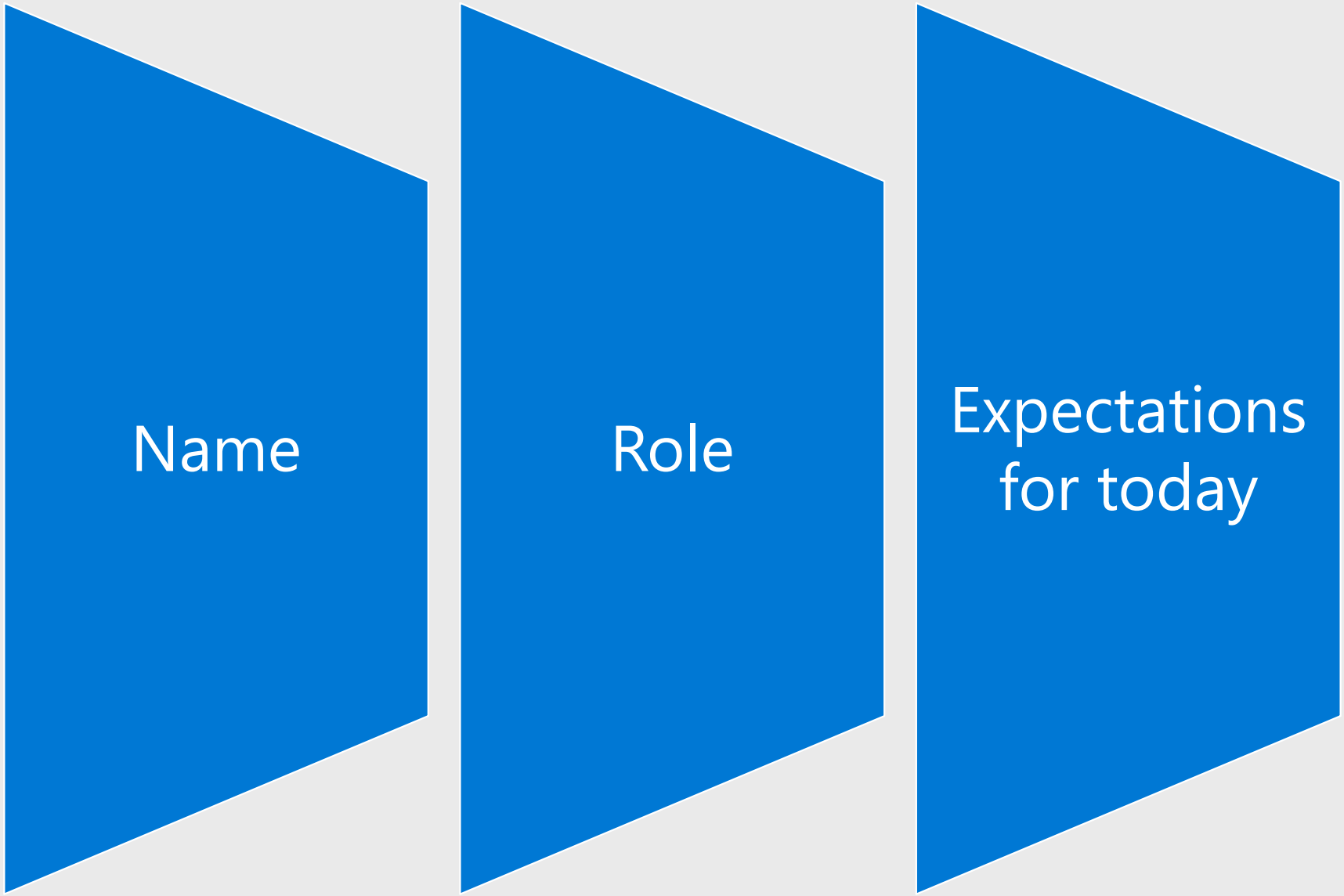
Microsoft

Microsoft CISO Workshop
1 – Cybersecurity Briefing

Microsoft Cybersecurity Solutions Group

Introductions

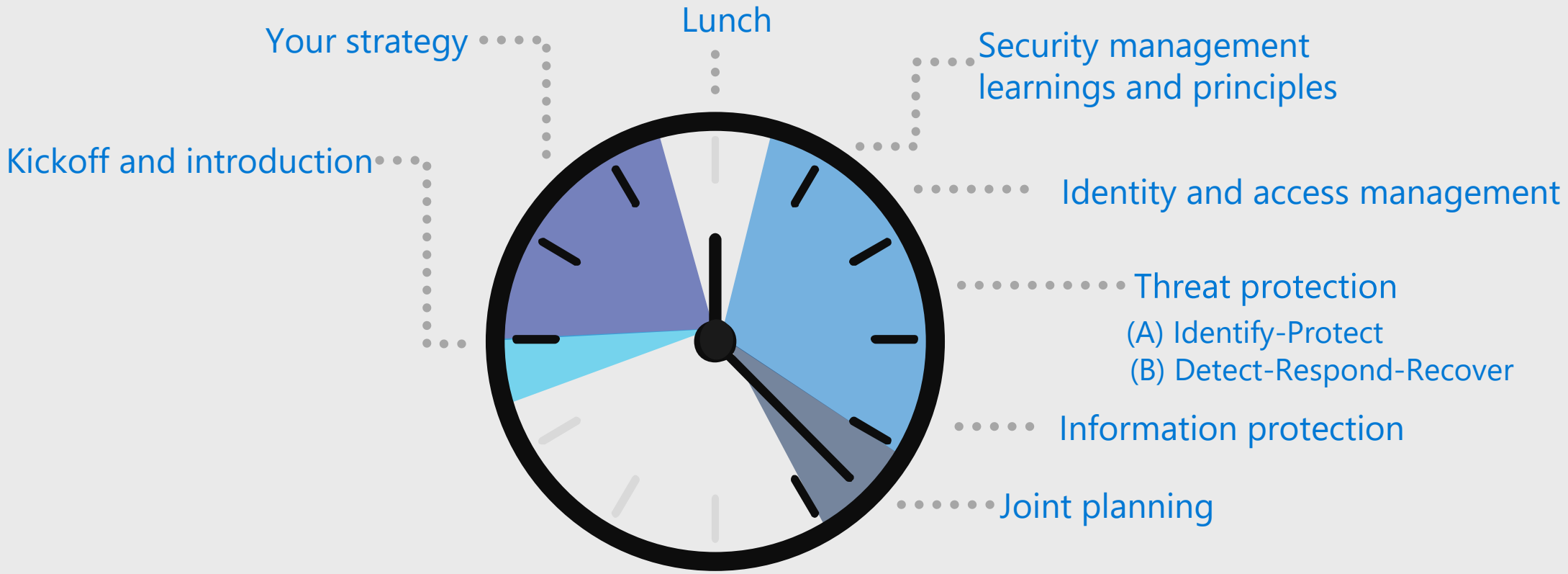


"Security is our top priority and we are committed to working with others across the industry to protect our customers."

Satya Nadella
Chief Executive Officer, Microsoft Corporation

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships

Microsoft CISO workshop



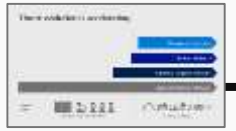
CISO WORKSHOP OBJECTIVE:
Learn how Microsoft can help you achieve your cybersecurity goals

Microsoft Cybersecurity Briefing

CxO View

Cybersecurity Resilience

CISO View – Cybersecurity Landscape + Microsoft Approach



Accelerating Threats

Digital Transformation

Imperatives & Opportunities

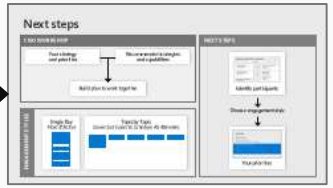
Platform

Intelligence

Partners

Key Strategies

Next steps



CISO Workshop

Security Hygiene

Critical Hygiene

Cloud Platform

TRUST BUT VERIFY

Security & Trust

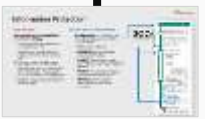
Technical capabilities

Reference Architecture

Identity & Access

PC & Mobile Devices

Software As A Service (Saas)



Information Protection

Security Operations Center (SOC)

Hybrid Cloud Infrastructure

IoT And Operational Technology

Threat evolution is accelerating

Malware-Less Attacks

'File-less' Malware

Tailored/Targeted Malware

Mass Distribution Malware

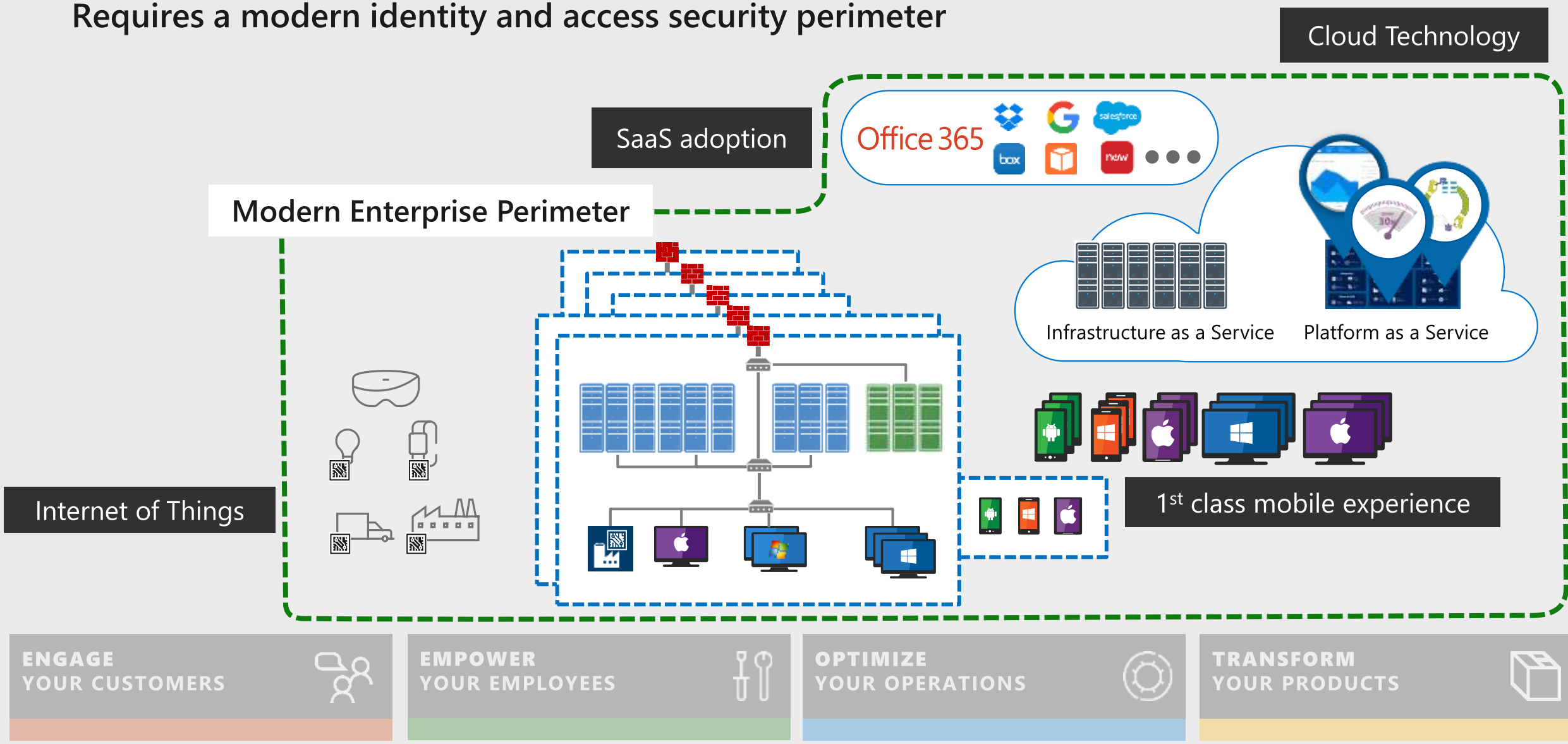
THREAT AGES

Malware and Infrastructure

Identity and Apps

Your enterprise in transformation

Requires a modern identity and access security perimeter



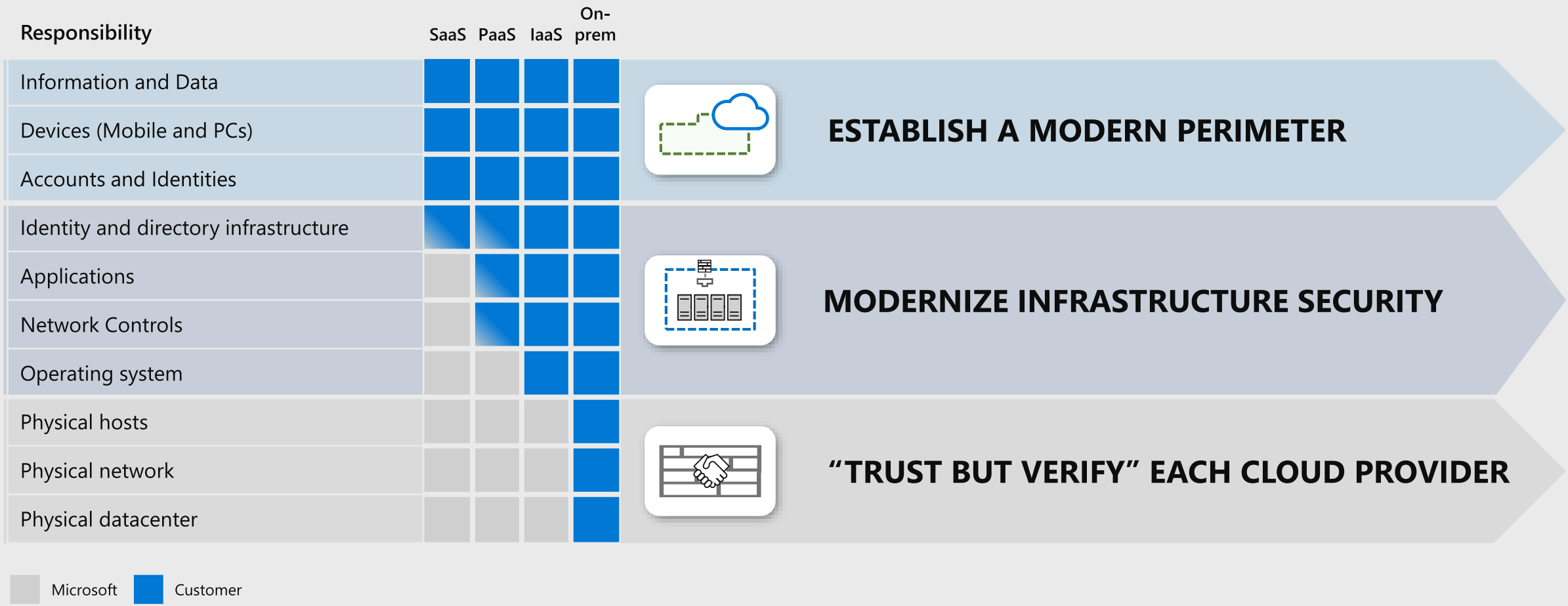
ENGAGE YOUR CUSTOMERS

EMPOWER YOUR EMPLOYEES

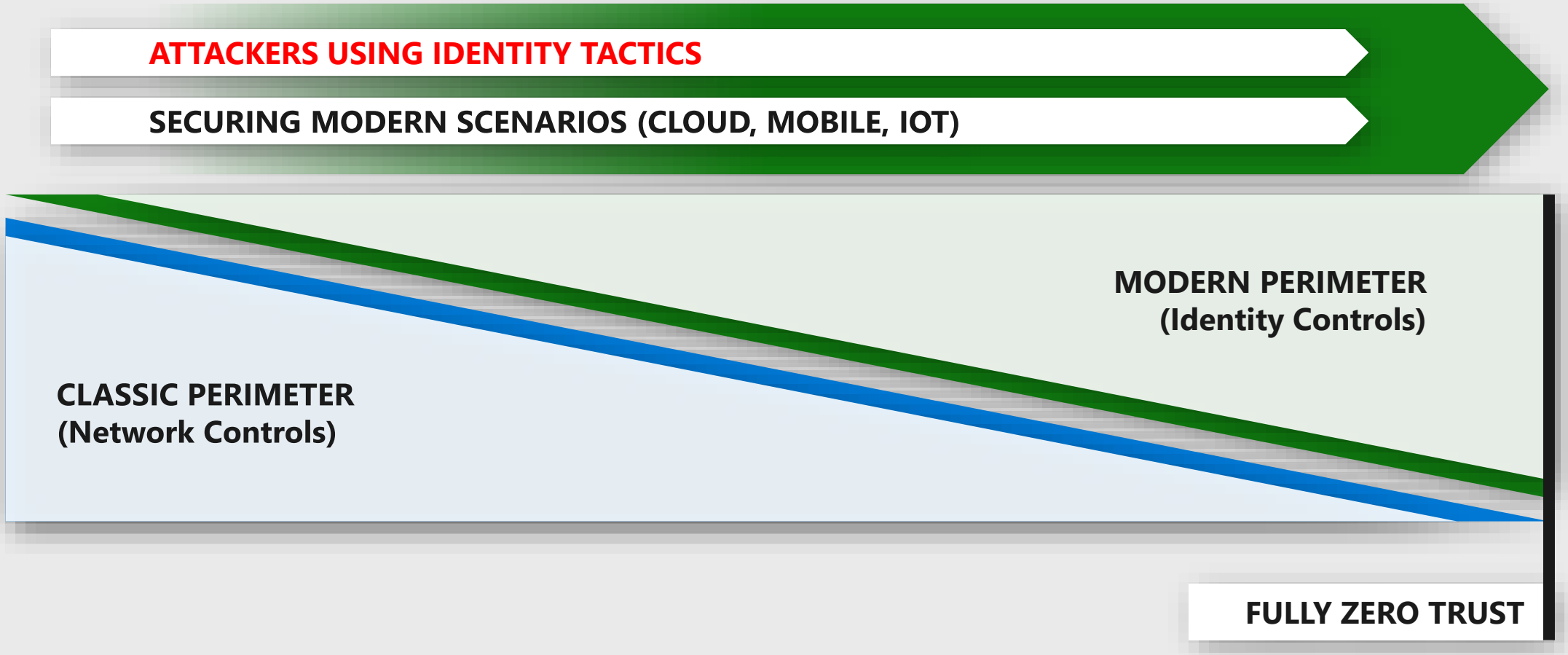
OPTIMIZE YOUR OPERATIONS

TRANSFORM YOUR PRODUCTS

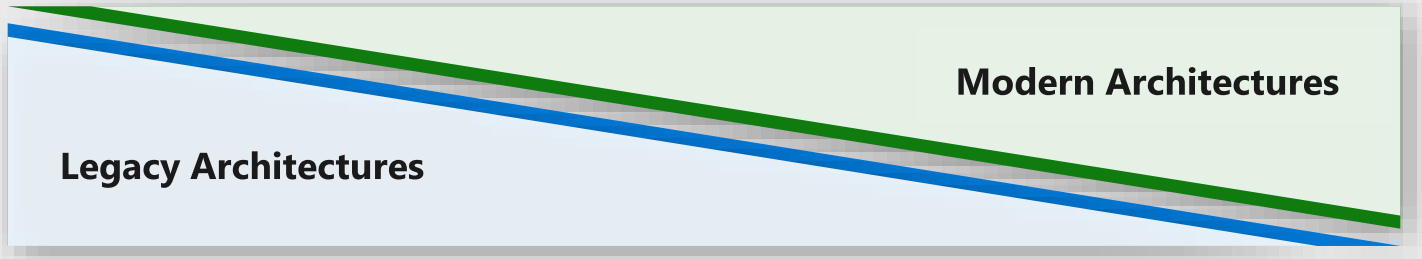
Building a resilient cybersecurity program



Running Dual Perimeters



Evolution of Roles and Responsibilities



"STOP THE PRESSES!" → CONTINUOUS VALIDATION

Security roles will change with architectural/operational models

Manual Resource Administration	**Administration**	Author & Govern Automation
Containment with Network	Network → **Containment**	Containment at all layers (Net, App, ID, Data, etc.)
Quality Check Before Release	**Development**	Security SME in DevOps process
Project based Engagement	**Architecture**	Continuous Engagement & Improvement

Imperatives and Opportunities

Recognize Fundamental Transformations

Meet Challenges + *Embrace Opportunities*

DRIVE STRATEGIC OUTCOMES

Security & Compliance Management

Gain end-to-end visibility into your organization's security and compliance + manage policy centrally

Identity and Access Management

Ensure only the right people have access to your organizational systems

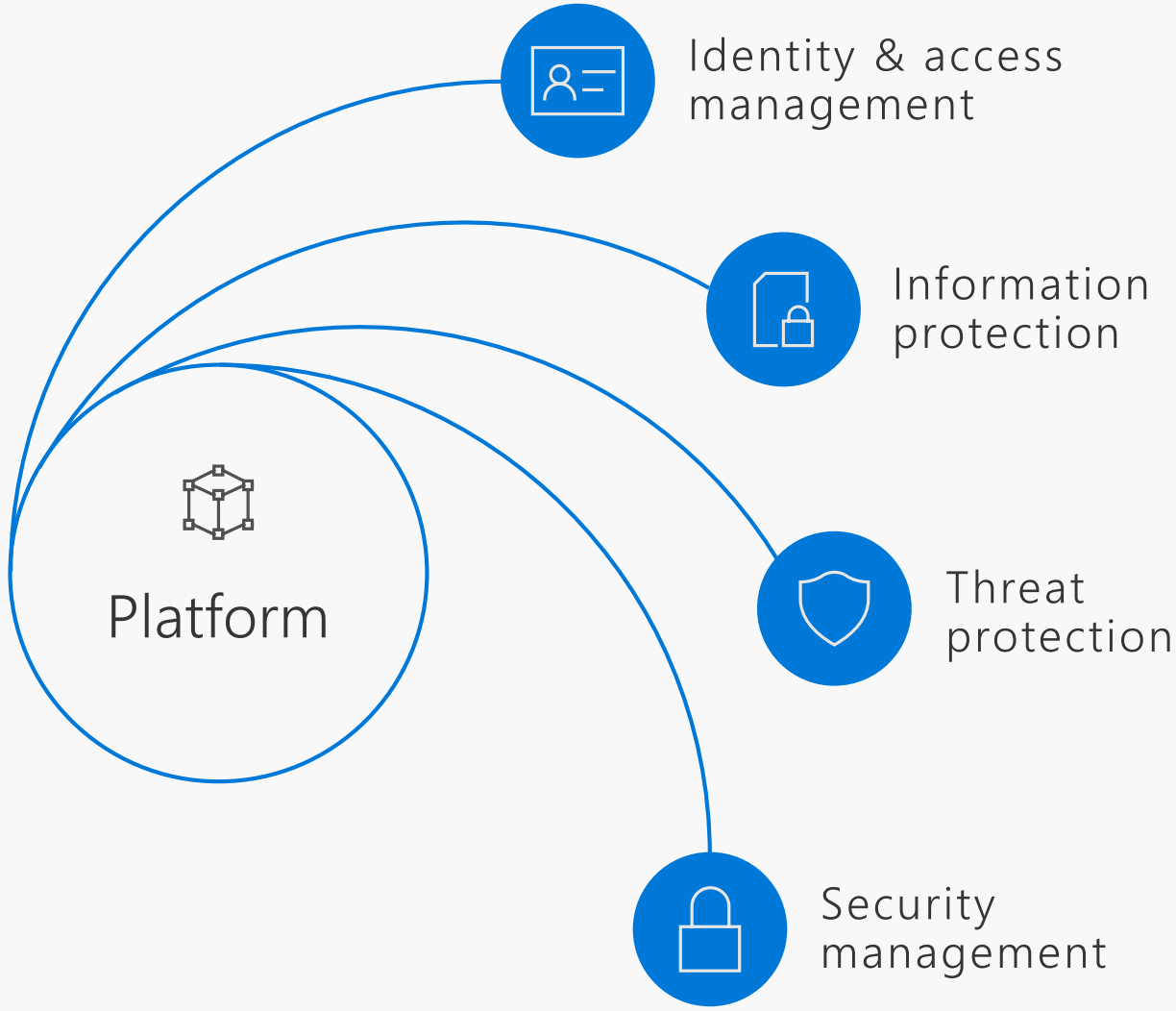
Information Protection

Protect documents, databases, and emails against leaks, tampering, and destruction

Threat Protection

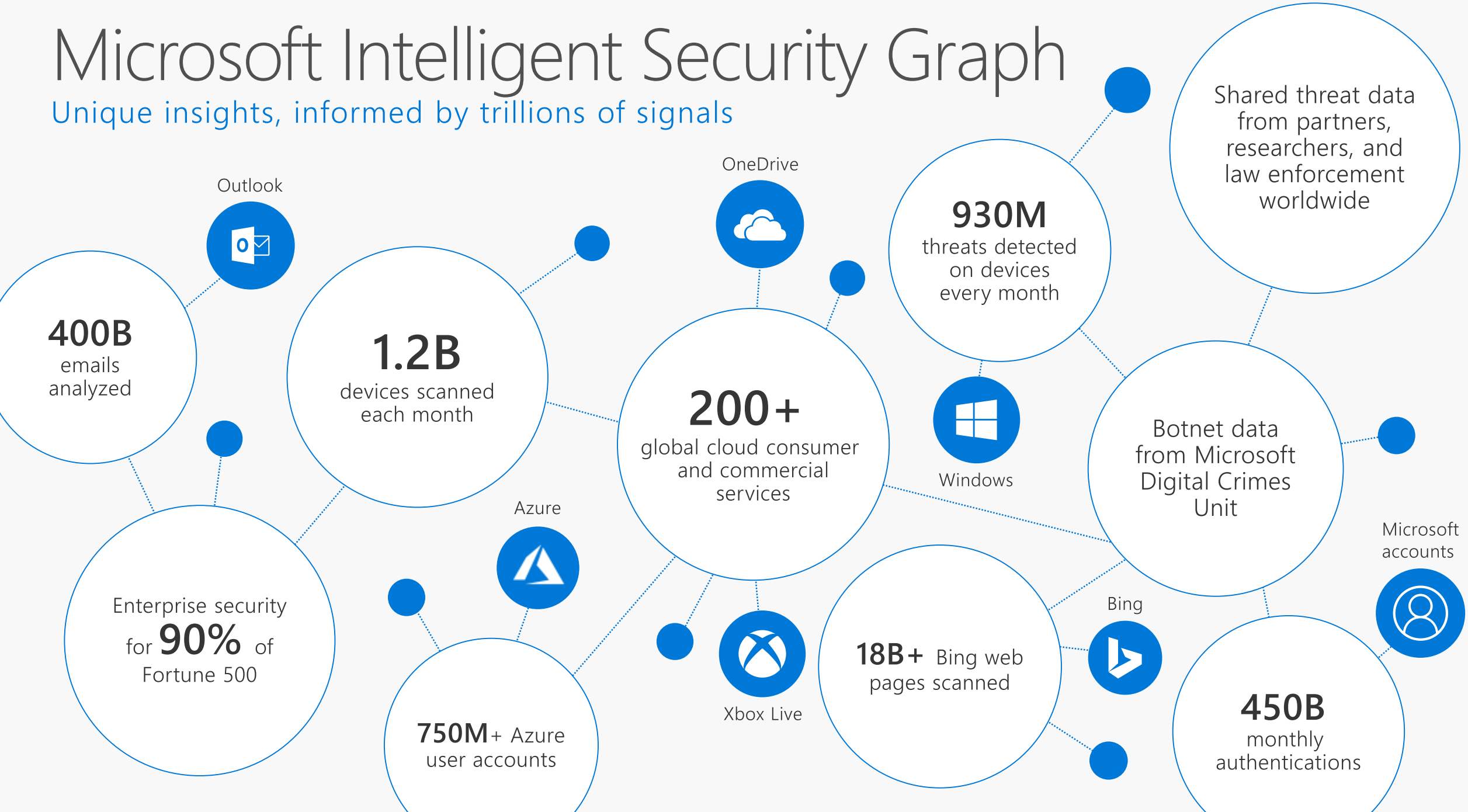
Thwart hackers and recover quickly if attacked

Built in security



Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals

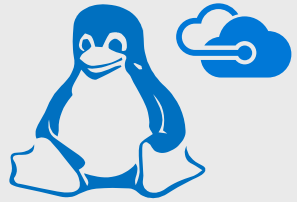


Integrating with your existing solution portfolio

Microsoft Intelligent Security Association

Active in security and open source communities

Top contributor
to GitHub in 2016



~50% of IaaS VMs
in Azure run Linux

Board Membership

CSA cloud security alliance®

security advisor alliance

THE LINUX FOUNDATION

fido alliance simpler stronger authentication

FINANCIAL SERVICES Information Sharing and Analysis Center

Key Challenges and Strategic Opportunities

Identity-based attacks are up 300% this year

Adopt identity-based protection

Information is your most attractive target

Protect information wherever it goes

Attackers constantly evolving techniques

Detect attacks faster and automate response

Most enterprises report using more than 60 security solutions

Use tools that integrate investigation experience and provide guidance

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
  - AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

- Unmanaged & Mobile Devices
- Intune MDM/MAM
- Managed Clients
- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS

Security Appliances

Express Route

Intranet Servers

- Windows Server 2016 Security
  Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring

S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

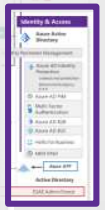
Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft



Identity and Access Management

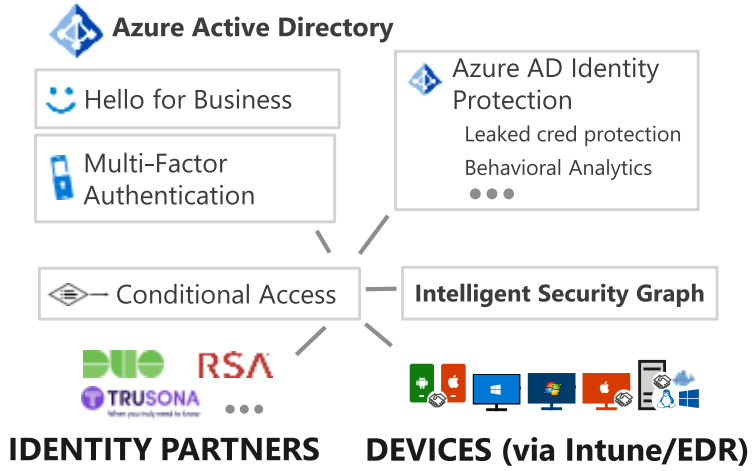
Microsoft

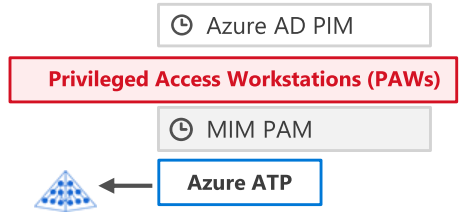
CHALLENGES

- **PRODUCTIVITY WHILE SECURING against**
  - **Phishing + password spray attacks**
  - **Compromised devices & accounts**
- **LATERAL TRAVERSAL ATTACKS** using Credential Theft
- **3RD PARTY ACCOUNT RISK**

MICROSOFT'S APPROACH

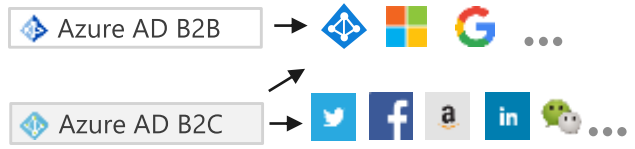
- ✓ Enable easy and secure **passwordless** authentication with biometrics
  - ...while **protecting passwords** today
- ✓ **Conditional Access** based on intelligence, device state, behavior, and MFA
- ✓ Guidance and Technology for **Securing Privileged Access (SPA)**
- ✓ Advanced **credential theft attack detection** with Azure ATP
- ✓ Move 3rd party accounts to **B2B/B2C solutions** to lower risk and increase productivity





Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)



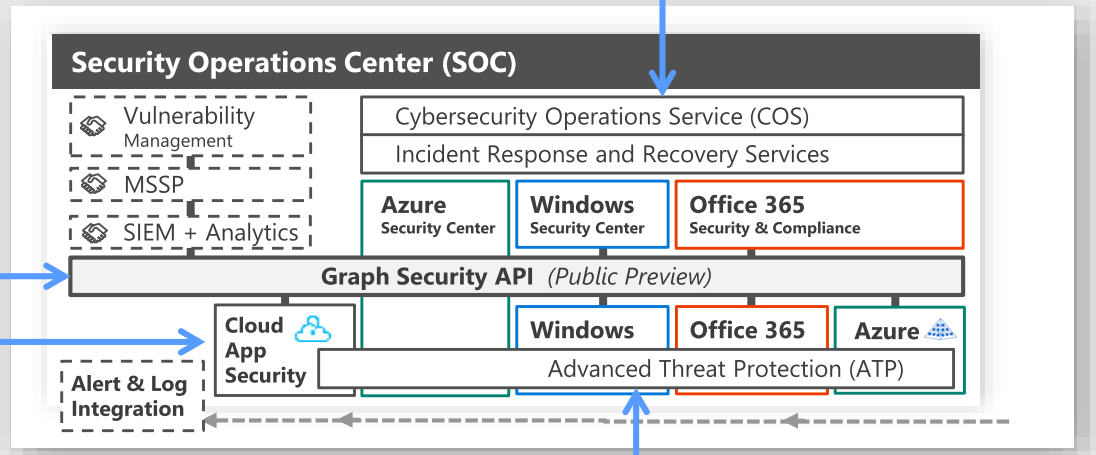
Security Operations Center (SOC)

CHALLENGES

- **Traditional SIEM centric model results in**
  - **High Event Volume** and associated cost
  - **Alert Overload** - too many false positives
  - **Poor Investigation Workflow**
- **Security expertise wasted on**
  - Manual integration of tools/intelligence
  - Constantly evaluating products

MICROSOFT'S APPROACH

- ✓ Assist with **Incident Response and Recovery** as well as proactively **hunting for adversaries**
- ✓ **Integrate existing SOC tools** and Microsoft capabilities with **Graph Security API (public preview)**
- ✓ Anomaly detection, alerts, and investigation across **SaaS applications** with Cloud App Security
- ✓ Advanced Threat Protection provides **integrated investigation experience** across Windows/Linux/Mac desktops and servers, Office 365, Active Directory, and Azure Tenants.
- ✓ Intelligent Security Graph provides **integrated intelligence** for detection



Intelligent Security Graph

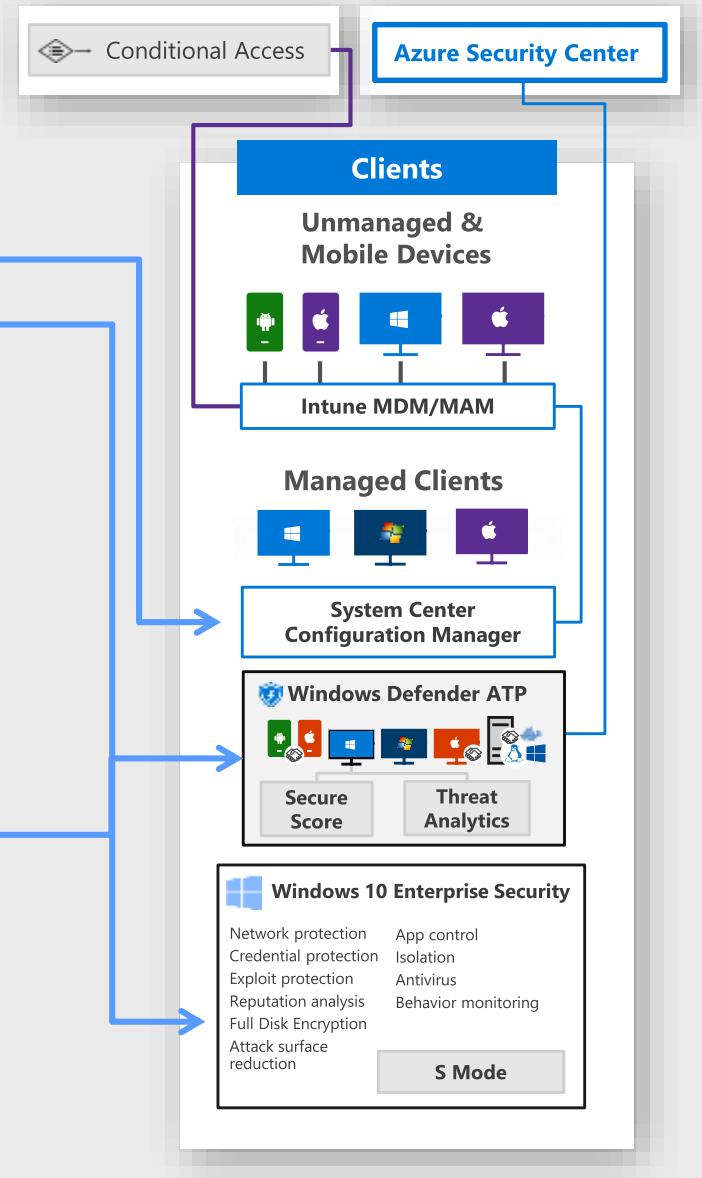
Clients - PC and Mobile Devices

CHALLENGES

- **Manage risk, health, and compliance** across broad spectrum of device platforms and ownership (BYOD, Corporate Devices, Macs, Unmanaged and Mobile Devices)
- Provide **secure managed PCs** through lifecycle (identify, protect, detect, respond, recover)

MICROSOFT'S APPROACH

- ✓ **Cross platform security and management** (Windows, Linux, Mac, iOS, and Android)
- ✓ **Endpoint protection platform (EPP)**
  - Leading capabilities for next generation antivirus (as recognized in industry tests), exploit & network protection, behavior monitoring, application control, and isolation
  - IT configuration management, policy enforcement and conditional access
  - Security administration with compliance, threat analytics, and secure score
- ✓ Integrated **Endpoint detection and response (EDR)** post-breach detection, automated investigation and response, and advanced hunting.



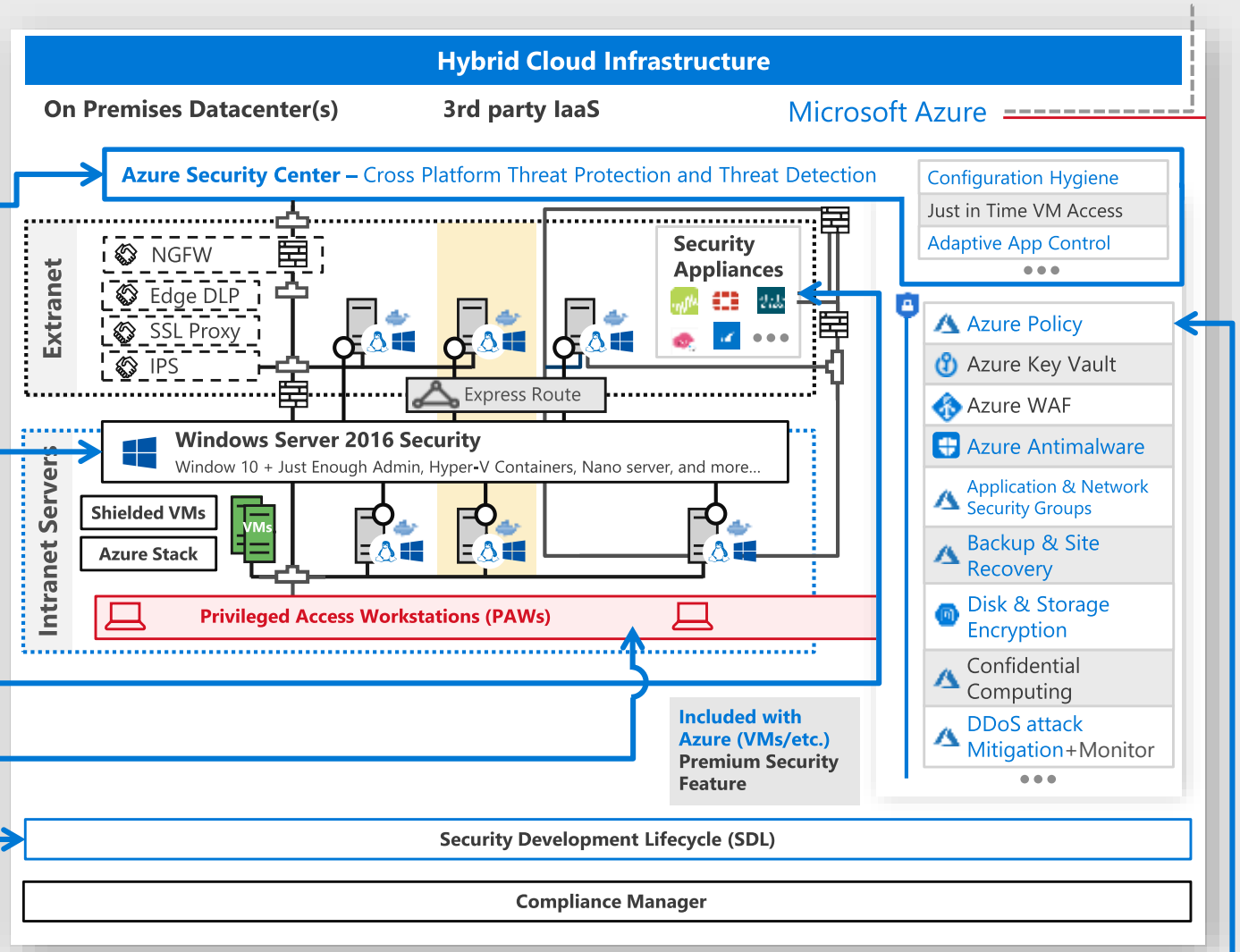
Hybrid Cloud Infrastructure

CHALLENGES

- **Limited experience and toolsets** for securing hybrid architecture and Platform as a Service
- **Critical Risks** - Privilege management and security hygiene critical for cloud workloads

MICROSOFT'S APPROACH

- ✓ **Cross-Platform and Cross-Cloud** – security capabilities to enable visibility and control
- ✓ **Deep Azure Defenses** – Integrated with platform to secure Azure workloads, assess compliance
- ✓ **On Premises security** investments to modernize security and leverage cloud learnings + technology
- ✓ **Marketplace –** Integrate existing capabilities and skills
- ✓ **Privilege Management** – Protect against high impact attacks against privileged accounts
- ✓ **Secure Development Lifecycle (SDL)** – Securing applications and PaaS workloads



Software as a Service (SaaS)

CHALLENGES

- **Governance, Risk, and Compliance** challenges of sprawling SaaS estate and unsanctioned shadow IT
- **Security Operations Center (SOC)** requires visibility into SaaS activities and threats

MICROSOFT'S APPROACH

✓ **Platform Security –** Deep investments in physical security, Red/Blue Teams, encryption, privileged access, & more

Software as a Service

Office 365

Dynamics 365

✓ **Manage Shadow IT Risk –** CAS enables you to discover, assess, approve, and manage SaaS (via API +Proxy)

Cloud App Security

✓ **SOC Enablement –** Microsoft Cloud App Security (CAS) provides anomaly detection, alerting, and SIEM integration

- Office 365 ATP provides advanced security (sandbox detonation, etc.) for email, SharePoint, Teams, and more
- Threat Intelligence provides analytics on attack trends for your tenant and your industry

Office 365
Advanced Threat Protection (ATP)

Office 365
Security & Compliance

✓ **Office 365 Guidance –** Security Roadmap + Secure Score recommendations guide you through security journey

Secure Score

Roadmaps and Guidance
1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks(Wannacrypt/Petya)

✓ **Compliance –** GDPR and NIST compliance visibility on Office 365 and Dynamics 365 with Compliance Manager

Compliance Manager

✓ **Information Protection –** CAS integration with Azure **Information Protection to discover + protect data**

- Customer Lockbox to provide final control of access to data by Microsoft personnel

Customer Lockbox

IoT and Operational Technology

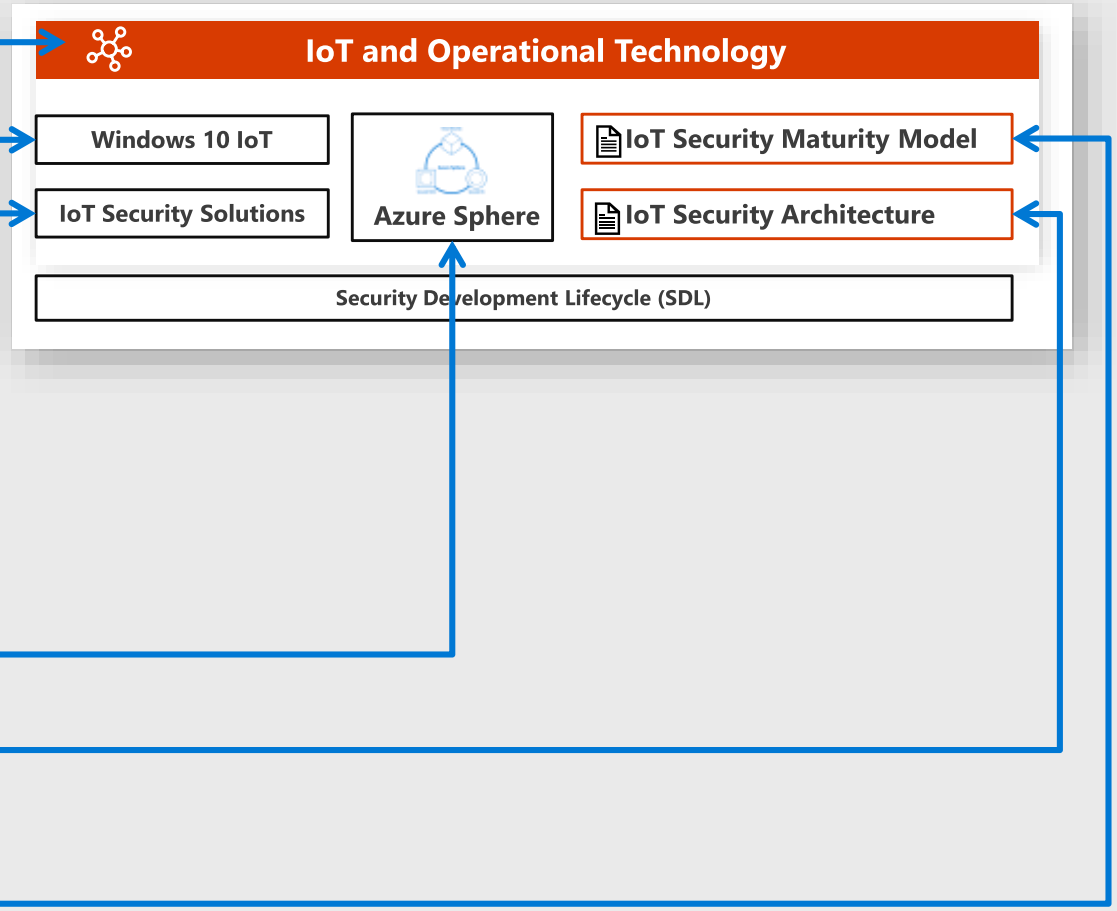
Significant potential value and security/privacy risks

CHALLENGES

- End to end approach required for effective IoT security
- **Large brownfield** of existing devices to manage and secure
- ~9 Billion **new microcontroller devices** shipping every year for a wide range of IoT devices from low power crop sensors to powerful devices for point of sale (POS)

MICROSOFT'S APPROACH

- ✓ Secure a ***wide range of HW platforms*** in partnership with silicon partners, OEMs, and suppliers (for Edge and IoT devices). Enable ***both brownfield and greenfield*** devices to achieve higher levels of security
- ✓ Support ***wide range of platforms*** including Linux, Windows and RTOS with open source SDKs in many languages
- ✓ Provide ***security monitoring, alerts and mitigation*** from the device to the cloud application using Azure Security Center for a wide range of IoT devices and solutions
- ✓ Provide best in class security from silicon to cloud for MCUs with ***Azure Sphere***
- ✓ Provide ***guidance, best practices, & tools*** for secure design + evaluation (threat modeling, SDL, pen testing, etc.)
- ✓ Contribute to and ***drive security standards*** across the IoT infrastructure (DICE, SMM and many more)



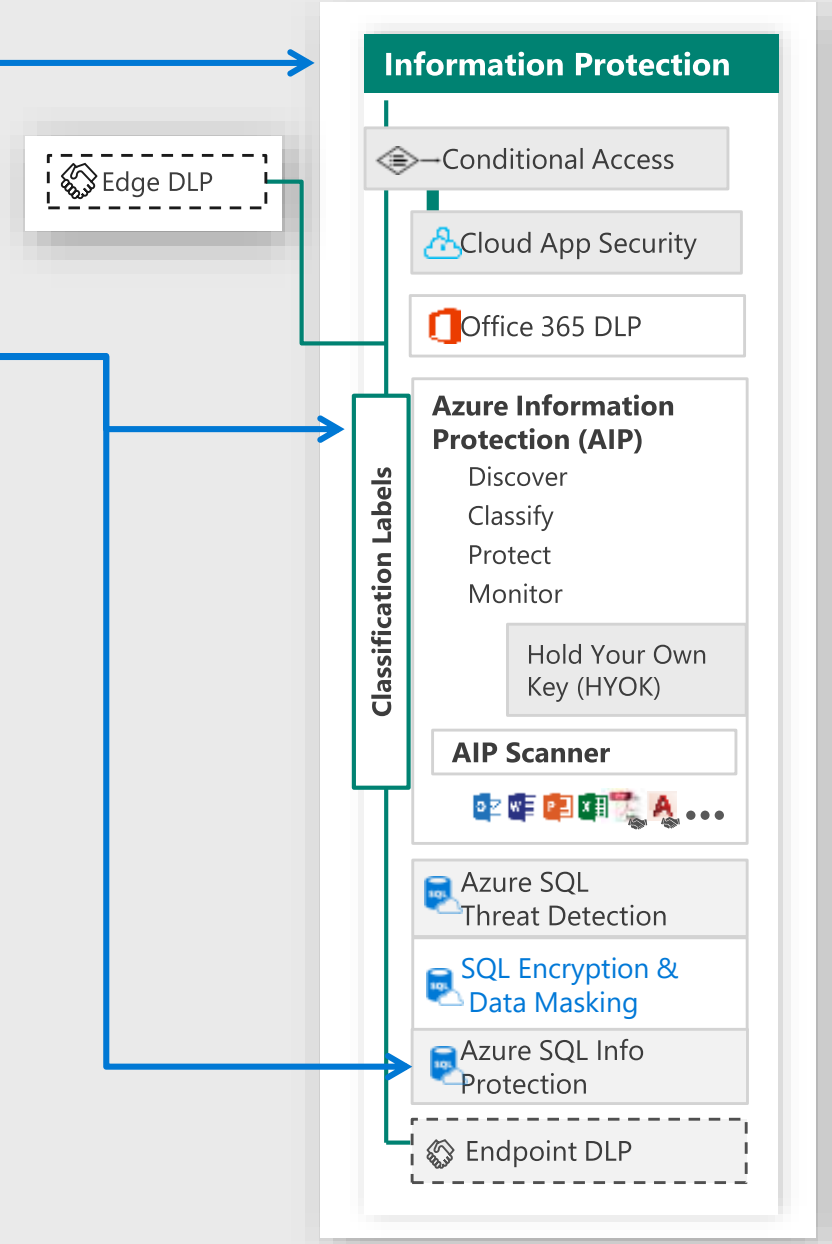
Information Protection

CHALLENGES

- **Information Protection and Data Governance Strategy**
  - Label, track, and show data loss or manipulation of a file.
  - Implement corporate policies to protect different levels of sensitive data
- **Protecting sensitive information**
  - Challenging to discover and classify data across mobile devices, SaaS, cloud infrastructure, and on-premises
  - Need full lifecycle data protection for identified data

MICROSOFT'S APPROACH

- ✓ **Broad Coverage** for structured and unstructured data across formats, cloud, & devices
- ✓ Full Information Lifecycle
  - **DISCOVER** existing and newly created sensitive data
  - **CLASSIFY** automatically + user control (based on policy), integration with DLP
  - **PROTECT** the data itself, not just storage or network locations
  - **MONITOR** and revocation capabilities for security and compliance



Next steps

CISO WORKSHOP

Your strategy and priorities

Recommended strategies and capabilities

Build plan to work together

ENGAGEMENT STYLES

Single Day
More Effective

Topic by Topic
Slower, but Easier to Schedule All Attendees

NEXT STEPS

Identify participants

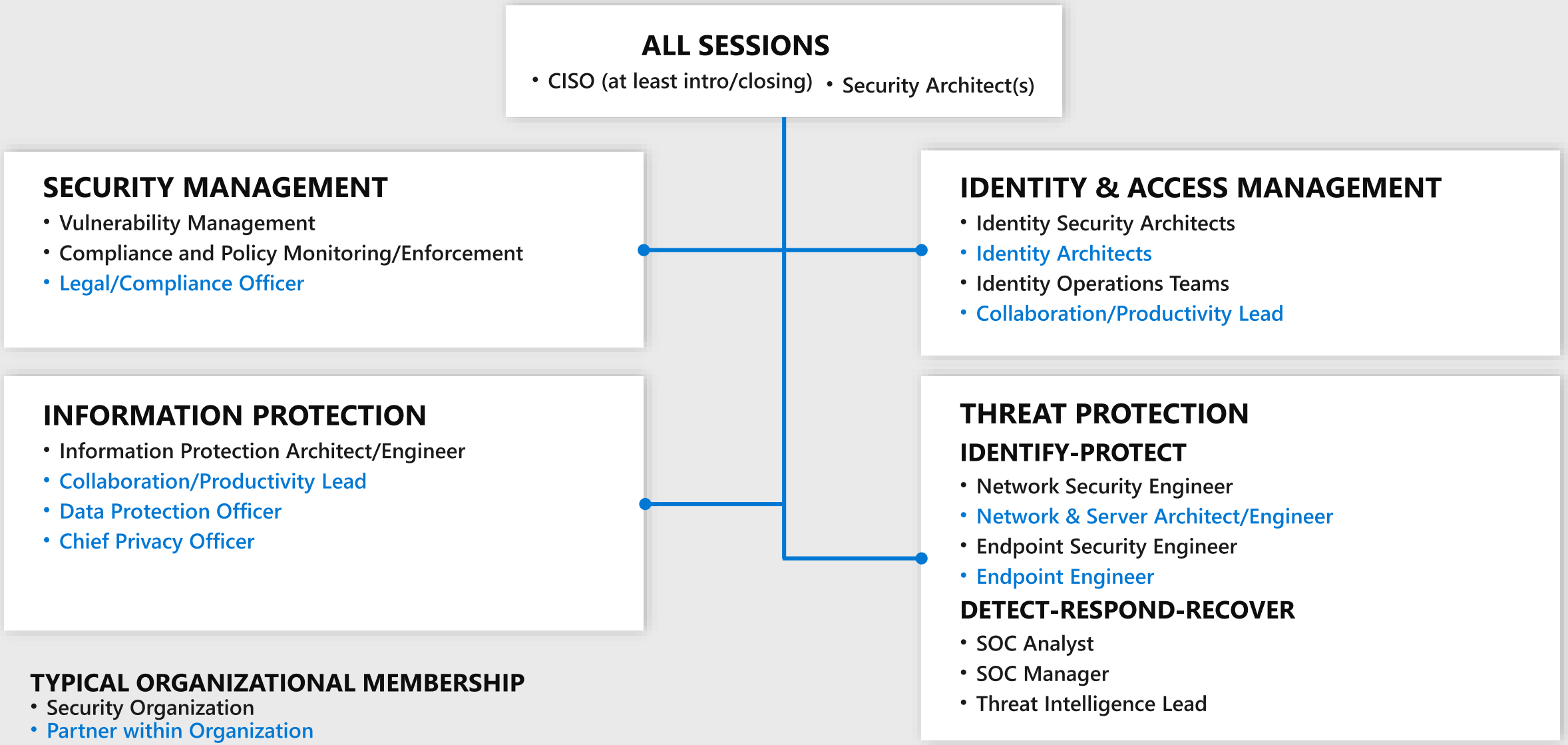
↓

Choose engagement style

↓

Your priorities

Suggested Stakeholders / Attendees



TYPICAL ORGANIZATIONAL MEMBERSHIP

- Security Organization
- Partner within Organization

Next steps

Schedule a workshop

Build a plan to work together:

Review your strategy and priorities

Review Microsoft's recommended strategies and capabilities

What are your top 3-5 strategic priorities?

1.

2.

3.

4.

5.

Un-Named
CFO

"The problem with CISOs, and the entire cyber security field for that matter, is that you keep asking for more money and resources but can't guarantee or even articulate what I'm buying."

Cyber Resiliency

Aligned - Align and Integrate cybersecurity with business strategy, processes, and initiatives

Mindset

Adopt a mindset that ***assumes compromise*** and focuses on:

- Raising attacker costs
- Rapid response/recovery

Cloud

Use cloud technologies to

- Tap into community resources and knowledge
- Accelerate innovation (security and productivity)

Hygiene

Lower overall risk by

1. Identify well-known risks
2. Steadily burn down list

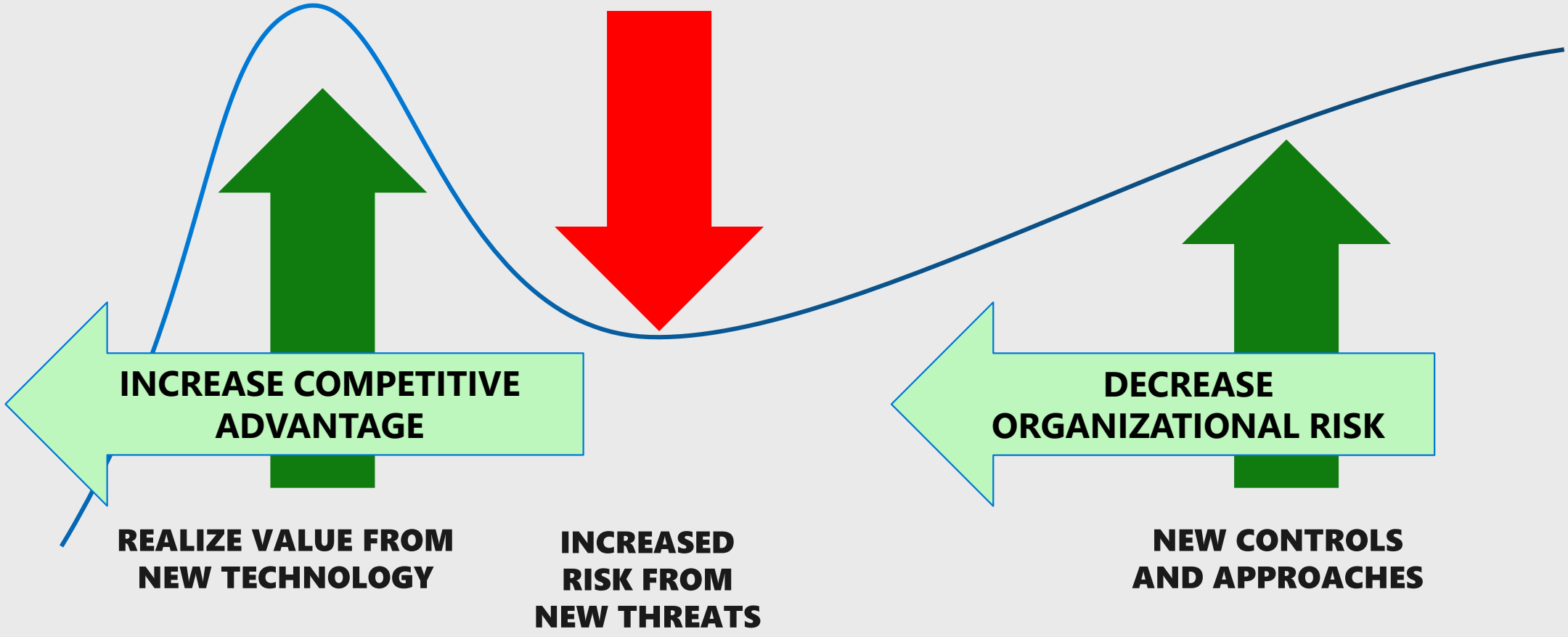
Key Measures of Success

Cost of Attack

Mean Time To Remediation (MTTR)

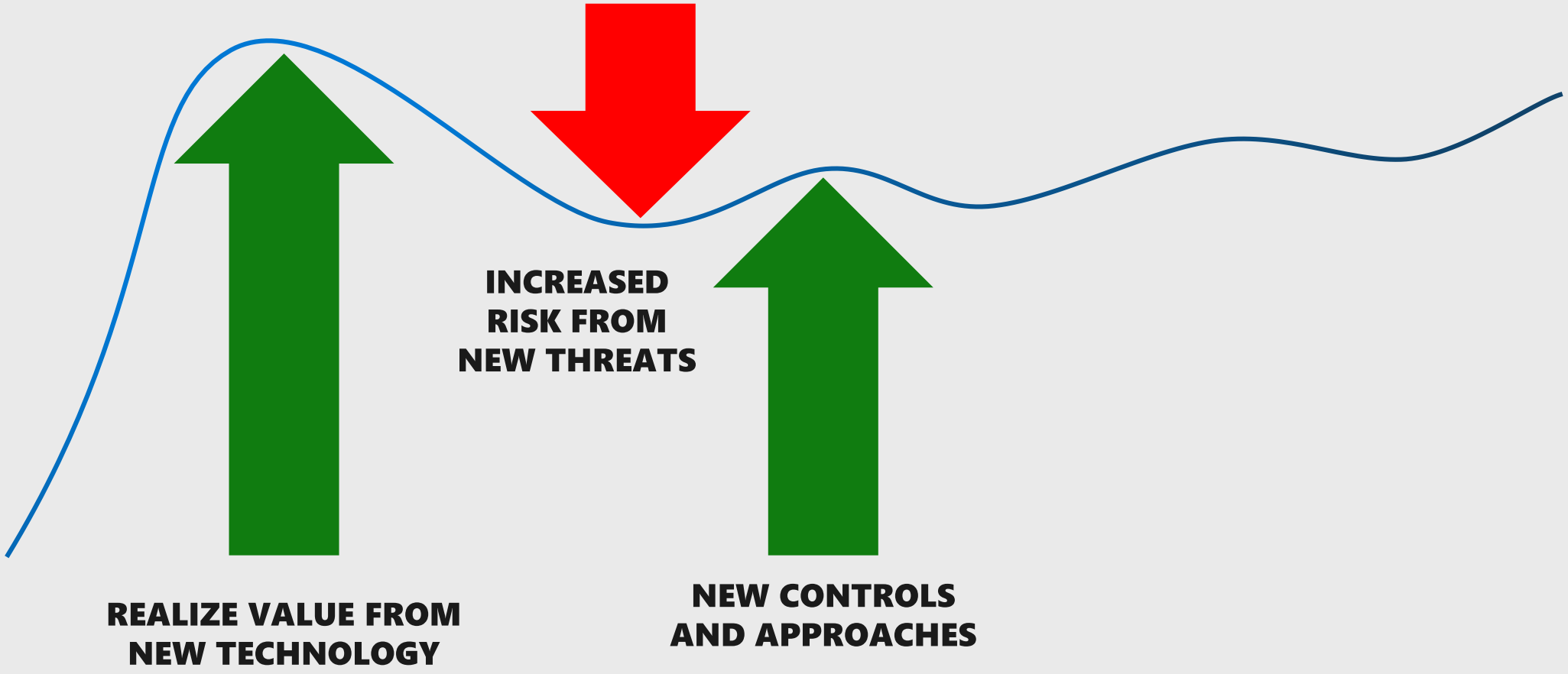
Three Major Forces in Digital Transformation

Adoption Speed impacts Benefit/Risk curve



Three Major Forces in Digital Transformation

Adoption Speed impacts Benefit/Risk curve



Machine Learning

Helps overcome human limitations using large datasets

1. Scales out Human Expertise

2. Shines a light in human blind spots

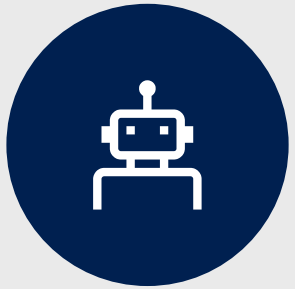
Microsoft Finance - Digital Transformation Areas

Financial Analysis & Reporting

[Revenue Reporting]
- Near Realtime Financial Reporting
- Scale to meet changing business

Strategy & Forecasting

[Financial Forecast]
- Predictive Analysis
- Instant Insights
- Broader and Deeper Views

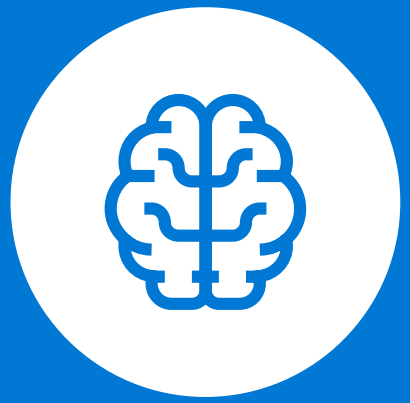


Business Process Automation

[Reconciliation]
- Cost savings
- Time savings
- Improved Accuracy

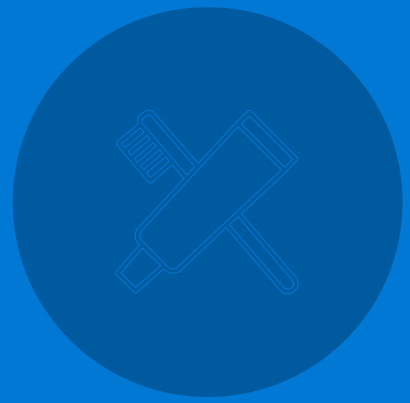
Risk Management

[Tax Processing]
- Cost Savings
- Compliance with New tax rules



MINDSET

CLOUD



HYGIENE

Quick Primer on Security Culture

Deeply respect truth and facts

Deeply care about keeping the organization safe

Limited background in business/ communications

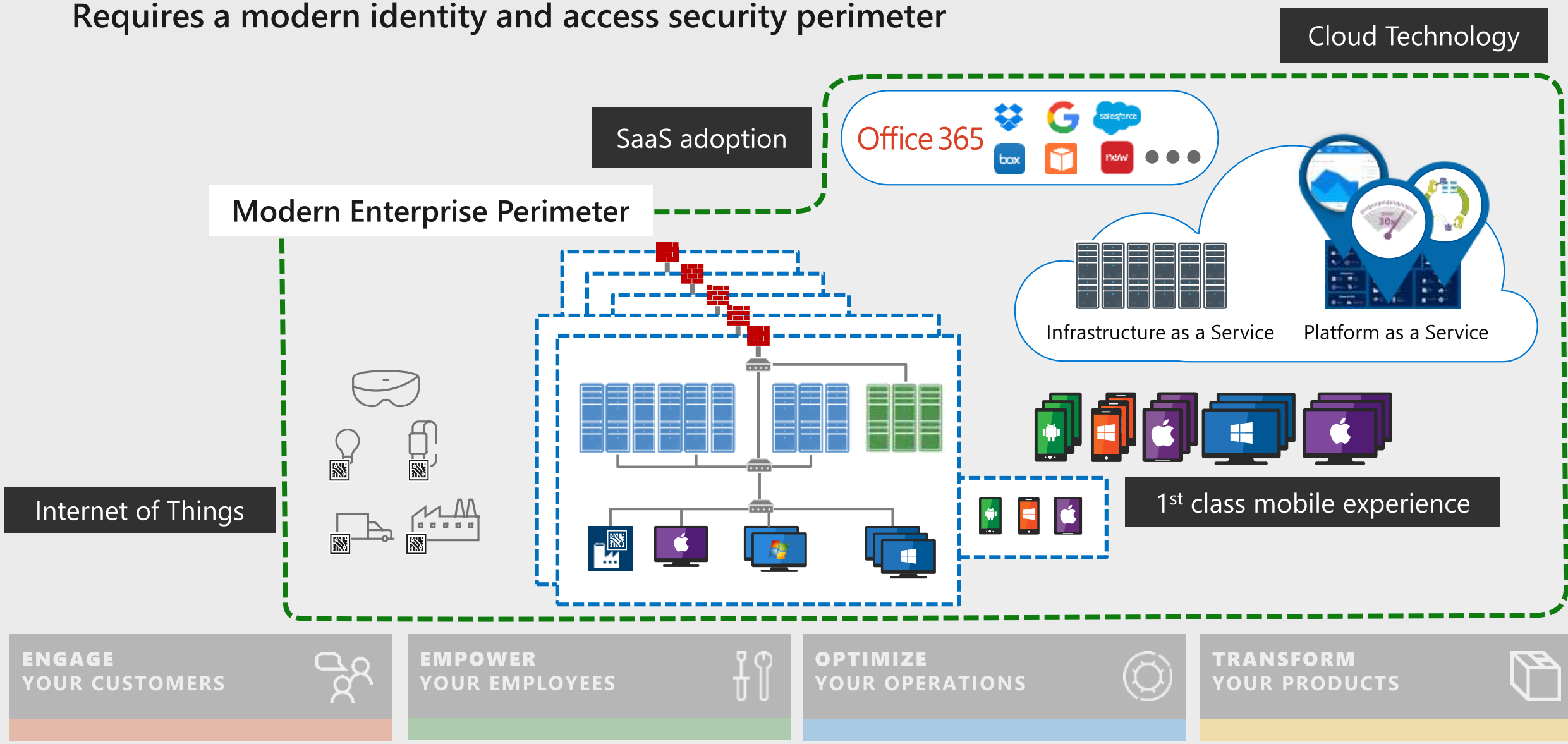
- Many security people incorrectly assume/ accept accountability
- Strained relationship with IT and Business backgrounds

Prevalent ‘Underdog’ attitude

- Not involved early in business/risk decision process

Your enterprise in transformation

Requires a modern identity and access security perimeter



ENGAGE YOUR CUSTOMERS

EMPOWER YOUR EMPLOYEES

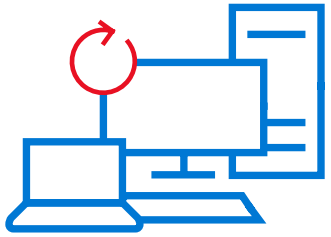
OPTIMIZE YOUR OPERATIONS

TRANSFORM YOUR PRODUCTS

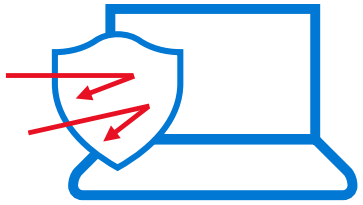
Designing for Failure – The Mindshift

THEN

Reliability:
Designed not to fail

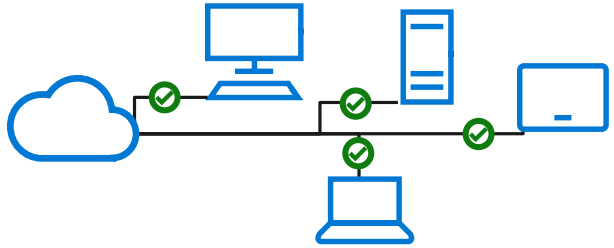


Prevent:
Every possible attack

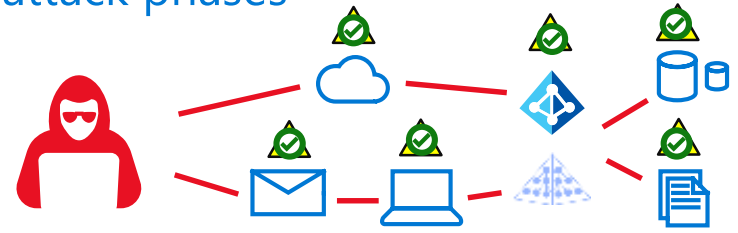


NOW

Resilience:
Designed to recover quickly



Assume Compromise:
Protect, detect, and respond along attack phases



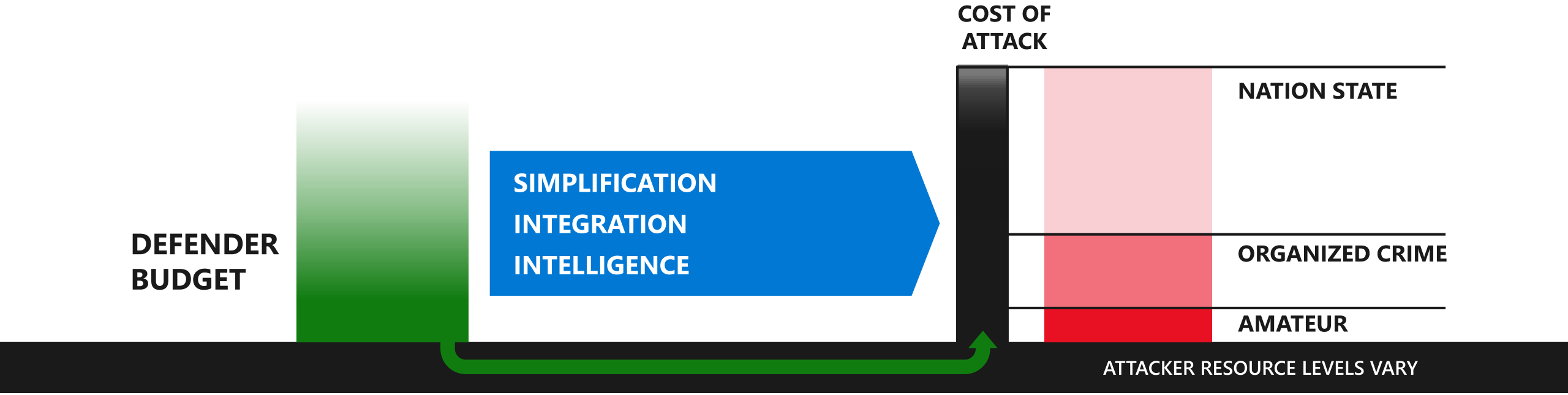
Ruin Their ROI

Changing the economics of cybersecurity

ATTACKERS:
MAXIMIZE RETURN ON INVESTMENT (ROI)
(return may be monetary/political/etc.)

DEFENDERS:
RUIN ATTACKER ROI
by raising attack cost with protection
+ rapid response/recovery

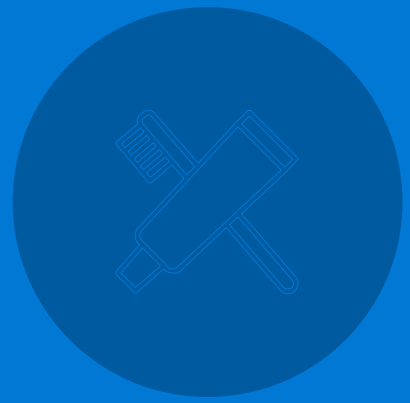
MICROSOFT:
SIMPLIFY ADVANCED CAPABILITIES
across platforms, clouds, and IoT



NOTE: Cost of attack is continuously changing with technical advancement + business model evolution

MINDSET

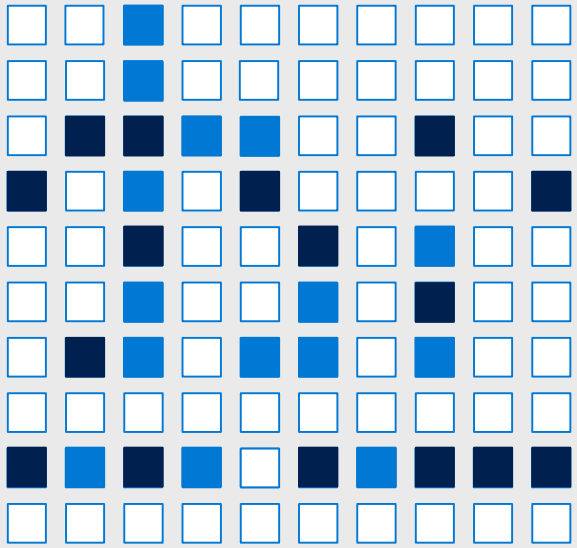
CLOUD

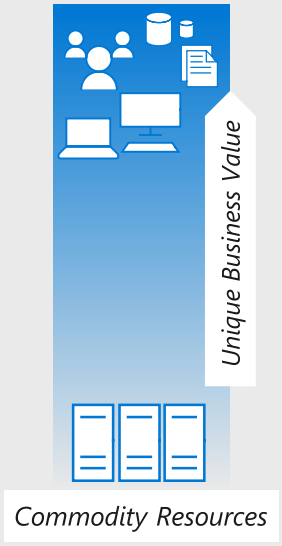


HYGIENE

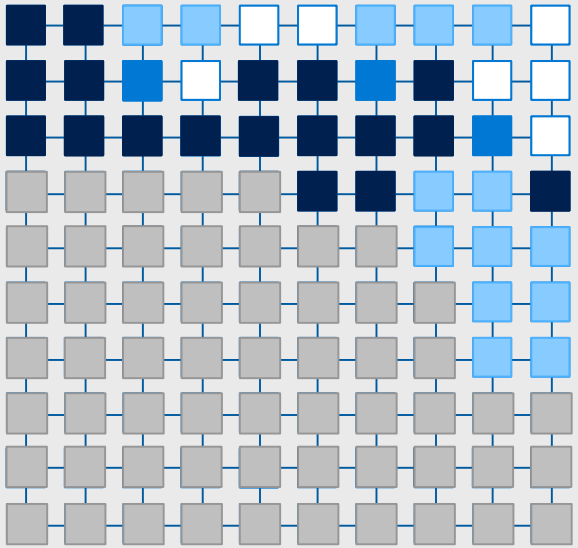
Security Advantages of Cloud Era

TRADITIONAL APPROACH





CLOUD-ENABLED SECURITY



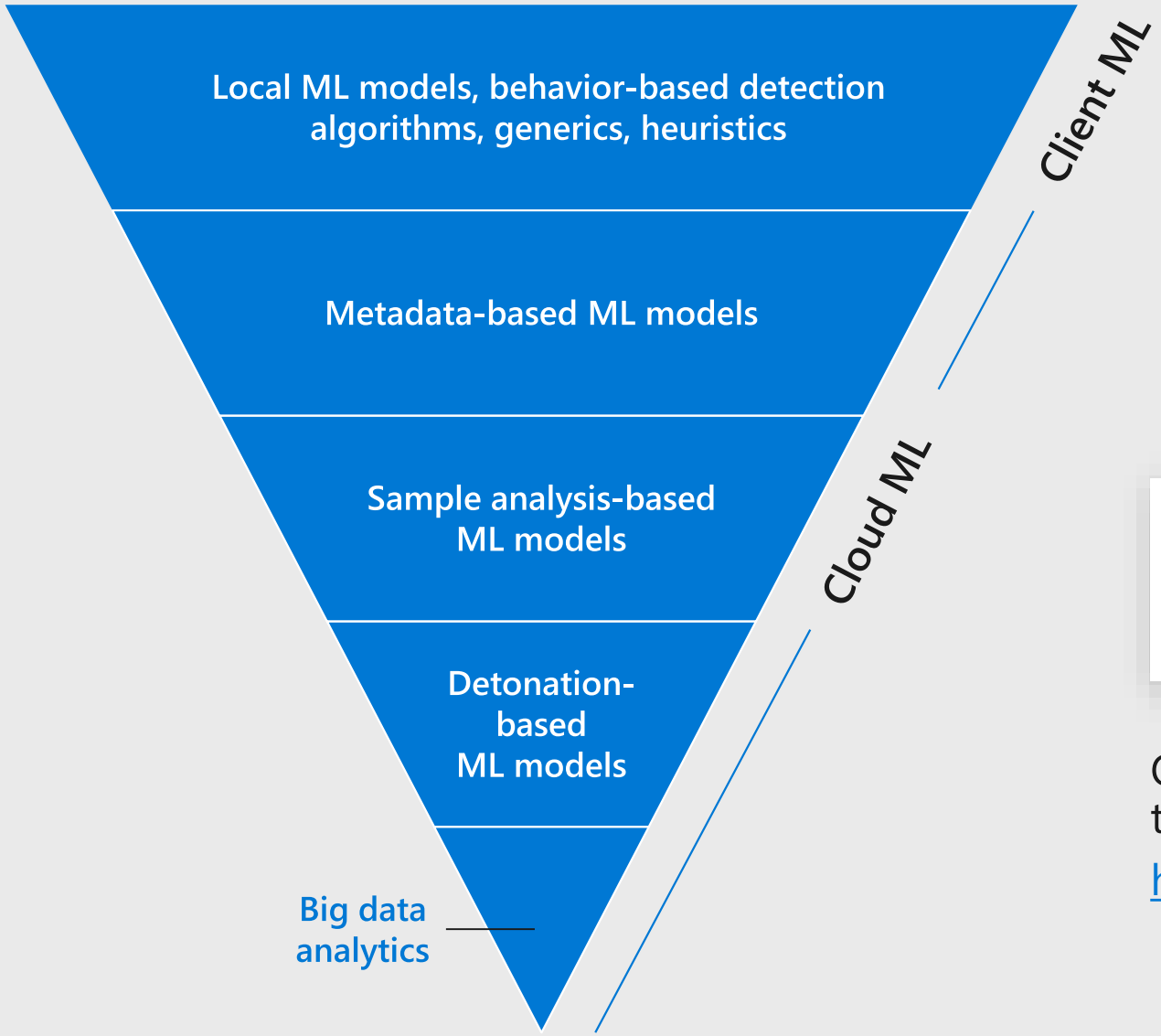
Security is a challenging and under-resourced function

- Satisfied responsibility
- Partially met responsibility
- Unmet responsibility
- Cloud Provider responsibility (Trust but verify)

Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use Cloud intelligence improve detection/response/time

Real world example – Dofoil / Smoke Loader



Protection in milliseconds

Just before noon, behavior-based algorithms detected a massive campaign

Protection in milliseconds

Most components of the attack were blocked at first sight by metadata-based ML models

Protection in seconds

Additional Protection was provided by sample analysis-based ML models for some components

On March 6, Windows Defender Antivirus blocked more than 400,000 instances of several sophisticated trojans

http://aka.ms/dofoil

Other recent cases: Emotet | Bad Rabbit

MINDSET

CLOUD

HYGIENE

Hygiene

Hygiene is critically important, but very difficult

Executive support needed to spend time/money to reduce "Black Swan Nest" of risk

Start with established guidance

NIST, Center For Internet Security (CIS), Microsoft, and DHS have built a clear prioritized roadmap to start with

https://aka.ms/CyberHygiene

Resiliency call to action

Getting to cybersecurity resiliency

Hit Refresh on security mindset, adopt “assume compromise”

- Incidents happen, but you ***must*** manage them well and learn from them

Adopt Cloud Rapidly (especially for security)

- Increase agility and community connection

Focus on hygiene efforts

- Clean up lingering technical debt

Measure Security Success better

- Cost of attack
- Mean time to remediation

Our Incident Learnings
http://aka.ms/IRRG

Hygiene Recommendations
https://aka.ms/CyberHygiene

Security ROI and Cost of Attack
https://youtu.be/maQh35MdFKY

References

Additional Resources

Microsoft Secure Blog
https://cloudblogs.microsoft.com/microsoftsecure/

Security Intelligence Report
www.microsoft.com/sir

Whitepaper - Microsoft as a Trusted Advisor and Partner on Cyber Resilience
https://info.microsoft.com/MicrosoftasaTrustedAdvisorandPartneronCyberResilience-Registration.html

Virtual Security Summit (Recorded)
https://buildazure.com/2018/02/16/microsoft-virtual-security-summit-2018/

Azure Benchmark from center for Internet Security (CIS)
https://www.cisecurity.org/benchmark/azure/

Compliance Manager
https://aka.ms/ComplianceManager

Secure DevOps Toolkit
Documents | Download

Microsoft Finance Digital Transformation

Revenue Reporting

- https://www.microsoft.com/itshowcase/Article/Content/895/Redesigning-our-revenue-reporting-system-for-cloud-architecture
- https://www.microsoft.com/itshowcase/Article/Content/933/Microsoft-reinvents-sales-processing-and-financial-reporting-with-Azure

---

Tax

- https://www.microsoft.com/itshowcase/Article/Content/759/Microsoft-IT-builds-a-big-data-tax-solution-for-Finance-with-Azure

---

Forecast

- https://www.microsoft.com/itshowcase/Article/Content/771/Using-predictive-analytics-to-improve-financial-forecasting
- https://www.microsoft.com/itshowcase/Article/Content/770/Predictive-analytics-improves-the-accuracy-of-forecasted-sales-revenue

TRUST BUT VERIFY

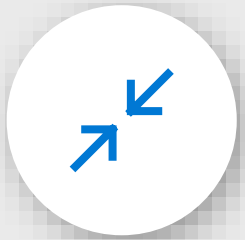
Carefully select & monitor cloud providers

Carefully select & monitor cloud providers

Ensure cloud providers (large or small) provide assurances you need

Compliance

- **Compliant-** Meet all compliance and data sovereignty requirements? (including yearly 3rd party reviews)
- **Assistance -** Does provider invest in helping my organization meet our compliance needs?
  - Self-service artifacts & documentation
  - Assessment & Reporting tools



Alignment

- **Business Model** - Does provider compete with our organization? E.g. (Retail, Advertising, industry services)
- **Data Ownership/Mining** – Does provider (or partners / underlying cloud provider) mine our data or our customers data?

  If so, for what purpose?
  Product Improvement?
  Advertising?
  Other line of business?

Security and Privacy

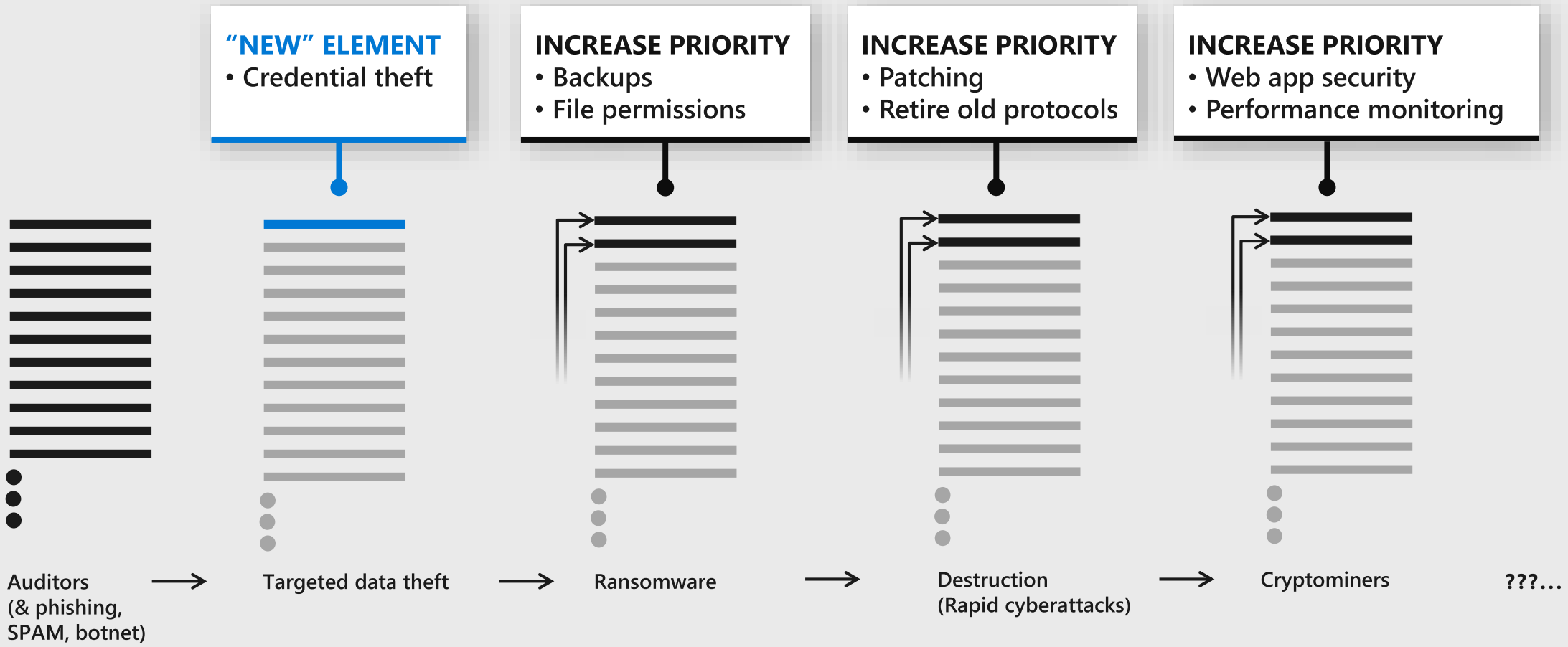
- **Responsible -** Execute well on security best practices? (physical security, patching, backups, secure coding practices, etc.)
- **Responsive/Proactive -** Rapidly correct security issues & notify me of breaches affecting my data? Help me with my security challenges?
- **Resolute -** Reject non-binding requests to disclose personal and other data?
- **Transparent -** Will provider tell me where my data is stored, who has access to it, and why?

"Businesses and users are going to embrace technology only if they can trust it."

Satya Nadella
Chief Executive Officer, Microsoft Corporation

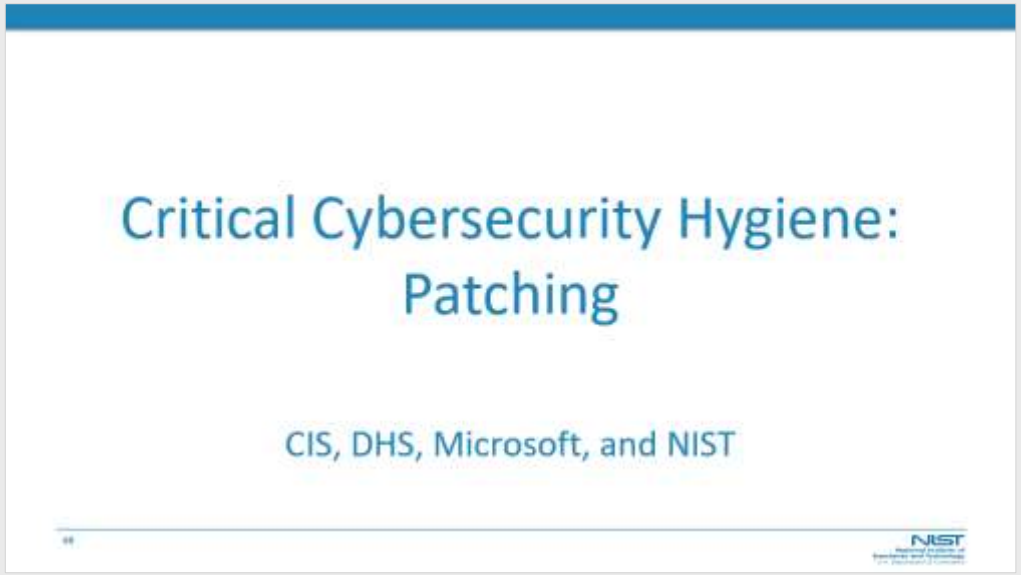
Critical Hygiene = Technical Debt to Pay Off

Cloud can speed this up, but some hard work must be done



New monetization models just reshuffle priorities of same old hygiene debt

Microsoft Investments into Critical Hygiene



CROSS-INDUSTRY PARTNERSHIPS

PLATFORM INVESTMENTS

Critical Cybersecurity Hygiene: Patching

CIS, DHS, Microsoft, and NIST

Security Must Meet Dual Challenges

Innovation

Adapt to new threats and cybersecurity capabilities

Hygiene

Prioritize, Implement, and Sustain well-established best practices

Image from https://upload.wikimedia.org/wikipedia/it/0/04/30-31_Cygni.jpg

Current Hygiene Landscape

- **Important -** Small number of hygiene root causes contribute to many security incidents (massive impact events, data breaches, malware infections, etc.)
  - Applying security hygiene practices make it harder for attackers to succeed and reduces risk of damage (both likelihood and impact)
- **Difficult** - How, when, and what to patch can be difficult decisions for any organization
  - Patching is often resource-intensive, and the act of applying patches can reduce system and service availability
  - Delays in patch deployment create a larger window of opportunity for attackers
  - Existing tools are insufficient for many environments and situations

cyberhygiene@nist.gov

Purpose

Increase cybersecurity ecosystem resiliency by engaging in activities that help organizations rapidly and effectively improve security hygiene.

Current Approach

(Focused on Implementation and Planning)

- **What to do first? –** Prioritized 30-90-beyond roadmaps that help organizations get started with key initiatives
- **How to be successful End-to-end?** – Discover and overcome common obstacles (e.g. stakeholder buy-in, success criteria, architecture/tool gaps, processes, etc.)
- **Connect to Existing Standards –** Connect initiatives to existing standards of good security hygiene

Workgroup Progress To Date (May 2018)

UPDATE + ENDORSE RECOMMENDATIONS
AT HTTP://AKA.MS/RAPIDATTACK
(COMPLETE)

END TO END GUIDANCE FOR
PATCHING PROCESS/TOOLS
(SEEKING INPUT AND FEEDBACK ON PLAN)

cyberhygiene@nist.gov

Summary of Key Recommendations

Measures that directly impact the known attack playbook

https://aka.ms/rapidattack

Quick wins: 0-30 Days

DIRECT ATTACK MITIGATION
RAPID ENABLEMENT

1. Create **destruction-resistant backups** of your critical systems and data
2. Immediately deploy **critical security updates** for OS, browser, & email
3. **Isolate (or retire) computers** that cannot be updated and patched
4. Implement **advanced e-mail and browser protections**
5. Enable host anti-malware and network defenses get near-**realtime blocking responses from cloud** (if available in your solution)
6. Implement **unique local administrator passwords** on all systems
7. Separate and protect **privileged accounts**

Less than 90 Days

DIRECT ATTACK MITIGATION
LONGER ENABLEMENT

1. **Validate** your backups using standard restore procedures and tools
2. **Discover and reduce** broad permissions on file repositories
3. Rapidly deploy all **critical security updates**
4. **Disable unneeded** legacy protocols
5. **Stay current –** Run only current versions of operating systems and apps

Next Quarter + Beyond

NIST National Cybersecurity Center of Excellence (NCCoE)

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

CyberHygiene@NIST.gov

- Share your thoughts and feedback
  - **Organization -** How your patch mitigation program works
    - Acquisition requirements for vendors
    - Patch Deployment processes (stages, speed, criteria)
    - Isolation strategies (for unpatchable assets like aging OT/ICS/SCADA/etc.)
    - Other insights
  - **Security Vendor**
    - Interested in participation in NCCoE lab testing