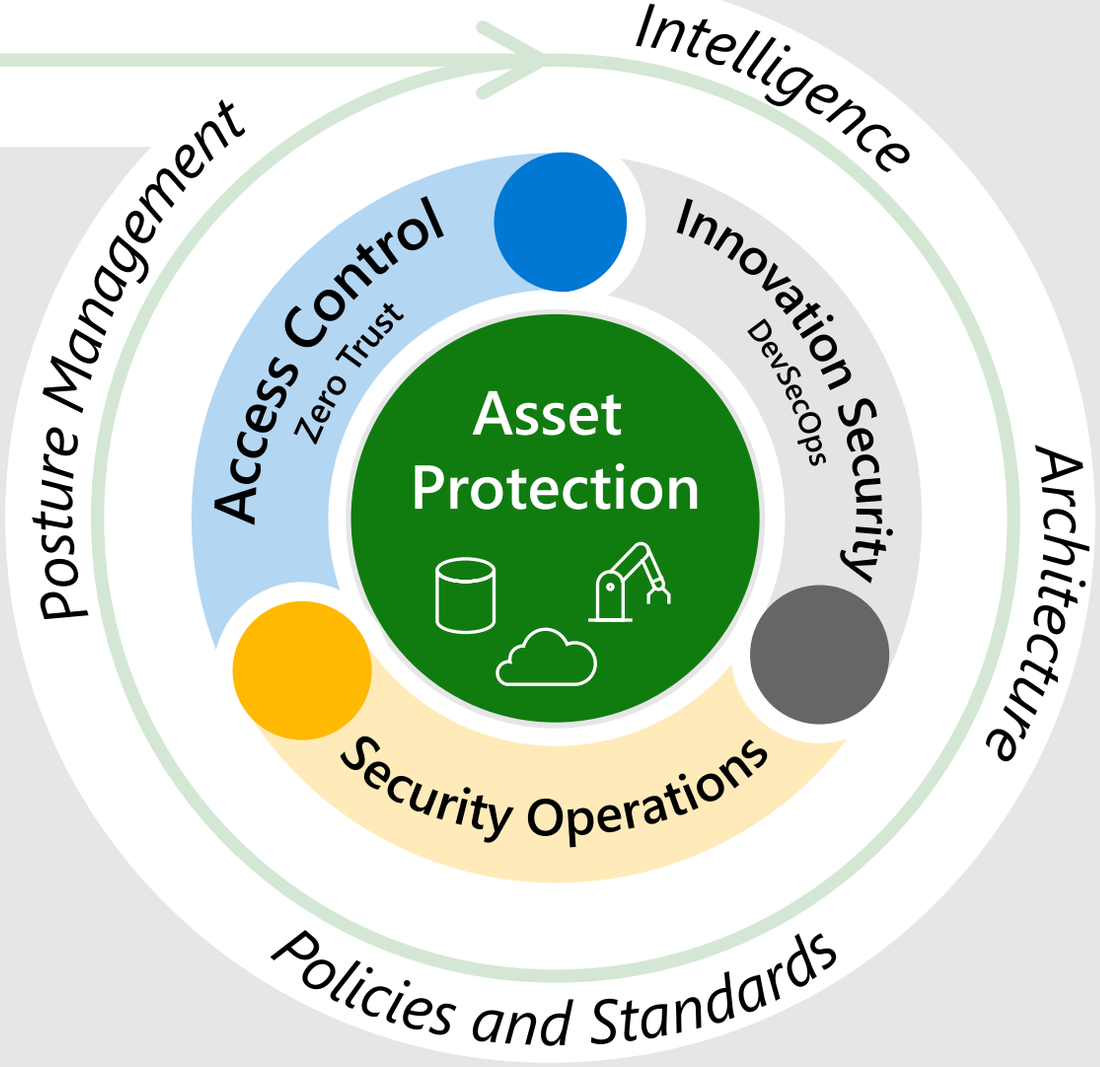
Security Shifts to Continuous Improvement

Security Imperatives

Governance

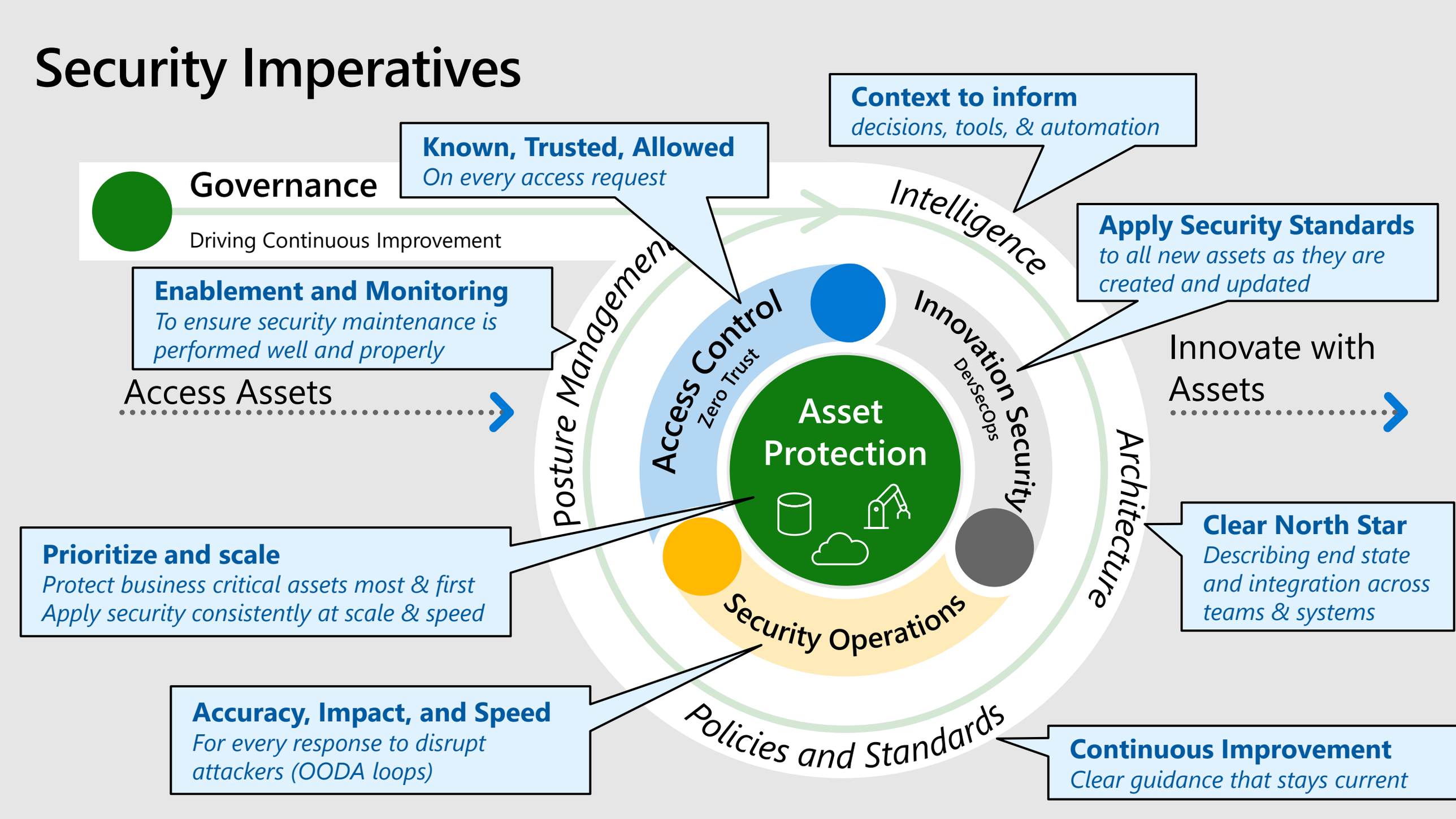
Driving Continuous Improvement

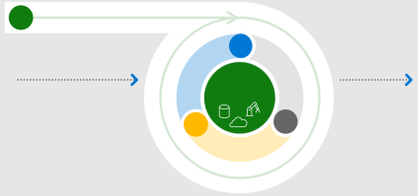
Access Assets



Innovate with Assets

Security Imperatives





Build Modern Security

Common Modernization Initiatives

Ransomware Recovery Readiness

Ensure backups are validated, secure, and immutable to enable rapid recovery

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

Security initiatives improve one or more disciplines

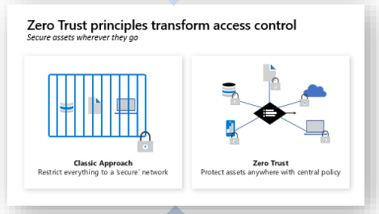
Access Control

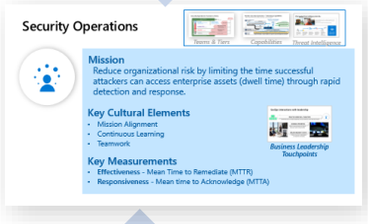
Security Operations

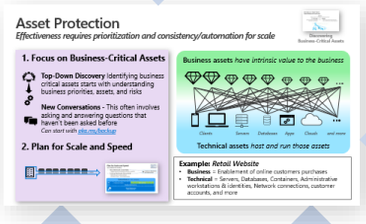
Asset Protection

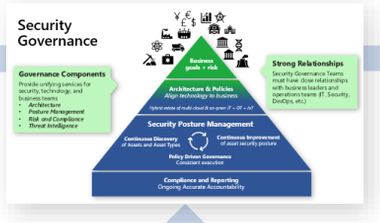
Security Governance

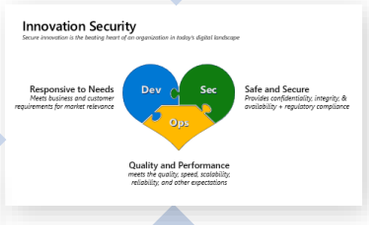
Innovation Security











Data & Governance, Risk, Compliance (GRC)

Module 5

Secure Identities and Access

Module 2

Modern Security Operations

Module 3

OT and IoT Security

Module 6

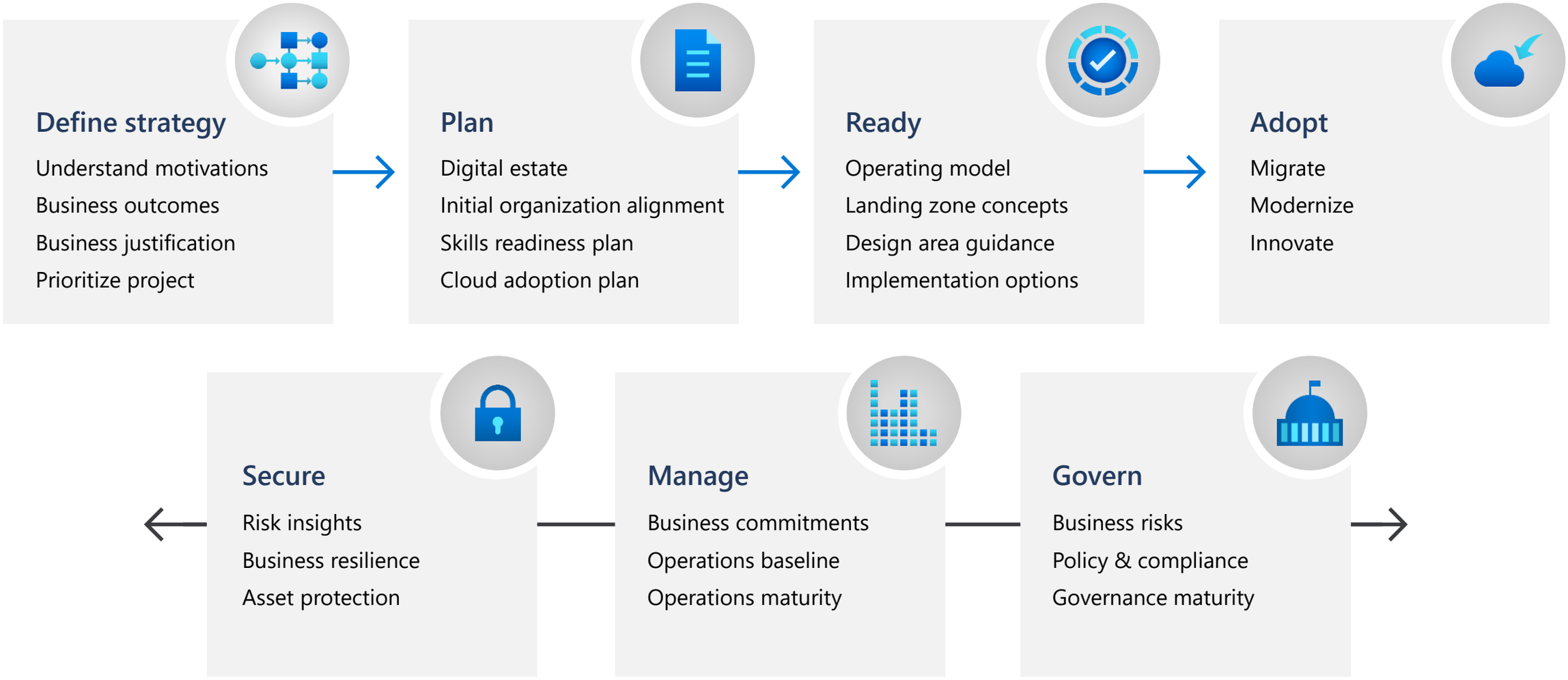
Infrastructure & Development

Module 4

Each initiative maps to an Architecture Design Session (ADS) Module

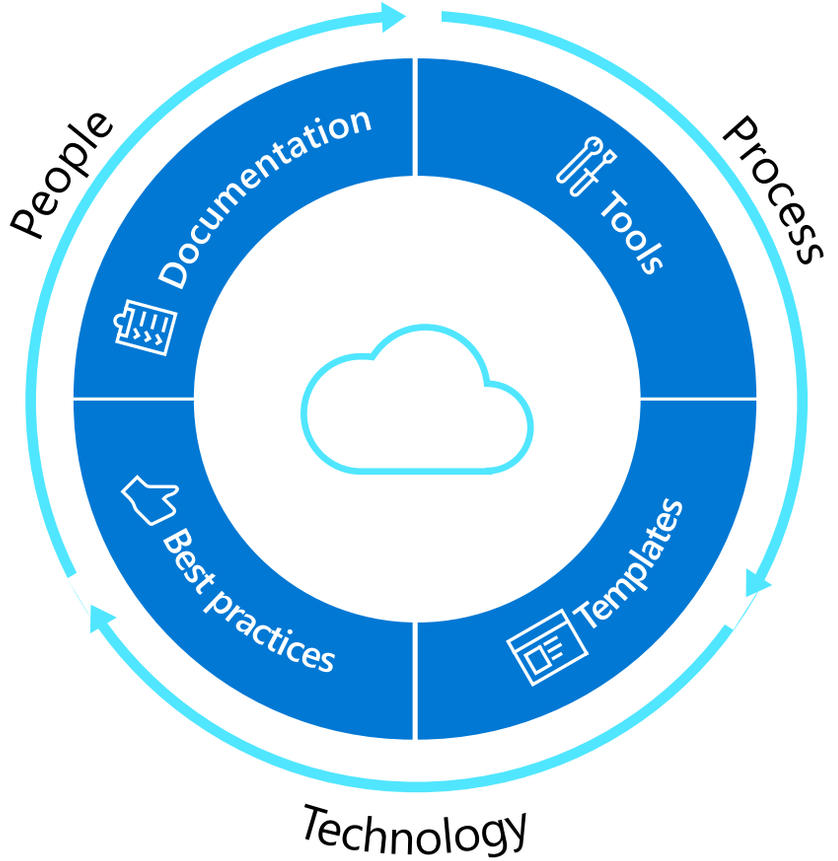
Microsoft Cloud Adoption Framework (CAF)

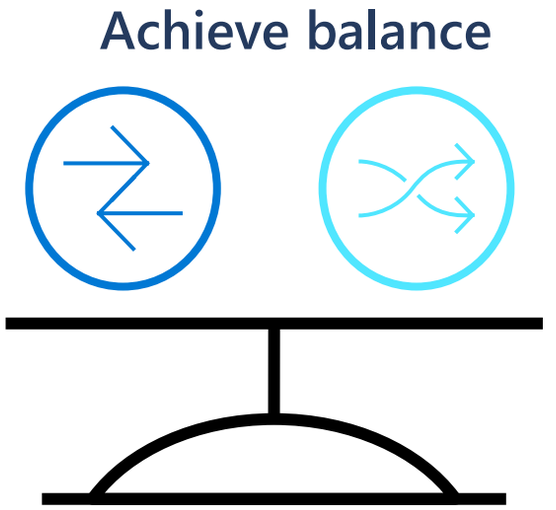
https://aka.ms/adopt/overview



https://aka.ms/CAFSecure

Microsoft Cloud Adoption Framework (CAF)

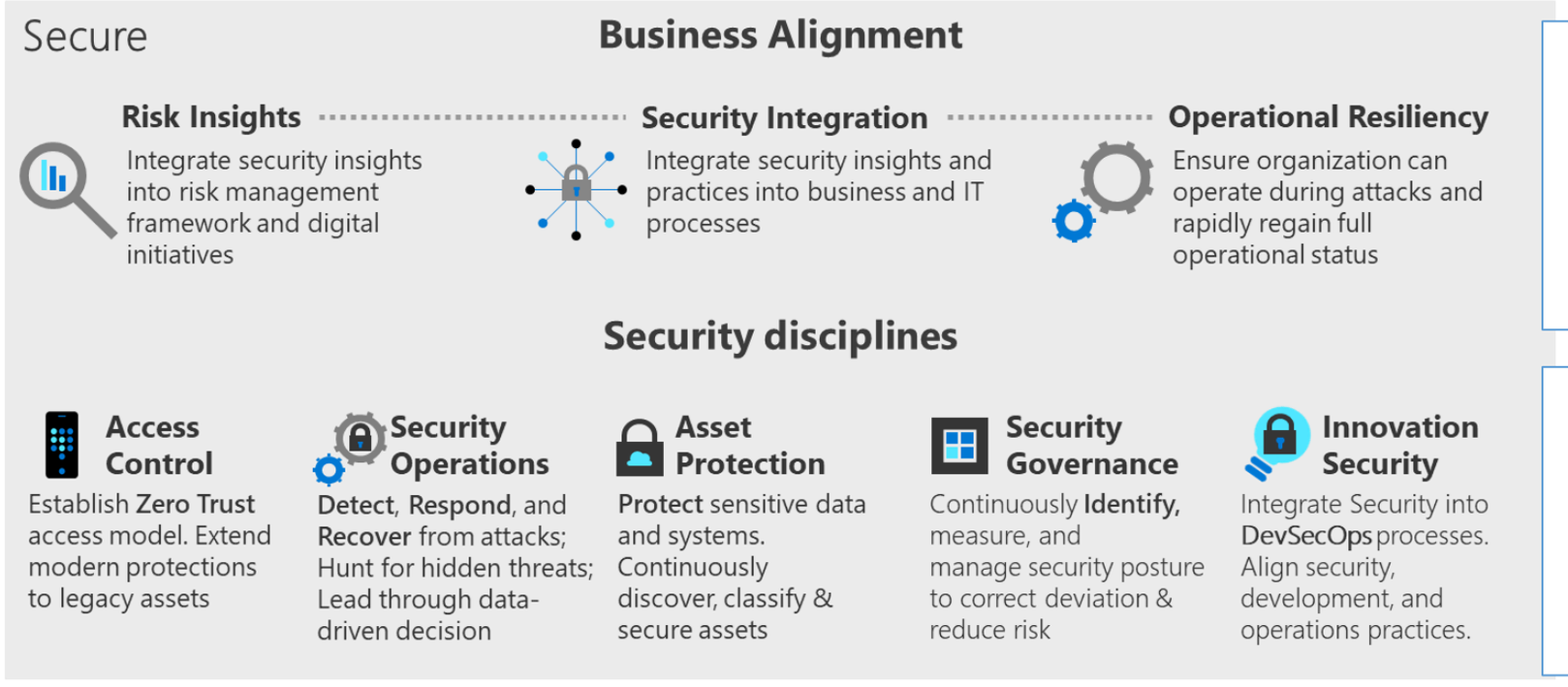




Align **business, people and technology strategy** to achieve business goals with **actionable, efficient, and comprehensive** guidance to deliver fast results with control and stability.

Cloud Adoption Framework | Secure Methodology

Security Program and Strategy Guidance



Business alignment

Establish cross-org processes to scale cloud security throughout your business

Security Disciplines

Implement proven security processes built on modern, cloud-based security tools

Convergence of Skillsets

- Cloud security requires expertise for ***both security and cloud.***
- Can be dedicated team *or* a cross-functional virtual team
  Security Team, Cloud Center of Excellence (CoE), Cloud Operations, IT Operations, and others.

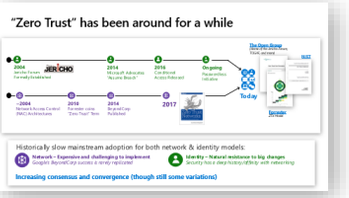
Zero trust principles

- Assume breach
- Explicitly Verify
- Least privileged

What is Zero Trust?

Assume breach | Explicitly Verify | Least privileged

Zero Trust History and Standards



Zero Trust Security Strategy – Secure digital business assets everywhere

Includes Multiple Technical Modernization Initiatives:

Secure Identities and Access
Modern identity & network access

Secure Access Service Edge (SASE)

Modern Security Operations (SOC)

Infrastructure & Development Security

Data Security & Governance, Risk, Compliance (GRC)

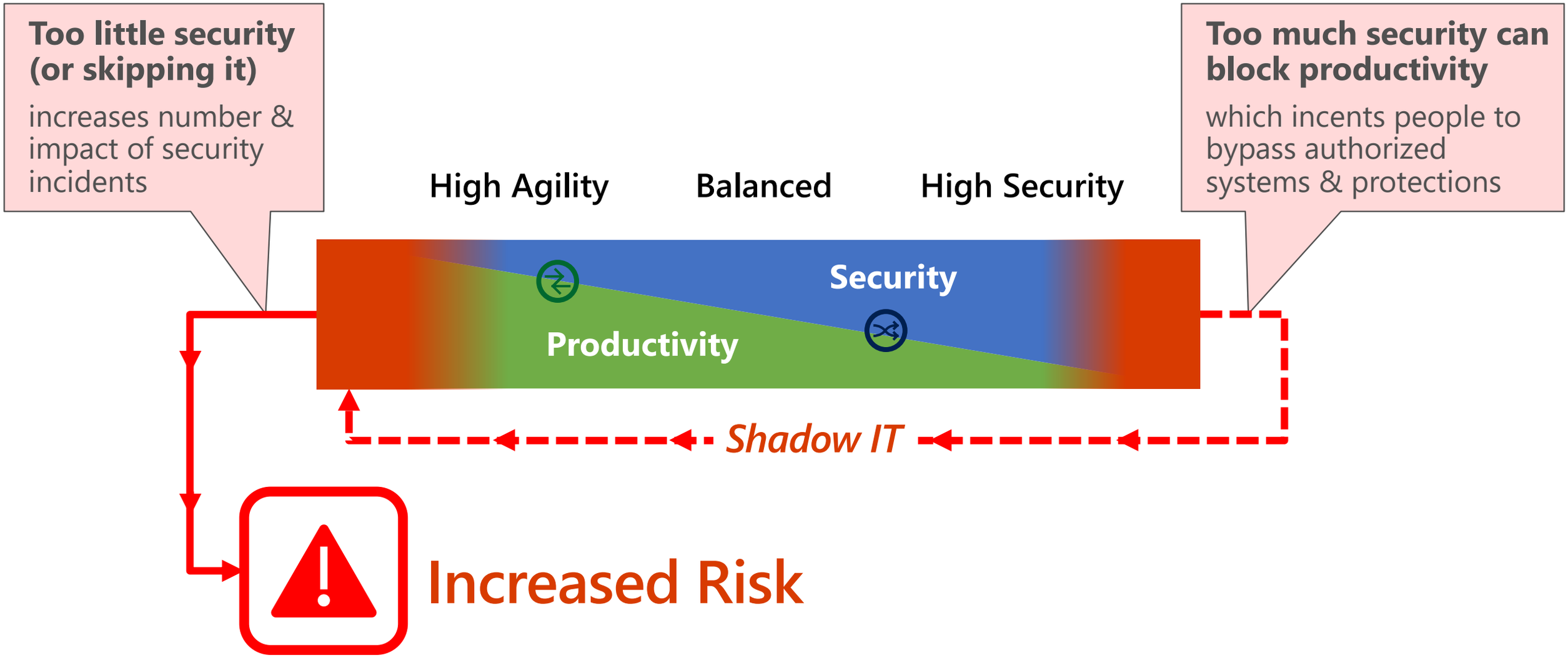
IoT and OT Security

Modernization, Integration, and Automation across technical controls

Identity, Endpoint, Network, Application, Infrastructure, Data, and Infrastructure

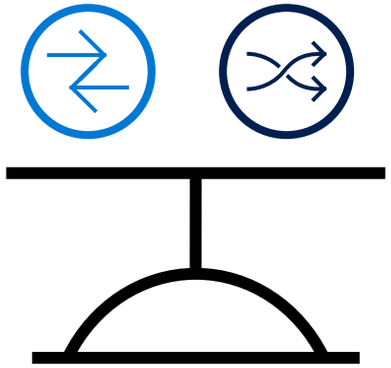
Security Must be Balanced

Too little or too much security can increase risk



Increase Business Agility and Mitigate Security Risk

Capture business opportunities



Strengthen Security

Digital Transformation

Agile - adapt rapidly to changing business conditions and technologies with regular contact between business, IT, and security.

Sustainable – Ensure sponsors, developers, users, IT, and security maintain a constant pace (and budget) indefinitely.

Simplify User Experience – ensure *each* user role and business process can execute with minimal friction and interruption

Zero Trust Principles

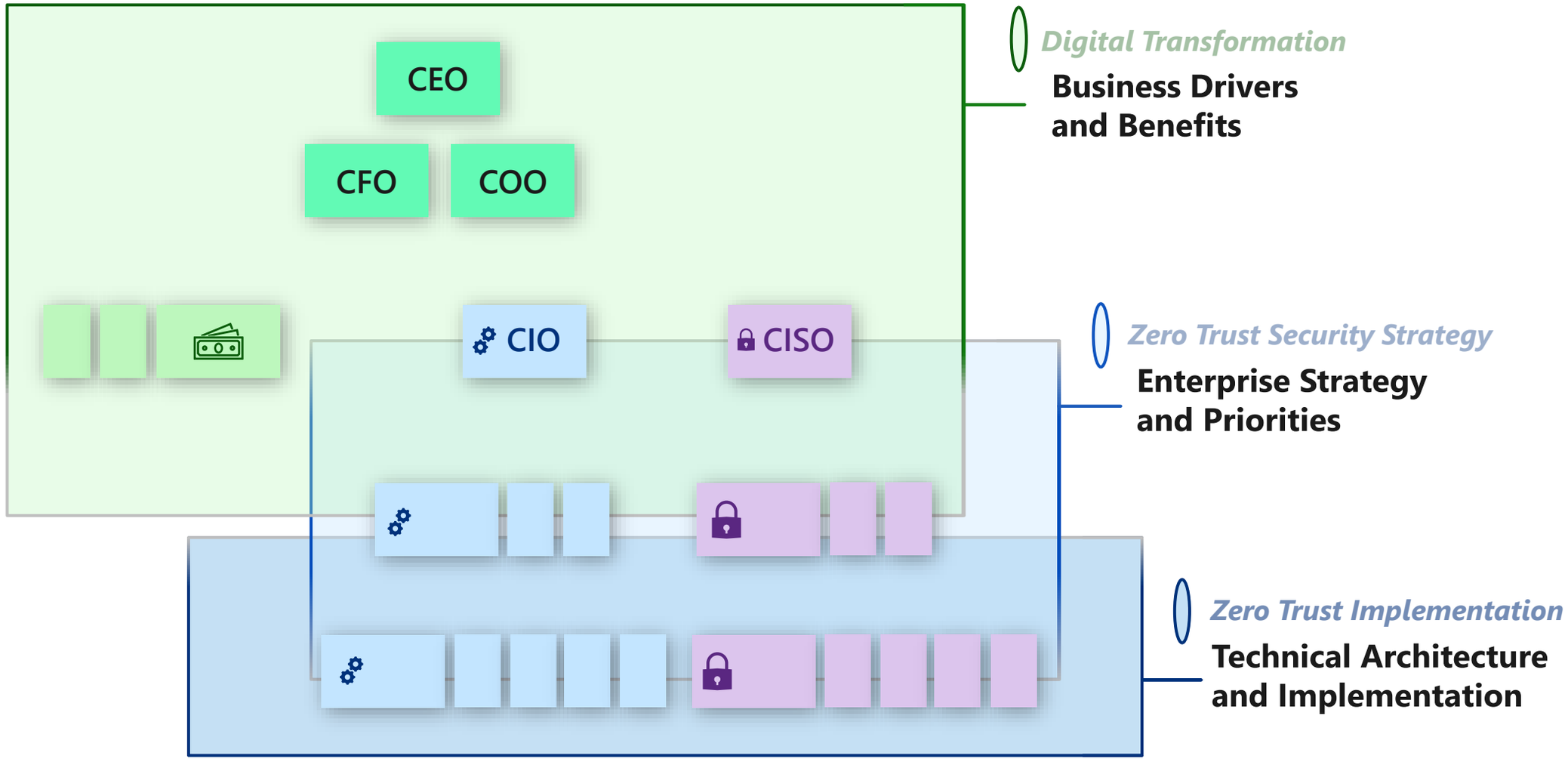
Assume Breach (Assume Compromise) Minimize blast radius with asset centric protections, micro-segmentation, continuous monitoring, and automated threat response

Verify explicitly Always make security decisions using all available data points, including identity, location, device health, resource, data classification, and anomalies.

Use least privilege access Limit access with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

Layers of a Zero Trust Security Strategy

A Journey that affects everyone a little differently



“Zero Trust” has been around for a while

2004
Jericho Forum
Formally Established

2014
Microsoft Advocates
“Assume Breach”

2016
Conditional
Access Released

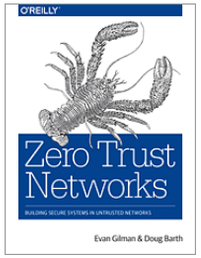
Ongoing
Passwordless
Initiative

~2004
Network Access Control
(NAC) Architectures

2010
Forrester coins
“Zero Trust” Term

2014
BeyondCorp
Published

2017



Today

The Open Group
(Home of the Jericho Forum, TOGAF, and more)

NIST

Forrester
ZTX Model

Historically slow mainstream adoption for both network & identity models:

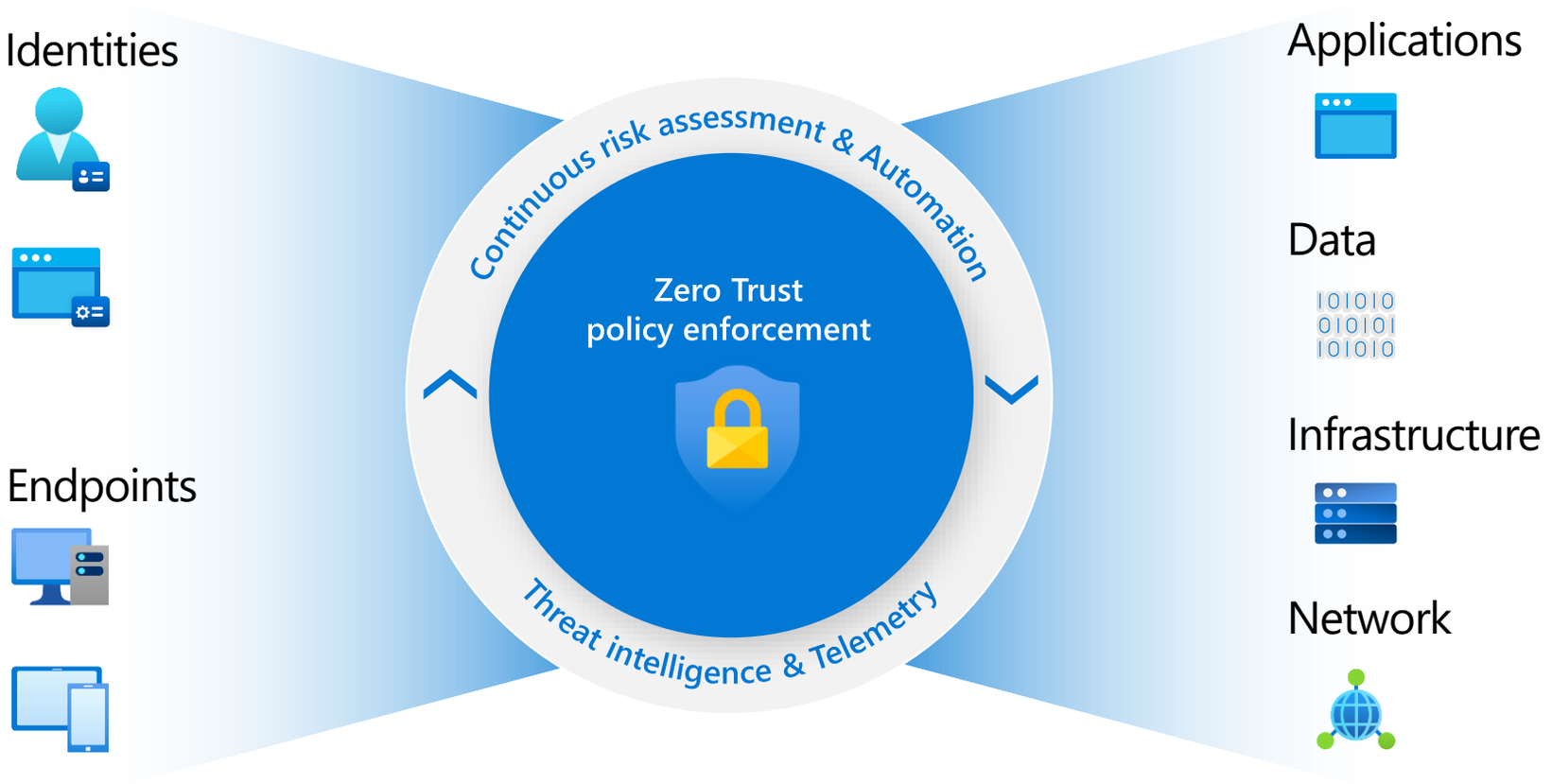
Network – Expensive and challenging to implement
Google’s BeyondCorp success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

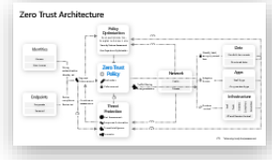
Increasing consensus and convergence (though still some variations)

Zero Trust Security Strategy

Technical Components

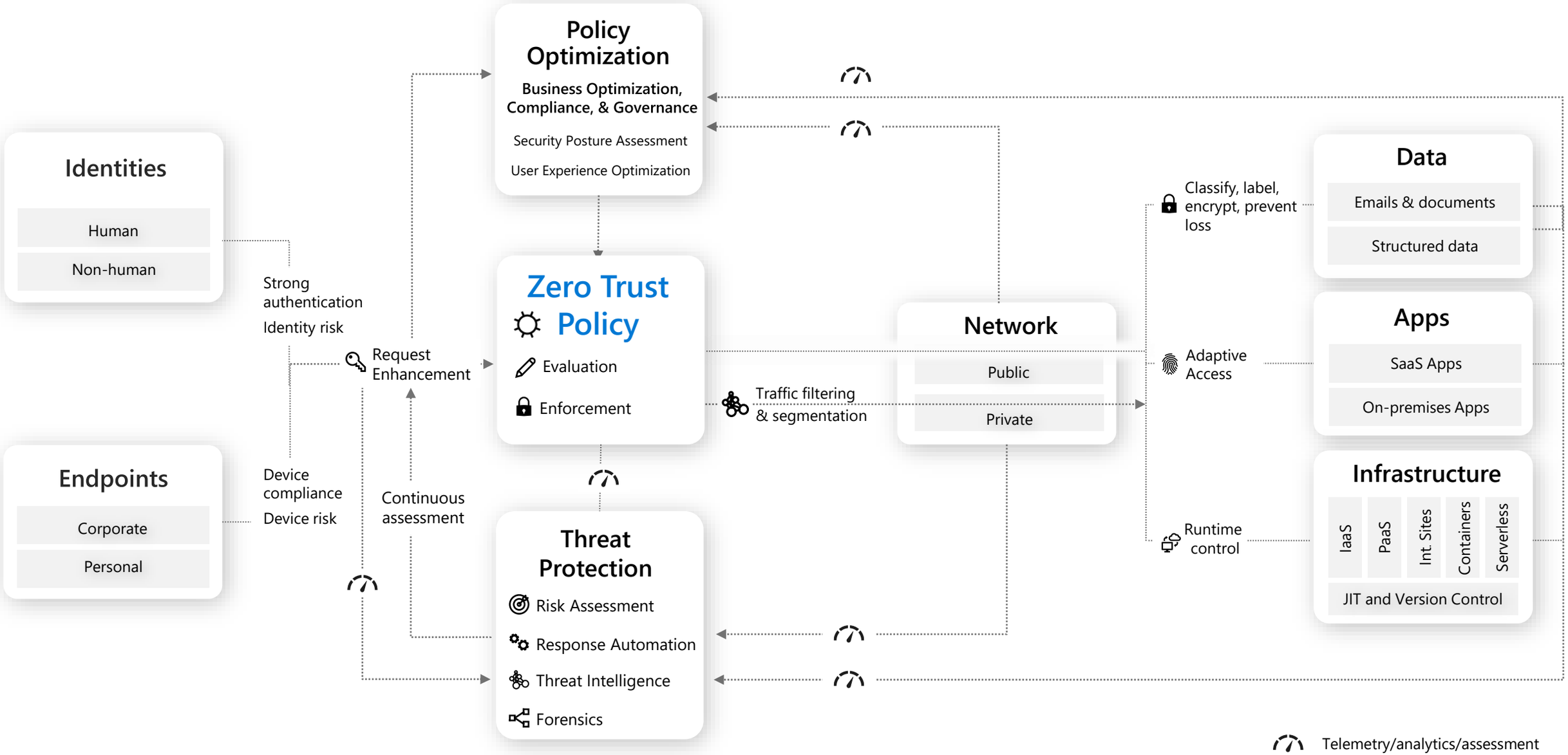


Assume breach | Explicitly Verify | Least privileged



Zero Trust Architecture

Zero Trust Architecture



Review - Strategy and Recommended Initiatives

- **Security's dual mission:** reduce risk + enable the business
- **Partner and collaborate** across Business, IT, and Security teams
- **Zero Trust Strategy** includes multiple initiatives
- **Zero Trust Principles** are critical to modernization

BACK TO MENU

Next Up:
1B Business Alignment

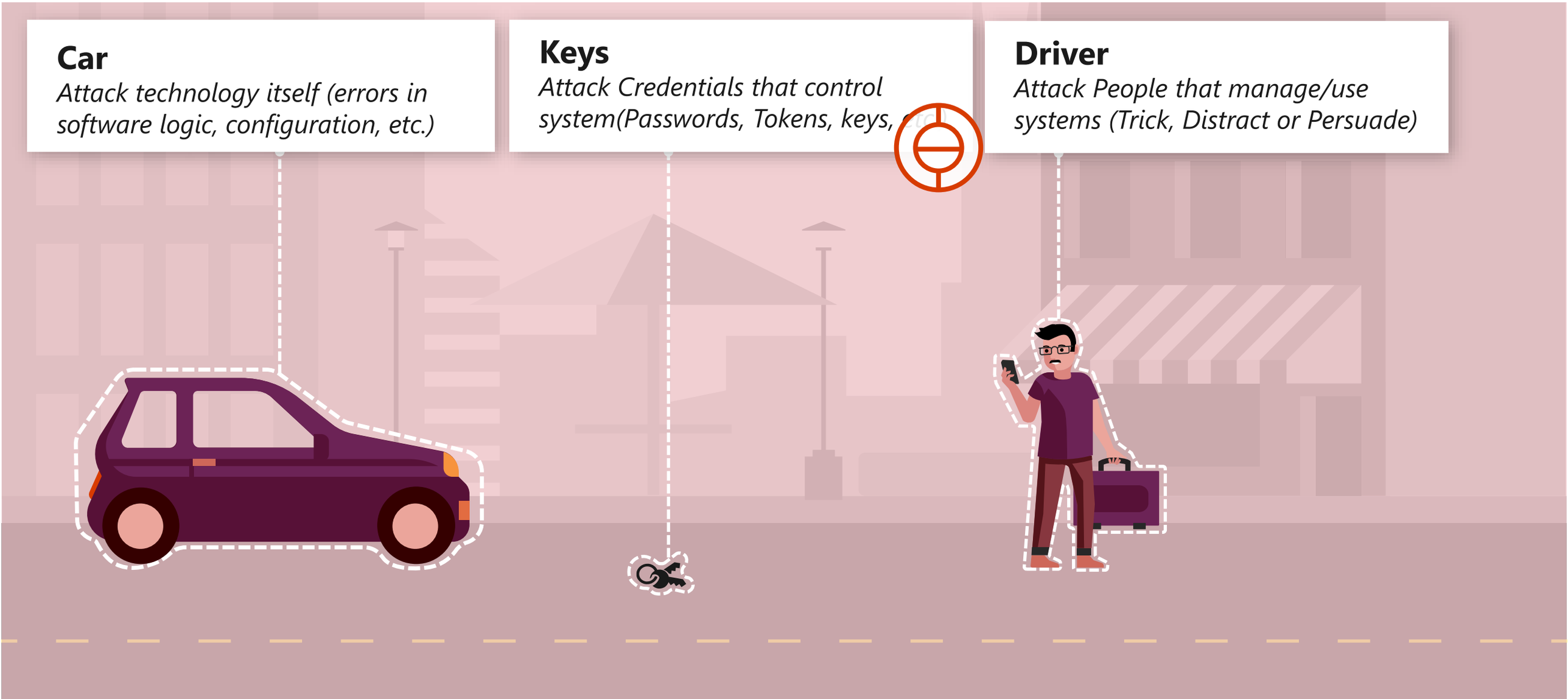
Security can be simple

Lots of details but really just 3 ways to get control

Car
Attack technology itself (errors in software logic, configuration, etc.)

Keys
Attack Credentials that control system(Passwords, Tokens, keys, etc.)

Driver
Attack People that manage/use systems (Trick, Distract or Persuade)



Security is a Team Sport

Example: Identifying what is business critical

Business

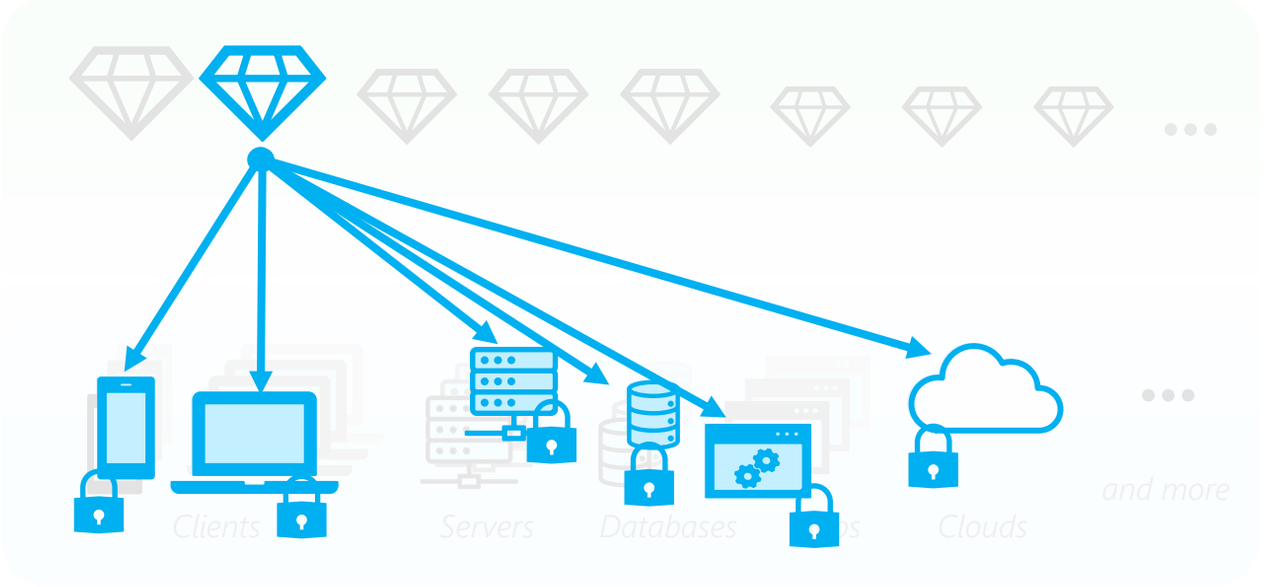
What would you restore first if everything was down?

IT / Technology

What are technical components of business critical assets?

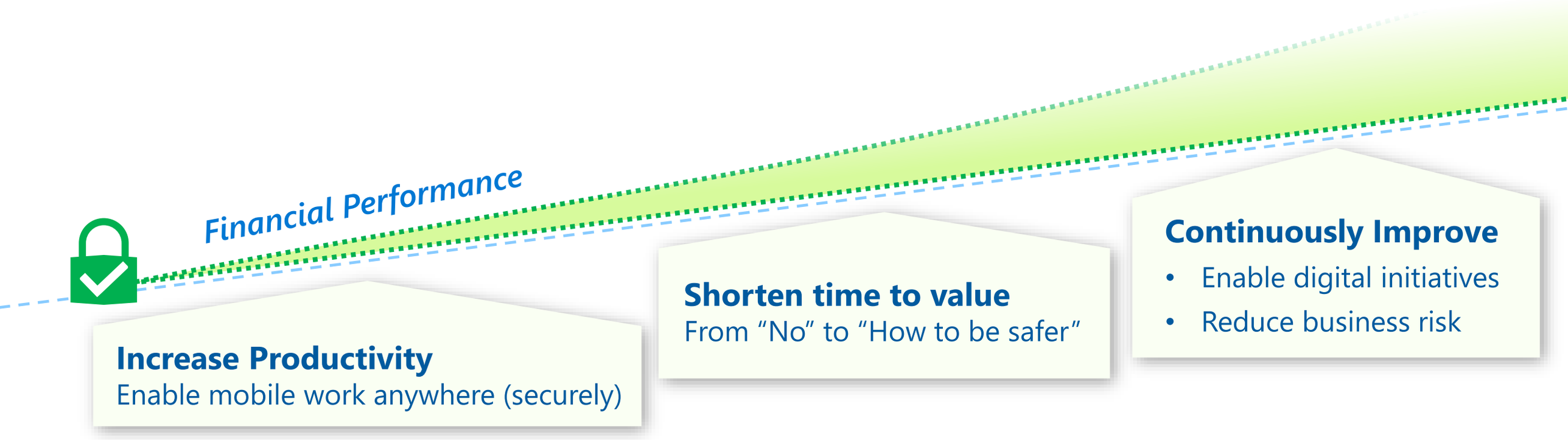
Security

- *What security threats could cause this?*
- *How to protect assets without disruption?*



Enable your business with a Trusted Digital Fabric

Reducing business friction and identifying opportunities



Reduced Business Friction = Increased Business Agility (and ability to capture opportunities)

Wise investments increase agility and reduce risk

Proactive security approach avoids business disruptions

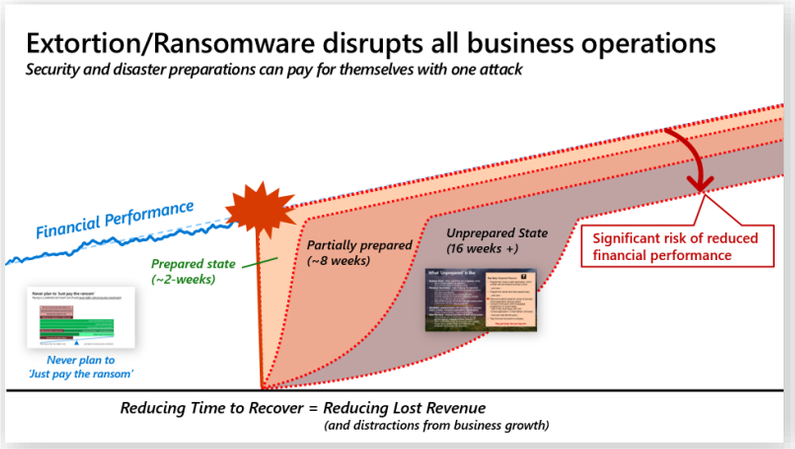
Security is not a technical problem (to be 'solved').

Security is an ongoing risk to be managed
(driven by groups of well funded humans)

Ongoing incremental progress on a Trusted Digital Fabric

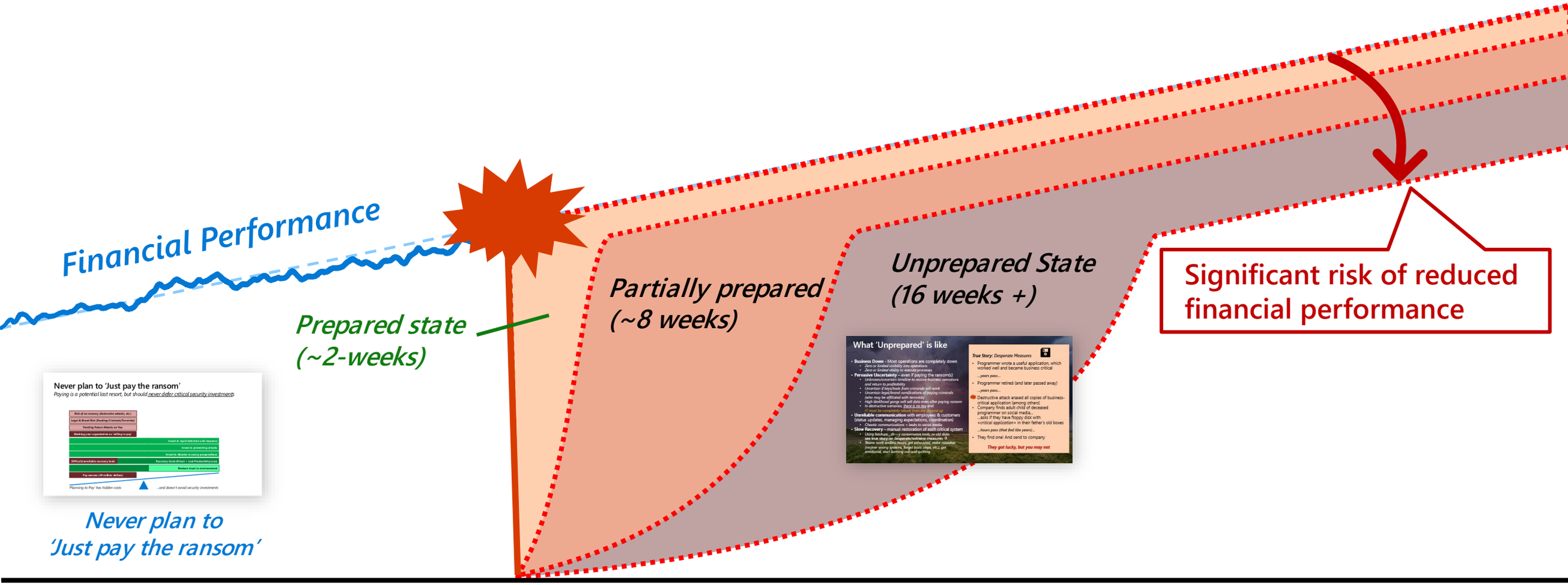
"Let's get ahead of this"

"That won't be us"



Extortion/Ransomware disrupts all business operations

Security and disaster preparations can pay for themselves with one attack



Never plan to 'Just pay the ransom'

Reducing Time to Recover = Reducing Lost Revenue

(and distractions from business growth)

What ‘Unprepared’ is like

- **Business Down** - Most operations are completely down
  - *Zero or limited visibility into operations*
  - *Zero or limited ability to execute processes*
- **Pervasive Uncertainty –** even if paying the ransom(s)
  - *Unknown/uncertain timeline to restore business operations and return to profitability*
  - *Uncertain if keys/tools from criminals will work*
  - *Uncertain legal/brand ramifications of paying criminals (who may be affiliated with terrorists)*
  - *High likelihood gangs will sell data even after paying ransom*
  - *In destructive scenarios, there is no key and IT must be completely rebuilt from the ground up*
- **Unreliable communication** with employees & customers (status updates, managing expectations, coordination)
  - *Chaotic communications + leaks to social media.*
- **Slow Recovery –** manual restoration of *each* critical system
  - *Using backups , sh---y ransomware tools, or old disks* **see true story on desperate/extreme measures →**
  - *Teams work endless hours, get exhausted, make mistakes (recover wrong systems, forget basic steps, etc.), get emotional, start burning out and quitting*

True Story: Desperate Measures

- Programmer wrote a useful application, which worked well and became business critical

  …years pass…

- Programmer retired (and later passed away)

  …years pass…

- Destructive attack erased all copies of business-critical application (among others)
- Company finds adult child of deceased programmer on social media…
  …asks if they have floppy disk with *<critical application>* in their father’s old boxes

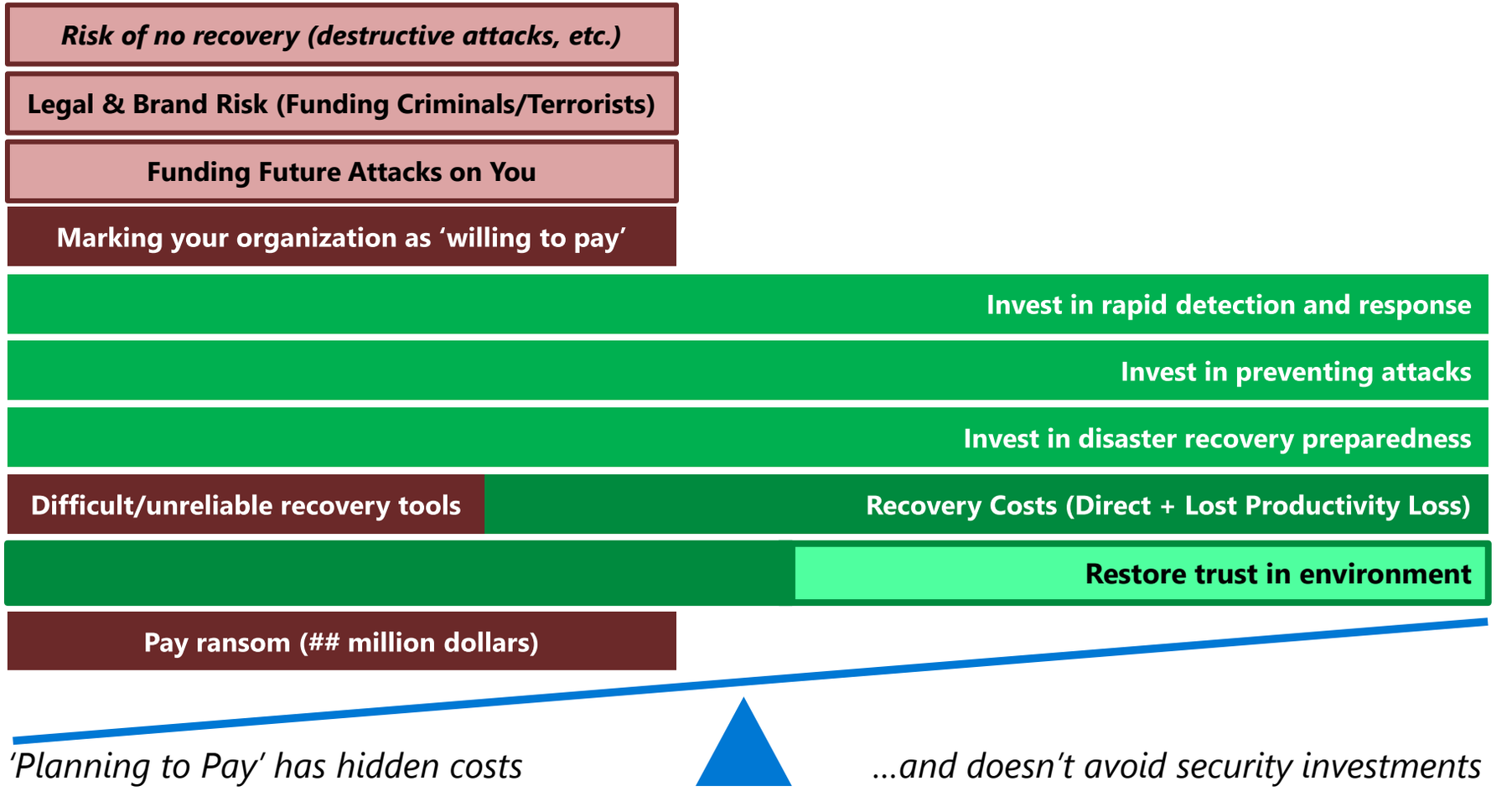
  …hours pass (that feel like years)…

- They find one! And send to company

They got lucky, but you may not

Never plan to ‘Just pay the ransom’

Paying is a potential last resort, but should never defer critical security investments



Secure cloud adoption enables rapid secure innovation

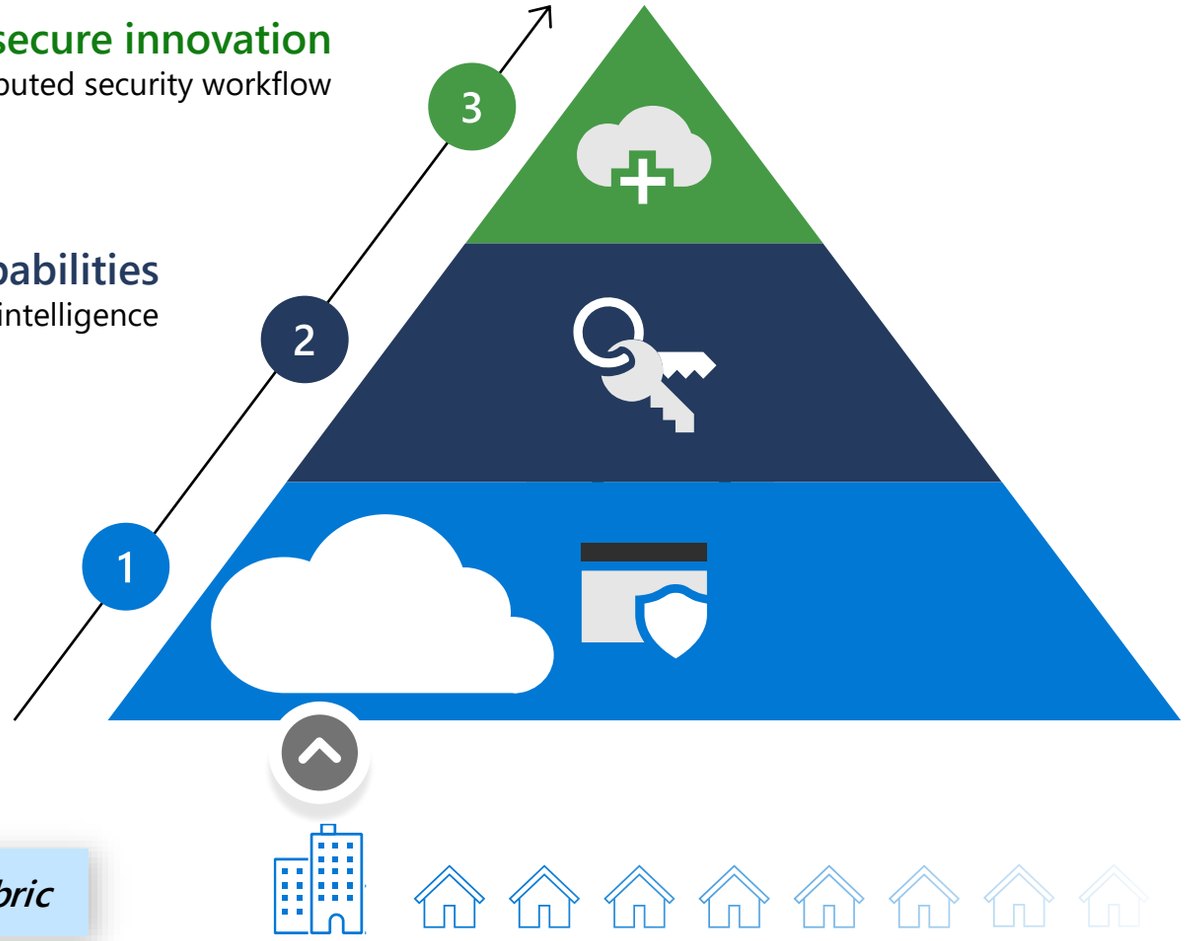
Secure innovation is the beating heart of an organization in today's digital landscape

Secure Cloud Adoption

Enables rapid secure innovation
DevSecOps, IaC security, distributed security workflow

Provides native Zero Trust security capabilities
Built-in controls, monitoring, threat protection, and threat intelligence

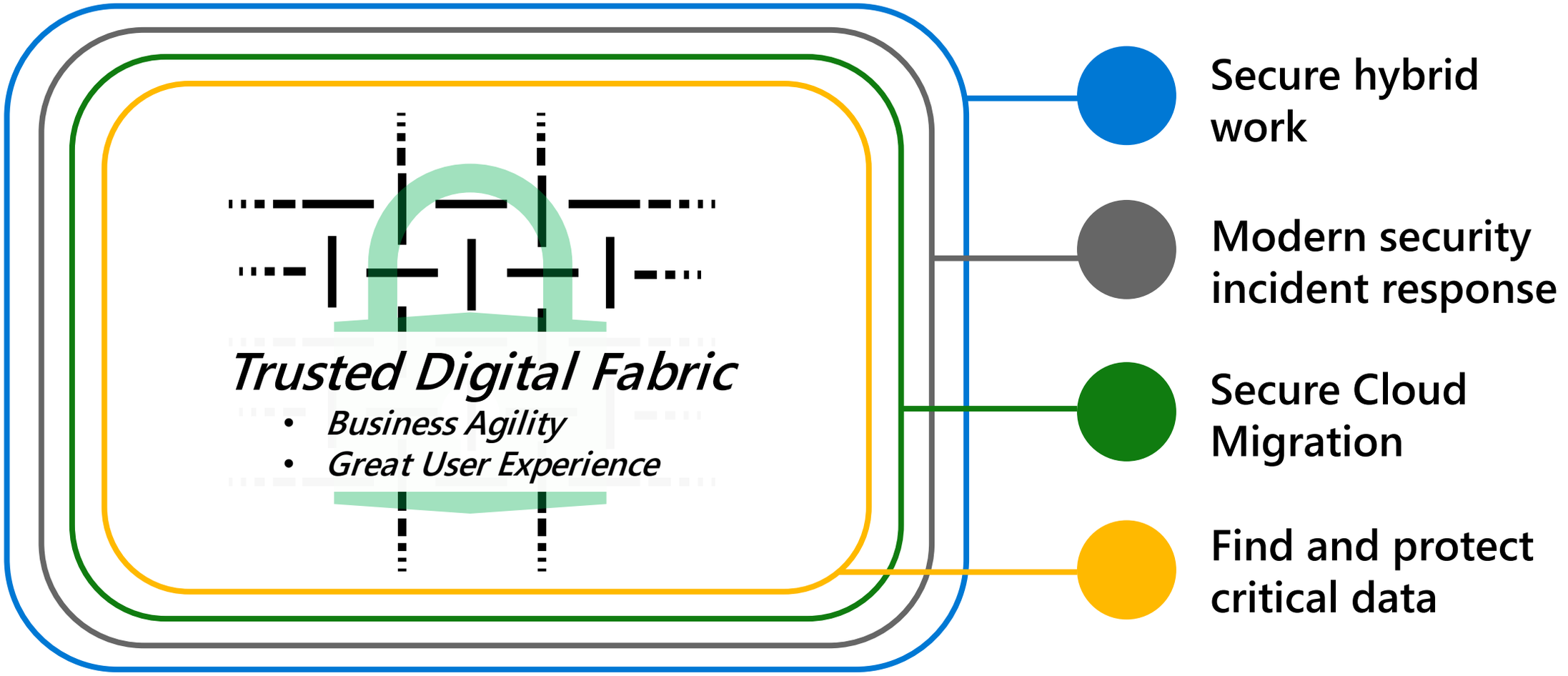
Provides a safe foundation
Confidentiality, integrity, availability, posture management, governance, and regulatory compliance



Secure cloud adoption is the foundation of a Trusted Digital Fabric

Components of a Trusted Digital Fabric

Safely Enable Business Agility from anywhere



Measuring Success of the Trusted Digital Fabric

Recommended Scorecard Metrics

Business Enablement

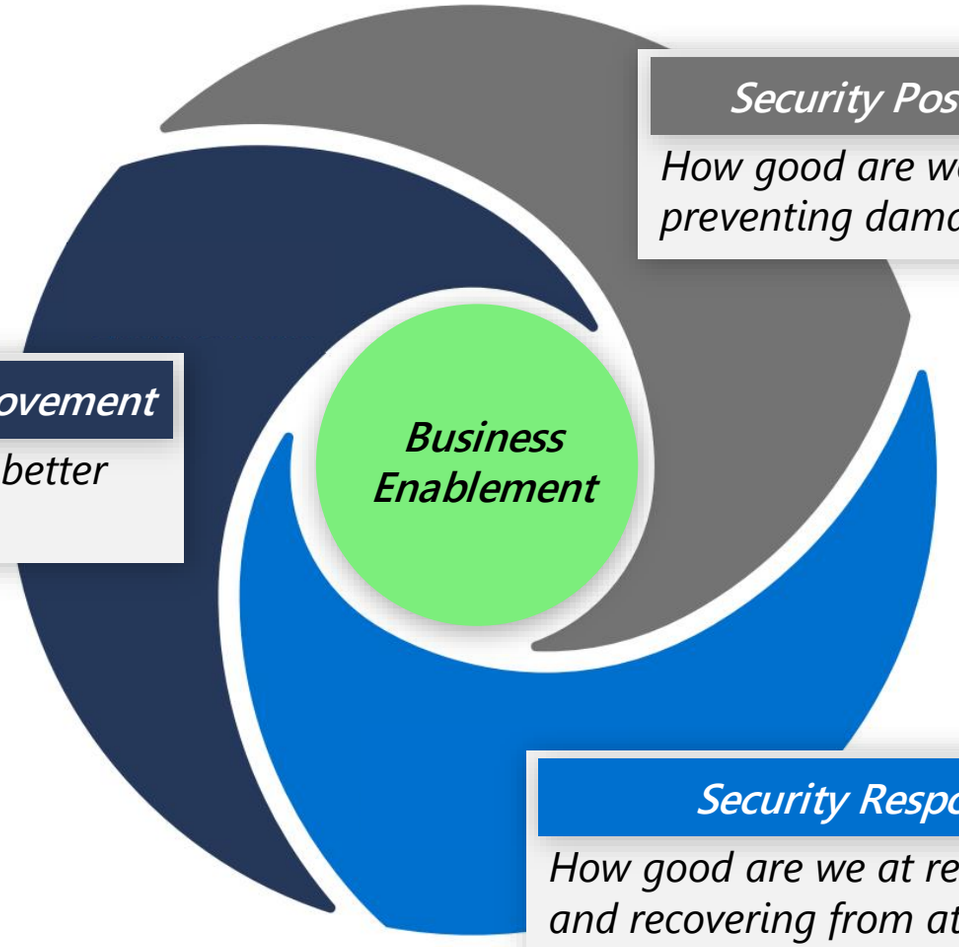
How much security friction is in user experience and business processes?

Security Posture

How good are we at preventing damage?

Security Improvement

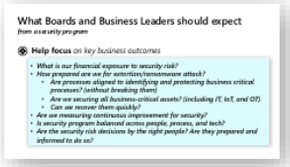
Are we getting better every month?



Security Response

How good are we at responding to and recovering from attacks?

Starting Points



Board Questions

Metrics

Example Metrics

Focus on continuous improvement

Security Scorecard Metrics

Supporting Performance Measurements

Business Enablement	*Security Posture*	*Security Response*	*Security Improvement*
Mean Time for security review	*% of new apps/etc. reviewed*	*Mean Time to Recover (MTTR)*	*# of modernization projects open*
# days for application security review	*Secure score*	*Mean Time to Acknowledge (MTTA)*	*# modernization project milestones achieved in last 60 days*
Average boot/logon time for managed devices.	*% Compliant apps*	*Time to Restore Critical Systems*	*Number of repetitive manual steps removed from workflows*
Number of security interruptions in user workflow	*# of privileged accounts meeting 100% of requirements*	*# of high severity incidents*	*# of Lessons learned from internal/external incidents*
% of IT help desk time spent on low-value security activities	*# of accounts meeting 100% of requirements*	*Incident growth rate (overall)*	

What Boards and Business Leaders should expect

from a security program

Help focus *on key business outcomes*

- *What is our financial exposure to security risk?*
- *How prepared are we for extortion/ransomware attack?*
  - *Are processes aligned to identifying and protecting business critical processes? (without breaking them)*
  - *Are we securing all business-critical assets? (including IT, IoT, and OT)*
  - *Can we recover them quickly?*
- *Are we measuring continuous improvement for security?*
- *Is security program balanced across people, process, and tech?*
- *Are the security risk decisions by the right people? Are they prepared and informed to do so?*

Benefits of a Modern Approach based on Zero Trust

Line of Business

- **Business Agility –** for continuous business environment changes:
  - Business Models and Partnerships
  - Technology Trends
  - Regulatory, Geopolitical, Cultural Forces
  - Disruptive Events
  - Paradigm Shift to Remote Work
- **Accelerate digital transformation** initiatives and lower risk

Business Support

(Finance, HR, etc.)

- **Accelerate process modernization** using cloud technologies
- **Rapidly apply policy** as people change roles

  Employee ←→ supplier ←→ partners
- **Better business risk visibility & mitigation** for acquisitions and new ventures

IT & Security

- **Simpler architectures** are more cost effective, easier to support, and reduce the threat surface
- **Less policy exceptions** and escalations to manage
- **Better visibility** into technical risks
- **Better prevention** of common security risks

Better security *and* user experience with Passwordless + working anywhere you want

Business Support Required for a Trusted Digital Fabric

Unlock business agility by supporting Zero Trust security transformation

NIST 800-40 on security maintenance


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Just as preventive maintenance on corporate fleet vehicles can help avoid costly breakdowns, patching should be viewed as a normal and necessary part of reliably achieving the organization's missions.

If an organization needs a particular technology to support its mission, it also needs to maintain that technology throughout its life cycle – and that includes patching.

https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

1. Prioritize secure cloud adoption + modernization investments

a. Accelerate secure cloud & app modernization
increases productivity and reduce risk

b. Normalize preventive maintenance for security
reduces downtime & disruption risk

2. Help protect business critical assets and processes

a. Identify business critical systems
Ensures teams know the top priorities

b. Sponsor + participate in Cybersecurity BC/DR exercises
Reduces impact of real incidents & extortion/ransomware

3. Shift security accountability and oversight to business owners

a. Prepare business owners for security risk
Owners need security context + expertise to make good decisions

b. Empower business owners to accept security risk
- *Ensures consideration of all opportunities and risks*
- *Enables agility and collaborative relationship with security*

Encourage continuous collaboration between business, IT, and security teams

National Institute of Standards and Technology
U.S. Department of Commerce

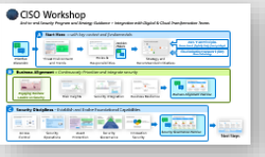
Just as preventive maintenance on corporate fleet vehicles can help avoid costly breakdowns, patching should be viewed as a normal and necessary part of reliably achieving the organization's missions.

If an organization needs a particular technology to support its mission, it also needs to maintain that technology throughout its life cycle – and that includes patching.

https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Review - Engaging Business Leaders on Security

BACK TO MENU



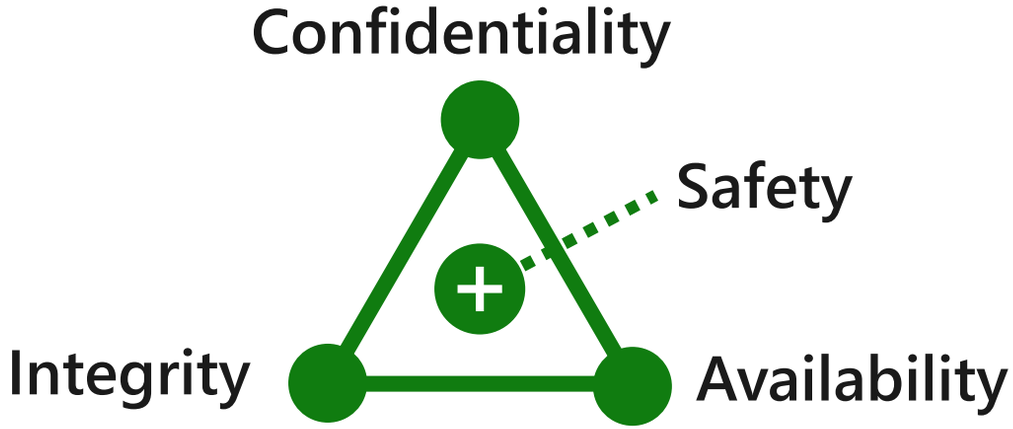
- **Presenting Security to Business Leaders**
  - **Simple view of security**
  - **Enable Business and Reduce Risk**
    - **Devastating Impacts of Ransomware / Destructive attacks**
  - **Enable Trusted Digital Fabric** with secure cloud adoption
  - **Recommended security metrics**
  - **Key Business Support** **needed for Security**

Next Up:

1B Risk Insights, Security Integration, Business Resilience

Security has a dual mission

- **Enable Business Goals –** Enable people to securely work anywhere and continuously identify how security/identity technology can enable business/mission
- **Reduce Risk to Organization –** Increase assurances for *all* data and systems across IT, OT, and IoT



- Business/asset owners should be **accountable** for security risk
- Security should be **responsible** to inform and help them.

Asset owners need to balance security risks against all other risks and benefits with security providing subject matter expertise as a trusted advisor.

Risk Insights

Organizational Leadership

Board
Organizational & Risk Oversight

Management
Business Model and Vision
Organizational Risk Appetite

Natural Disasters | **Market Relevancy** | **IT Operations** | **Cybersecurity** | •••

Competition from startups is disrupting markets, requiring businesses to digitally transform

Cybersecurity is emerging from IT as a distinct risk discipline for business leaders and boards

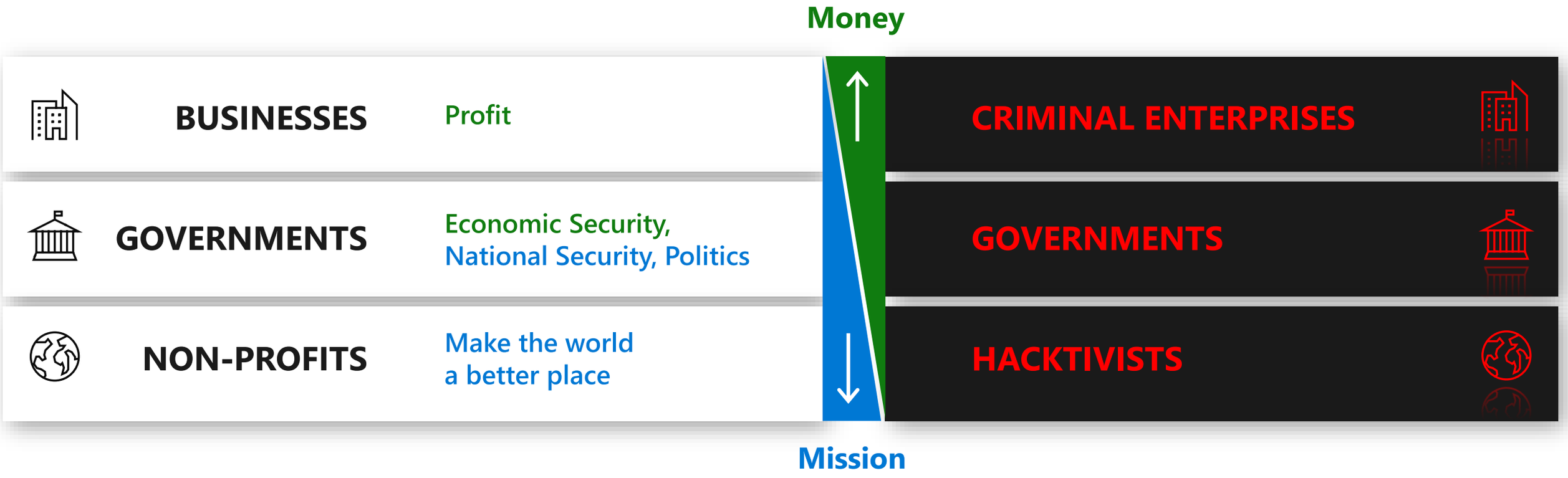
Security Alignment

Healthy two-way relationship focused on

- **Business Priorities**
  Business critical initiatives, applications, and data
- **Risk Management Framework**
  Risk Register, Prioritization, Impact, Language, etc.

Into a Mirror Darkly

The nature of attacker “return” varies by motivation

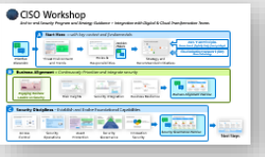


Disruption Strategies differ

- **Money** requires high predictability and is vulnerable to disruption
- **Mission** return can withstand greater uncertainty and can be more opaque

Review – Risk Insights

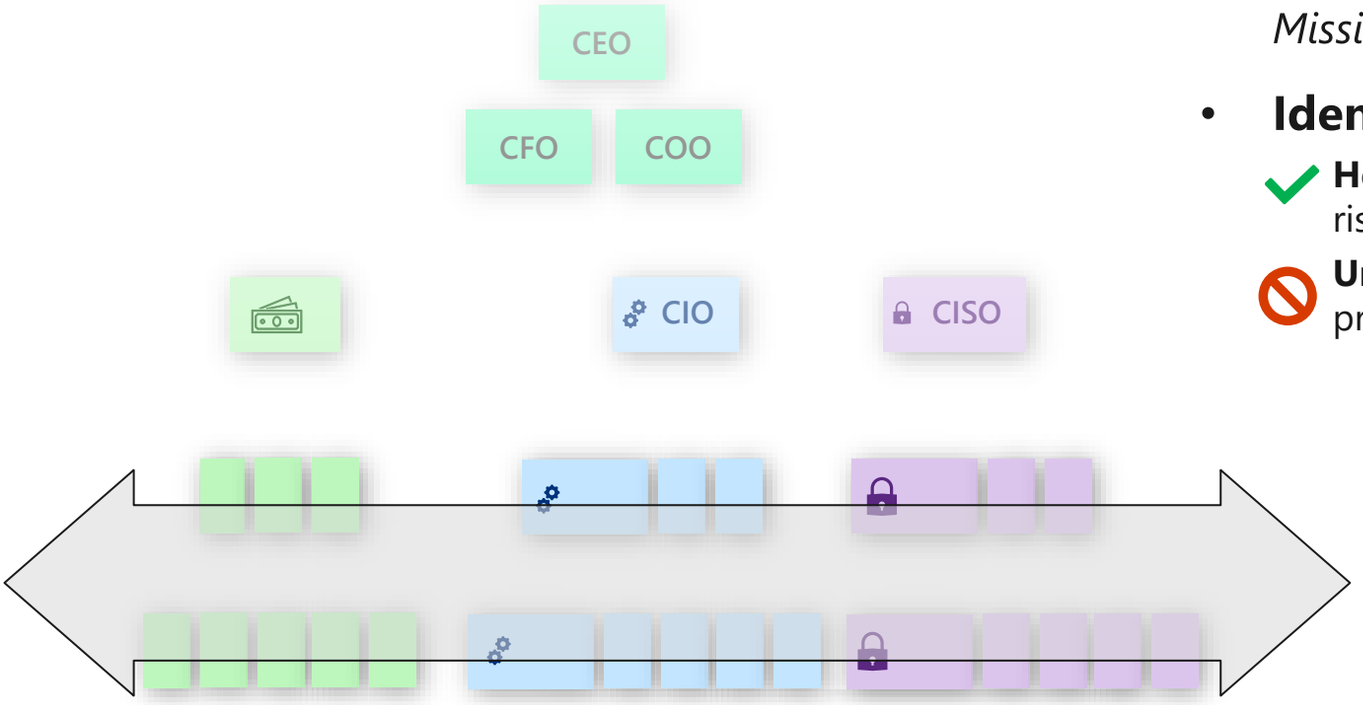
BACK TO MENU



- **Align Security Priorities to Business**
  - *Business critical initiatives, applications, and data*
- **Integrate Security Risk into Existing Processes**
  - *Risk Management Framework, Risk Register, Prioritization, Impact, Language, etc.*
- **Threat Awareness and Planning**
  - *Increase security literacy for organizational leaders*
  - *Prioritize security investments around your likely threats*

Next Up:
1B Risk Insights, Security Integration, Business Resilience

Security Integration

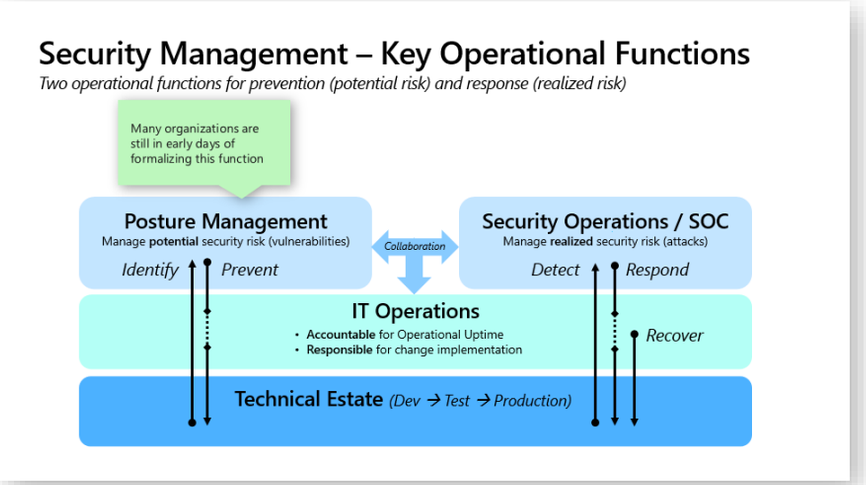


Normalize Relations

Integrate Skills, Culture, Process, and Priorities

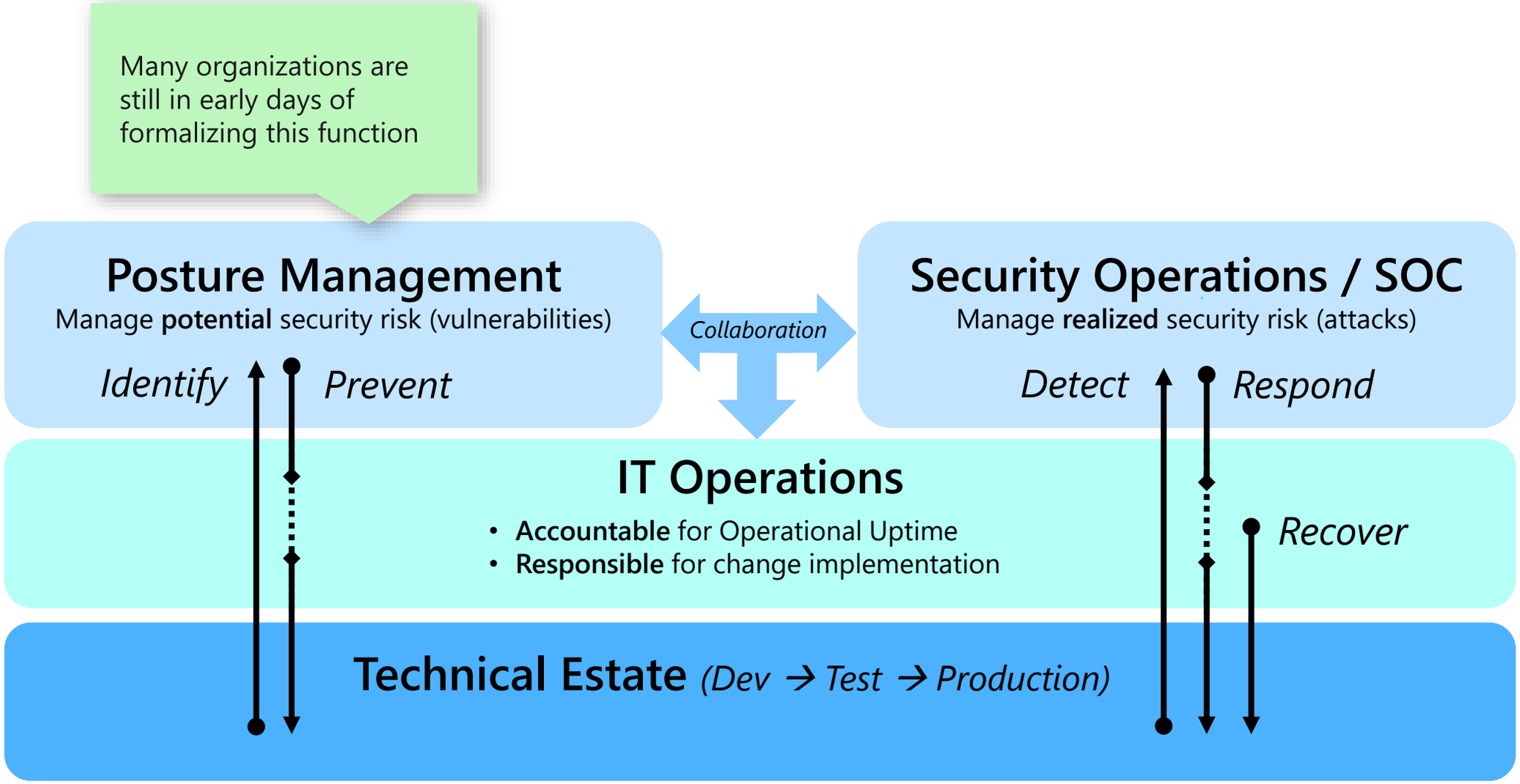
- **Identify shared goals and outcomes**
  Mission, business continuity, safety, and more
- **Identify right level of security**
  - **Healthy Friction** – Critical thinking that reduces risk *but doesn't break processes.*
  - **Unhealthy friction** – impedes more value than it protects.

Top Focus: IT Operations Integration & Posture Management



Security Management – Key Operational Functions

Two operational functions for prevention (potential risk) and response (realized risk)



Security Operating Model

Security Governance

Risk, Architecture, Compliance, Threat Intelligence (Strategic)

Posture Management

Manage **potential** security risk (vulnerabilities)

Identify *Prevent*

Collaboration

Security Operations / SOC

Manage **realized** security risk (attacks)

Detect *Respond* *Recover*

People Security

Education, Insider Risk

IT Operations & Data Governance

- **Accountable** for Productivity and Operational Uptime
- **Responsible** for change implementation and lifecycle management

People

Employees, Partners, Customers

Access Control

Technical Estate *(Dev → Test → Production)*

Asset Protection *(Data and Systems)*

DevOps Teams

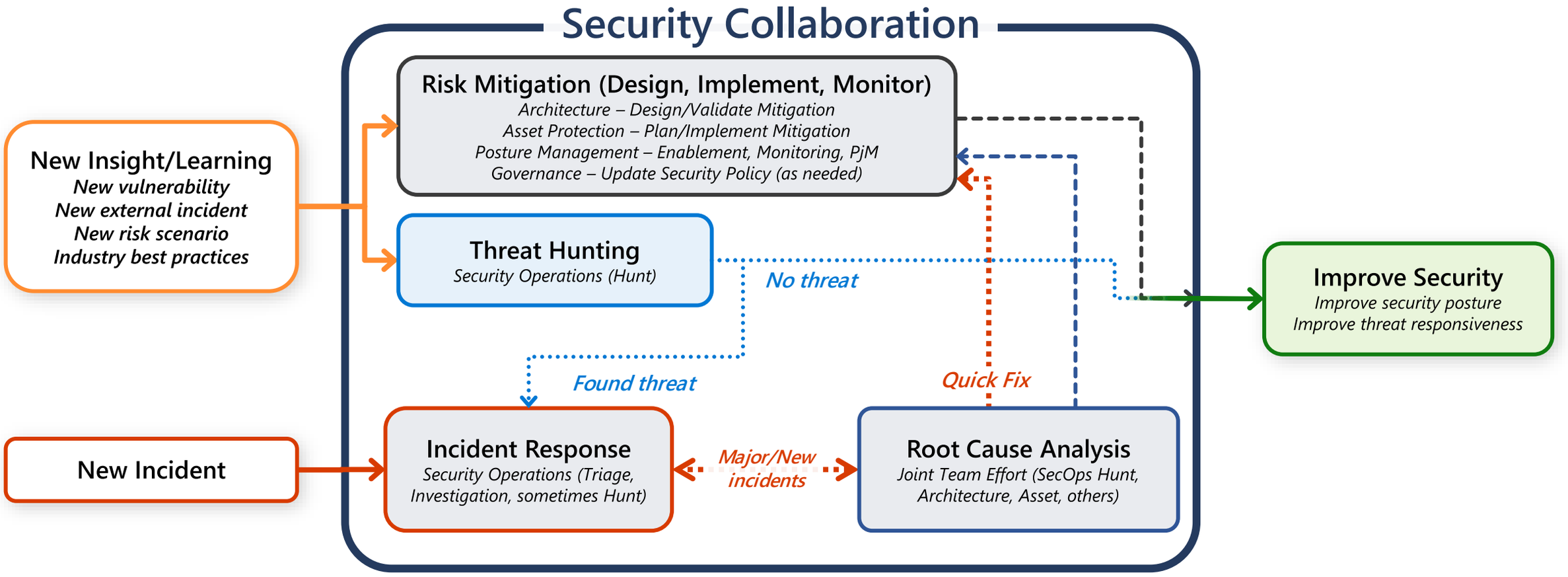
Innovation Security

Application Security

Citizen Developers

Continuously Learning to Reduce Risk

Collaborative approach to mitigate potential and realized risk



Note: Threat Intelligence and Security Engineering (automation) is a supporting function for all security activities

Evolution of Posture Management

New Tooling Available
On-demand insights into security posture, threat intelligence helps prioritize

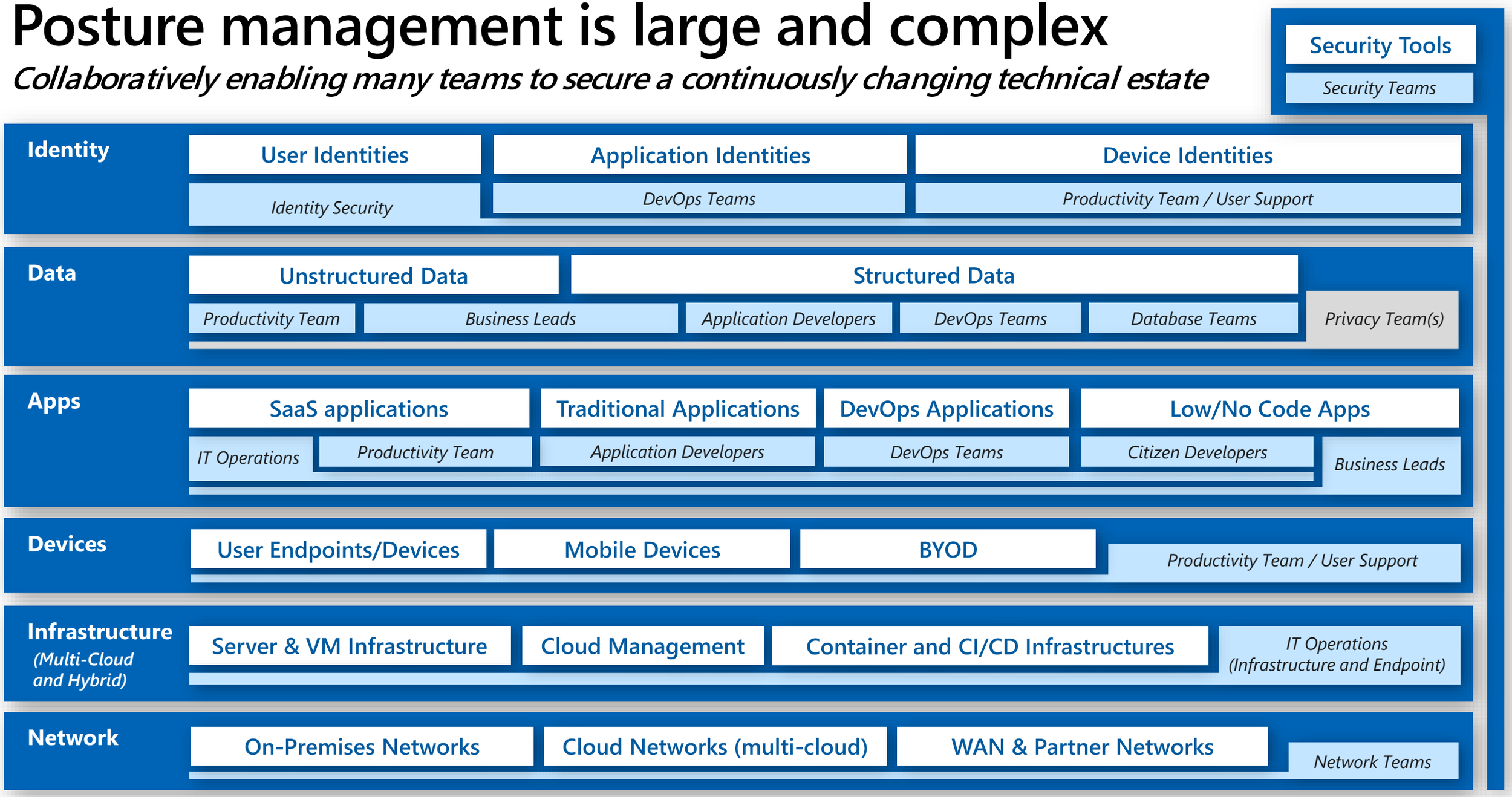
Traditional Vulnerability Management
Focused on Operating System vulnerabilities

Security Posture Management

- **Measure and Report Risk** across all sources:
  - **Software vulnerabilities** – *Operating System (OS), app, middleware, etc.*
  - **Configuration** – *OS, networks, apps, SaaS, PaaS, IaaS, Containers, Low-code apps, and more*
  - **Operation** – *processes and practices that create risk (e.g. overuse of privileged accounts, entitlements, etc.)*
- **Mitigate Risk *by enabling teams* -** Proactively work with IT operations and DevOps teams to assist with remediation (expertise, planning, tooling, education, etc.)

Posture management is large and complex

Collaboratively enabling many teams to secure a continuously changing technical estate



Posture Management

Rapid Modernization Plan (RaMP)

MENU

1. Start with Cloud Infrastructure (via CSPM)

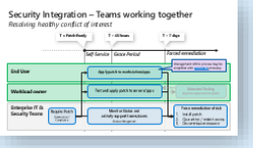
- ***Tooling*** *- Cloud Security Posture Management (CSPM) for VMs, Containers, Databases, etc. (e.g. Defender for Cloud)*
- ***Process*** *- Build shared responsibility model between teams + enablement processes for IT/Dev Ops teams*
- ***Configuration Baseline –*** *start with vendor/industry recommendations (ASB, M365 Secure Score, CIS Benchmark for AWS, etc.)*

2. Extend CSPM to all clouds and on-premises datacenters

- ***Extend Tools & Processes*** *– add on-premises assets to CSPM (e.g. via Azure Arc) & extend processes to new teams*
- ***Integrate TVM Team and Tools*** *– to monitor all assets consistently*

3. Proactively engage IT Ops and DevOps

- ***Adopt a self-service model*** *for patching on clients and servers*
- ***Build security engineering*** *capacity & accountability to accelerate risk reduction*



4. Establish Automated Guardrails

Enables business agility by reducing process friction and delays

- ***Automate –*** *security into DevOps & Infrastructure as code (IaC) with Azure Policy, ARM, Terraform, etc.*

5. Continuously improve and extend

Prepare and Build

- *Leadership support*
- *Team skillsets*
- *Processes*

Extend to more assets & controls

- *Improve baseline configuration beyond default configuration*
- *Add more controls across technologies (identities, apps, network, infrastructure, etc.)*
- *Integrate with application security engagement team(s) (e.g. SDL/DevSecOps)*

Review – Security Integration

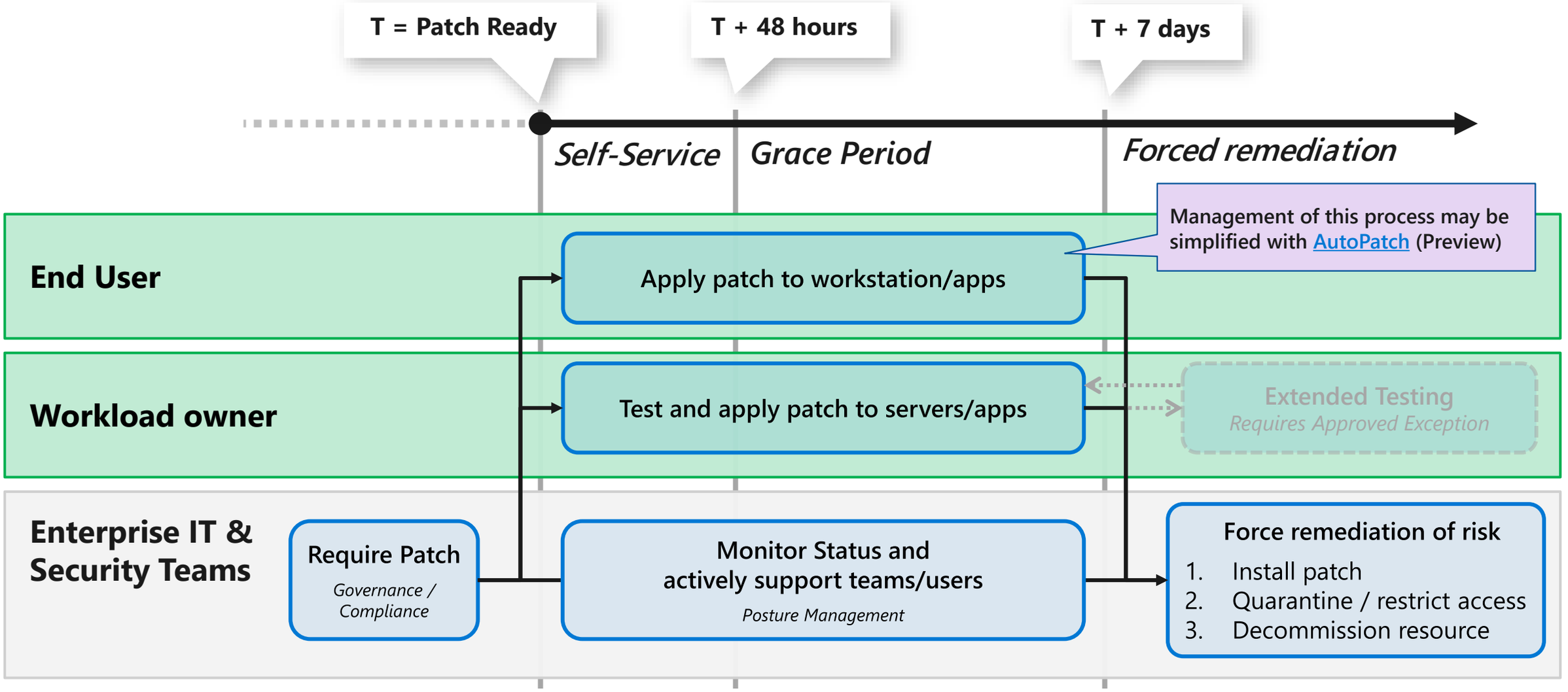
BACK TO MENU

- **Build consistent processes to integrate across security and IT teams**
  - Align to shared goals, outcomes, risk understanding
  - Always seek *<u>healthy</u>* level of security friction for IT and Business
- **Build Posture Management operations**
  - Combines vulnerability management + CSPM/EASM/others
  - Critically important, but large & complex problem to solve
  - Follow Rapid Modernization Plan (RaMP) for quick wins and incremental progress
  - Provides visibility needed to make business case for improving security maintenance and measuring progress

Next Up:
1B Risk Insights, Security Integration, Business Resilience

Security Integration – Teams working together

Resolving healthy conflict of interest

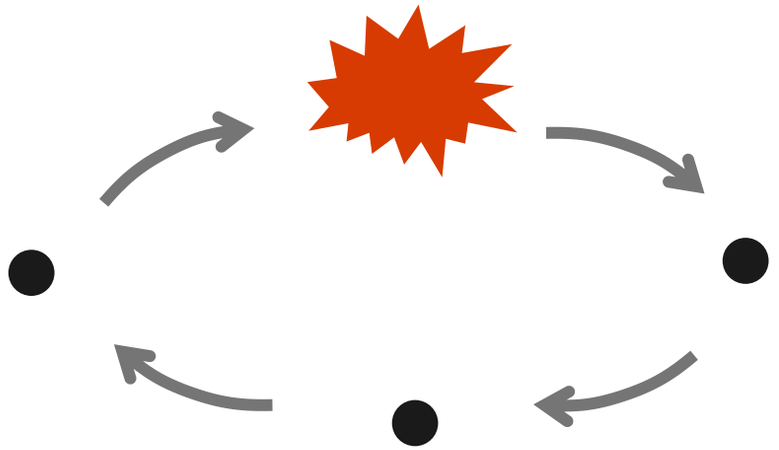


Business Resilience

Limiting operational impact of security incidents

During an Incident

- *Rapidly remediate active attacks*
- *Prioritize continuity of critical operations*



Before an Incident

Limit business operations impact and likelihood of security incidents

After an Incident

Rapidly restore full business operations

Feedback Loop

Learn lessons and integrate changes

Business Resilience

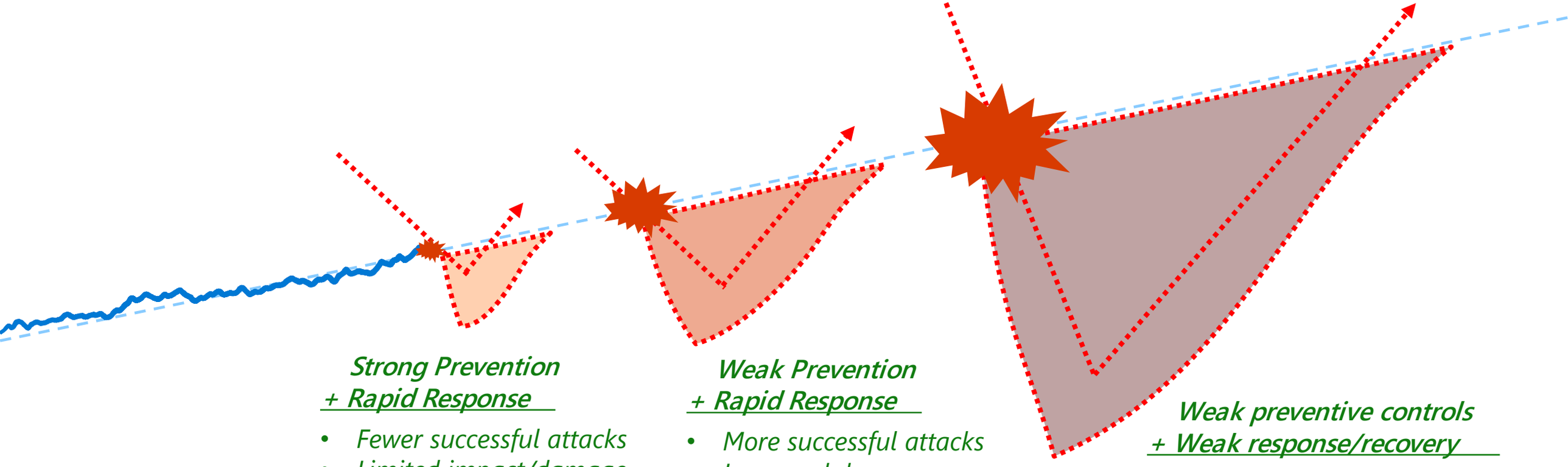
is the consistent goal of security program and disciplines

Balance investments across *prevention, response, and recovery*

- **Grow capabilities efficiently and rapidly**
- **Ensure minimum investment in each area**

Focus on **Continuous Learning** and **Continuous Improvement**

Why you need prevention *and* rapid response



Strong Prevention + Rapid Response

- *Fewer successful attacks*
- *Limited impact/damage*

Weak Prevention + Rapid Response

- *More successful attacks*
- *Increased damage*
  (attackers get farther before containment/recovery)

Weak preventive controls + Weak response/recovery

- *More successful attacks*
- *Highly impactful/damaging*
  (Bigger breaches take a long time to contain & recover, often requiring outside expertise)

A balanced strategy reduces risk faster

Review – Business Resilience

BACK TO MENU

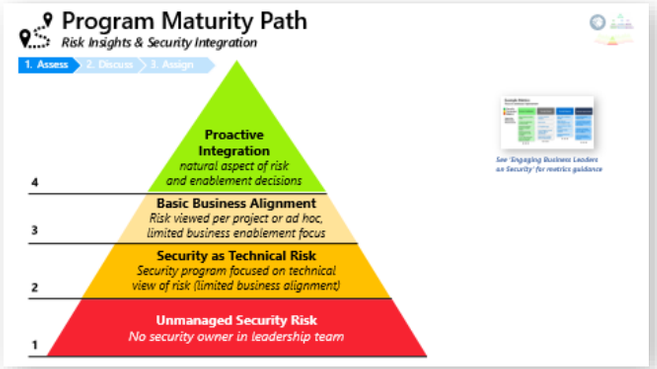
- **Business Resilience is North Star of security program**
  - *Reducing business impact and rapidly restoring business operations*
- **Balance Investments across security lifecycle**
  - *Before, During, After an incident + follow up on learnings/feedback*
- **Balanced approach reduces business impact**
  - *Reduces damage attacker can inflict before detection*
  - *Reduces time to recover from an attack*

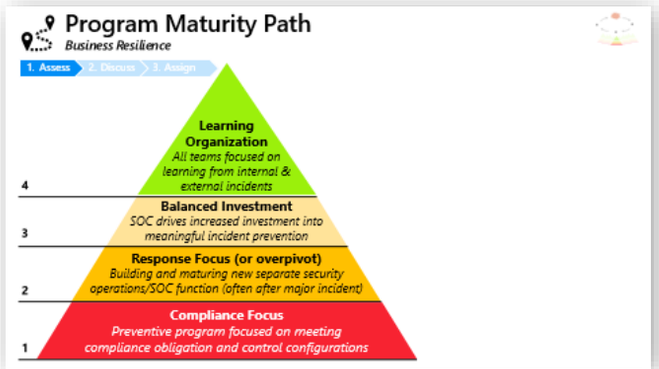
Next Up:
Business Alignment Exercise

MENU

Business Alignment Exercise

1. **Assess** Current State
2. **Discuss** Focus Areas
3. **Assign** Next Steps





Risk Insights

Integrate security insights into risk management framework and digital initiatives

Security Integration

Integrate security insights and practices into business and IT processes, integrate security disciplines together

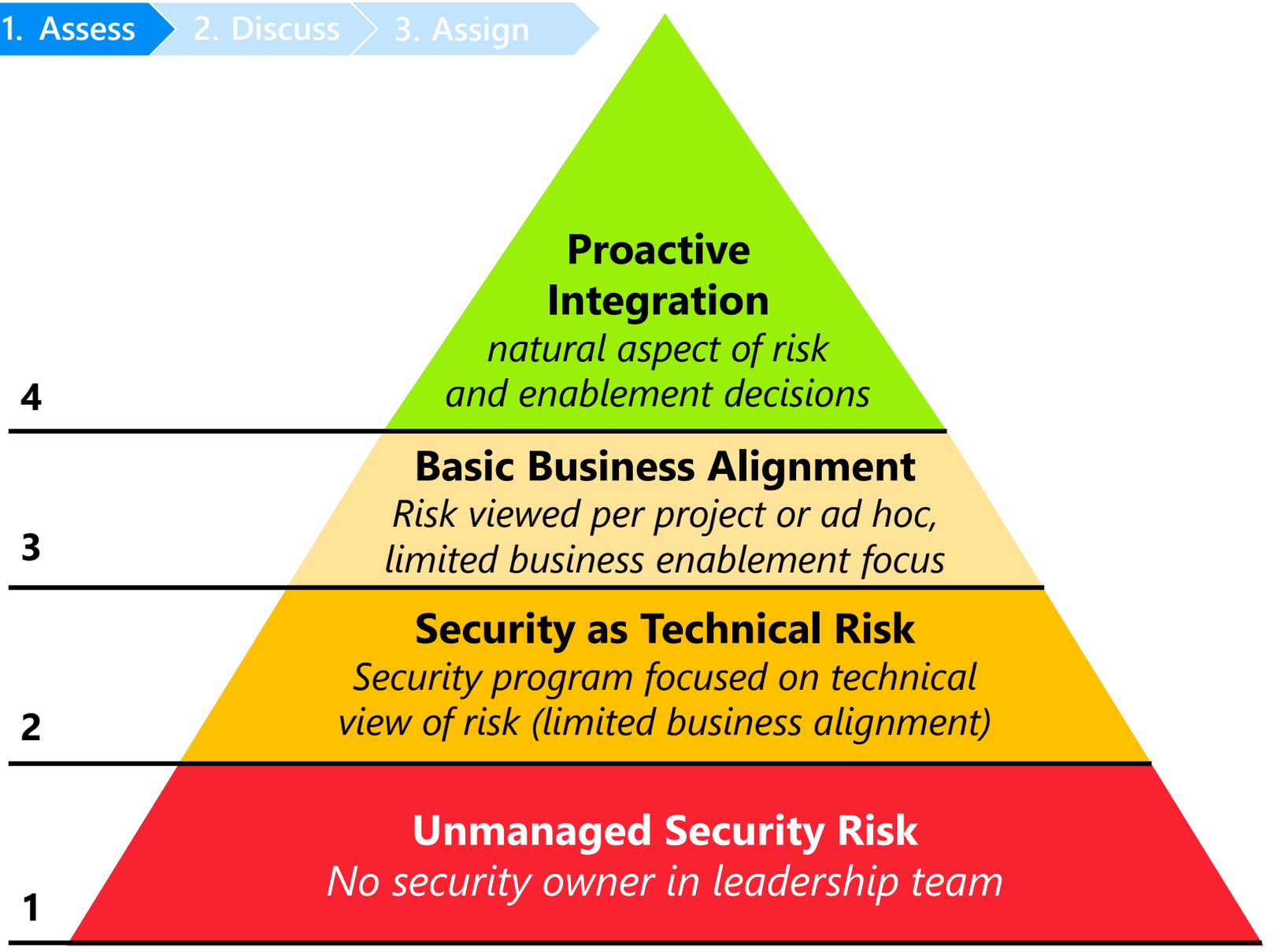
Business Resilience

Ensure organization can operate during attacks and rapidly regain full operational status

Program Maturity Path

Risk Insights & Security Integration

1. Assess
2. Discuss
3. Assign

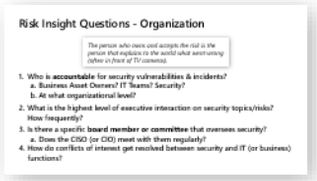


See 'Engaging Business Leaders on Security' for metrics guidance

Discuss Improvement Steps

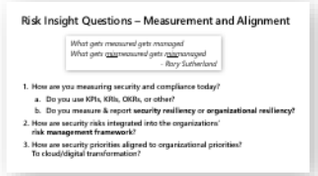
Risk Insights & Security Integration

1. Assess | 2. Discuss | 3. Assign


Risk Insight Questions - Organization

The person who owns and accepts the risk is the person that explains to the world what went wrong (when in front of TV cameras).

1. Who is **accountable** for security vulnerabilities & incidents?
   a. Business Asset Owners? IT Teams? Security?
   b. At what organizational level?
2. What is the highest level of executive interaction on security topics/risks? How frequently?
3. Is there a specific **board member or committee** that oversees security?
   a. Does the CISO (or CIO) meet with them regularly?
4. How do conflicts of interest get resolved between security and IT (or business) functions?


Risk Insight Questions – Measurement and Alignment

What gets measured gets managed
What gets ~~re~~measured gets ~~re~~managed
– Rory Sutherland

1. How are you measuring security and compliance today?
   a. Do you use KPIs, KRIs, OKRs, or other?
   b. Do you measure & report **security resiliency** or **organizational resiliency**?
2. How are security risks integrated into the organizations' **risk management framework**?
3. How are security priorities aligned to organizational priorities? To cloud/digital transformation?


Security Integration

"Trust is knowing that when a team member does push you, they're doing it because they care about the team."
— Patrick Lencioni

1. How are you investing into integrating security into business and IT processes?
   a. How prepared are **organizational leaders** to make security/risk decisions?
   b. How prepared are **business line leaders** to make security/risk decisions?
2. What would business and IT leaders say about the progress on that integration?
3. How is security budgeted? Proportional to IT? to organization's FTEs or revenue? Ad Hoc/Custom?

Click Here

- Integrate security into risk management framework
- Enable business asset owners to make informed security risk decision (similar to other risks) and implement mitigations
- Identify business enablement opportunities for security (e.g. rapid entry of markets, enable remote work, etc.)

Click Here

- Align security risk to business goals and risks
- Link critical business processes to IT systems

Next: *Business Resilience*

Risk Insight Questions - Organization

> *The person who owns and accepts the risk is the person that explains to the world what went wrong (often in front of TV cameras).*

1. Who is **accountable** for security vulnerabilities & incidents?
   a. Business Asset Owners? IT Teams? Security?
   b. At what organizational level?
2. What is the highest level of executive interaction on security topics/risks? How frequently?
3. Is there a specific **board member or committee** that oversees security?
   a. Does the CISO (or CIO) meet with them regularly?
4. How do conflicts of interest get resolved between security and IT (or business) functions?

Risk Insight Questions – Measurement and Alignment

> *What gets measured gets managed*
> *What gets mismeasured gets mismanaged*
> *- Rory Sutherland*

1. **How are you measuring security and compliance today?**
   a. **Do you use KPIs, KRIs, OKRs, or other?**
   b. **Do you measure & report security resiliency or organizational resiliency?**
2. **How are security risks integrated into the organizations' risk management framework?**
3. **How are security priorities aligned to organizational priorities? To cloud/digital transformation?**

Security Integration

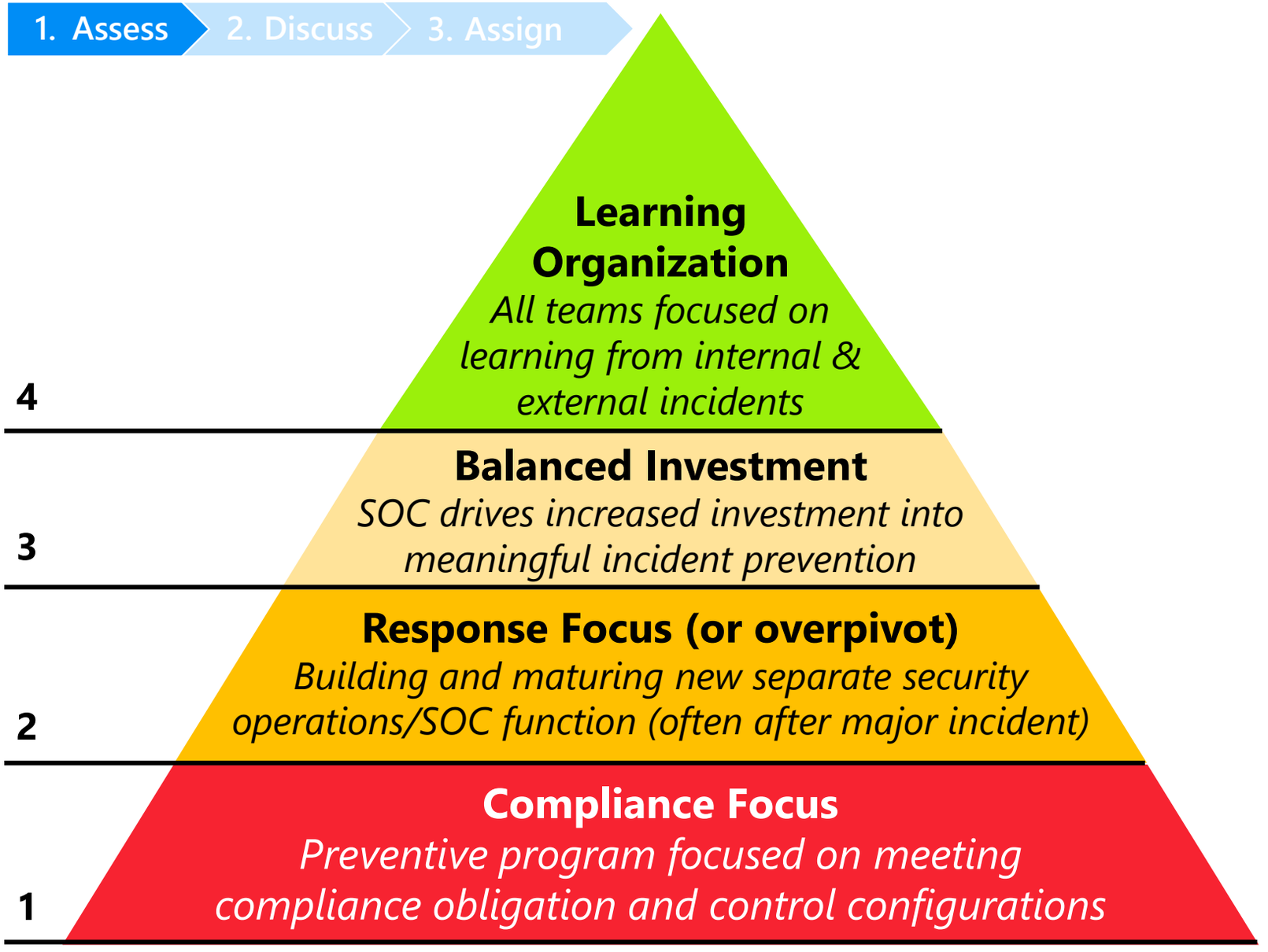
> *"Trust is knowing that when a team member does push you, they're doing it because they care about the team."*
> *— Patrick Lencioni*

1. **How are you investing into integrating security into business and IT processes?**
    a. **How prepared are organizational leaders to make security/risk decisions?**
    b. **How prepared are business line leaders to make security/risk decisions?**
2. **What would business and IT leaders say about the progress on that integration?**
3. **How is security budgeted? Proportional to IT? to organization's FTEs or revenue? Ad Hoc/Custom?**

Program Maturity Path

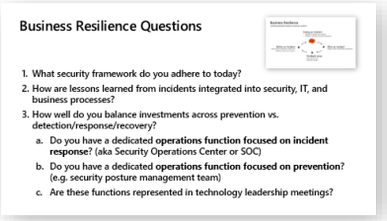
Business Resilience

1. Assess
2. Discuss
3. Assign



Discuss Improvement Steps

Business Resilience



1. Assess | **2. Discuss** | 3. Assign

4 — Learning Organization
All teams focused on learning from internal & external incidents

3 — Balanced Investment
SOC drives increased investment into meaningful incident prevention

2 — Response Focus (or overpivot)
Building and maturing new separate security operations/SOC function (often after major incident)

1 — Compliance Focus
Preventive program focused on meeting compliance obligation and control configurations

Click Here

- Continuous improvement of inter-team processes (and automation of them)
- Continuous learning culture across all teams
- Continuously empower business asset owners with security knowledge and accountability

Click Here

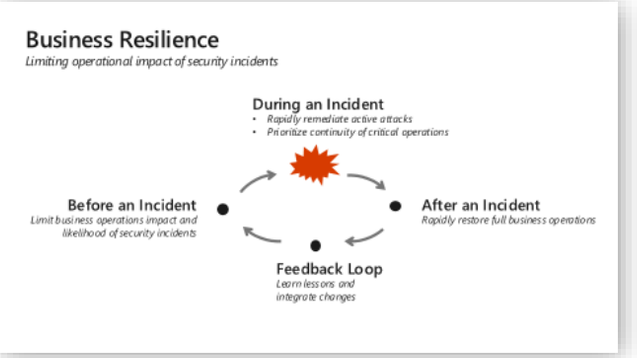
- Integrate incident response learnings into strategy and preventive controls
- Shift security left (earlier) in technical processes

Click Here

- Build incident response capability (Security Operations / SOC)

Next: *Assign Next Steps*

Business Resilience Questions



1. What security framework do you adhere to today?
2. How are lessons learned from incidents integrated into security, IT, and business processes?
3. How well do you balance investments across prevention vs. detection/response/recovery?
    a. Do you have a dedicated **operations function focused on incident response**? (aka Security Operations Center or SOC)
    b. Do you have a dedicated **operations function focused on prevention**? (e.g. security posture management team)
    c. Are these functions represented in technology leadership meetings?

Assign Next Steps (Part 1)

1. Assess
2. Discuss
3. Assign

Capture next step and who owns following up on it

#	Next Step	Point of Contact
1		
2		
3		
4		
5		

BACK TO MENU

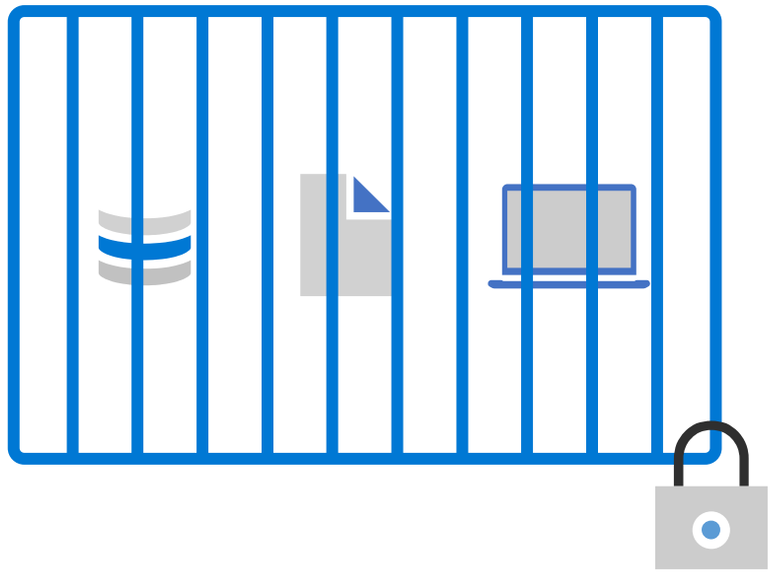
Review – Business Alignment Exercise

1. **Assess**
   Current State
2. **Discuss**
   Focus Areas
3. **Assign**
   Next Steps

Next Up:
1C – Security Disciplines

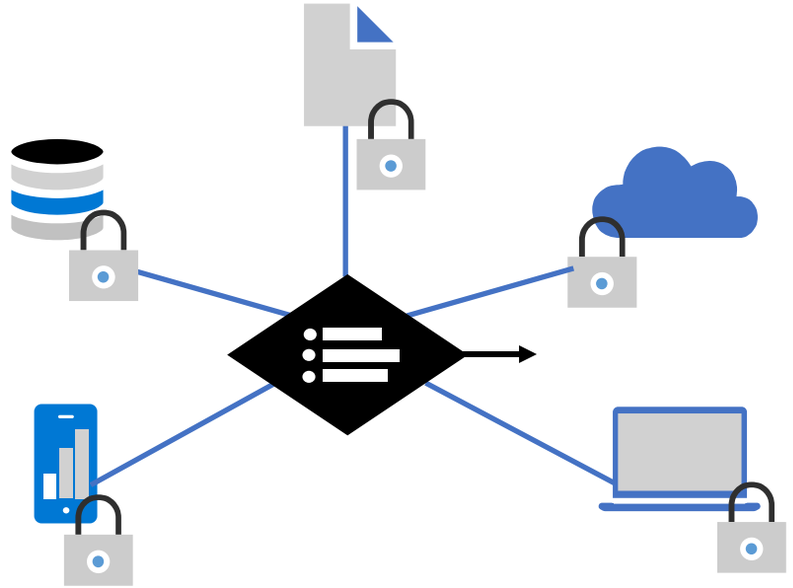
Zero Trust principles transform access control

Secure assets wherever they go



Classic Approach

Restrict everything to a ‘secure’ network

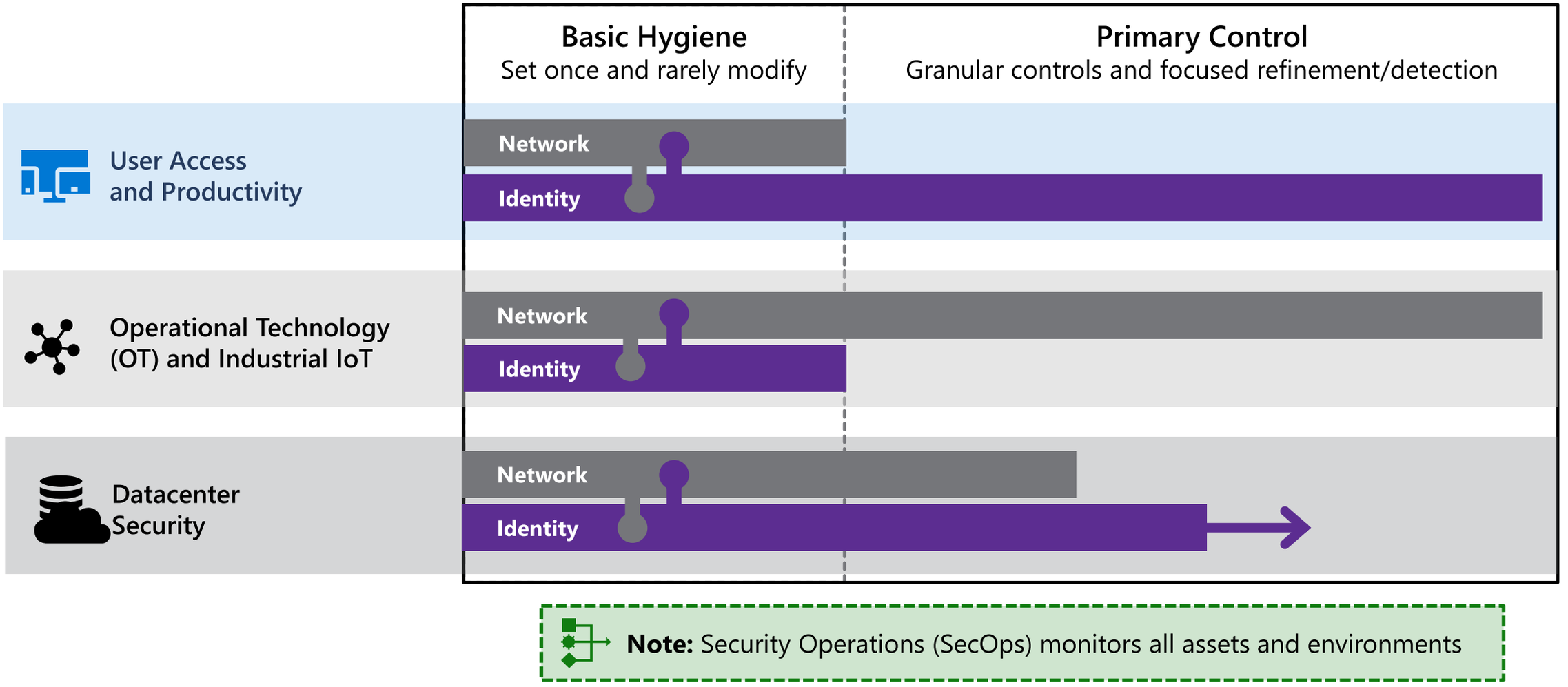


Zero Trust

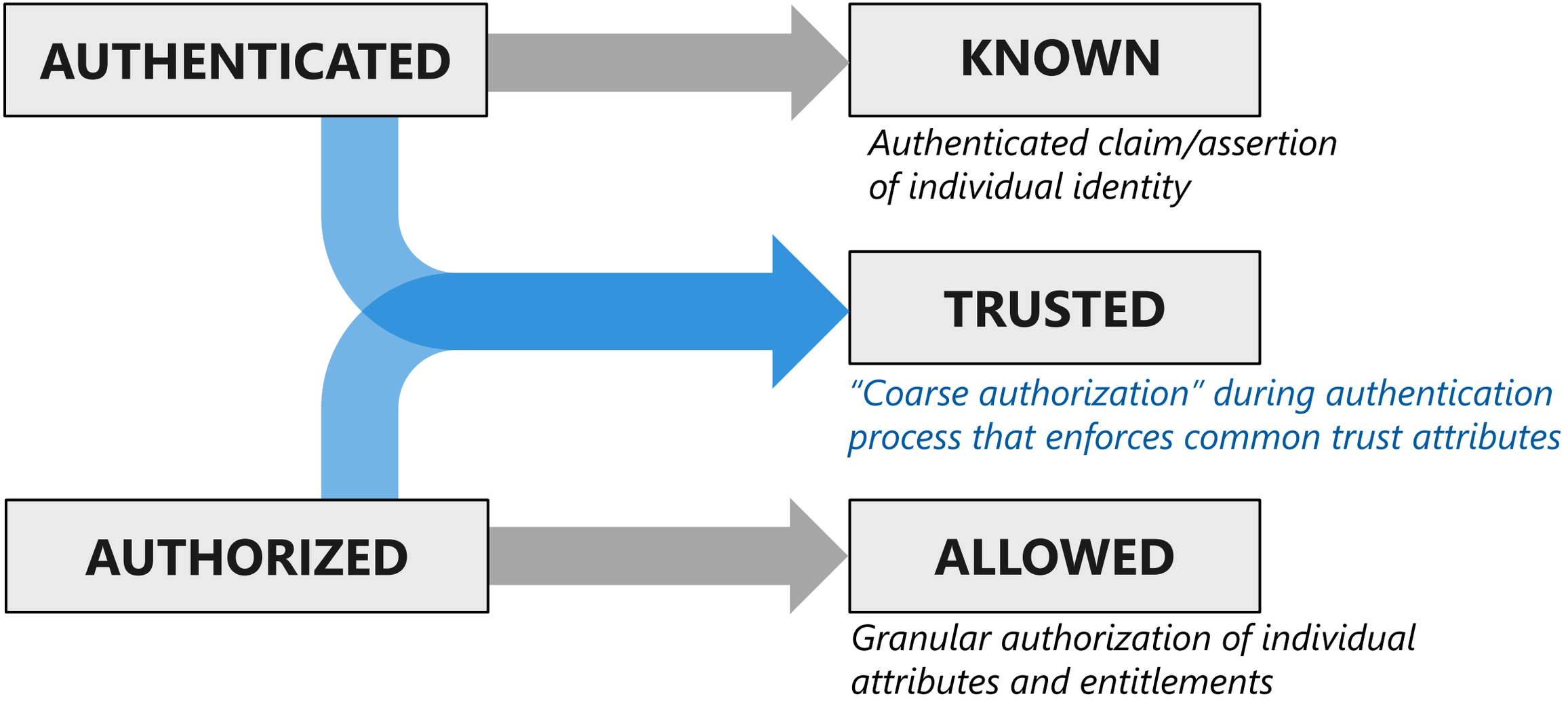
Protect assets anywhere with central policy

Blend network and identity access controls

Choose the right tool for the job

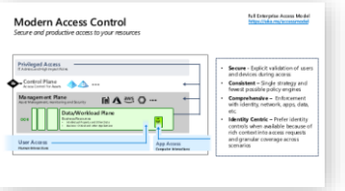


Evolution of Authentication and Authorization



Air travel analogy

High Level Access Model



I WANT TO FLY

Please show me your ID

Can we trust this person?

✓ KNOWN
✓ TRUSTED

✓ ALLOWED

Airport Security
(Identity System)

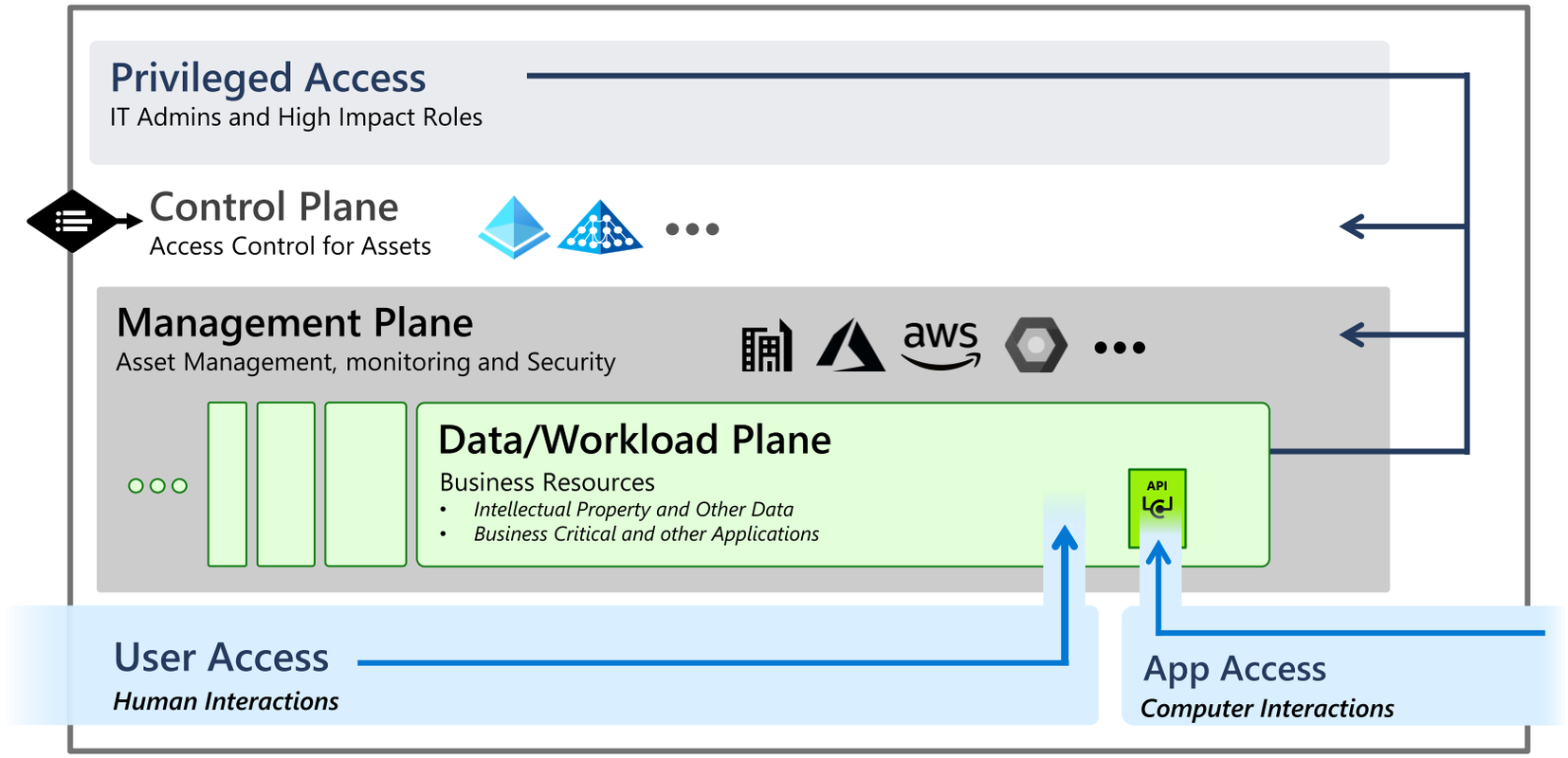
What city? Seat? Luggage?

Airline
(Application)

Modern Access Control

Secure and productive access to your resources

Full Enterprise Access Model
https://aka.ms/accessmodel



- **Secure -** Explicit validation of users and devices during access
- **Consistent –** Single strategy and fewest possible policy engines
- **Comprehensive –** Enforcement with identity, network, apps, data, etc.
- **Identity Centric –** Prefer identity controls when available because of rich context into access requests and granular coverage across scenarios

BACK TO MENU

Review – Access Control

Zero Trust Approach Required

- *Known, Trusted, and Allowed before accessing assets*
- *Blend Identity + Network together into single approach*
- *Strong Authentication is top priority*

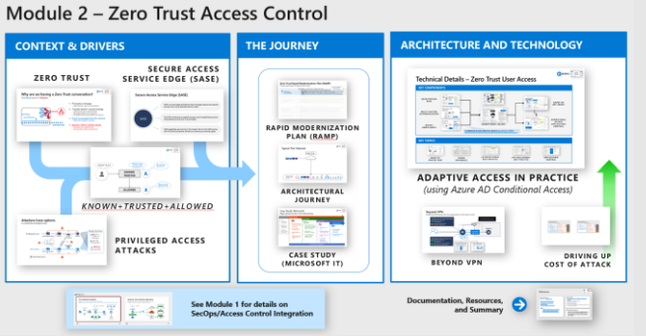
Next Up:

1C – Access Control, Security Operations, Asset Protection, Security Governance, Innovation Security

More Details in
Module 2 – Secure Identities and Access

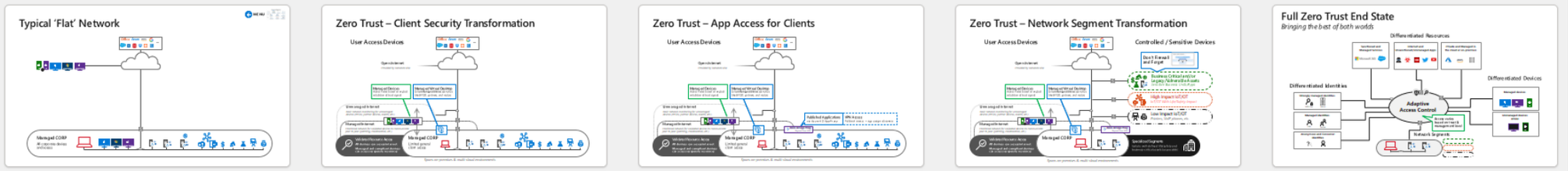
Secure Access Service Edge (SASE)

Transformational Forces & end to end architecture

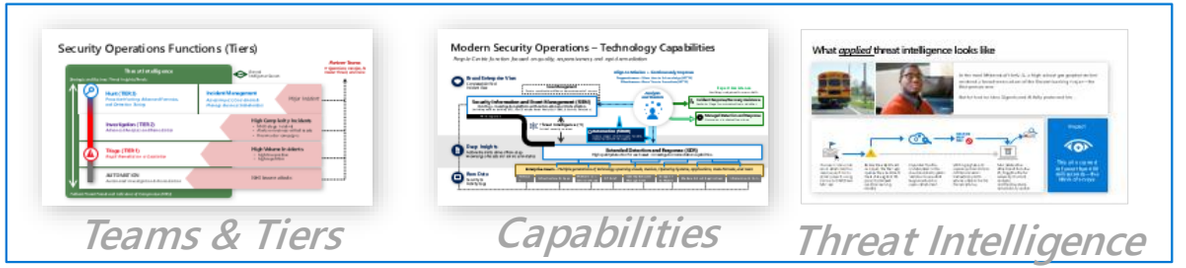


Reference Plans

End to end architecture journey with Zero Trust Principles



Security Operations



Teams & Tiers *Capabilities* *Threat Intelligence*

Mission

Reduce organizational risk by limiting the time successful attackers can access enterprise assets (dwell time) through rapid detection and response.

Key Cultural Elements

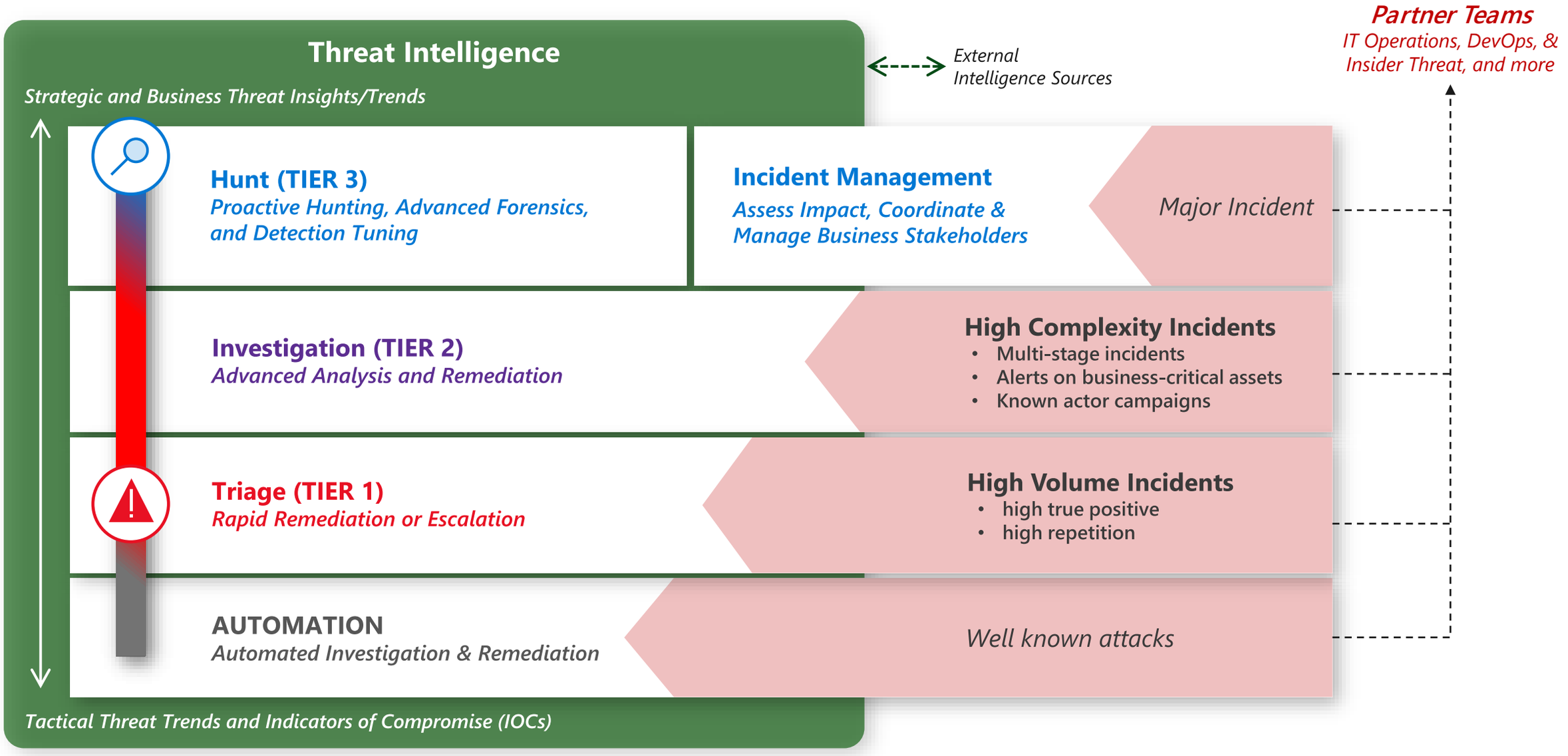
- Mission Alignment
- Continuous Learning
- Teamwork

Business Leadership Touchpoints

Key Measurements

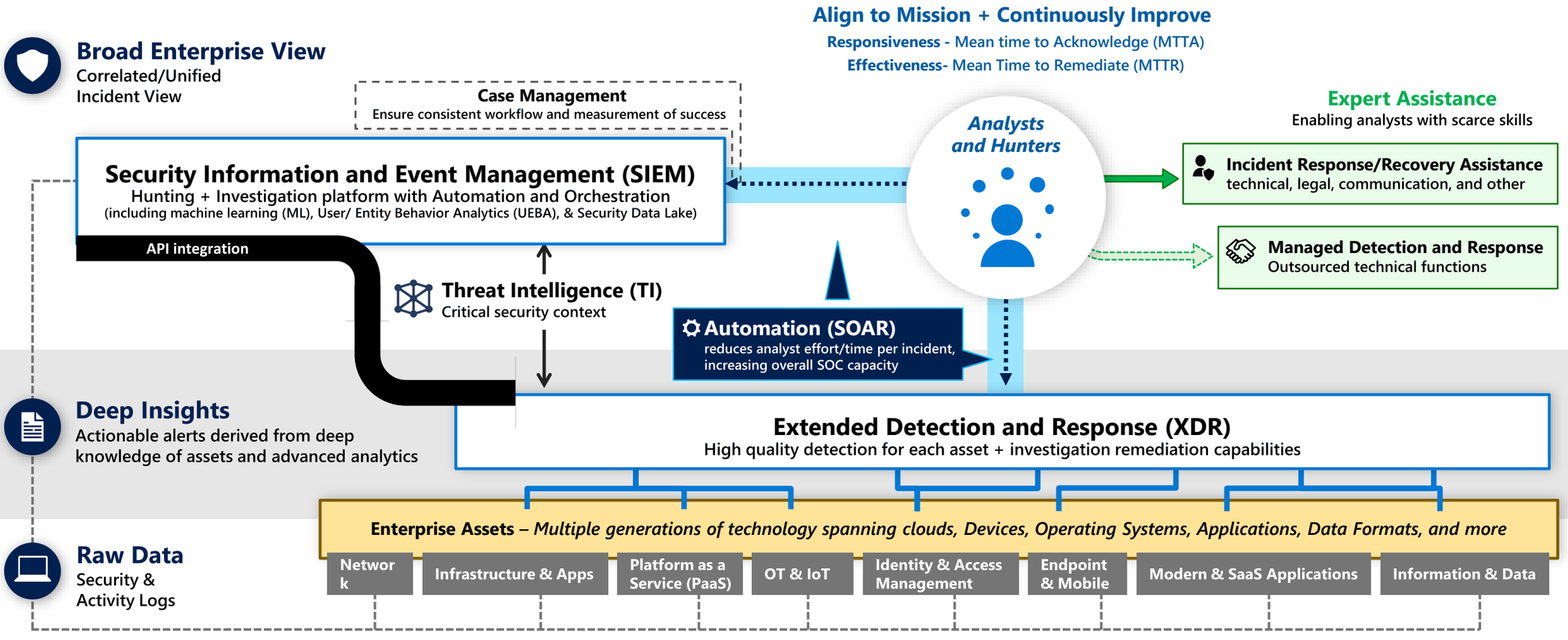
- **Effectiveness -** Mean Time to Remediate (MTTR)
- **Responsiveness -** Mean time to Acknowledge (MTTA)

Security Operations Functions (Tiers)

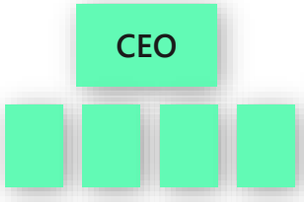


Modern Security Operations – Technology Capabilities

People-Centric function focused on quality, responsiveness, and rapid remediation



SecOps interactions with leadership



PRACTICE EXERCISES / TABLETOPS

Leadership joins to build awareness, muscle memory, and improve process

BUSINESS PRIORITIES

Inform security teams of critical business assets and priorities

MAJOR INCIDENT STATUS

Inform business stakeholders of incidents and status

Review – Security Operations

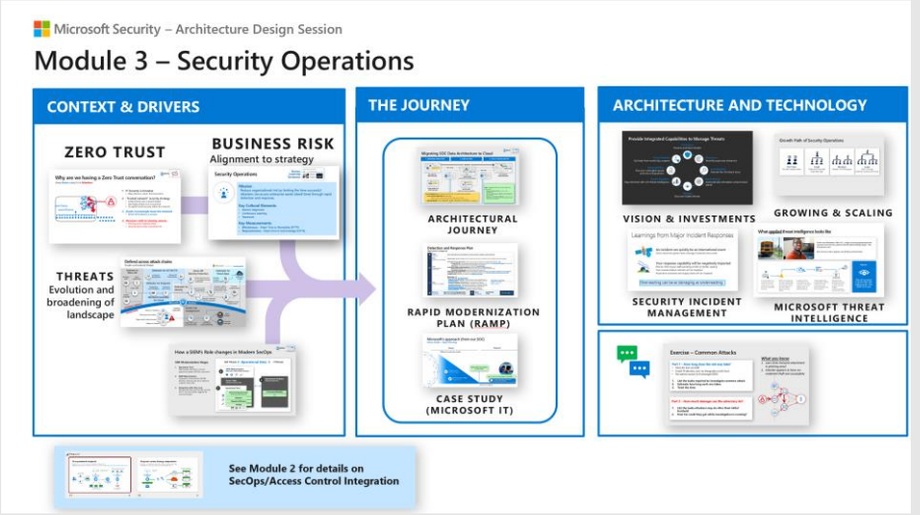
BACK TO MENU

- Focus on reducing Mean Time to Recover (MTTR)
  - *Limits attacker access, which reduces organizational risk*
- Drive Collaborative Culture
  - *Within security operations and with other teams*
- Define touchpoints with business

Next Up:

1C – Access Control, Security Operations, Asset Protection, Security Governance, Innovation Security

More Details in
Module 4 Modern Security Operations



Asset Protection

Effectiveness requires prioritization and consistency/automation for scale

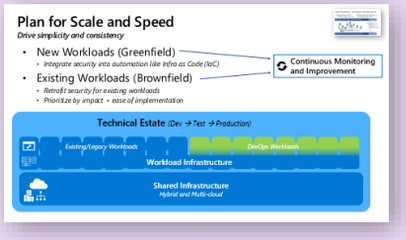
Discovering
Business-Critical Assets

1. Focus on Business-Critical Assets

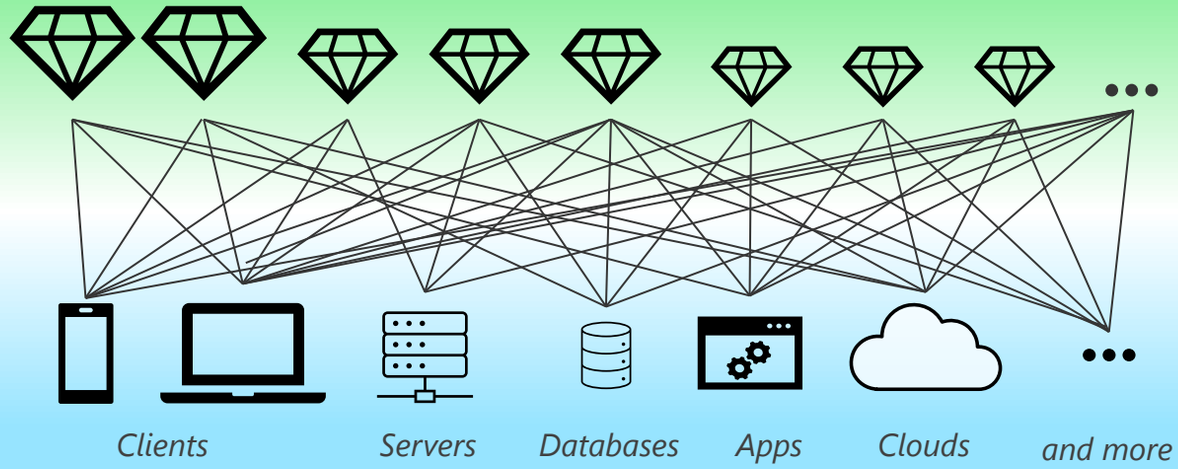
Top-Down Discovery Identifying business critical assets starts with understanding business priorities, assets, and risks

New Conversations - This often involves asking and answering questions that haven't been asked before
Can start with aka.ms/backup

2. Plan for Scale and Speed



Business assets *have intrinsic value to the business*



Technical assets *host and run those assets*

Example: *Retail Website*

- **Business** = Enablement of online customers purchases
- **Technical** = Servers, Databases, Containers, Administrative workstations & identities, Network connections, customer accounts, and more

Plan for Scale and Speed

Drive simplicity and consistency

- New Workloads (Greenfield)
  - *Integrate security into automation like Infra as Code (IaC)*
- Existing Workloads (Brownfield)
  - *Retrofit security for existing workloads*
  - *Prioritize by impact + ease of implementation*

Continuous Monitoring and Improvement

Technical Estate *(Dev → Test → Production)*

Existing/Legacy Workloads

DevOps Workloads

Workload Infrastructure

Shared Infrastructure

Hybrid and Multi-cloud

BACK TO MENU

Review – Asset Protection

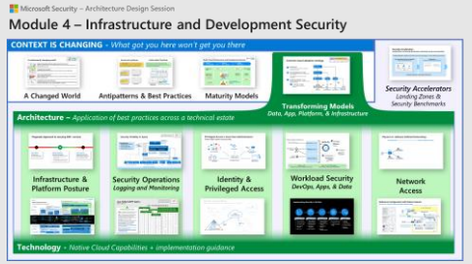
- **Identify Business Critical Assets with top-down approach**
  - *Ask and answer the hard questions on what matters most*
- **Plan for Scale and Speed**
  - *Partner security teams with IT/OT Operations and DevOps teams*
  - *Greenfield – integrate to prevent creation of more risk*
  - *Brownfield – burn down technical debt to reduce risk*

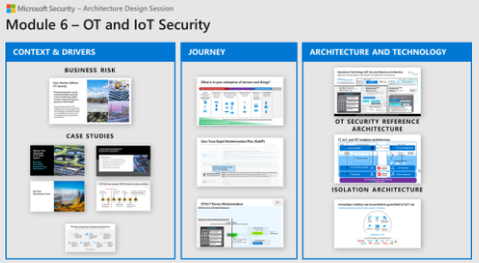
Next Up:

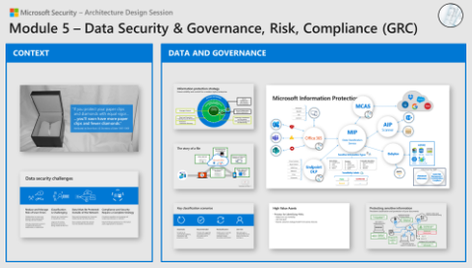
1C – Access Control, Security Operations, Asset Protection, Security Governance, Innovation Security

More Details in

Module 4 – Infrastructure & Development
Module 5 – Data Security & Governance, Risk, Compliance (GRC)
Module 6 – IoT and OT Security







Asset Protection – Get Secure and Stay Secure

Get Secure – Apply security standards

- Protect data at rest and in transit
- Asset specific configurations & protections

Stay Secure – Ongoing Asset Maintenance

- Keep software/firmware/etc. patched & up to date
- Keep software and protocols current

Standards - *Architecture, Policy, and Guidance for each asset type*

Continuously Improve

- Standards
- Discovery Mechanisms
- Application and automation of standards

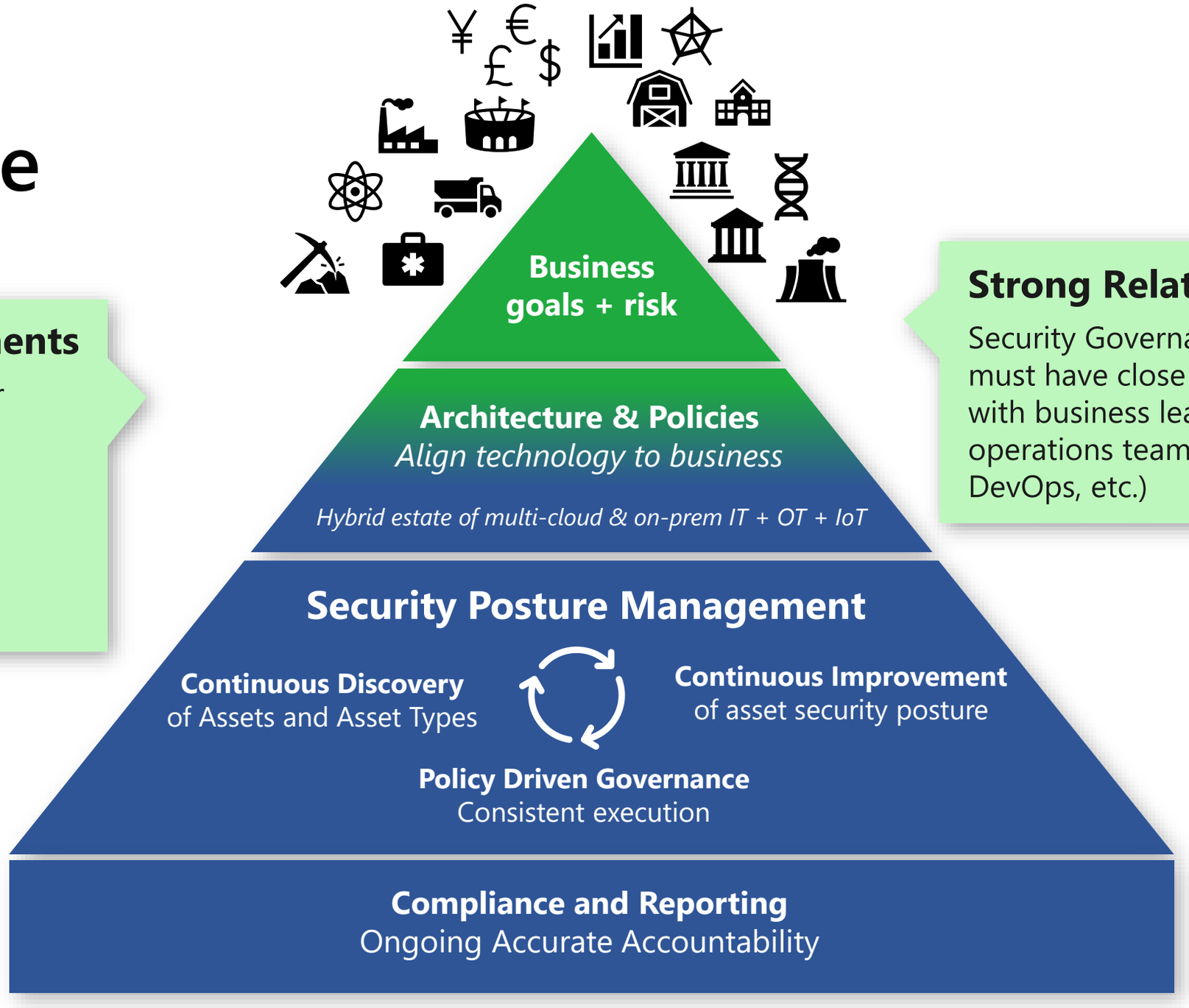
Automation – *Integrate security into new and existing automation*

Security Governance

Governance Components

Provide unifying services for security, technology, and business teams

- ***Architecture***
- ***Posture Management***
- ***Risk and Compliance***
- ***Threat Intelligence***

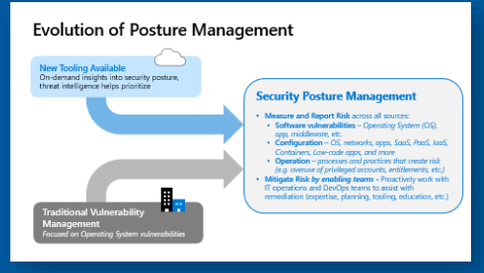


Strong Relationships

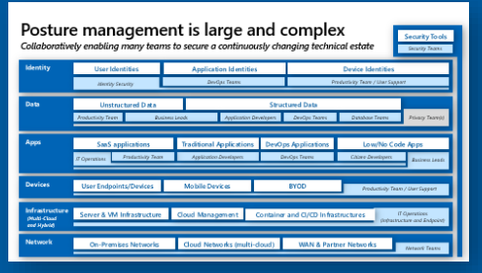
Security Governance Teams must have close relationships with business leaders and operations teams (IT, Security, DevOps, etc.)

Posture Management is critical to continuous improvement

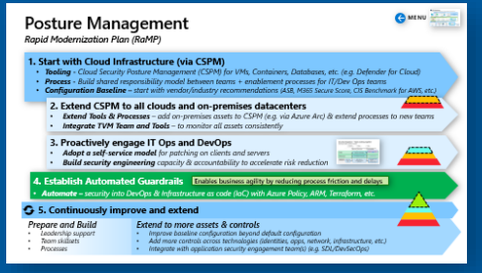
Security Posture Management



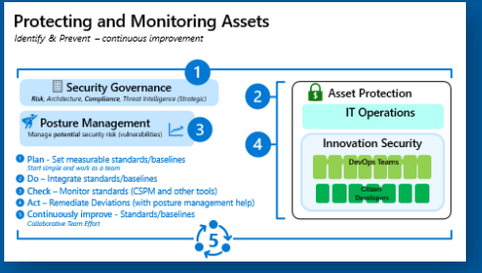
Origin & Evolution



Ideal End State



Rapid Modernization Plan (RaMP)



Integration into Process

Protecting and Monitoring Assets

Identify & Prevent – continuous improvement

1

Security Governance

***Risk**, Architecture, **Compliance**, Threat Intelligence (Strategic)*

Posture Management

Manage **potential** security risk (vulnerabilities)

3

2

4

Asset Protection

IT Operations

Innovation Security

DevOps Teams

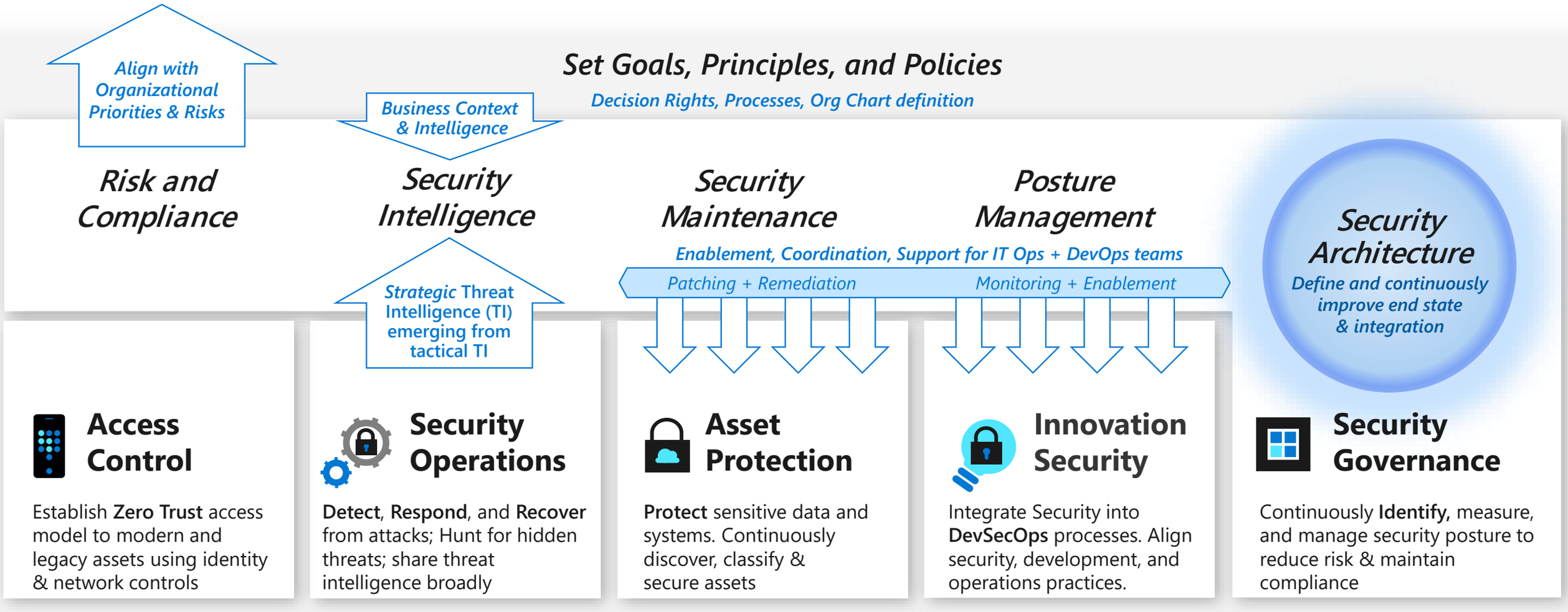
Citizen Developers

1. **Plan** - Set measurable standards/baselines
   Start simple and work as a team
2. **Do** – Integrate standards/baselines
3. **Check** – Monitor standards (CSPM and other tools)
4. **Act** – Remediate Deviations (with posture management help)
5. **Continuously improve** - Standards/baselines
   Collaborative Team Effort

5

Security Governance

Key Functions and Relationships



BACK TO MENU

Review – Security Governance

- **Role of Security Governance**
  - *Bridges business with technical implementation*
  - *Provides unifying services across security and technology*
    - ***Architecture*** *– Define ideal end state and integration, drive continuous improvement*
    - ***Posture Management*** *– Enable and support risk mitigation efforts across the organization*
    - ***Risk and Compliance*** *– Align security with organizational priorities & risks, manage policies*
    - ***Threat Intelligence*** *– Provide context to stakeholders in business, IT, and security*
- **Proactive security posture management is essential to reducing risk**
  - *Provides enablement for Ops teams to support meeting policy and standard requirements*

Next Up:

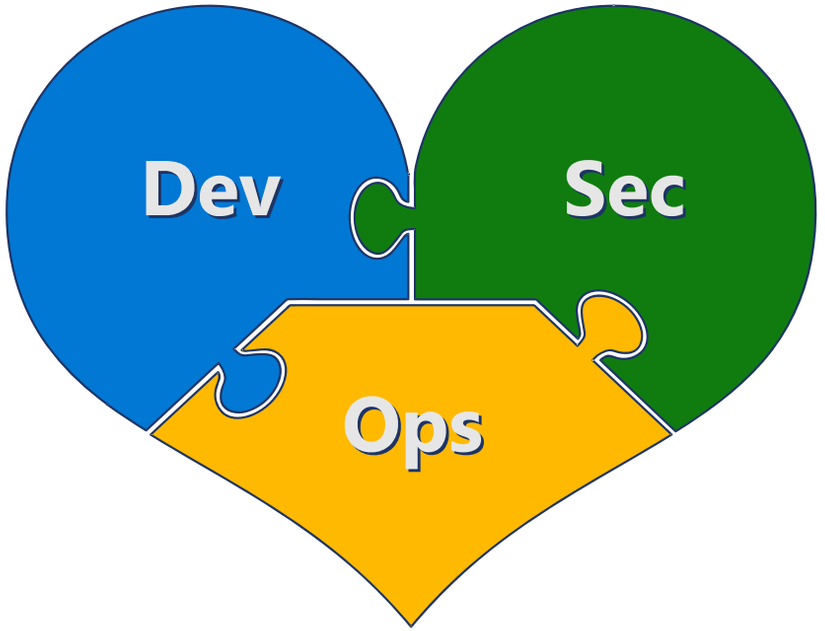
1C – Access Control, Security Operations, Asset Protection, Security Governance, Innovation Security

Innovation Security

Secure innovation is the beating heart of an organization in today's digital landscape

Responsive to Needs

Meets business and customer requirements for market relevance



Safe and Secure

Provides confidentiality, integrity, & availability + regulatory compliance

Quality and Performance

meets the quality, speed, scalability, reliability, and other expectations

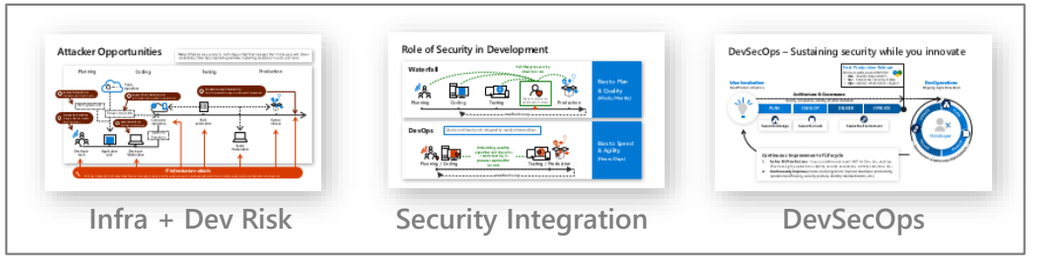
Evolution of Innovation Security

DevOps Processes
Agile rapid delivery enables ability to continuously mitigate security risks and continuously refine security processes

Traditional Application Security
Focused on generating reports with scanning tools

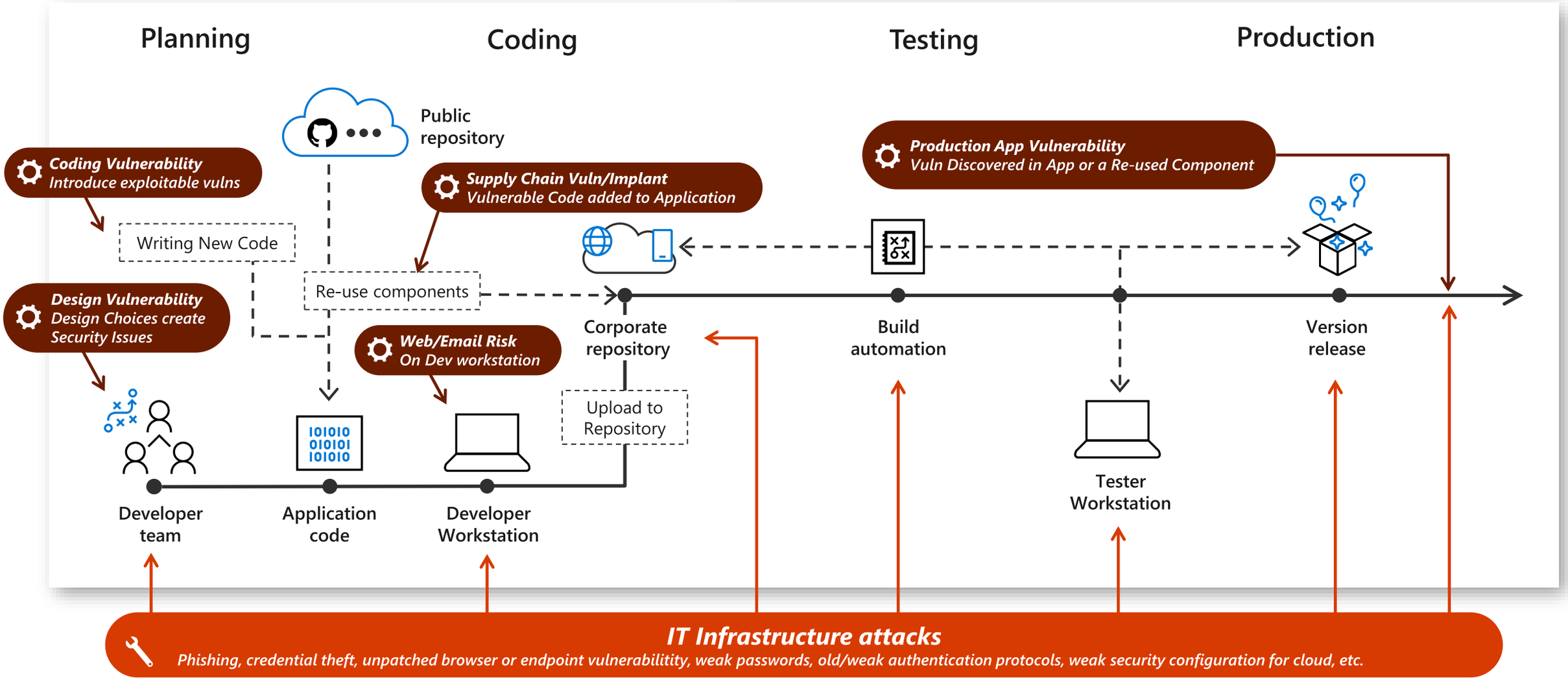
Innovation Security

- Focused on rapid and secure development / low friction
  - Focused on high quality results
  - **Integrated into development process** – automate using CI/CD processes, reporting bugs through normal processes, etc.
- **Mitigate Risk *by enabling teams*** - Proactively work with developers and DevOps teams to educate, evangelize, and assist with remediation (expertise, planning, tooling, education, etc.)



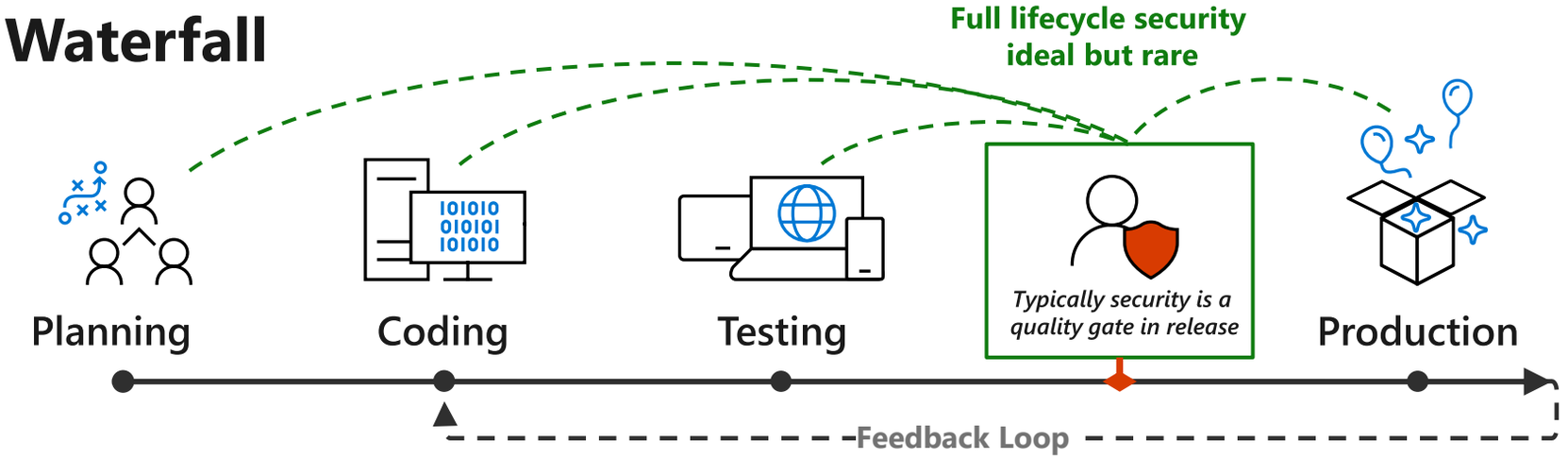
Attacker Opportunities

Note: Attackers may conduct a multi-stage attack that increases their illicit access with stolen credentials, stolen keys, implanting malware, implanting backdoors in code, and more



Role of Security in Development

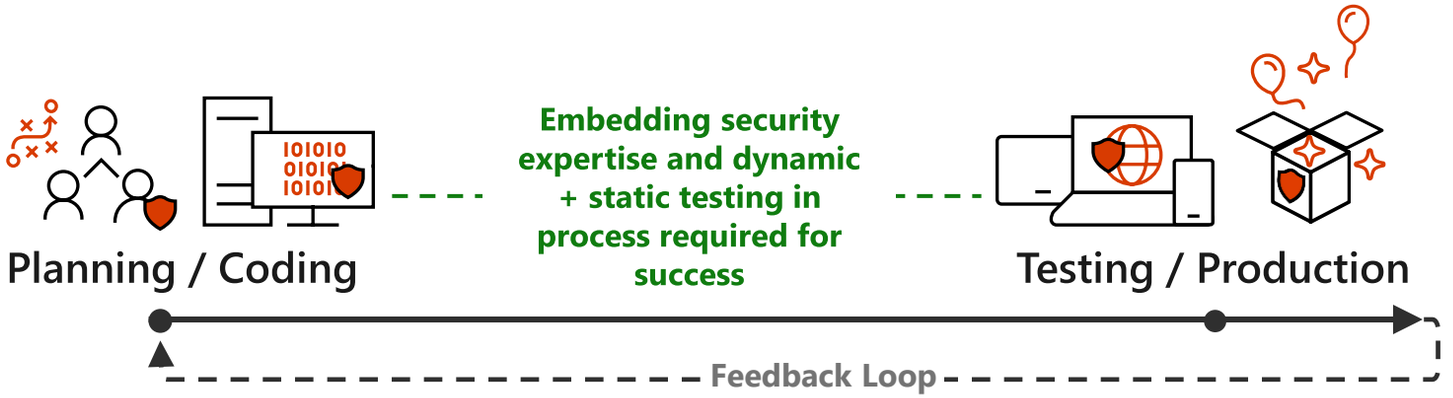
Waterfall



Bias to Plan & Quality *(Weeks/Months)*

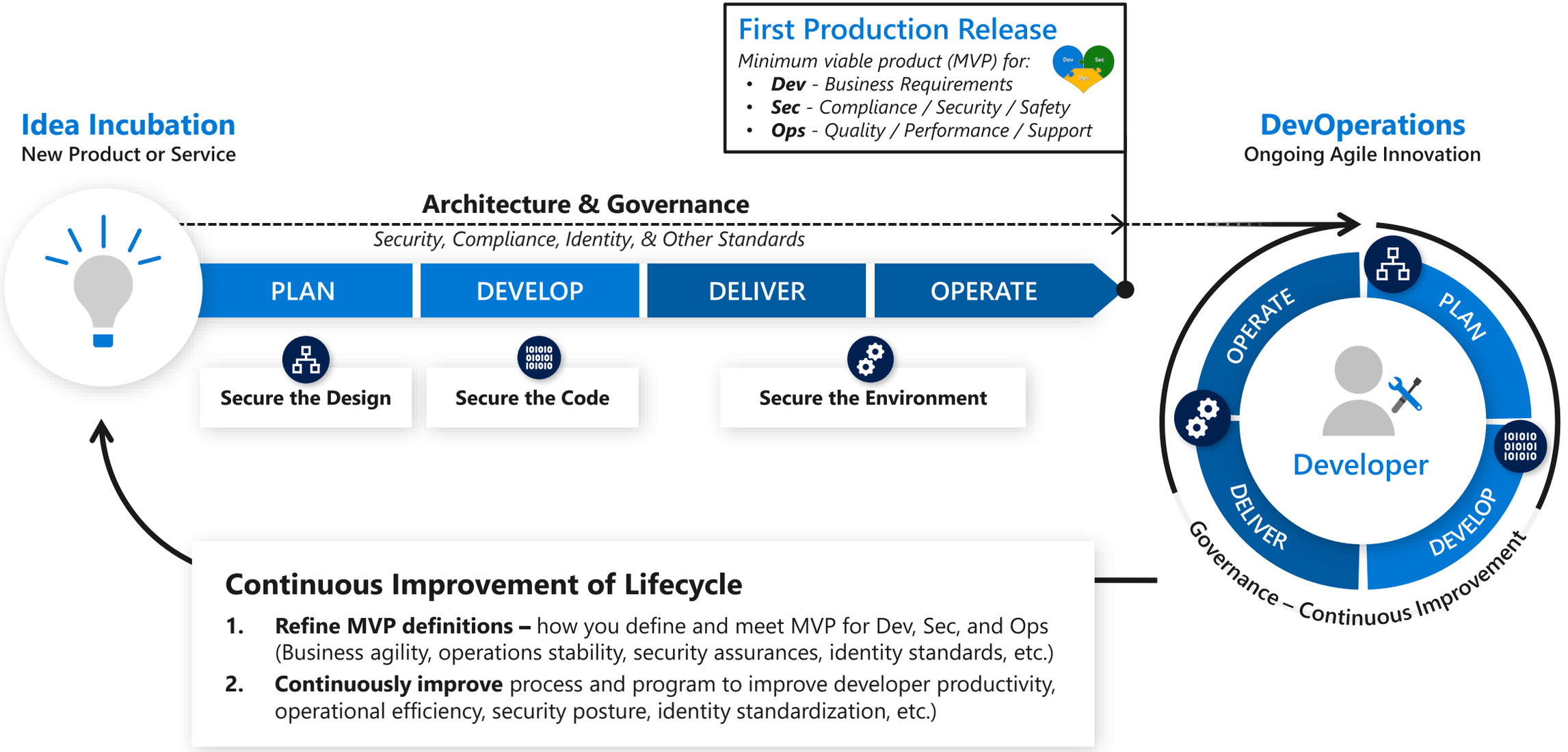
DevOps

Quality and Security risk mitigated by rapidly release of fixes



Bias to Speed & Agility *(Hours/Days)*

DevSecOps – Sustaining security while you innovate



Review – Innovation Security

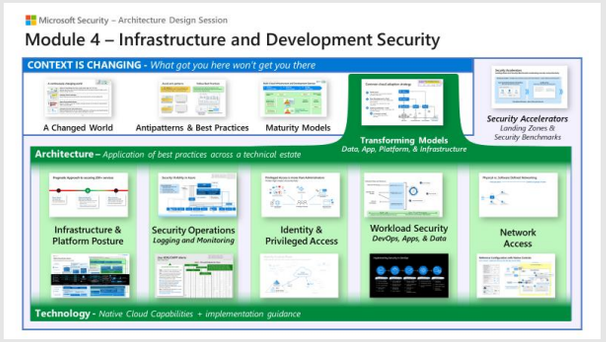
BACK TO MENU

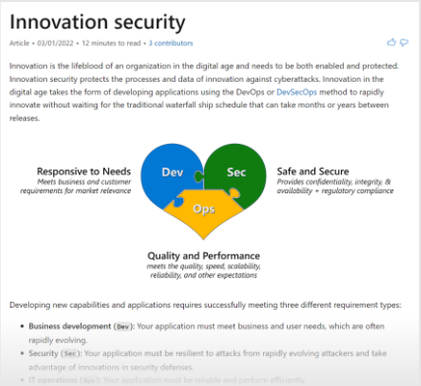
- Successful innovation requires integrating **Dev**elopment, **Sec**urity, and **Ops** (Operations)
- Traditional Application Security Evolves
  - *Focus on high quality findings (actionable, low false positive rate)*
  - *Focus on enablement and seamless integration into development process*

Next Up:
Security Governance Exercise

More Details in

- *Module 4 Infrastructure & Development*
- *CAF Secure – Innovation Security*
  aka.ms/CAFSecure-InnovationSecurity



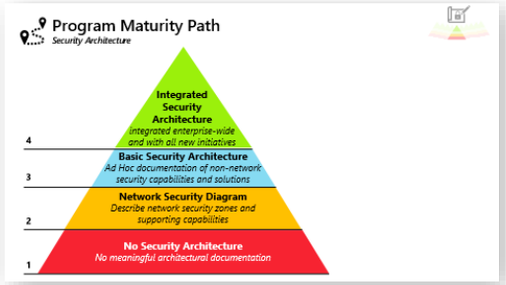


Security Governance Exercise

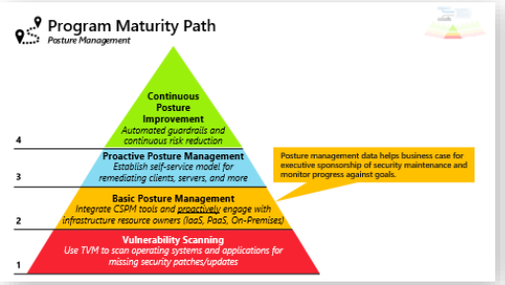
BACK TO MENU

1. Assess Current State → **2. Discuss** Focus Areas → **3. Assign** Next Steps

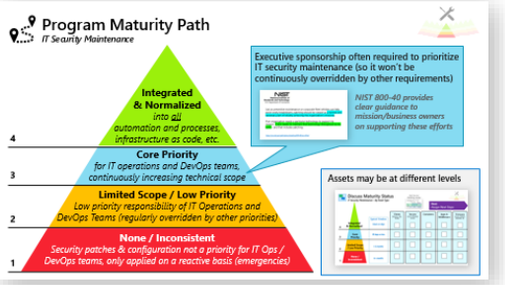
Security Architecture



Posture Management



Security Maintenance



Security Governance

Continuously **Identify**, measure, and manage security posture to reduce risk & maintain compliance

CISO workshop *and* Security ADS Module 1 *(same exercise)*

Access Control

Establish **Zero Trust** access model to modern and legacy assets using identity & network controls

Security ADS Module 2

Security Operations

Detect, **Respond**, and **Recover** from attacks; Hunt for hidden threats; share threat intelligence broadly

Security ADS Module 3

Asset Protection

Protect sensitive data and systems. Continuously discover, classify & secure assets

Security ADS Modules 4 & 6

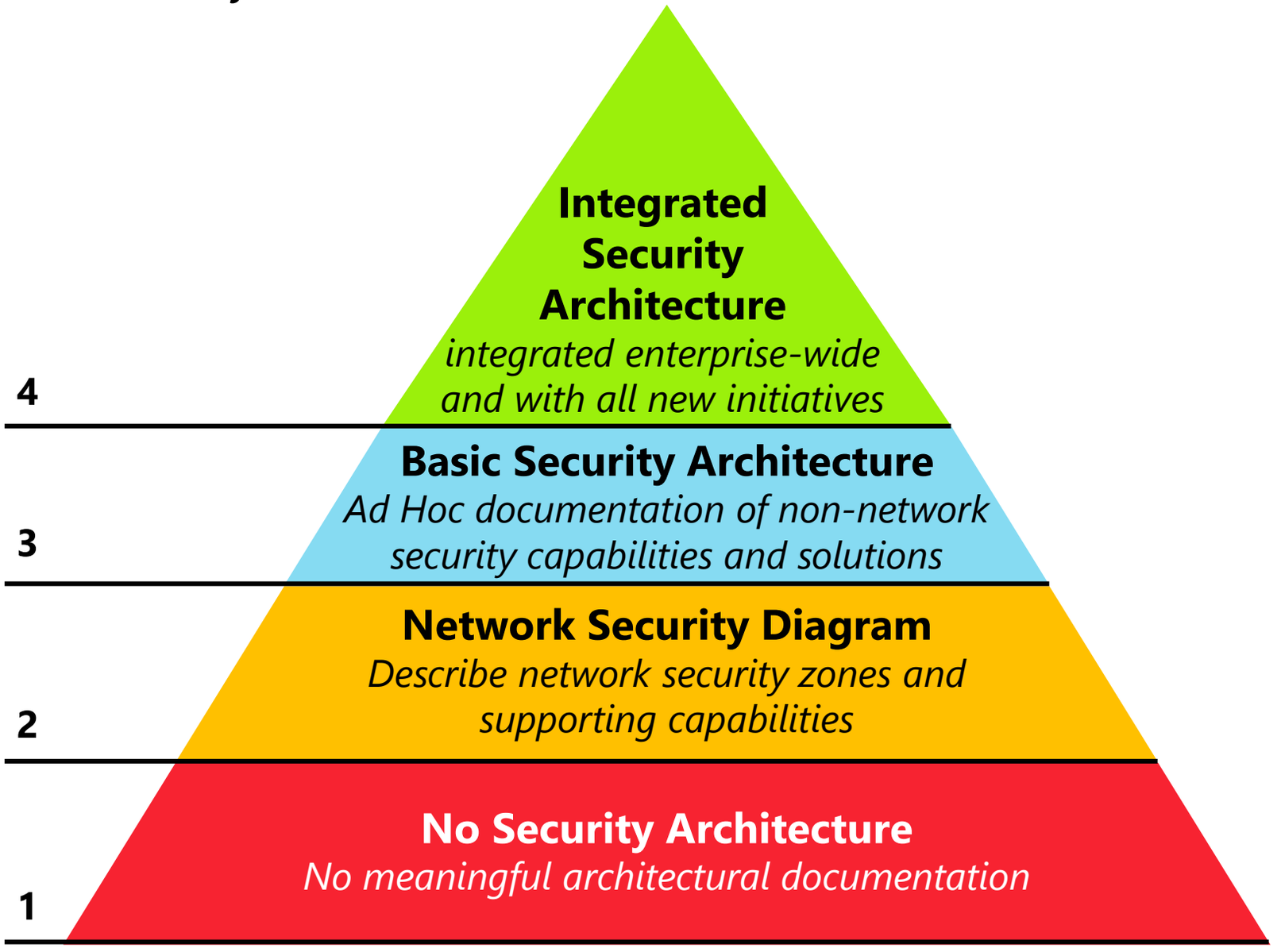
Innovation Security

Integrate Security into **DevSecOps** processes. Align security, development, and operations practices.

Security ADS Module 4

Program Maturity Path

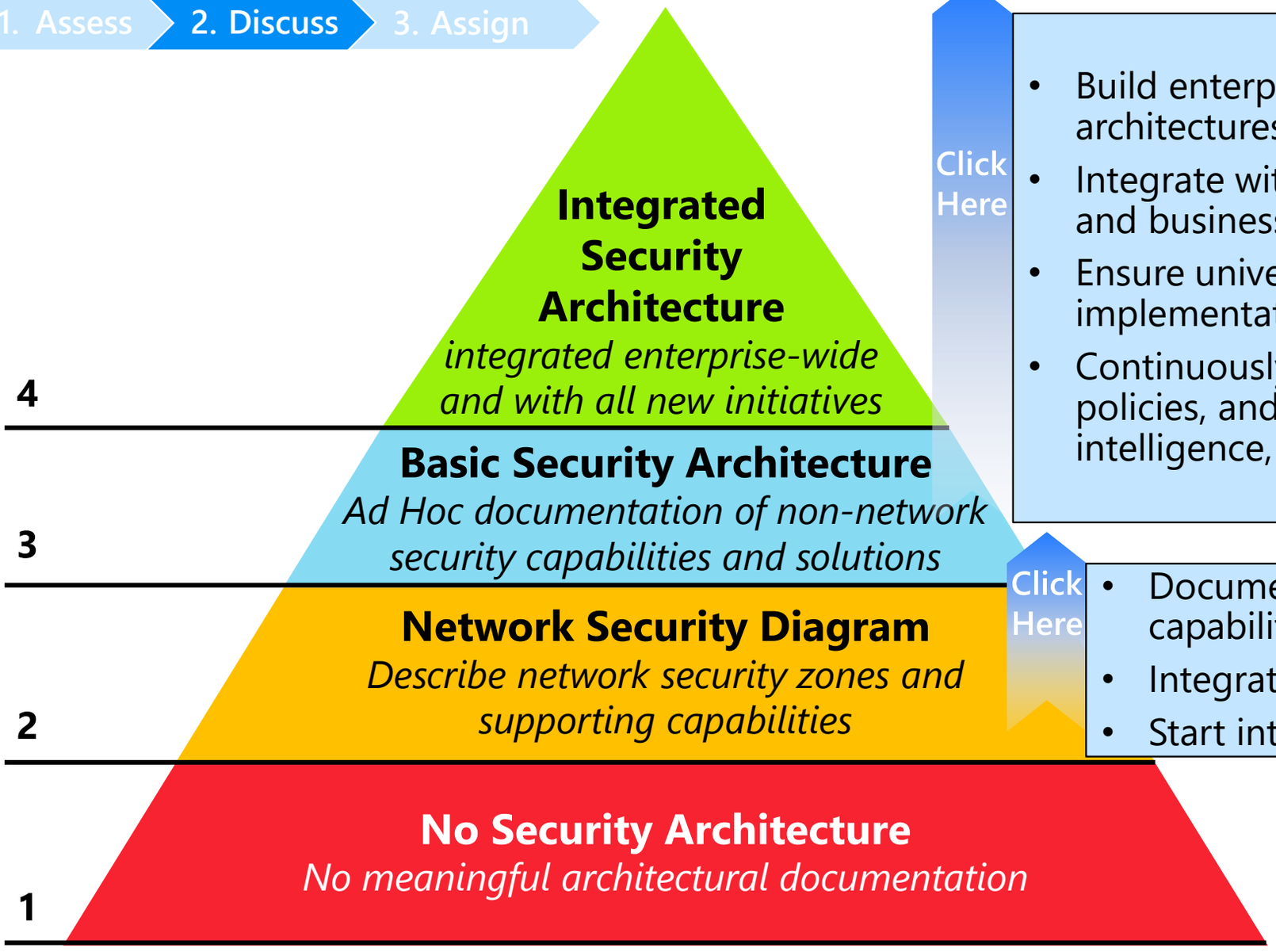
Security Architecture



Discuss Improvement Steps

Security Architecture

1. Assess > 2. Discuss > 3. Assign



Click Here

- Build enterprise-wide integrated security architectures (diagrams and documentation)
- Integrate with enterprise architecture (if present) and business architectures (as appropriate)
- Ensure universal adoption by engineering and implementation teams (IT, OT, IoT, DevOps)
- Continuously update and refine architectures, policies, and standards based on threats, business intelligence, technical platforms, and more

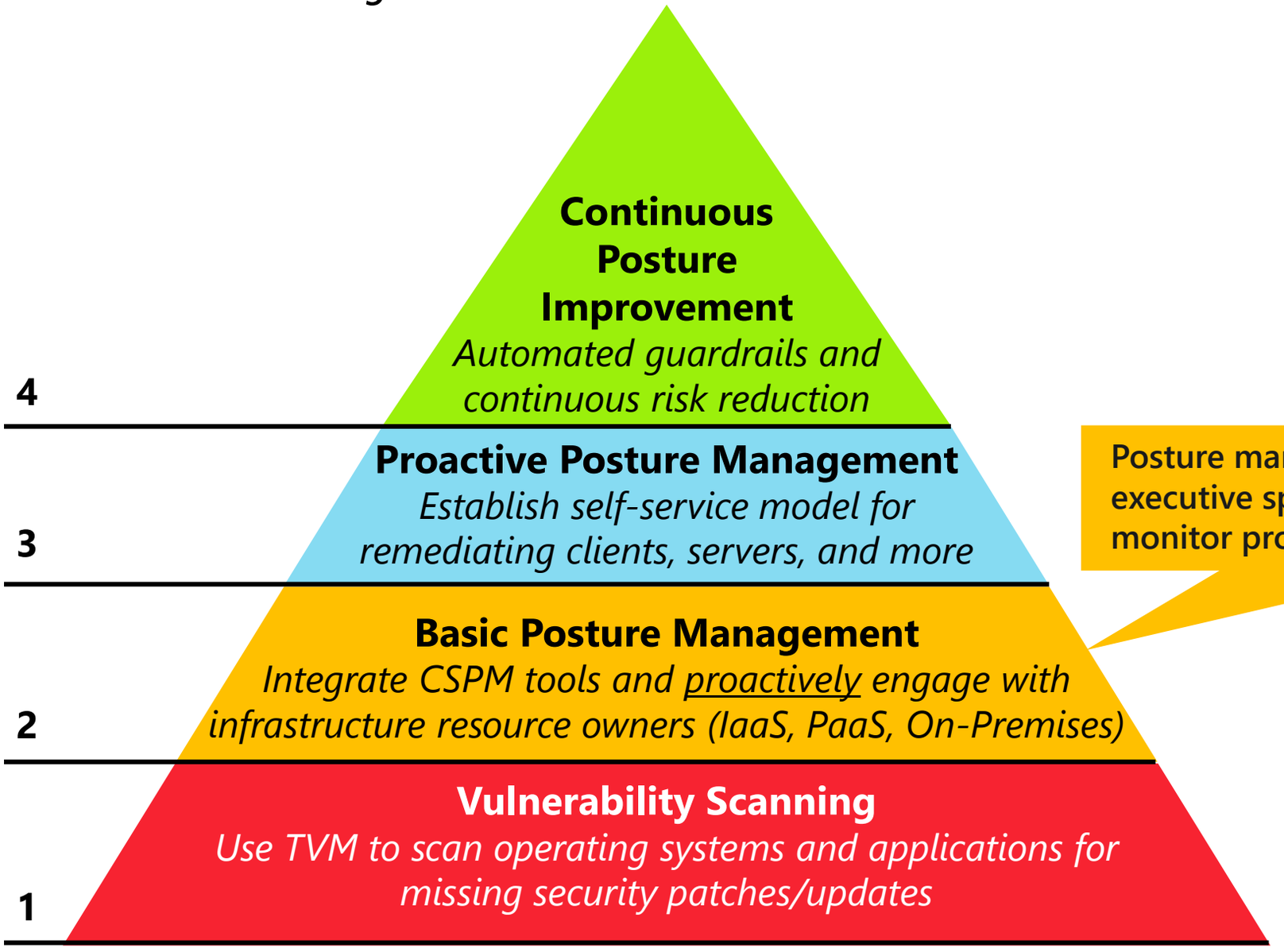
Click Here

- Document enterprise-wide security capabilities (beyond network)
- Integrate security in new enterprise solutions
- Start integrating with standards and policies

Next: *Posture Management*

Program Maturity Path

Posture Management

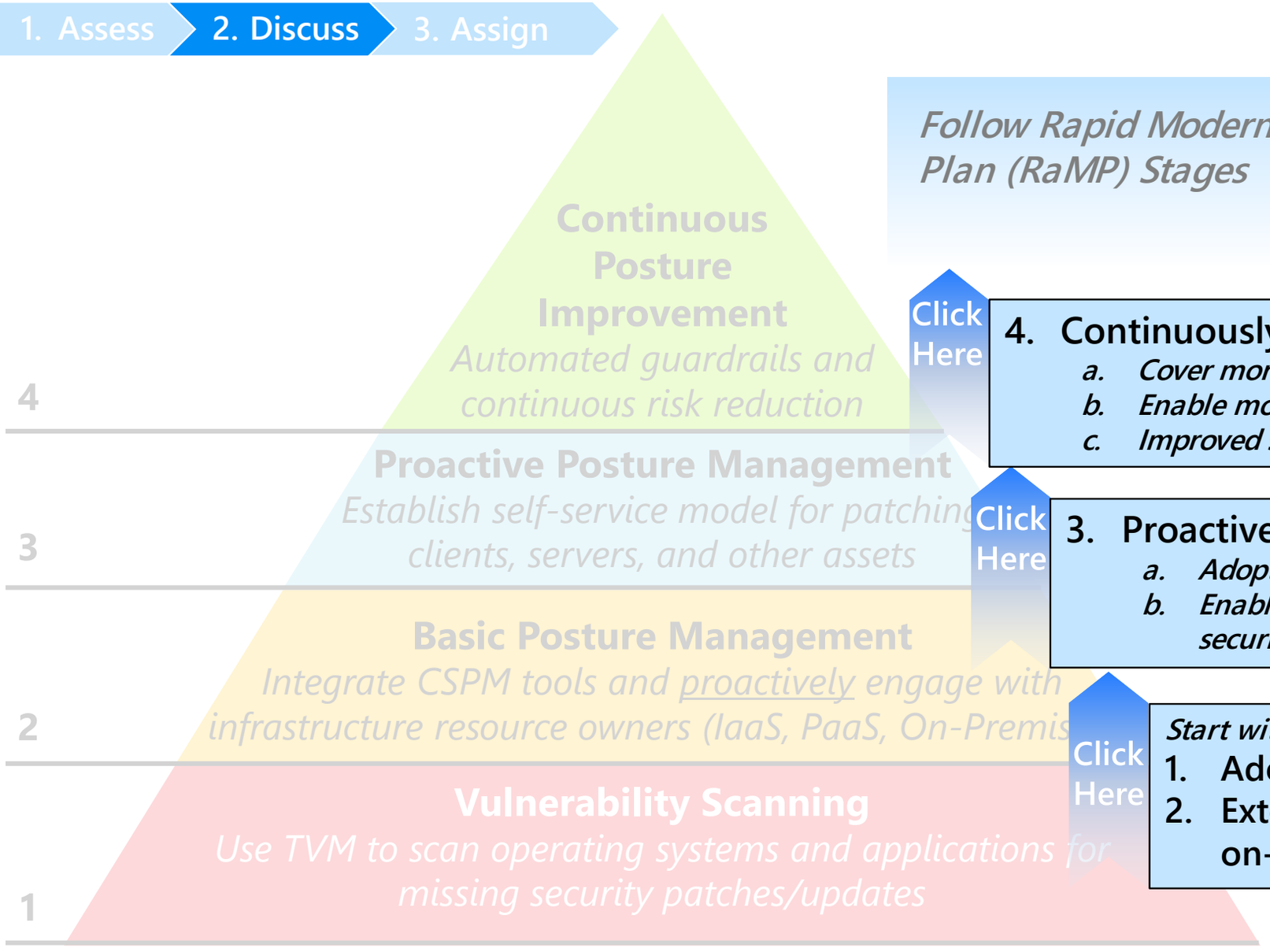


Posture management data helps business case for executive sponsorship of security maintenance and monitor progress against goals.

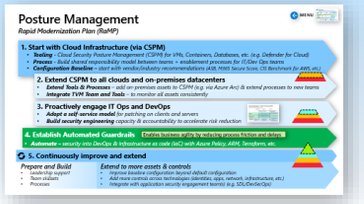
Discuss Improvement Steps

Posture Management

1. Assess | 2. Discuss | 3. Assign



Follow Rapid Modernization Plan (RaMP) Stages



Click Here

4. Continuously improve and extend
   a. *Cover more resources and resource types*
   b. *Enable more teams*
   c. *Improved support mechanisms and processes*

Click Here

3. Proactively engage IT Ops and DevOps
   a. *Adopt Self-service patching model*
   b. *Enable IT Ops and DevOps teams (with training, security engineering, and advocacy)*

Click Here

Start with Cloud Security Posture Management:

1. Adopt CSPM for Cloud Infrastructure
2. Extend CSPM to all clouds and on-premises datacenters

Next: *IT Security Maintenance*

Program Maturity Path

IT Security Maintenance

4 **Integrated & Normalized**
into <u>all</u> automation and processes, infrastructure as code, etc.

3 **Core Priority**
for IT operations and DevOps teams, continuously increasing technical scope

2 **Limited Scope / Low Priority**
Low priority responsibility of IT Operations and DevOps Teams (regularly overridden by other priorities)

1 **None / Inconsistent**
Security patches & configuration not a priority for IT Ops / DevOps teams, only applied on a reactive basis (emergencies)

Executive sponsorship often required to prioritize IT security maintenance (so it won't be continuously overridden by other requirements)


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

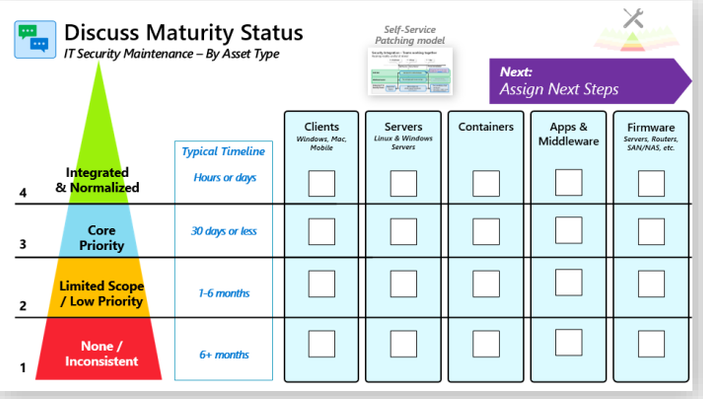
Just as preventive maintenance on corporate fleet vehicles can help avoid costly breakdowns, patching should be viewed as a normal and necessary part of reliably achieving the organization's missions.

If an organization needs a particular technology to support its mission, it also needs to maintain that technology throughout its life cycle – and that includes patching.

https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

NIST 800-40 provides clear guidance to mission/business owners on supporting these efforts

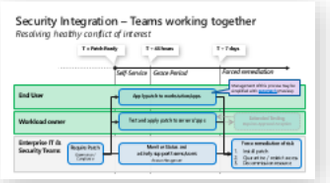
Assets may be at different levels



Discuss Maturity Status

IT Security Maintenance – By Asset Type

Self-Service Patching model



Next:
Assign Next Steps

		Typical Timeline	Clients *Windows, Mac, Mobile*	Servers *Linux & Windows Servers*	Containers	Apps & Middleware	Firmware *Servers, Routers, SAN/NAS, etc.*
4	**Integrated & Normalized**	*Hours or days*	☐	☐	☐	☐	☐
3	**Core Priority**	*30 days or less*	☐	☐	☐	☐	☐
2	**Limited Scope / Low Priority**	*1-6 months*	☐	☐	☐	☐	☐
1	**None / Inconsistent**	*6+ months*	☐	☐	☐	☐	☐

Assign Next Steps (Part 2)

1. Assess
2. Discuss
3. Assign

Capture next step and who owns following up on it

#	Next Step	Point of Contact
1		
2		
3		
4		
5		

BACK
TO MENU

Review – Security Governance Exercise

1. **Assess**
   Current State
2. **Discuss**
   Focus Areas
3. **Assign**
   Next Steps

Next Up:
Module 1 Key Takeaways and Next Steps

Key Takeaways & Next Steps

No "silver bullets" will eliminate all security risk, but quick wins can drive towards the north star

Secure Access starting with MFA

Rapidly reduce risk from common threats by modernizing access control with passwordless & multi-factor authentication (MFA)

Modernize Security Posture & Operations

Modernize tools and processes with cloud technology (XDR, SIEM, CSPM) to proactively manage security posture and rapidly respond to attacks

Manage Compliance, Risk, and Privacy

Manage compliance and risk processes for data with modern cloud technology (eDiscovery, insider risk, and more)

Commit to a Zero Trust Strategy

Commit to a security modernization roadmap based on zero trust principles.

Module 2 – Secure Identities and Access

Module 3 – Modern Security Operations (SOC)

Module 4 – Infrastructure & Development Security

Module 5 – Data Security & Governance, Risk, Compliance (GRC)

Module 1 – Zero Trust Architecture

Engage your teams to drive and plan critical security modernization initiatives

BACK TO MENU

Workshop Summary

Security Strategy and Program best practices:

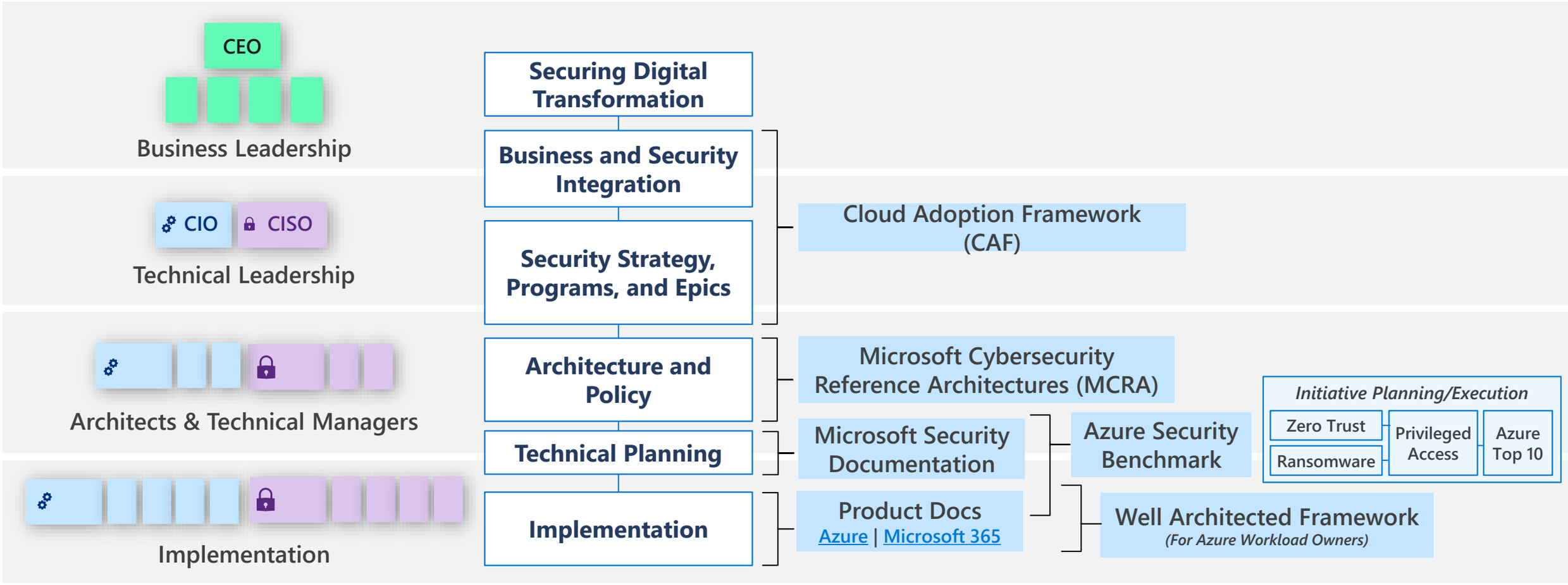
- **Business Alignment** guidance, including security goal of Business Resilience
- **Roles and responsibilities** references to inform career/skill/role decisions
- Suggested **Metrics** to help track and report program success
- **Security Disciplines** for durable program elements
- Prescriptive **Security Initiatives** to guide security modernization (with deeper dives in subsequent modules)

Next Up:
Security Architecture Design Session (ADS)

Security Guidance

December 2021 - https://aka.ms/MCRA

Microsoft



Feedback and additional resources: https://aka.ms/markslist @MarkSimos

Videos and Documentation

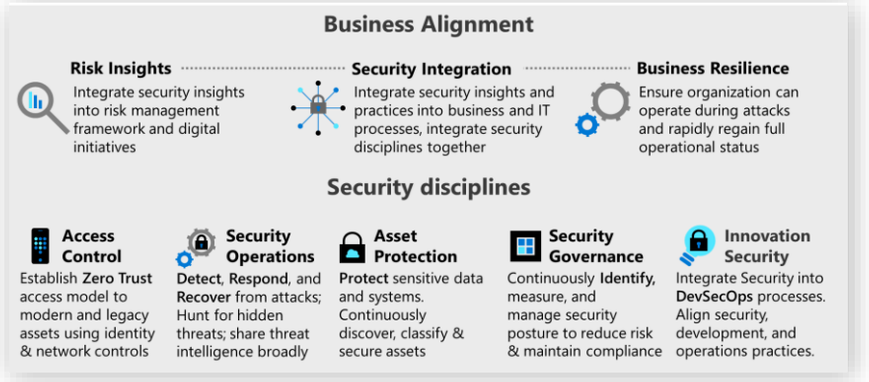
MCRA and CAF Secure

Interactive Guides

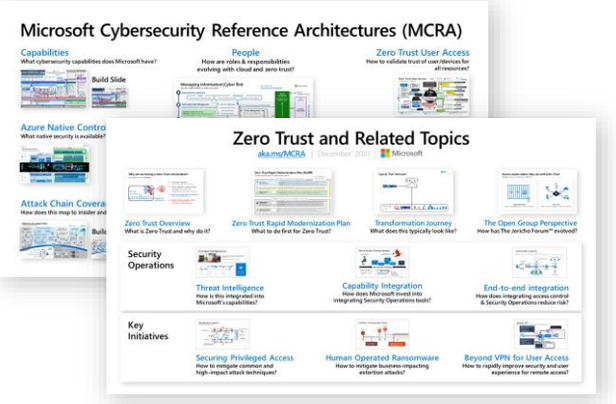
For Those New to Cybersecurity

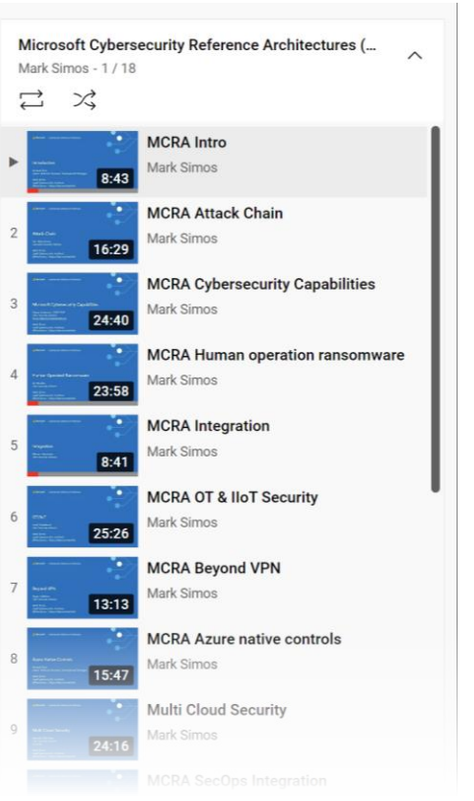
- MCRA - Capabilities
- Zero Trust User Access
- Roles and Responsibilities

aka.ms/CAFSecure



aka.ms/MCRA





aka.ms/MCRA-Videos

Key Zero Trust Resources

to guide your Zero Trust journey

Zero Trust Resources

aka.ms/zerotrust

Maturity Model

aka.ms/zerotrust

Business Plan

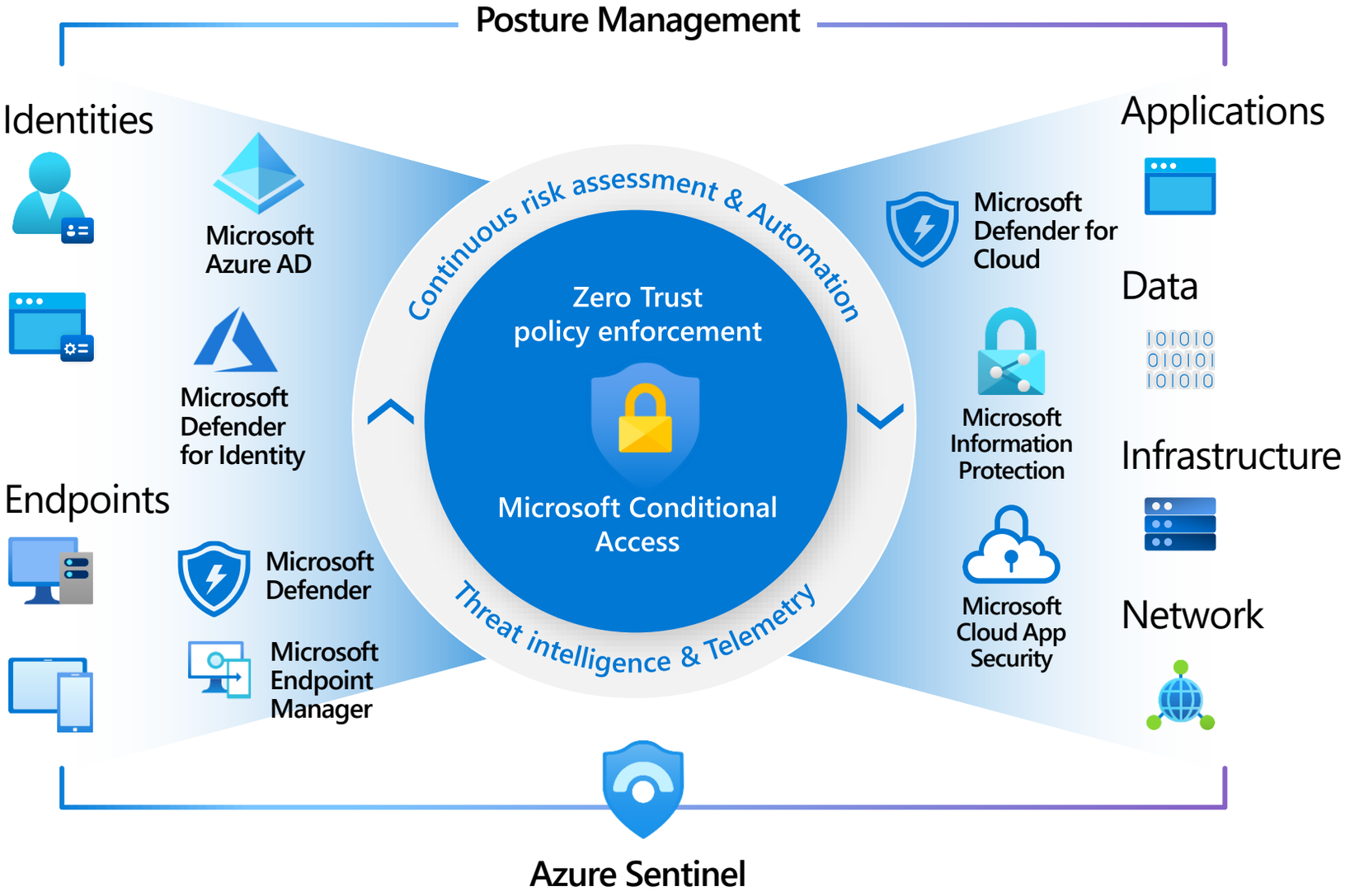
aka.ms/ztbizplan

Deployment Guidance

aka.ms/ztguide

- Zero Trust: Security Through a Clearer Lens session (Recording | Slides)
- Microsoft's IT Learnings from (ongoing) Zero Trust journey

Microsoft Zero Trust Capabilities



Mapping these roles/responsibilities to initiatives

Security organizational functions

https://aka.ms/SecurityRoles

Guidance that maps to these functions:

- Azure Security Top 10
  https://aka.ms/azuresecuritytop10
- Azure Security Benchmark
  https://aka.ms/benchmarkdocs
- Securing Privileged Access – Rapid Modernization Plan (RaMP)
  https://aka.ms/sparoadmap

Cloud Adoption Framework – Secure

Business Alignment

Risk Insights

Integrate security insights into risk management framework and digital initiatives

Security Integration

Integrate security insights and practices into business and IT processes, integrate security disciplines together

Business Resilience

Ensure organization can operate during attacks and rapidly regain full operational status

Security disciplines

Access Control

Establish **Zero Trust** access model to modern and legacy assets using identity & network controls

Security Operations

Detect, **Respond**, and **Recover** from attacks; Hunt for hidden threats; share threat intelligence broadly

Asset Protection

Protect sensitive data and systems. Continuously discover, classify & secure assets

Security Governance

Continuously **Identify,** measure, and manage security posture to reduce risk & maintain compliance

Innovation Security

Integrate Security into **DevSecOps** processes. Align security, development, and operations practices.

What *applied* threat intelligence looks like

In the rural Midwest of the U.S., a high school geography teacher received a brand-new variant of the Emotet banking trojan—the first person ever.

But he had no idea. Signals and AI fully protected him.

The user clicks on an email attachment he receives, sent to his Gmail account, using the built-in Windows Mail app

Before the attachment can open, the Mail app queries the attachment meta-data against 80-plus cloud-based machine learning models

In parallel, the file is 'detonated' in the cloud and an AI system 'watches' to see what happens when he opens attachment

Utilizing signals and outcomes from trillions of historical email transactions, both services determine the file is malicious

Mail deletes the attachment from the PC, flags the file for review by (human) analysts, and the AI systems automatically update

Impact

This all occurred in fewer than 400 milliseconds—the blink of an eye

To protect customers and make the internet safer, our global security teams use machine learning to process:

- **Trillions** of raw security signals, which generates
- **Billions** of complex predictions and
- **Millions** of automated actions

Microsoft Threat Intelligence

Built on diverse signal sources and AI