Microsoft

Microsoft CISO Workshop
2 – Security Management

Microsoft Cybersecurity Solutions Group

Overall Principles + Security Management Strategy

KEY PRINCIPLES

RUIN
ATTACKER ROI

PRODUCTIVITY
AND SECURITY

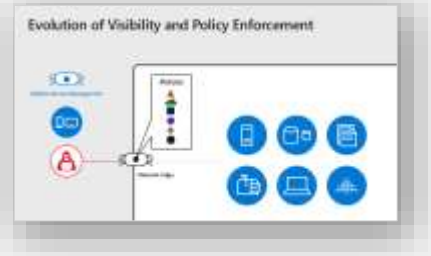
ASSUME
COMPROMISE

SHARED
RESPONSIBILITY

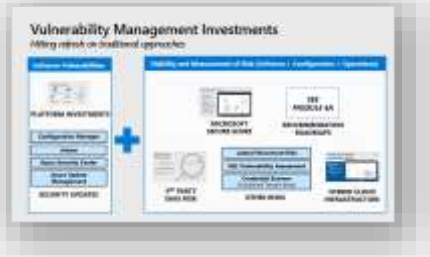
CLOUD IS
MORE SECURE

SECURITY MANAGEMENT

SUCCESS CRITERIA
& USE CASES



VISIBILITY, CONTROL,
& GUIDANCE

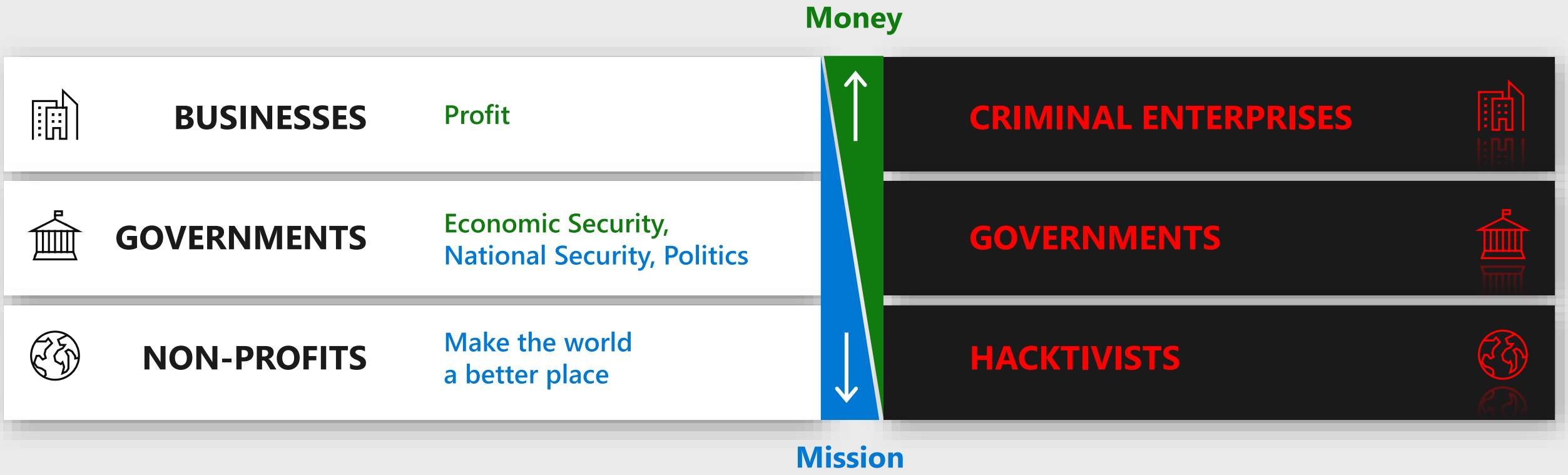


VULNERABILITY
MANAGEMENT

SECURITY
TRANSFORMATION

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

Disrupt Attacker ROI

Prioritize investments to maximize impact

Security Return on Investment (SROI)

Defender Return:

Ruin Attacker ROI

Deters opportunistic attacks

Slows or stops determined attacks

Defender Investment:

Security budget

Team time/attention

Rapid detection and response drives down predictability and quantity of return

Attacker Return:
Successful Monetization

Attacker Investment:
Increase Attack Friction & Cost

Prioritizing defense can rapidly raise impact attacker cost & friction

Cost of Attack Video

https://youtu.be/maQh35MdFKY

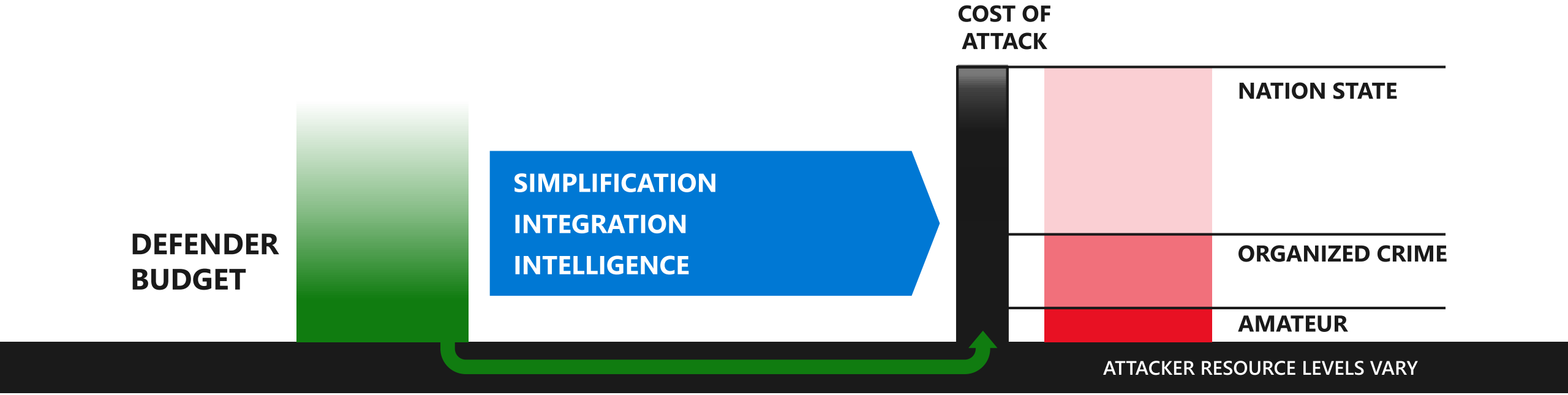
Ruin Their ROI

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

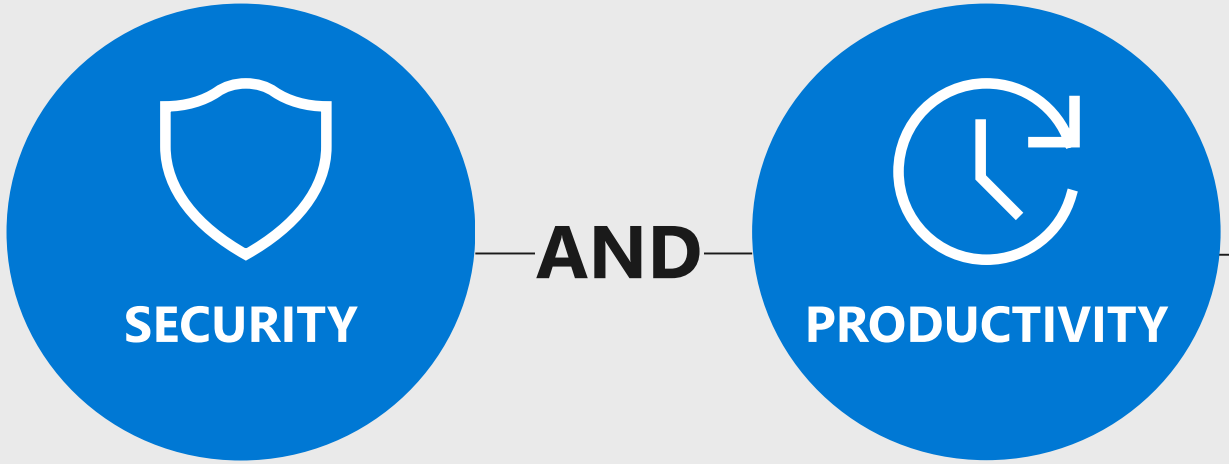
MICROSOFT:
SIMPLIFY ADVANCED CAPABILITIES
across platforms, clouds, and IoT



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

The New Imperative

Enable people to use devices and apps that work best for them, from anywhere, while protecting against current threats



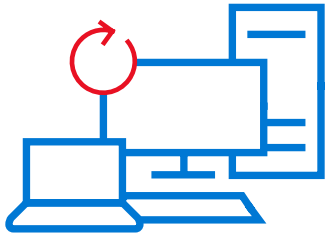
COMMON INITIATIVES

Biometric and Smart Card Authentication
Mobile Application Management
Self Service Password Reset
Conditional Access to Resources
...and more

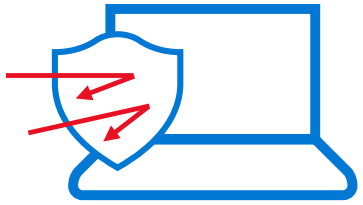
Designing for Failure – The Mindshift

THEN

Reliability:
Designed not to fail

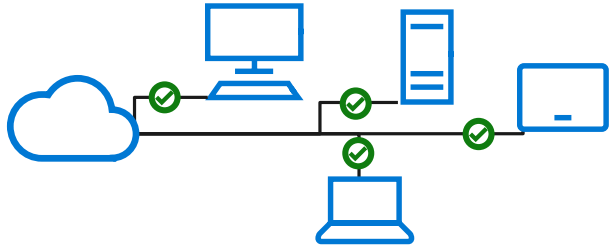


Prevent:
Every possible attack

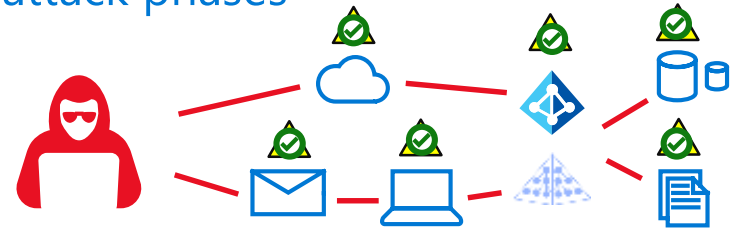


NOW

Resilience:
Designed to recover quickly



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



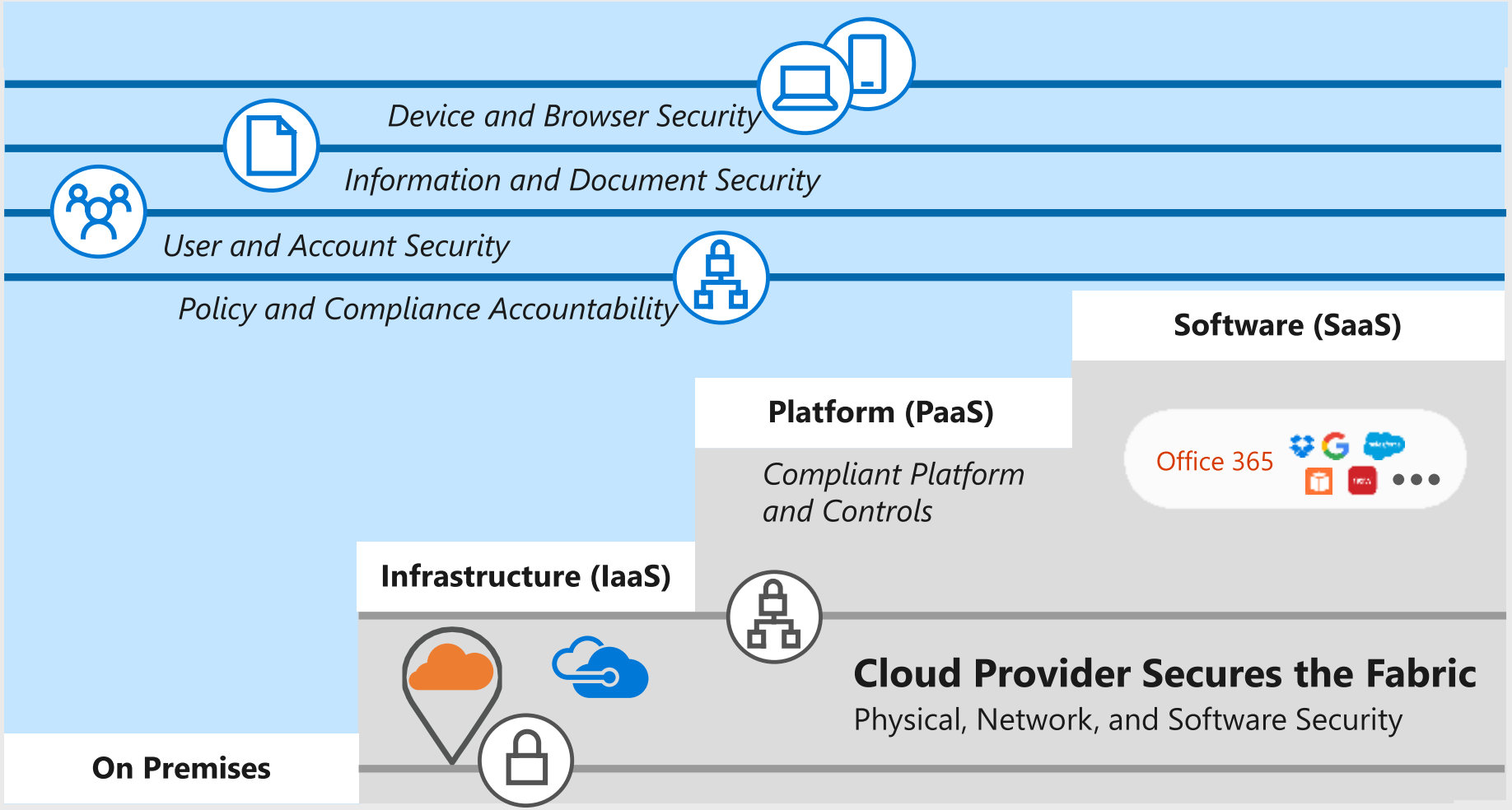
Cloud Security is a partnership

Sharing *security*, *privacy*, and *compliance* responsibility with cloud provider(s)

Usage
Always your responsibility

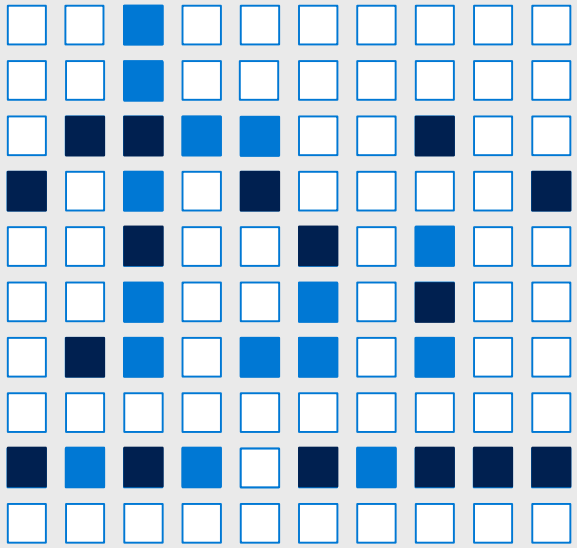
Service
Responsibility varies by service type

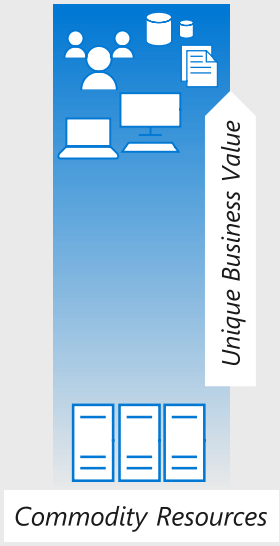
Fabric
Your or your cloud provider's responsibility



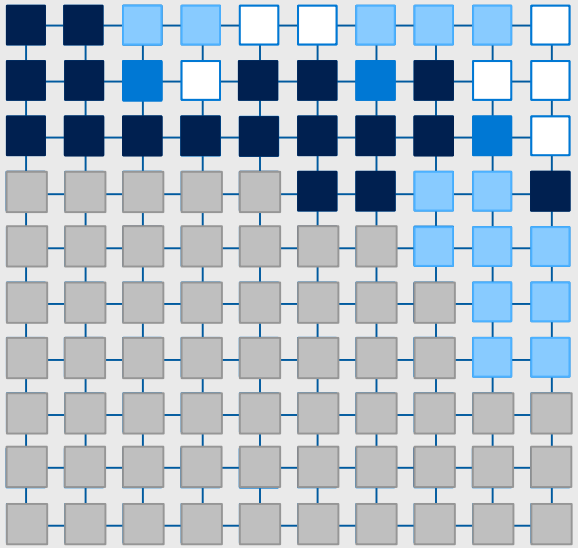
Security Advantages of Cloud Era

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 to improve detection/response time

Imperatives and Opportunities

Recognize Fundamental Transformations

Meet Challenges + *Embrace Opportunities*

DRIVE STRATEGIC OUTCOMES

Security Management

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

Identity and Access Management

Ensure only the right people have access to your organizational systems

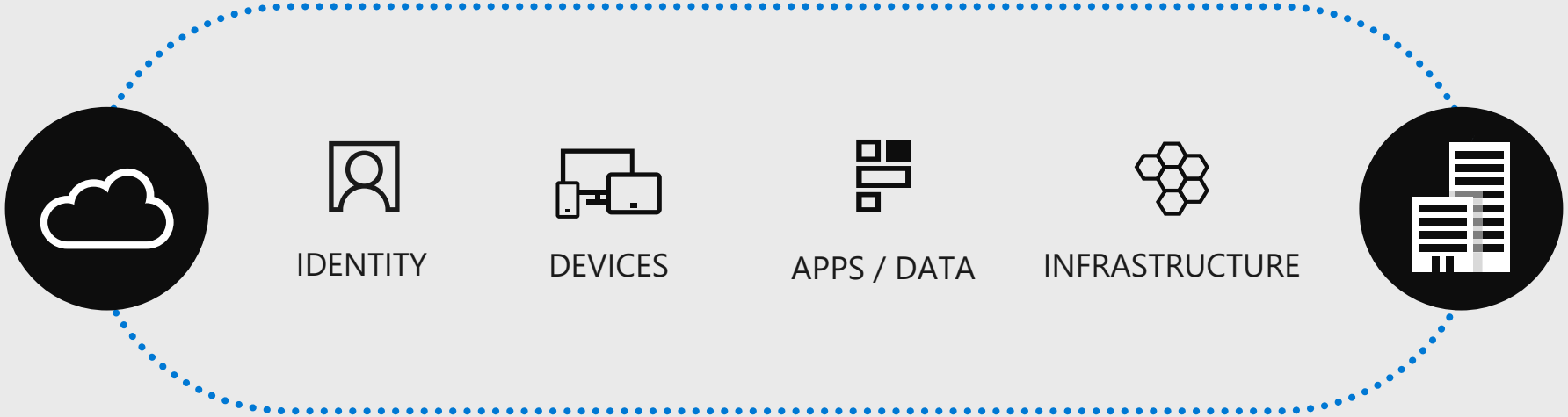
Information Protection

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

Threat Protection

Thwart hackers and recover quickly if attacked

SECURITY MANAGEMENT IMPERATIVES



VISIBILITY

Understand the security state and risks across resources

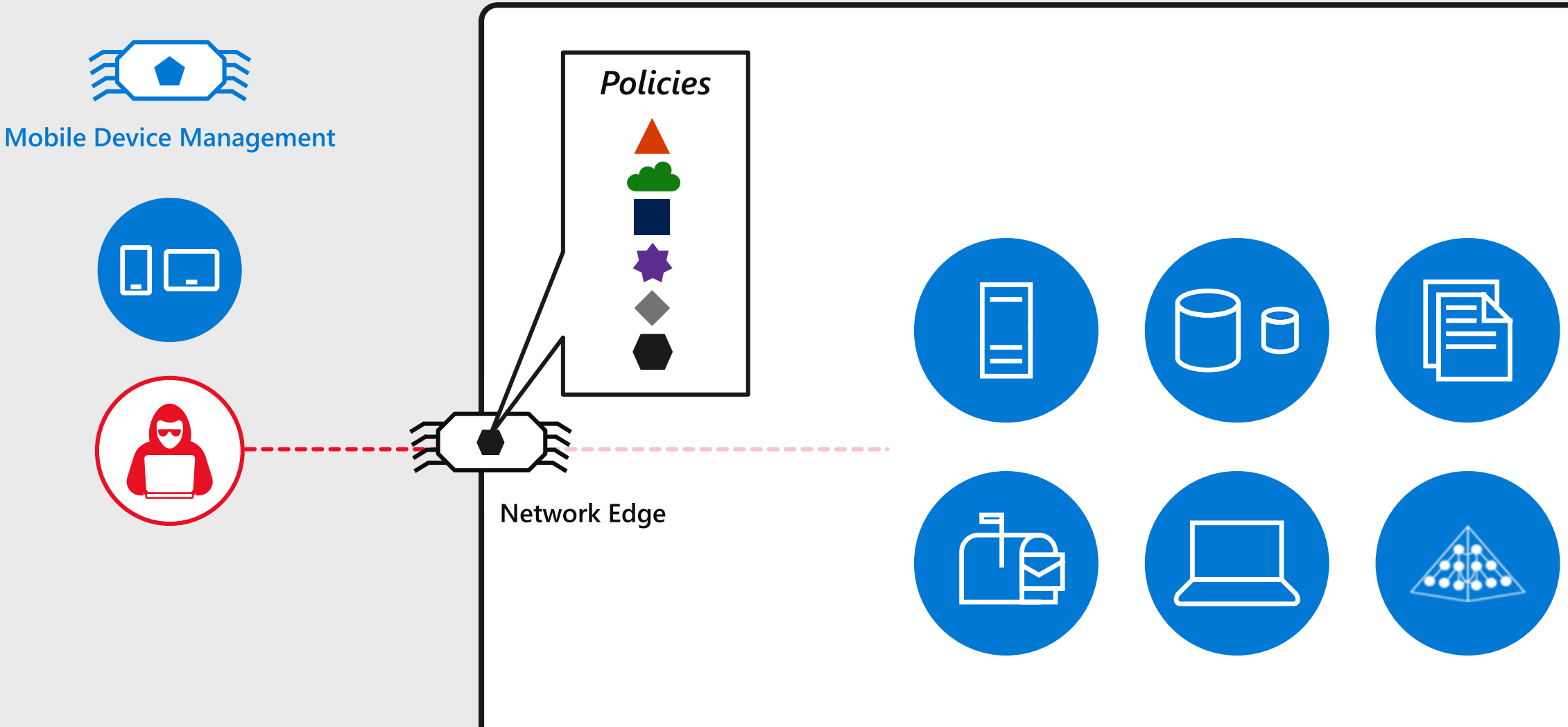
CONTROL

Define consistent security policies and enable controls

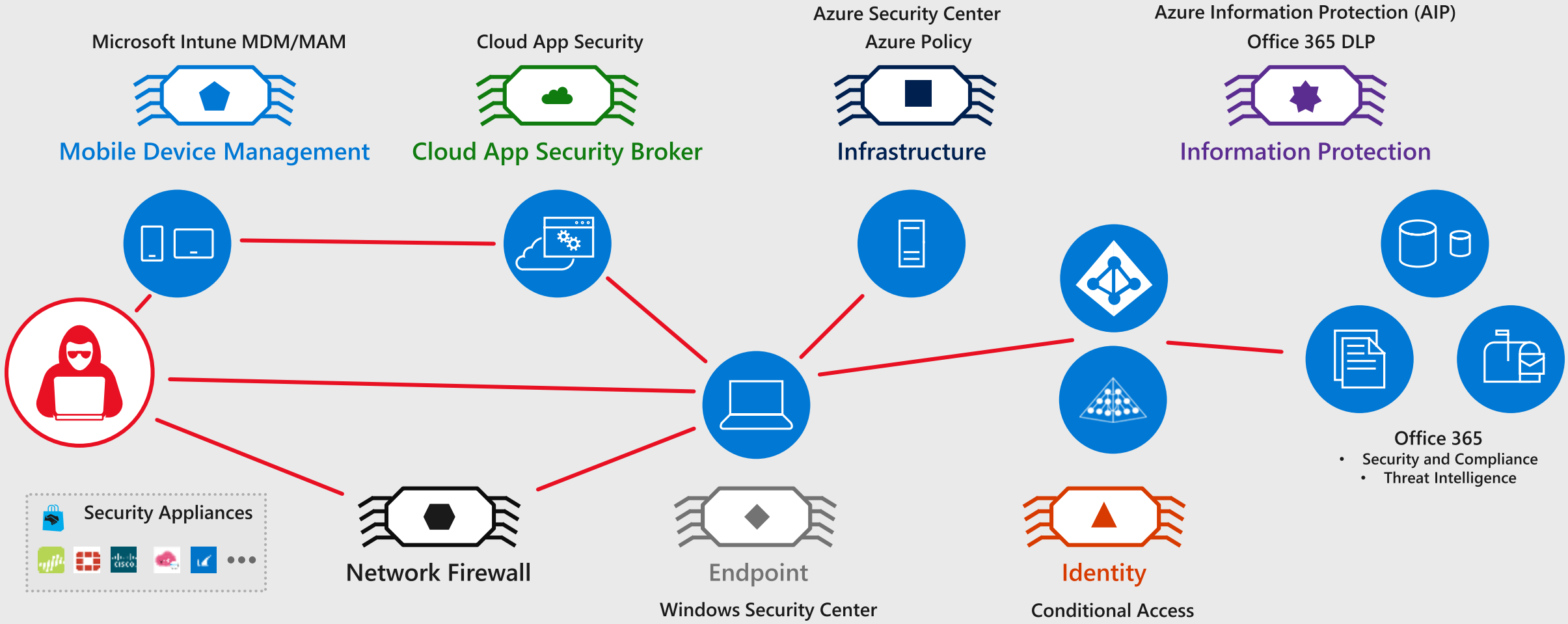
GUIDANCE

Elevate security through built-in intelligence and recommendations

Evolution of Visibility and Policy Enforcement



Evolution of Visibility and Policy Enforcement



As assets leave the single managed network, use policy controls focused on managing them

Visibility, Control, and Recommendations across your estate

Infrastructure

On Premises & Other Clouds

Microsoft Azure

Apps and Data

Office 365

Devices

Mobile & Unmanaged

Managed

IoT

Visibility

Monitor policy compliance across hybrid cloud infrastructure
- Security Updates
- Anti-malware signatures
- Security Configuration

Enterprise Configuration Management

Discover 14,000+ SaaS apps, manage them

Sensitive document classification and tracking (anywhere on internet)

Trends on Tenant and Industry

Measure Device Health and Compliance
- Managed, Compliant, (Not) Compromised)

Inventory & Manage IoT Devices

Enterprise Configuration Management

Control

Alert on policy violations

Automated vulnerability remediation in Azure (runbooks + native webhooks)

Single identity across SaaS + Intranet

Alert and take action on policy violations (e.g. quarantine overshared files)

Sensitive document encryption access revocation

Mobile Device & Application Management

Author policies, track deployment & state

Conditional Access to accounts/apps

Guidance

Recommended security configurations

Threat intelligence reports and mitigation guidance

Risk ratings on 16k+ SaaS applications

O365 Tailored Security Guidance and Prescriptive Recommendations

Tailored Security Guidance and Prescriptive Recommendations

IoT Reference Architecture with Threat Modelling, Security Maturity Model, and other Guidance

Vulnerability Management Investments

Hitting refresh on traditional approaches

Software Vulnerabilities

PLATFORM INVESTMENTS

- Configuration Manager
- Intune
- Azure Security Center
- Azure Update Management

SECURITY UPDATES

Visibility and Measurement of Risk (Software + Configuration + Operations)

MICROSOFT SECURE SCORE

SEE MODULE 4A

RECOMMENDATION ROADMAPS

3RD PARTY SAAS RISK

- Lateral Movement Risk
- SQL Vulnerability Assessment
- Credential Scanner (Published Tenant Keys)

OTHER RISKS

HYBRID CLOUD INFRASTRUCTURE

Security Transformation

Consider a **program of change** including strategy, planning, execution, and governance

Common challenges:

... network security is regularly bypassed with phishing and credential theft

... SIEMs and other tools overload analysts more than empowering them

... overwhelming security hygiene requirements for devices, identity, applications, etc.

... data is everywhere and constantly at risk

Imagine a future where:

... your identities cannot be stolen

... untrusted software cannot run

... and users can click fearlessly (and safely)

... data is automatically classified and protected wherever it goes

Align with Business Leaders

Digital transformation is challenging for business leaders to navigate and security can partner to help them manage risk while enabling productivity

Services to Accelerate Transformation

Microsoft Enterprise Cybersecurity Advisory Service (ECAS) can help accelerate security's digital transformation by helping create a cybersecurity program of change. http://aka.ms/ECAS-Datasheet

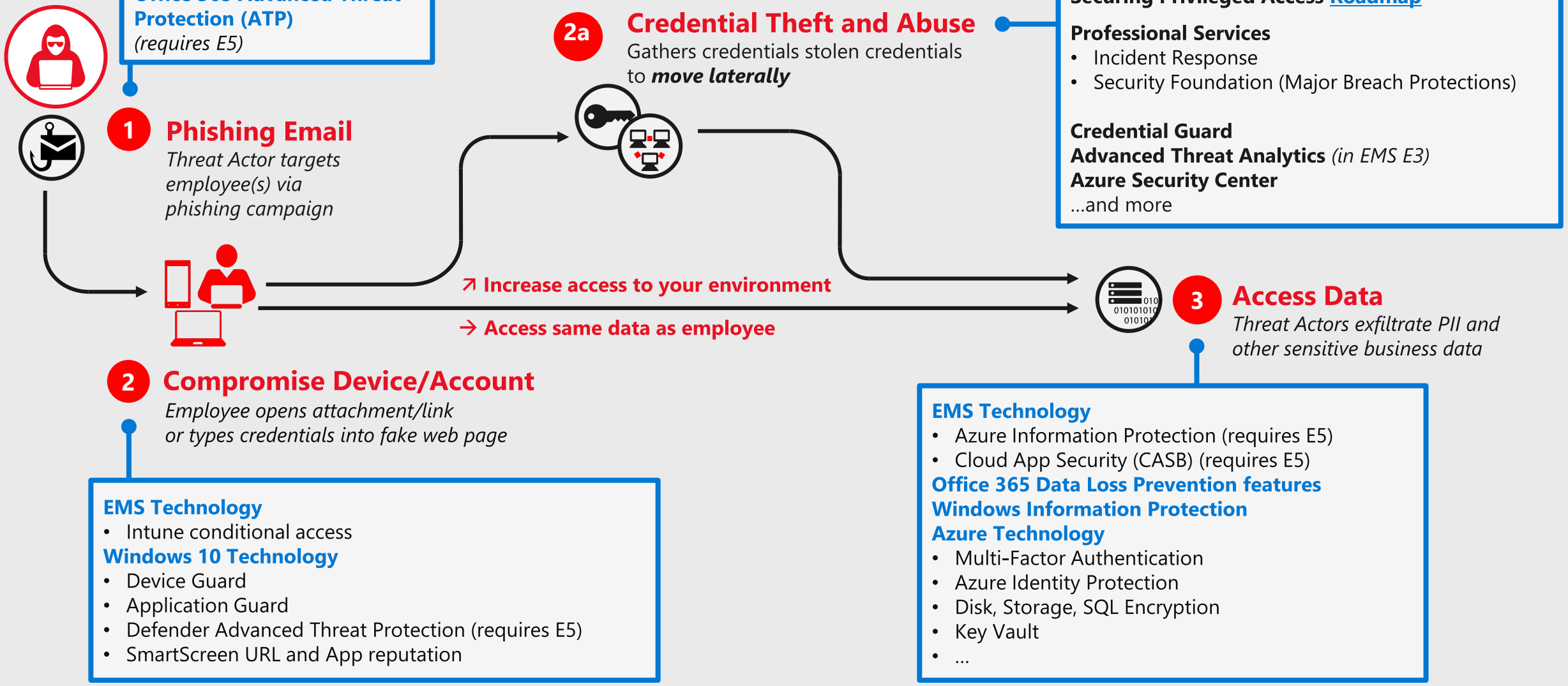
Microsoft

Questions?

Microsoft

References

Common attack steps and mitigations



Common Attacks

PLAN | ENTER | TRAVERSE | EXECUTE MISSION

A. Enter and Navigate

Any employee opens attack email
→ **Access to most/all corporate data**

Any

Office 365 Technology
- Advanced Threat Protection *(requires E5)*

1 Threat Actor targets employee(s) via phishing campaign

2a Workstation compromised, threat actor gathers credentials

Windows 10 Technology
- Device Guard
- Credential Guard
- Defender Advanced Threat Protection *(requires E5)*

3a Threat Actors use stolen credentials to *move laterally*

Published Guidance
- Securing Privileged Access Roadmap

Professional Services
- Security Foundation
- Enhanced Security Admin Environment (ESAE)

Technology
- Advanced Threat Analytics (in EMS E3)
- Azure Security Center
- ...and more

B. Device Compromise

Targeted employee opens attack email
→ **Access to same data as employee**

2b Employee B opens infected email (Mobile or PC). Attacker disables antivirus

EMS Technology
- Intune conditional access

C. Remote Credential Harvesting

Targeted employee(s) enter credentials in website
→ **Access to same data as employee(s)**

2c Credentials harvested when employee logs into fake website

Windows 10 Technology
- SmartScreen URL and App reputation
- Application Guard

3bc Compromised credentials/ device used to access cloud service / enterprise environment

EMS Technology
- Cloud App Security (CASB) *(requires E5)*

Office 365 Technology
- Advanced Security Management (basic CASB) *(requires E5)*

Azure Technology
- Multi-Factor Authentication
- Azure Identity Protection

4 Threat Actors exfiltrate PII and other sensitive business data

EMS Technology
- Azure Information Protection (requires E5)

Office 365 Technology
- Data Loss Prevention

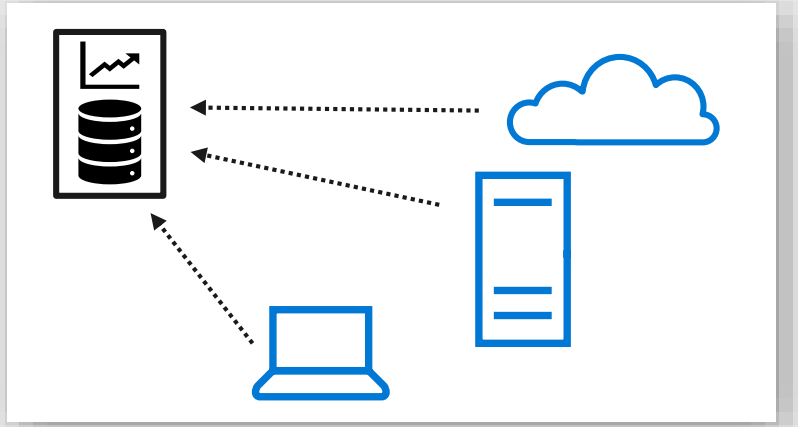
Windows 10 Technology
- Windows Information Protection

Azure Technology
- Disk, Storage, SQL Encryption
- Key Vault
- ...

Microsoft **Incident Response** Teams can be engaged to investigate any incident type as well as to assess your organization for existing compromises

Integrating with your SIEM

Two different approaches to connect to your existing SIEM tool and processes



1. Graph Security API

SIEM Integration - https://docs.microsoft.com/en-us/graph/security-siemintegration

Solutions already Integrated - https://docs.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-1.0

2. Individual Capabilities

- **Windows Defender ATP**

  https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/enable-siem-integration-windows-defender-advanced-threat-protection

- **Azure Advanced Threat Protection**

  https://docs.microsoft.com/en-us/azure-advanced-threat-protection/cef-format-sa

- **Office 365**

  https://docs.microsoft.com/en-us/office365/securitycompliance/siem-server-integration

  https://docs.microsoft.com/en-us/office365/securitycompliance/siem-integration-with-office-365-ti

- **Cloud App Security**

  https://docs.microsoft.com/en-us/cloud-app-security/siem

- **Azure SIEM Integration (includes Azure AD)**

  https://docs.microsoft.com/en-us/azure/azure-monitor/overview

VISIBILITY

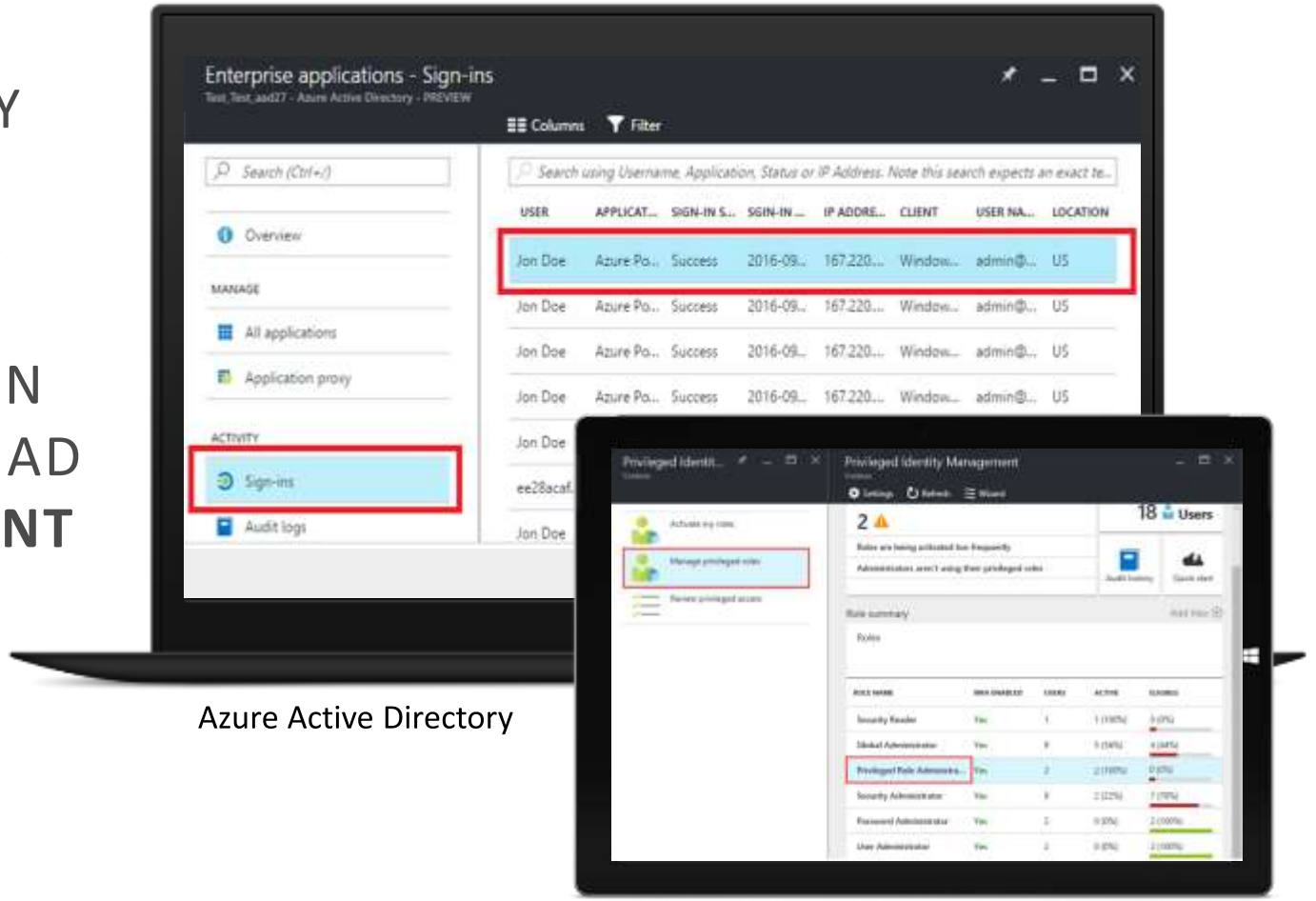
Understand the security state and risks across resources

IDENTITY

UNDERSTAND SECURITY STATE OF USERS

GAIN VISIBILITY INTO THE SECURITY OF YOUR DIRECTORY WITH **ACCESS** AND **USAGE REPORTS** IN AZURE AD

DISCOVER PRIVILEGED ACCOUNTS IN YOUR ENVIRONMENT WITH AZURE AD **PRIVILEGED IDENTITY MANAGEMENT**



Azure Active Directory

UNDERSTAND SECURITY STATE OF DEVICES

BROAD VISIBILITY INTO THE **ENDPOINT SECURITY**

QUICKLY ASSESS THE SCOPE OF **INCIDENTS AND ROOT CAUSES**

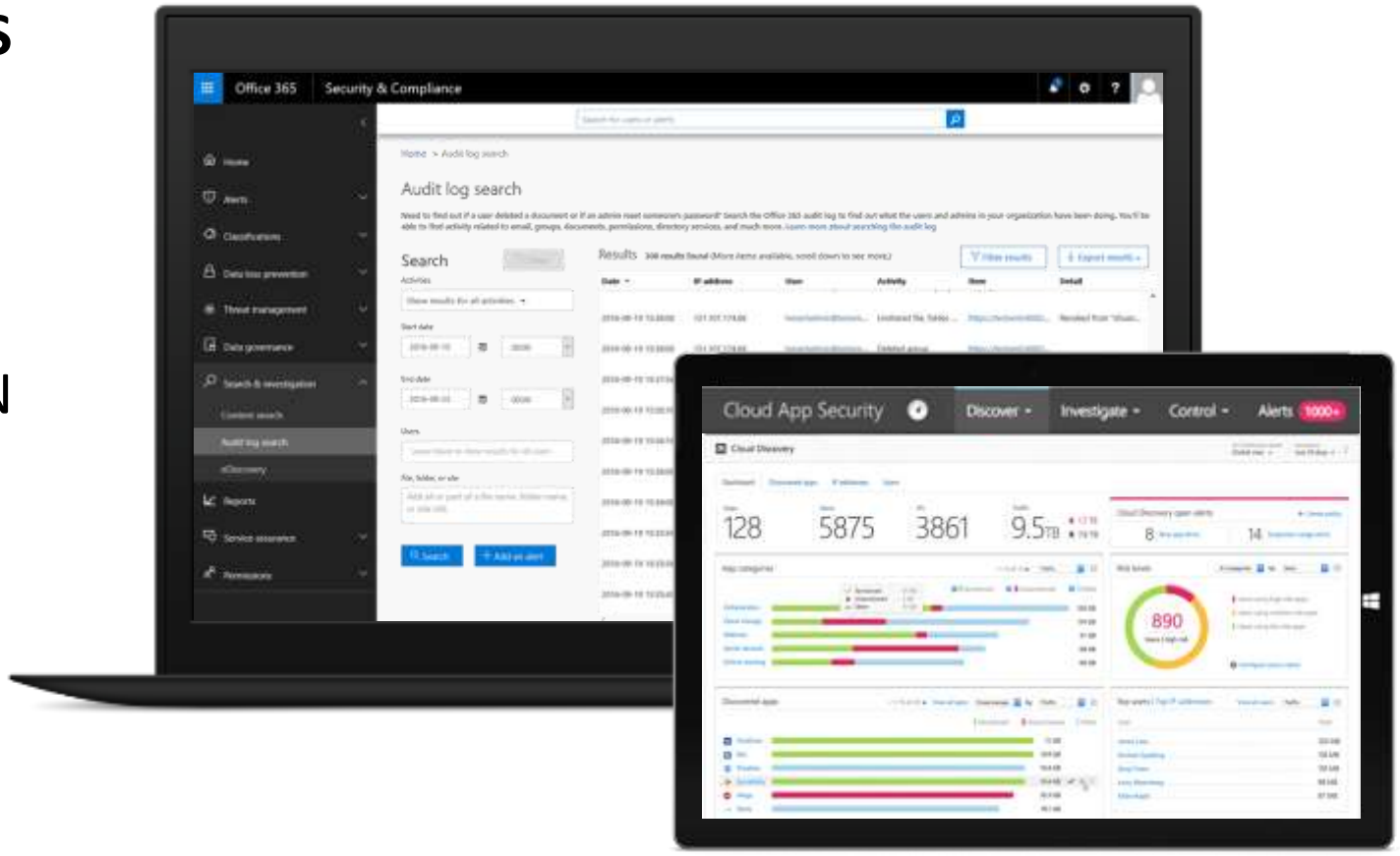
RICH TOOLSET FOR **INVESTIGATION AND REMEDIATION ACTIONS**

UNDERSTAND SECURITY STATE OF APPS & DATA

GAIN VISIBILITY INTO **CLOUD APPS** USED IN YOUR ENVIRONMENT & GET A **RISK ASSESSMENT**

AUDIT LOGS AND REPORTS TO HELP **DETECT ACTIVITY** WITHIN PRODUCTIVITY APPS

ALERTS TO HELP YOU **SEE ANOMALOUS ACTIVITY**

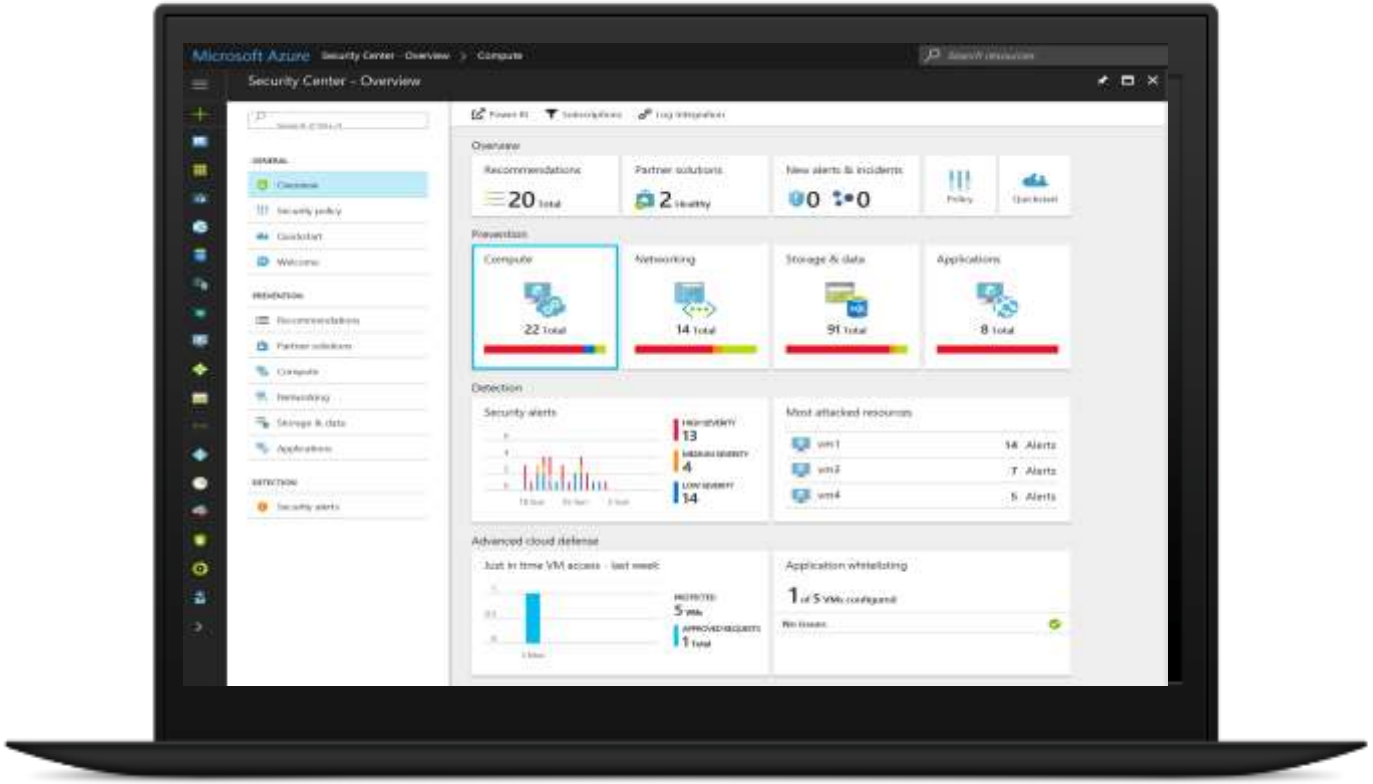


UNDERSTAND SECURITY STATE OF WORKLOADS ACROSS HYBRID INFRASTRUCTURE

MONITOR SECURITY STATE OF RESOURCES ACROSS **CLOUD AND ON-PREMISES**

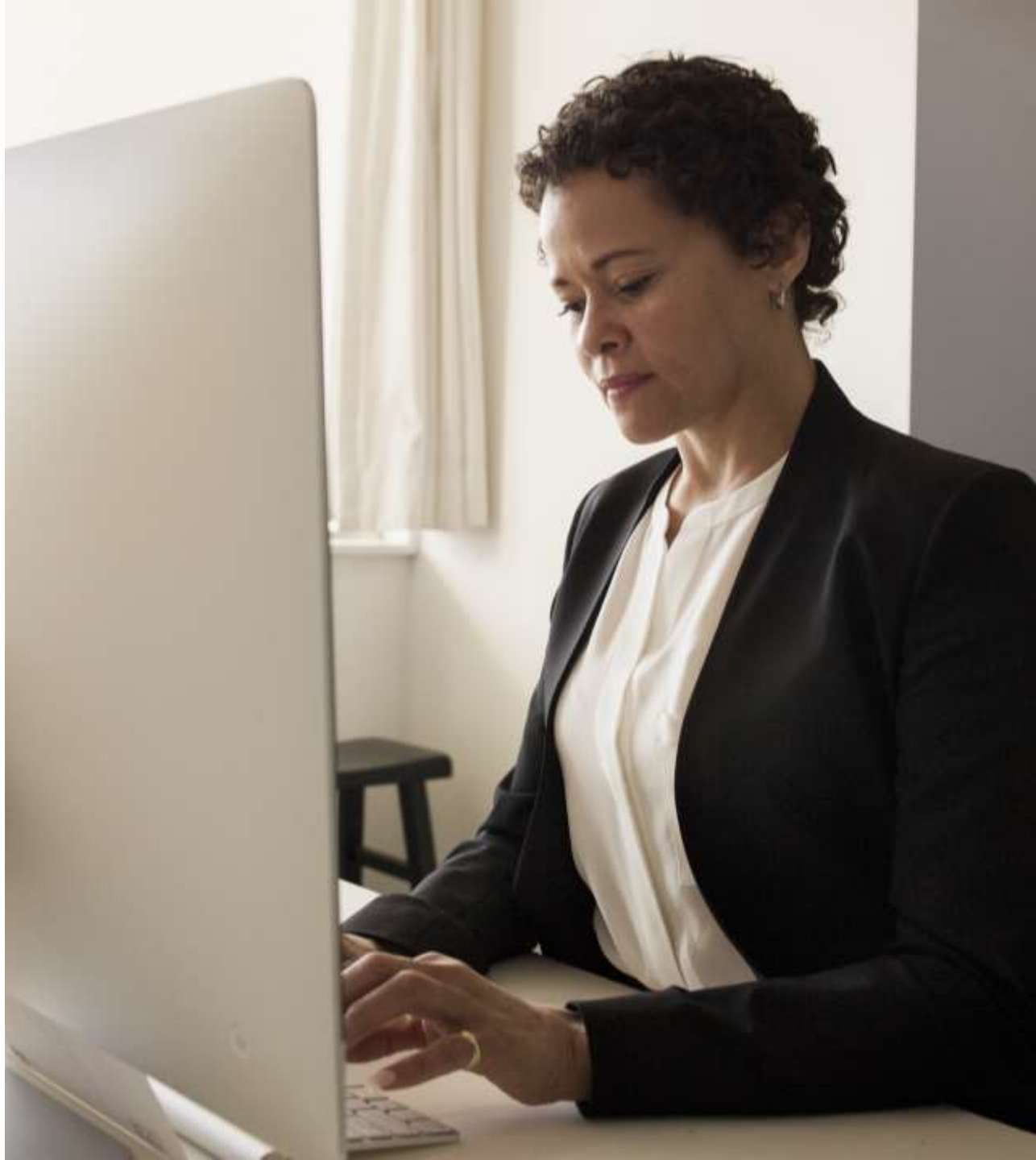
IDENTIFY VULNERABILITIES **WITH CONTINOUS ASSESSMENT**

INVESTIGATE WITH **ADVANCED LOG ANALYTICS AND SIEM INTEGRATION**



CONTROL

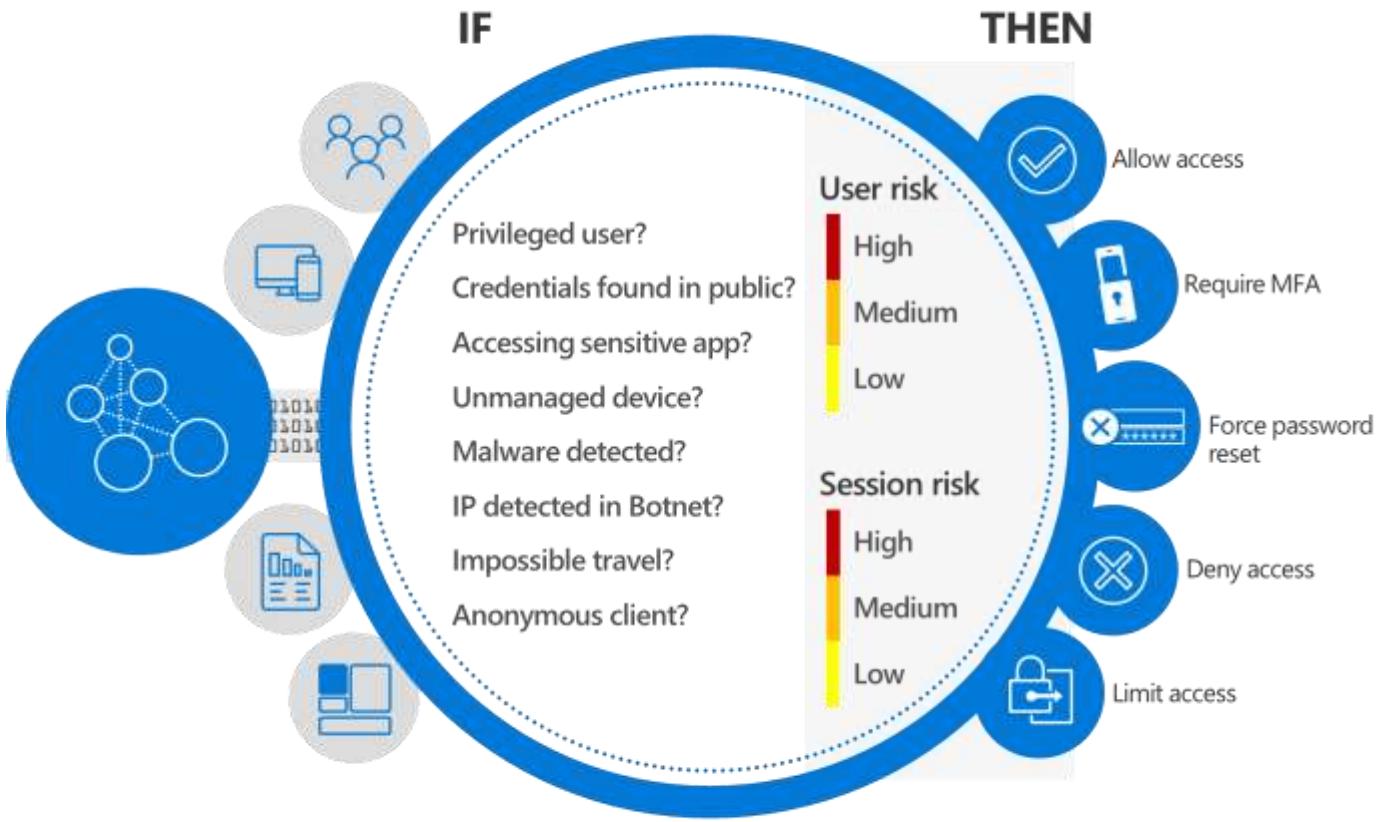
Define consistent security policies and enable controls



DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR USERS

USE **CONDITIONAL ACCESS** TO PROTECT YOUR ORGANIZATION AT THE FRONT DOOR

CONTROL AND PROTECT **PRIVILEGED IDENTITIES**

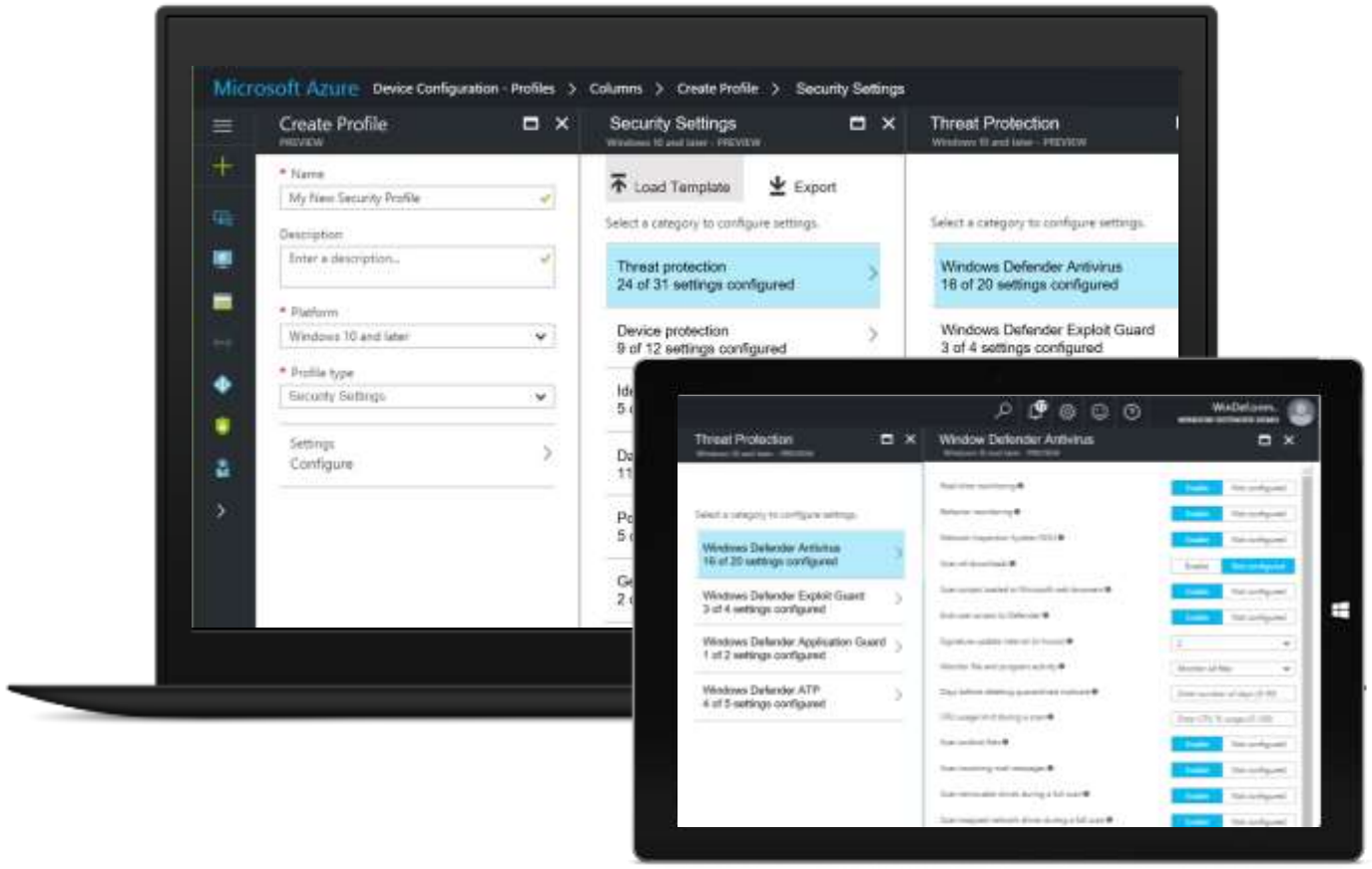


DEVICES

DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR DEVICES

ONE PLACE TO CONFIGURE THE **FULL WINDOWS SECURITY STACK**

CONTROL **DEVICE SECURITY POLICIES** AND SEE THE **DEPLOYMENT STATUS** IN A CENTRAL PLACE

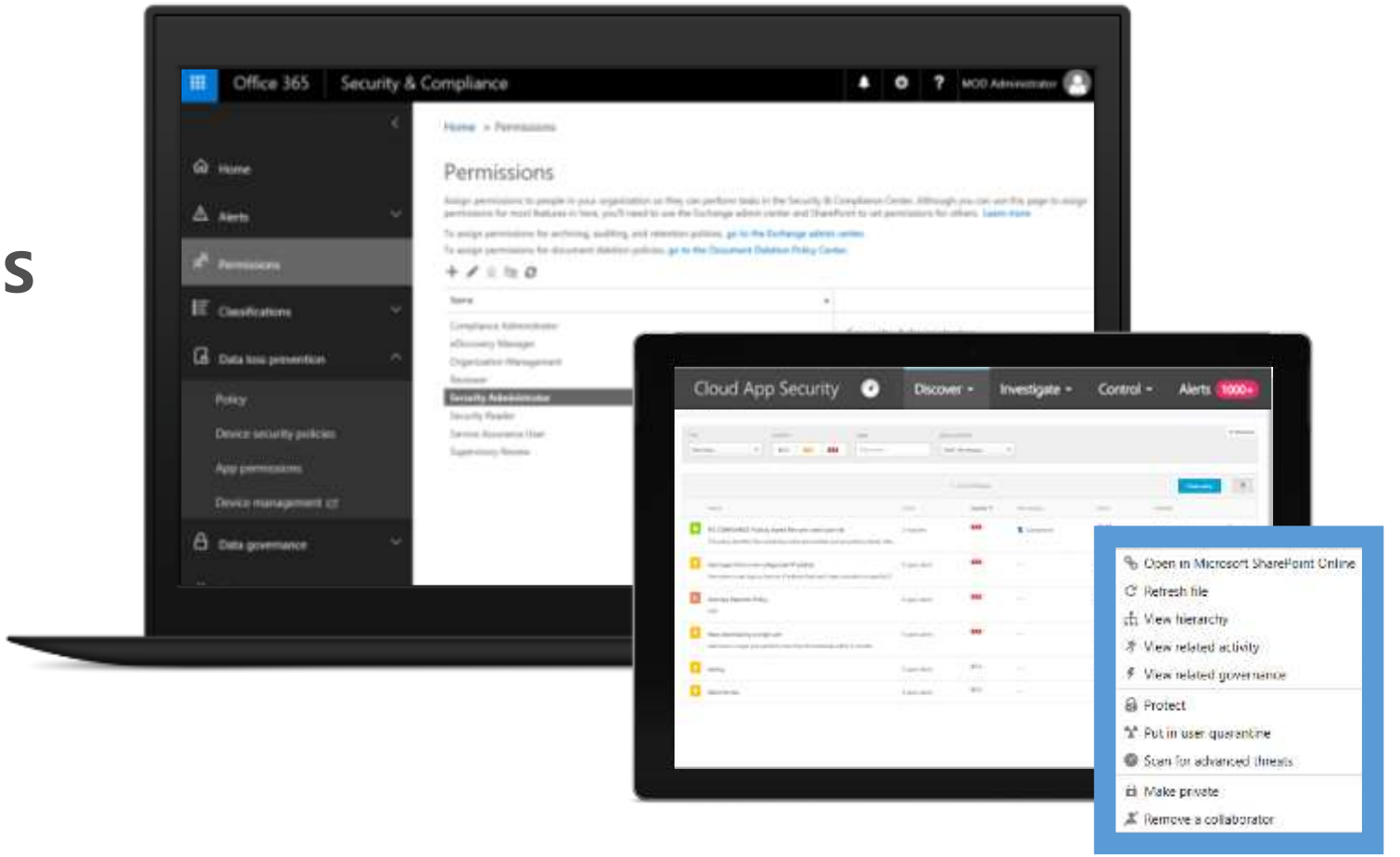


DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR APPS & DATA

CUSTOMIZABLE PORTAL FOR MOST IMPORTANT SECURITY FEATURES FOR **PRODUCTIVITY APPS**

CONTROL DATA **IN CLOUD APPS** WITH GRANULAR POLICIES FOR DLP AND DATA SHARING

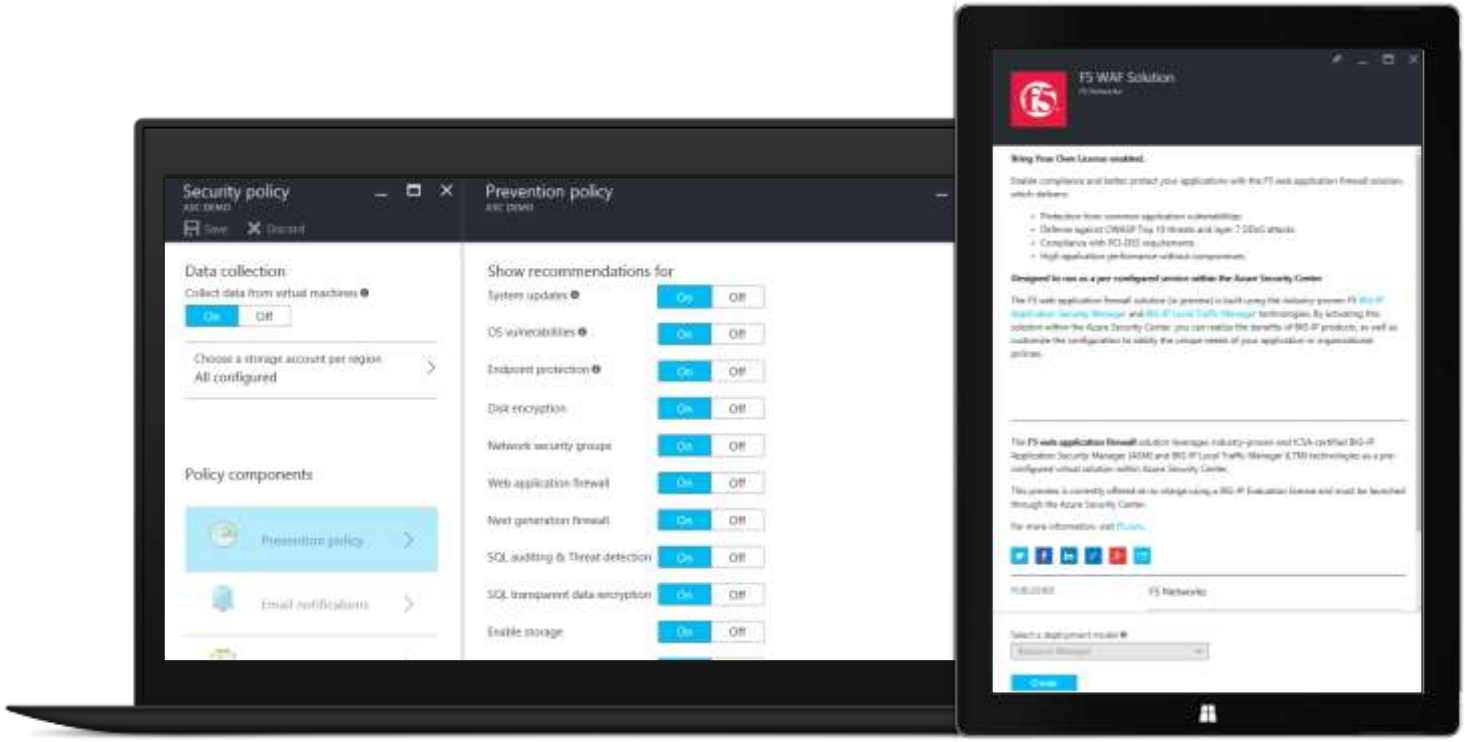
SEE **SECURITY CONTROLS AND THEIR STATUS** FROM DIFFERENT WORKLOADS



DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR WORKLOADS ACROSS HYBRID INFRASTRUCTURE

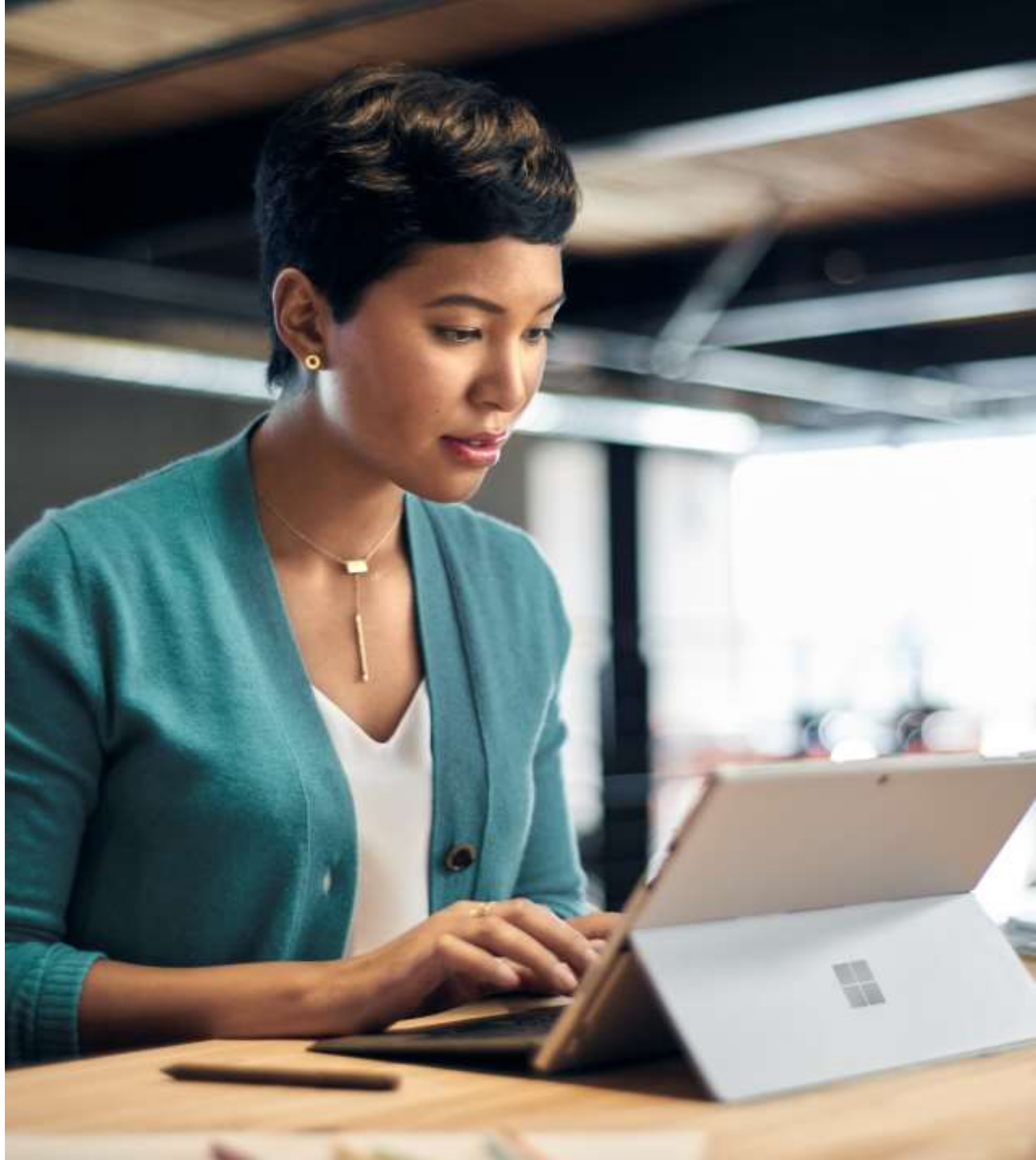
SET SECURITY POLICIES FOR RESOURCES IN THE CLOUD

RAPIDLY DEPLOY **BUILT-IN CONTROLS AND PARTNER SOLUTIONS** FOR THE CLOUD



GUIDANCE

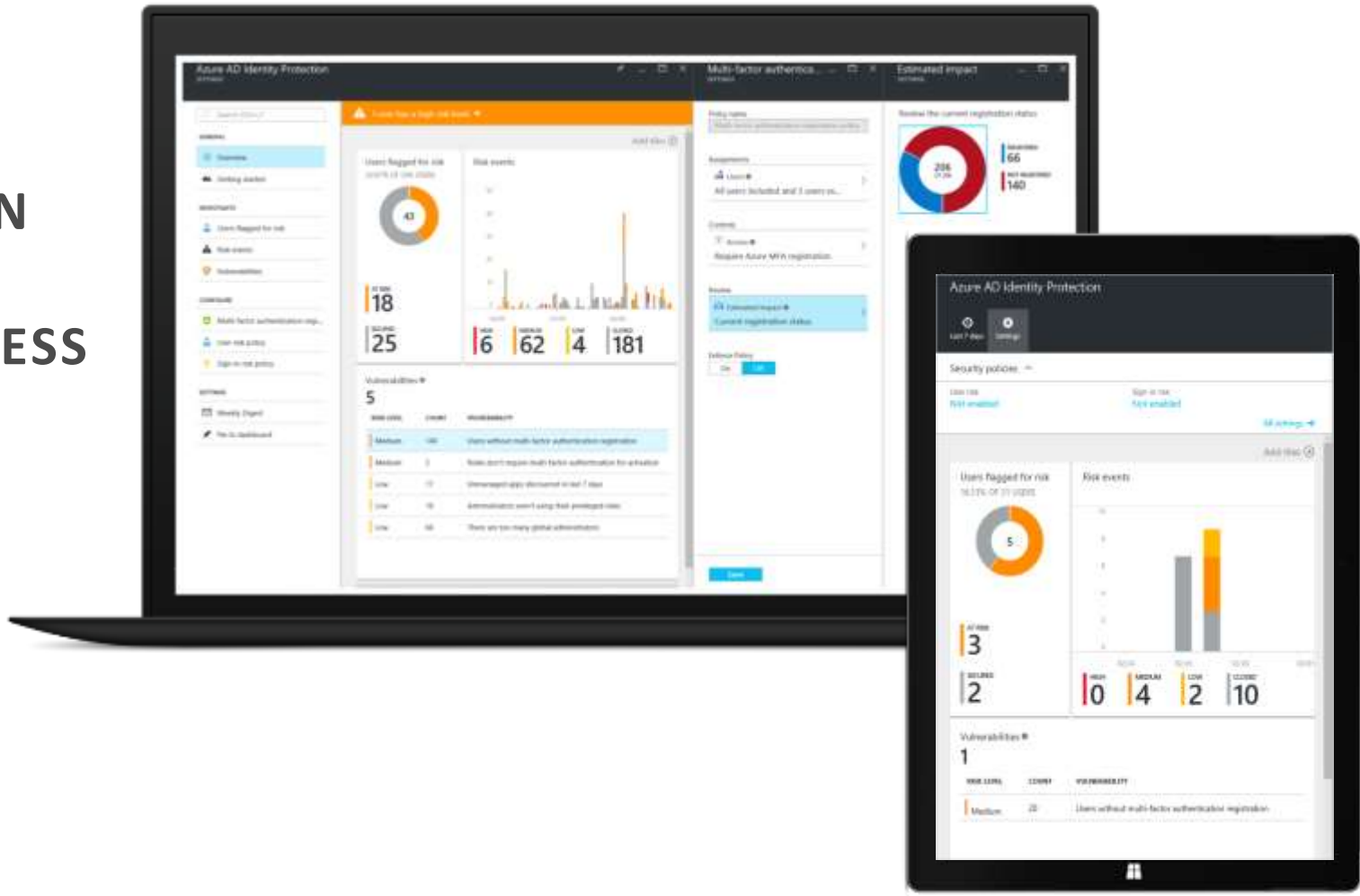
Enhance security through built-in intelligence and recommendations



BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR USERS

IDENTITY

TAKE ADVANTAGE OF ADVANCED SECURITY REPORTS, **REMEDIATION RECOMMENDATIONS** AND RISK-BASED POLICIES TO **PROTECT ACCESS** IN YOUR ORGANIZATION

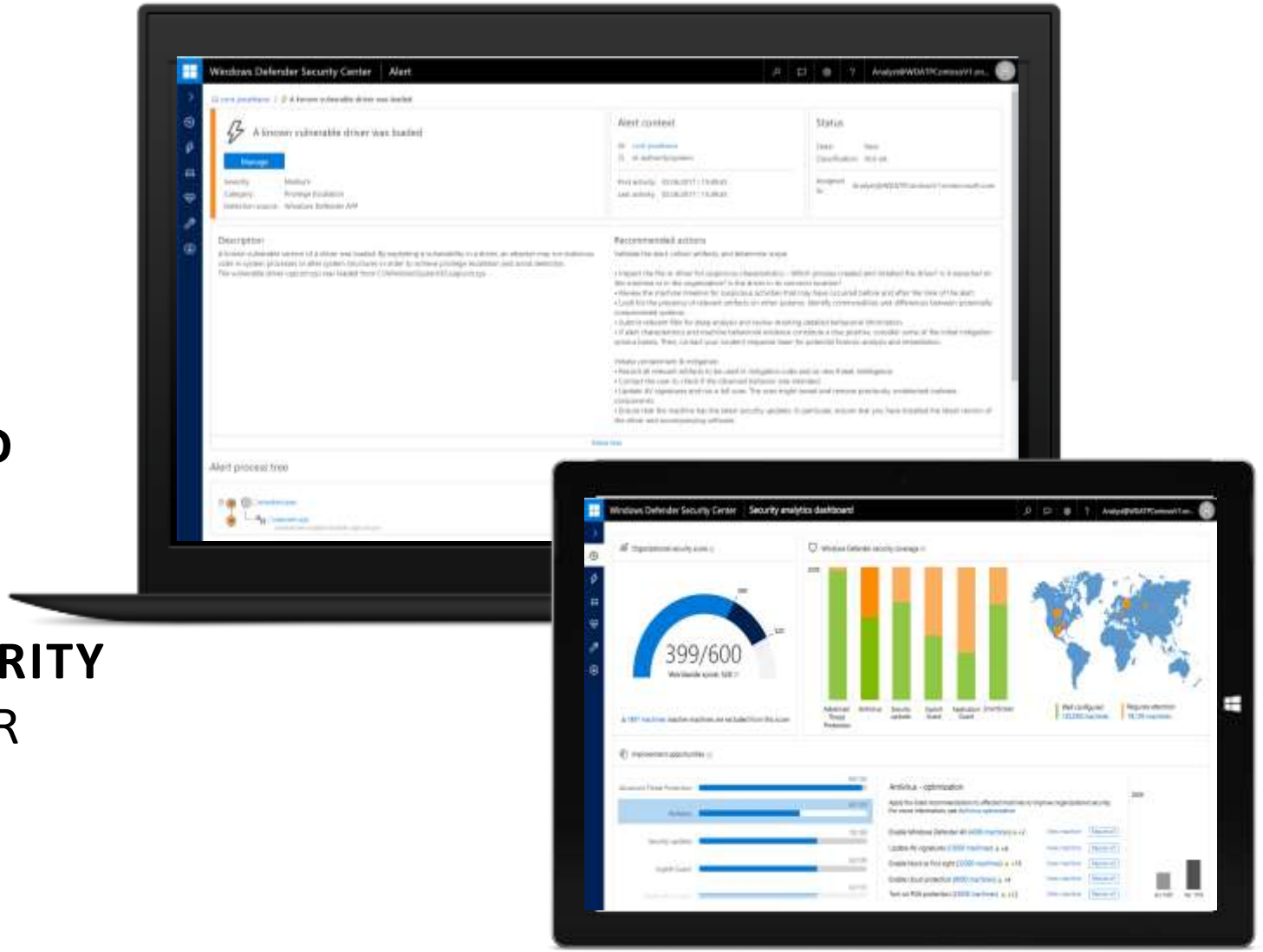


BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR DEVICES

RECOMMENDATIONS DRIVEN BY YOUR ENDPOINTS FOR **ENHANCED SECURITY**

ALERTS COME WITH RECOMMENDATION FOR **REMEDIATION OF THREATS AND FUTURE RISKS**

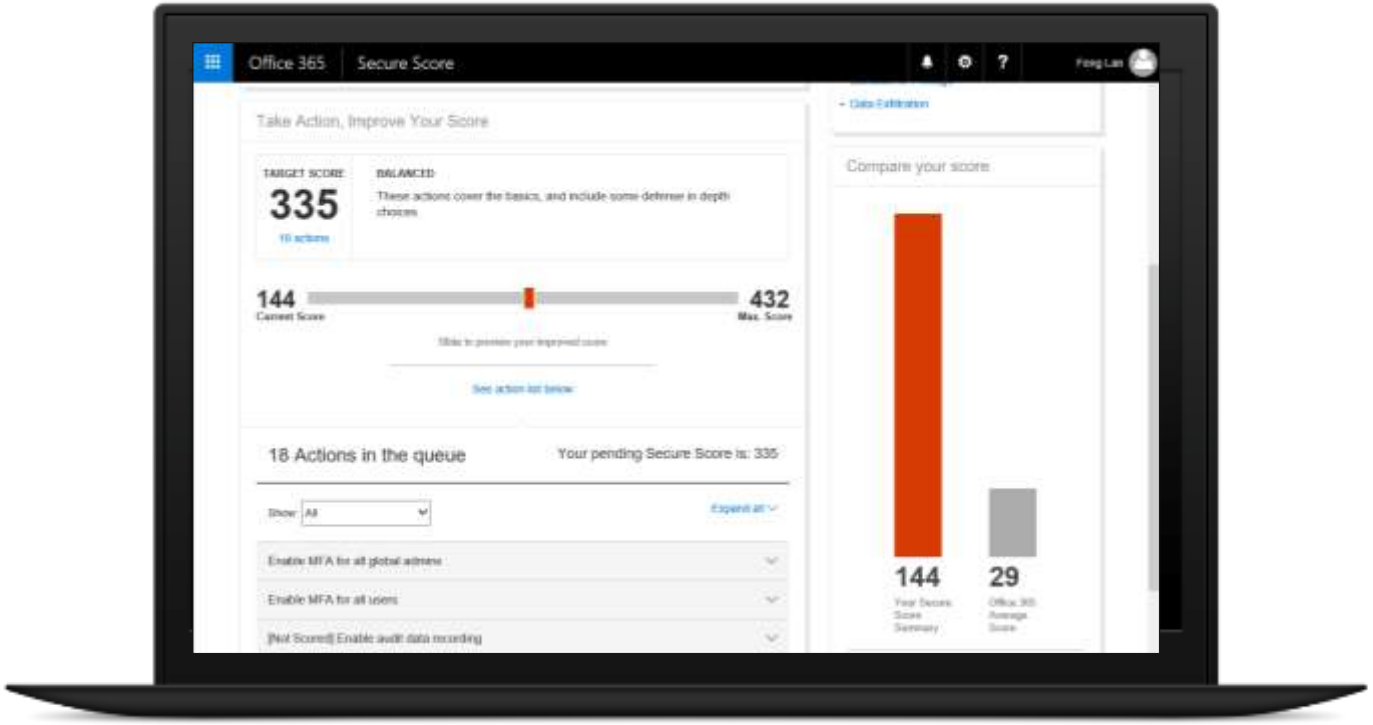
ASSESS **ORGANIZATIONAL SECURITY SCORE** INCLUDING TRENDS OVER TIME



BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR APPS & DATA

MACHINE LEARNING BASED RECOMMENDATIONS DRIVEN BY **SIGNALS SPECIFIC TO YOUR ORGANIZATION**

LEVERAGE THE MOST EFFECTIVE CONTROLS BASED ON BEST PRACTICES AND YOUR GOALS



BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR WORKLOADS ACROSS HYBRID INFRASTRUCTURE

180+ RECOMMENDED SECURITY CONFIGURATIONS

PRIORITIZED RECOMMENDATIONS TO FIX VULNERABILITIES FOR **AZURE RESOURCES**

AUTOMATED REMEDIATION WITH PLAYBOOKS