Microsoft Security Management

Microsoft

OUR COMMITMENT TO **YOU**
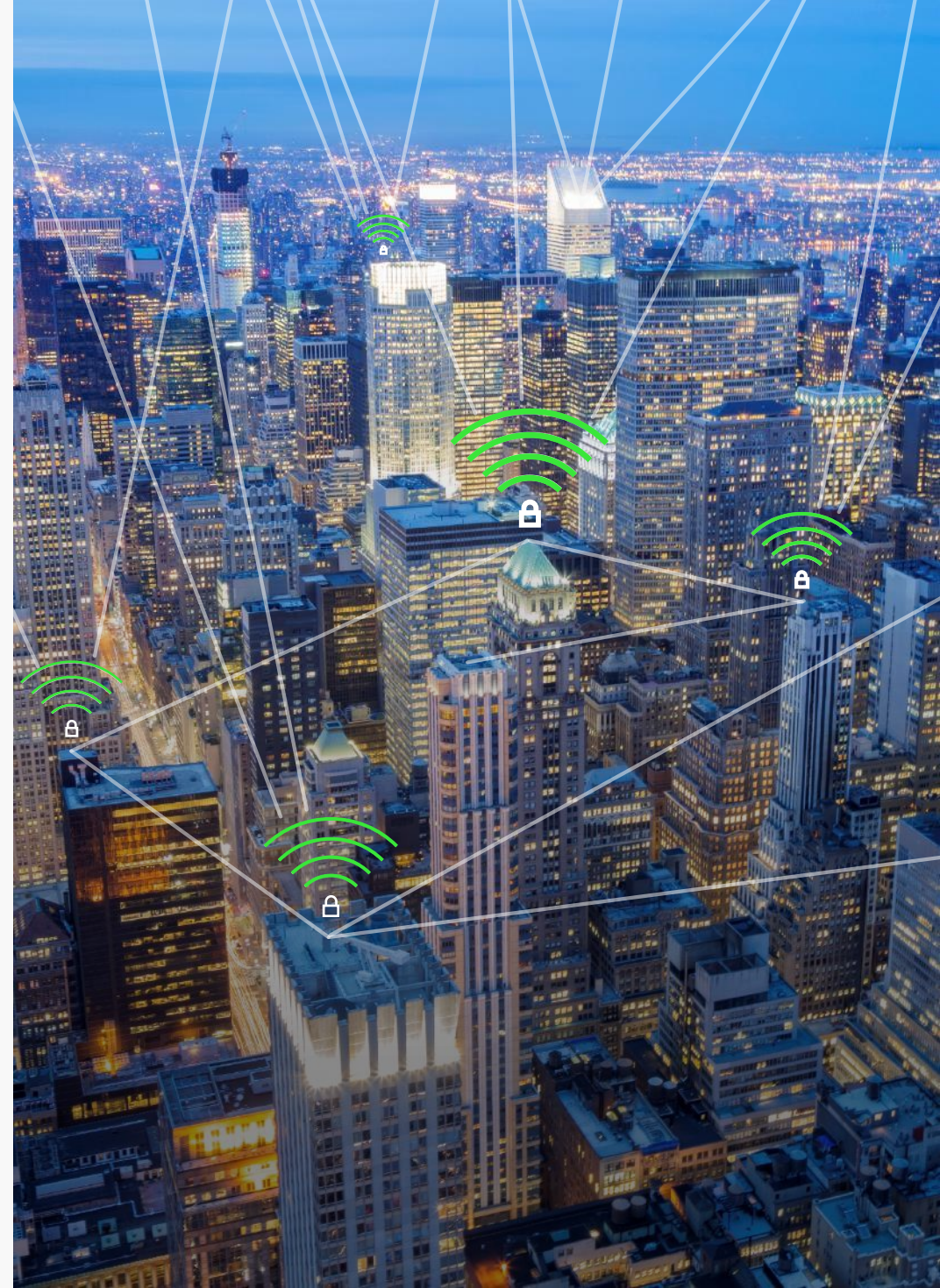
TRANSPARENCY

PRIVACY & CONTROL

COMPLIANCE

SECURITY

Microsoft Secure

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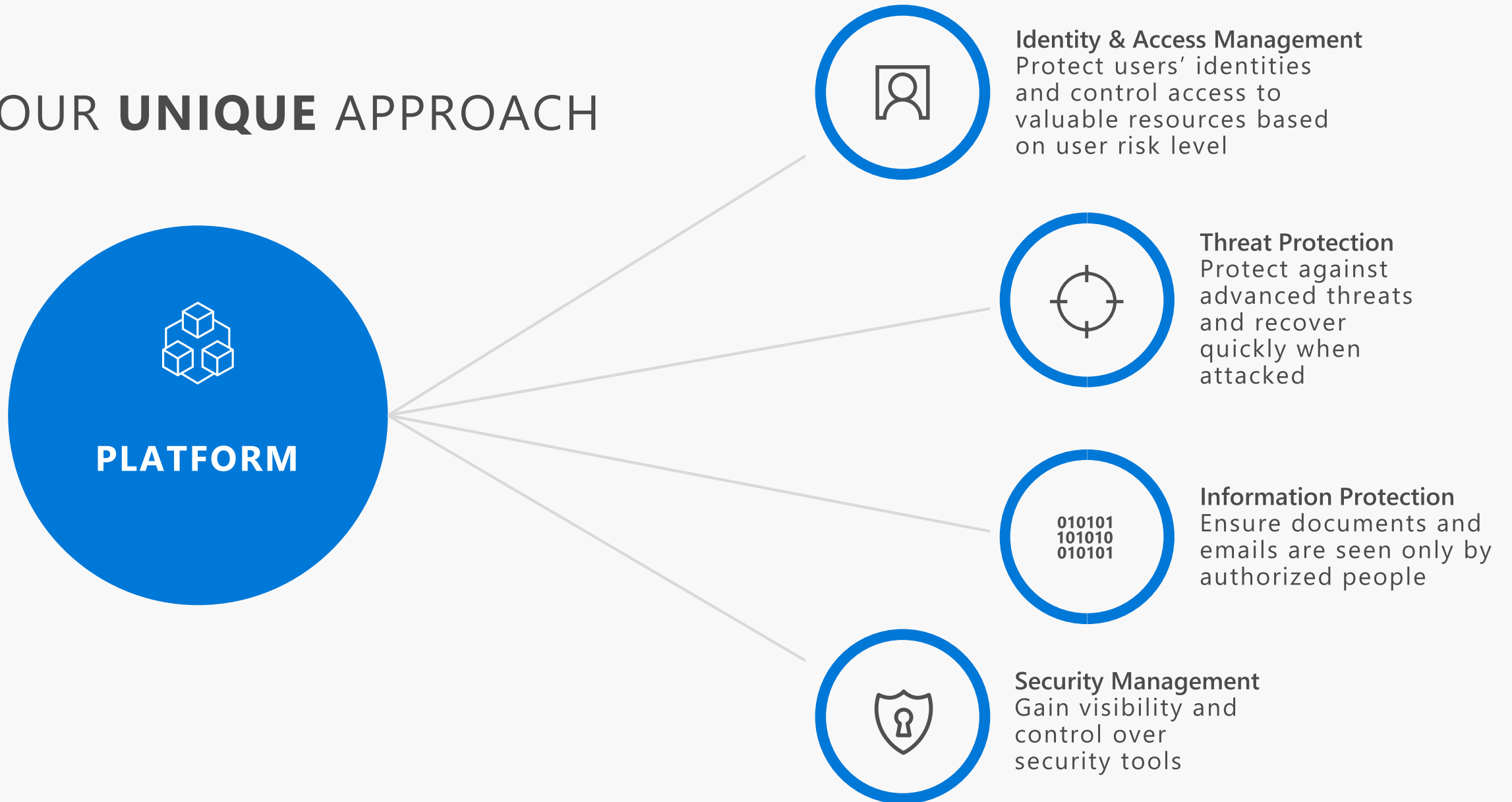
Microsoft

MICROSOFT **SECURITY MANAGEMENT**

SECURITY MANAGEMENT
## CHALLENGES

Increasing complexity

Lack of visibility

Ineffective response

"Some large financial services organizations **have as many as 40 or more different security vendors** inside their networks"

"Every different product will have separate management systems, often with limited connectivity to work alongside others.... thus **slowing down response and remediation times** "

"This results in the ironic situation of actually having more security devices in your network which **actually makes it less secure**"

SECURITY MANAGEMENT IMPERATIVES
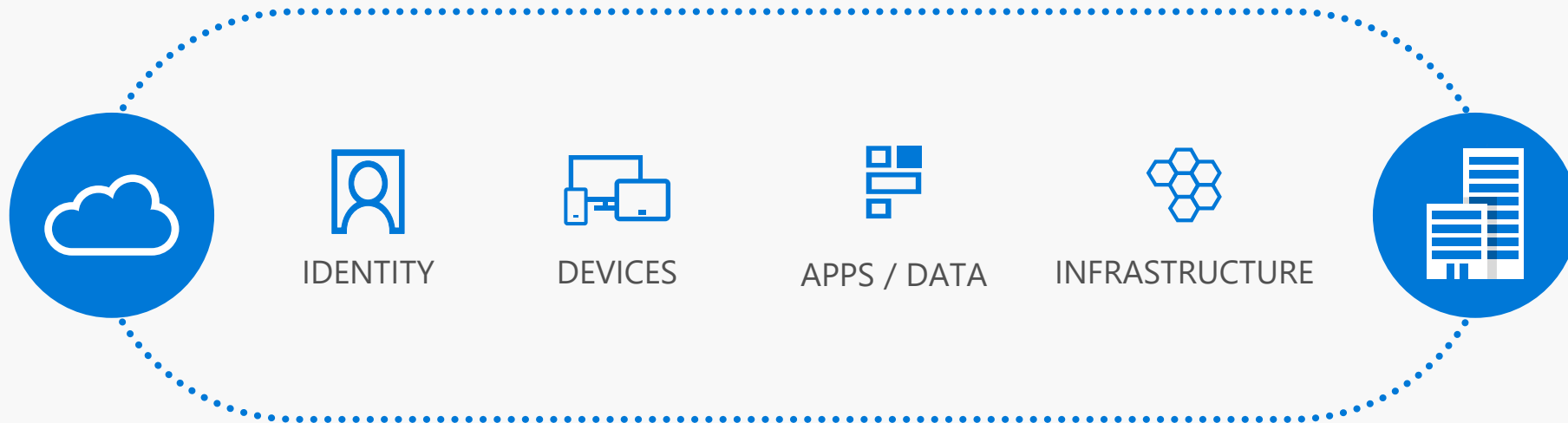
IDENTITY   DEVICES   APPS / DATA   INFRASTRUCTURE

VISIBILITY

Understand the security state and risks across resources
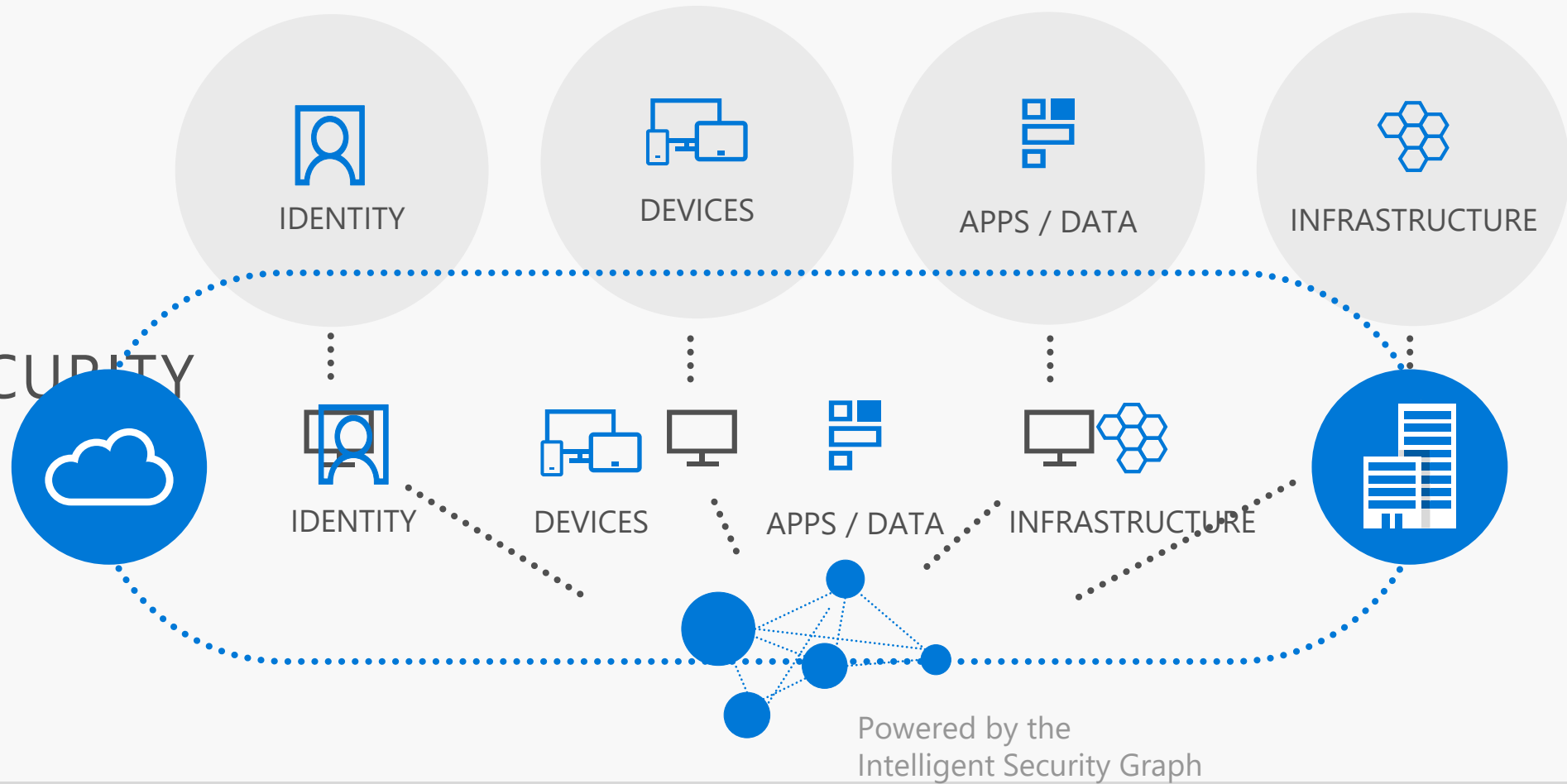
CONTROL

Define consistent security policies and enable controls

GUIDANCE

Elevate security through built-in intelligence and recommendations

HOW MICROSOFT HELPS

INTELLIGENT SECURITY MANAGEMENT

IDENTITY

DEVICES

APPS / DATA

INFRASTRUCTURE

IDENTITY

DEVICES

APPS / DATA

INFRASTRUCTURE

Powered by the
Intelligent Security Graph

VISIBILITY

Understand the security
state and risks across
resources

CONTROL

Define consistent security
policies and enable
controls

GUIDANCE

Enhance security through
built-in intelligence and
recommendations

VISIBILITY
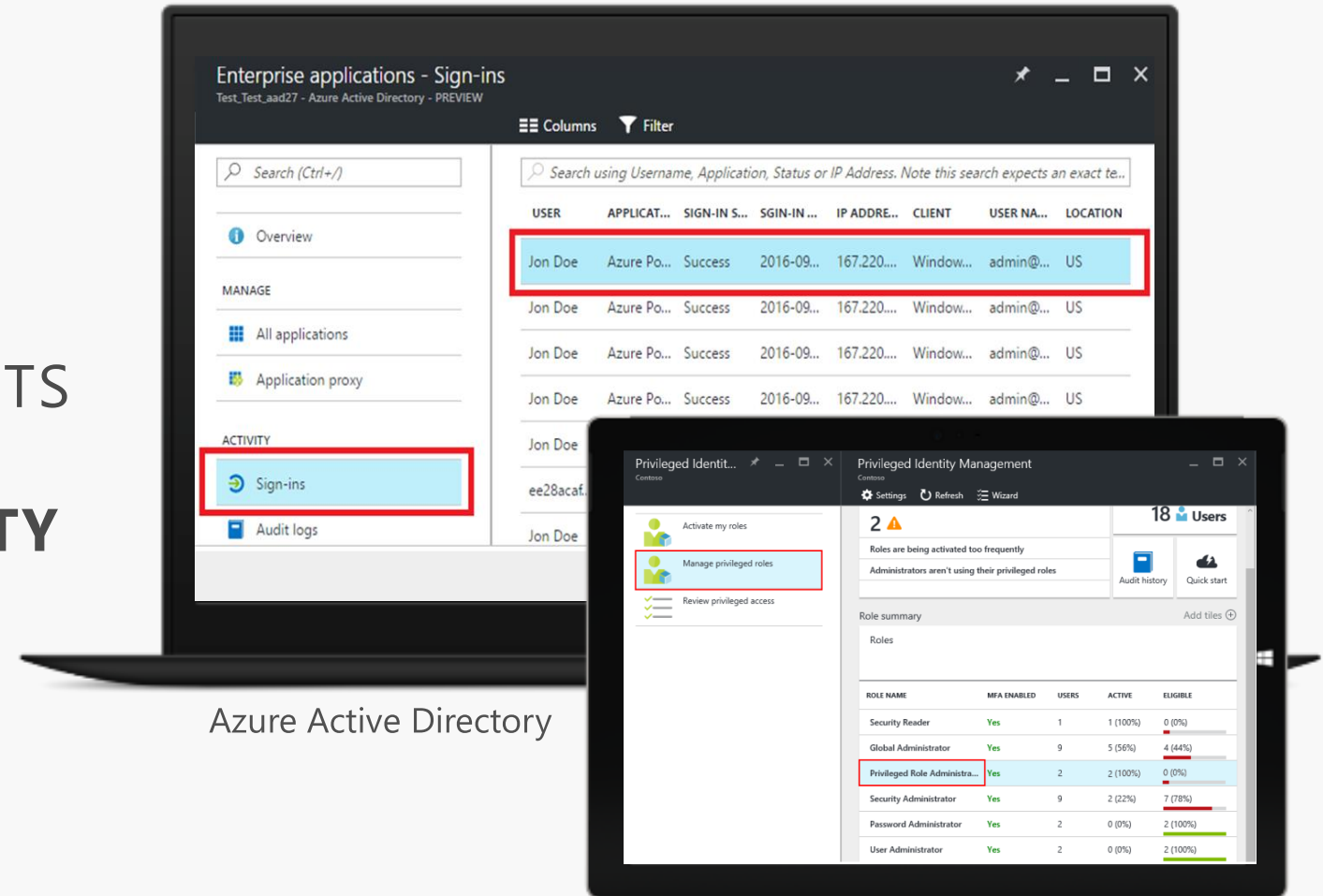
Understand the security state and risks across resources

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
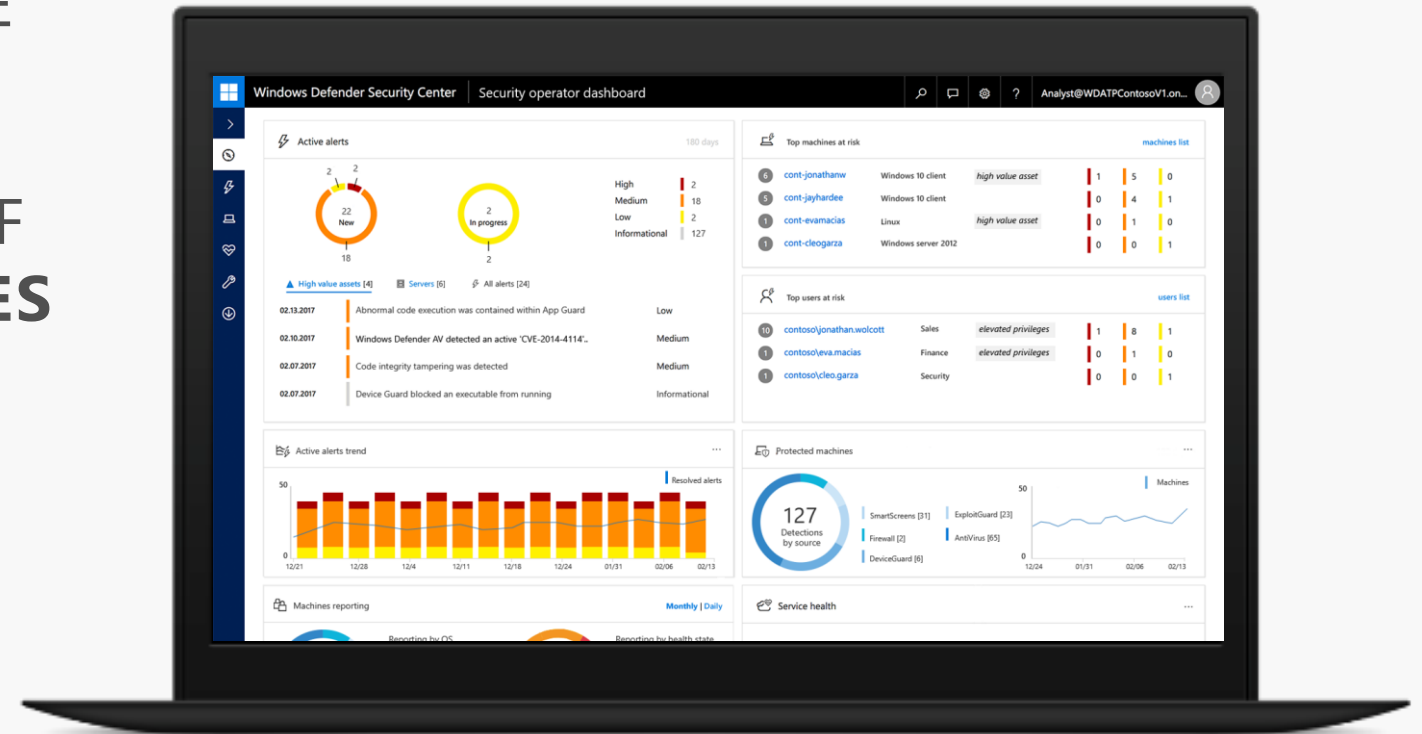
UNDERSTAND SECURITY STATE OF DEVICES

COMPLETE VISIBILITY INTO THE
ENDPOINT SECURITY

QUICKLY ASSESS THE SCOPE OF
INCIDENTS AND ROOT CAUSES

RICH TOOLSET FOR
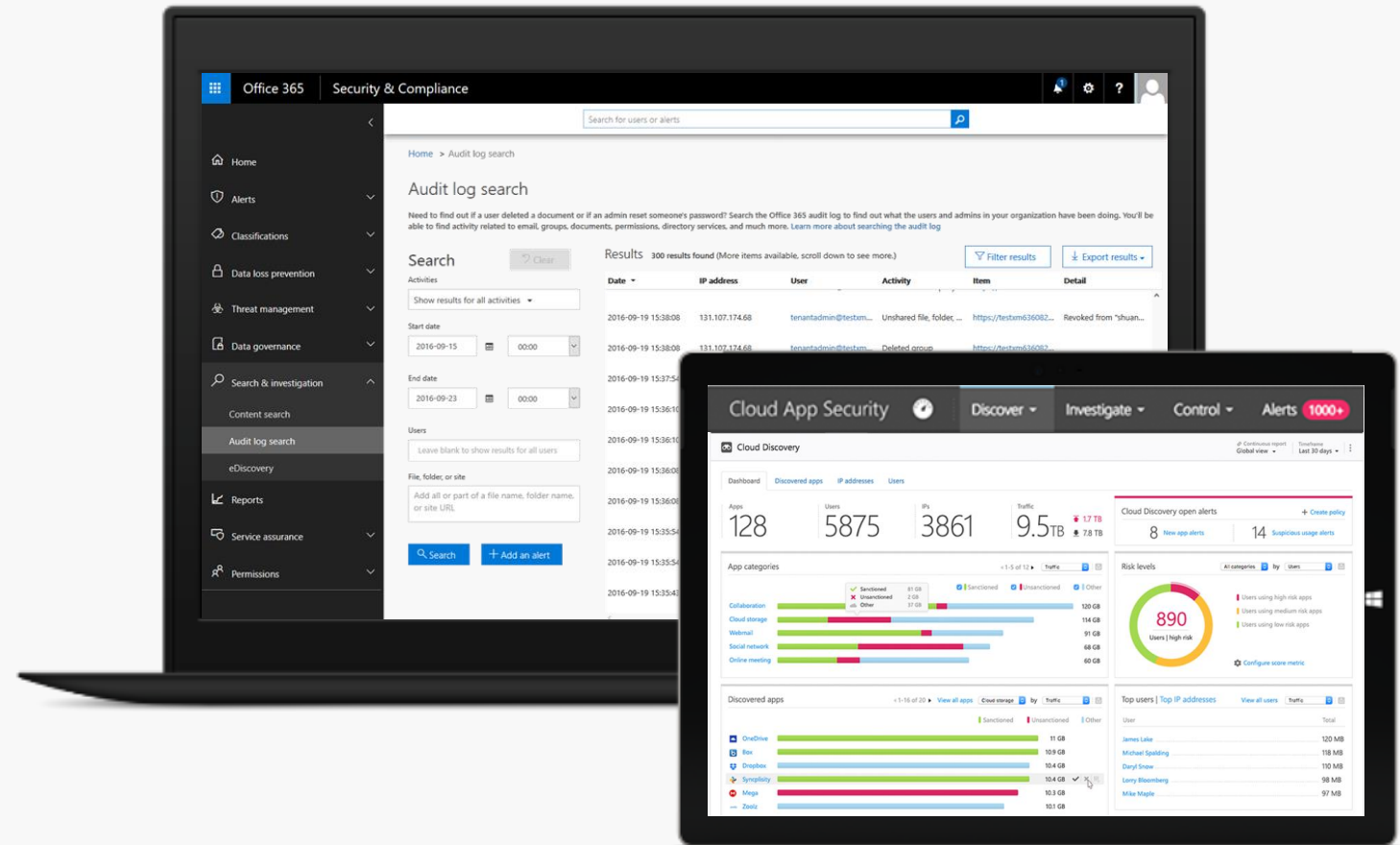**INVESTIGATION AND
REMEDIATION ACTIONS**

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

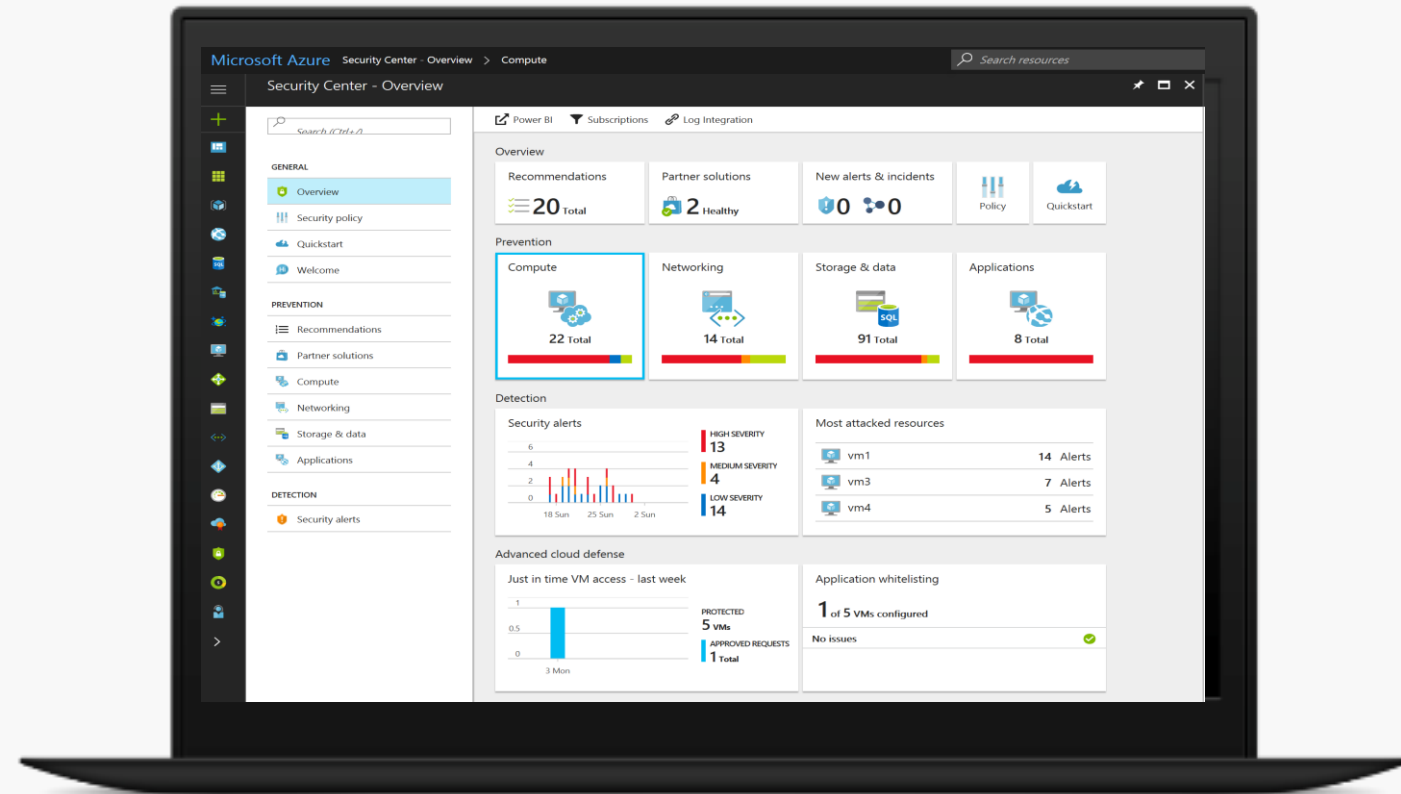ALERTS TO HELP YOU **SEE ANOMALOUS ACTIVITY**

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

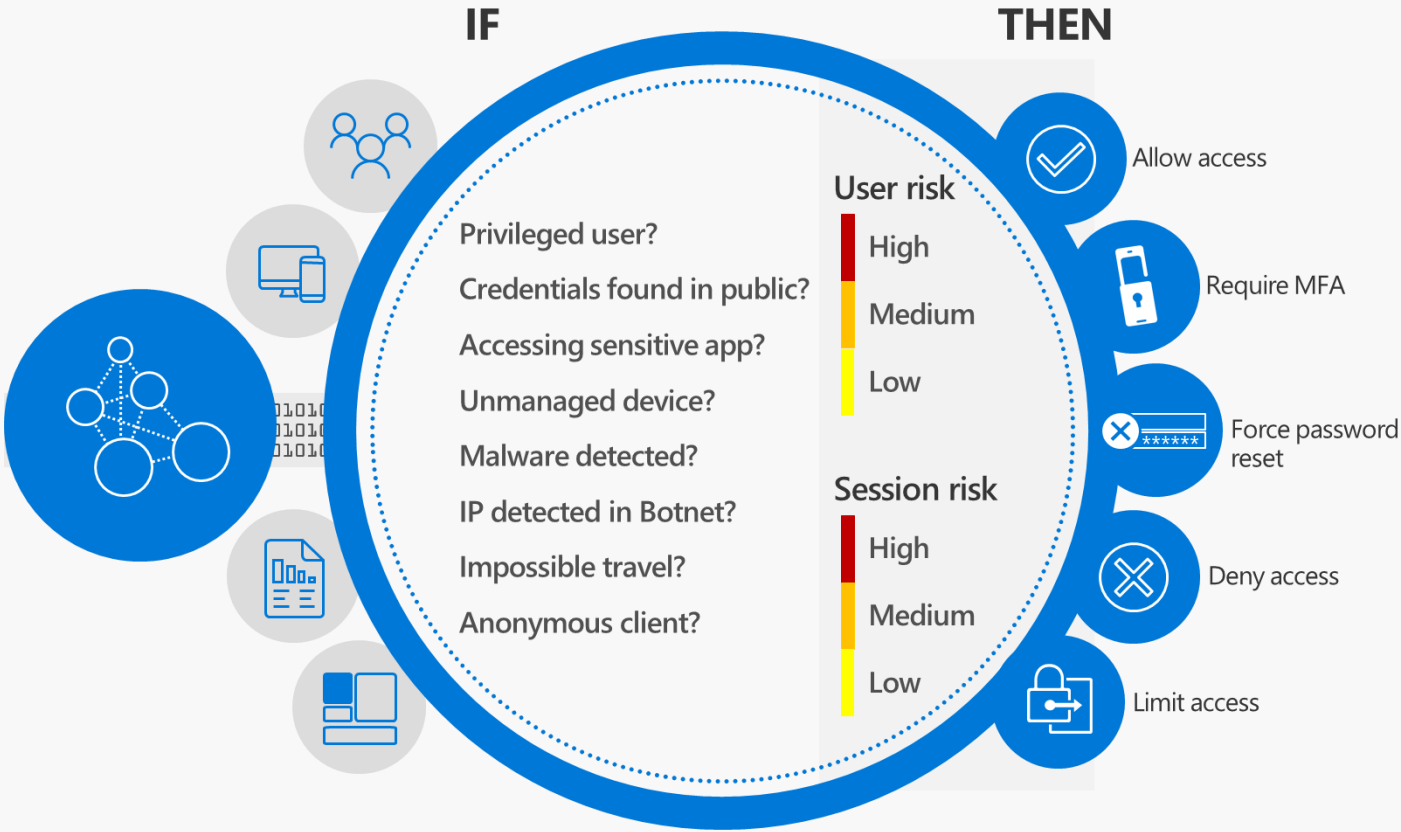Define consistent security policies and enable controls

DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR USERS

IDENTITY

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

CONTROL AND PROTECT **PRIVILEGED IDENTITIES**

IF

Privileged user?

Credentials found in public?

Accessing sensitive app?

Unmanaged device?

Malware detected?

IP detected in Botnet?

Impossible travel?

Anonymous client?

User risk

High

Medium

Low

Session risk

High

Medium

Low

THEN

Allow access

Require MFA

Force password reset

Deny access

Limit access

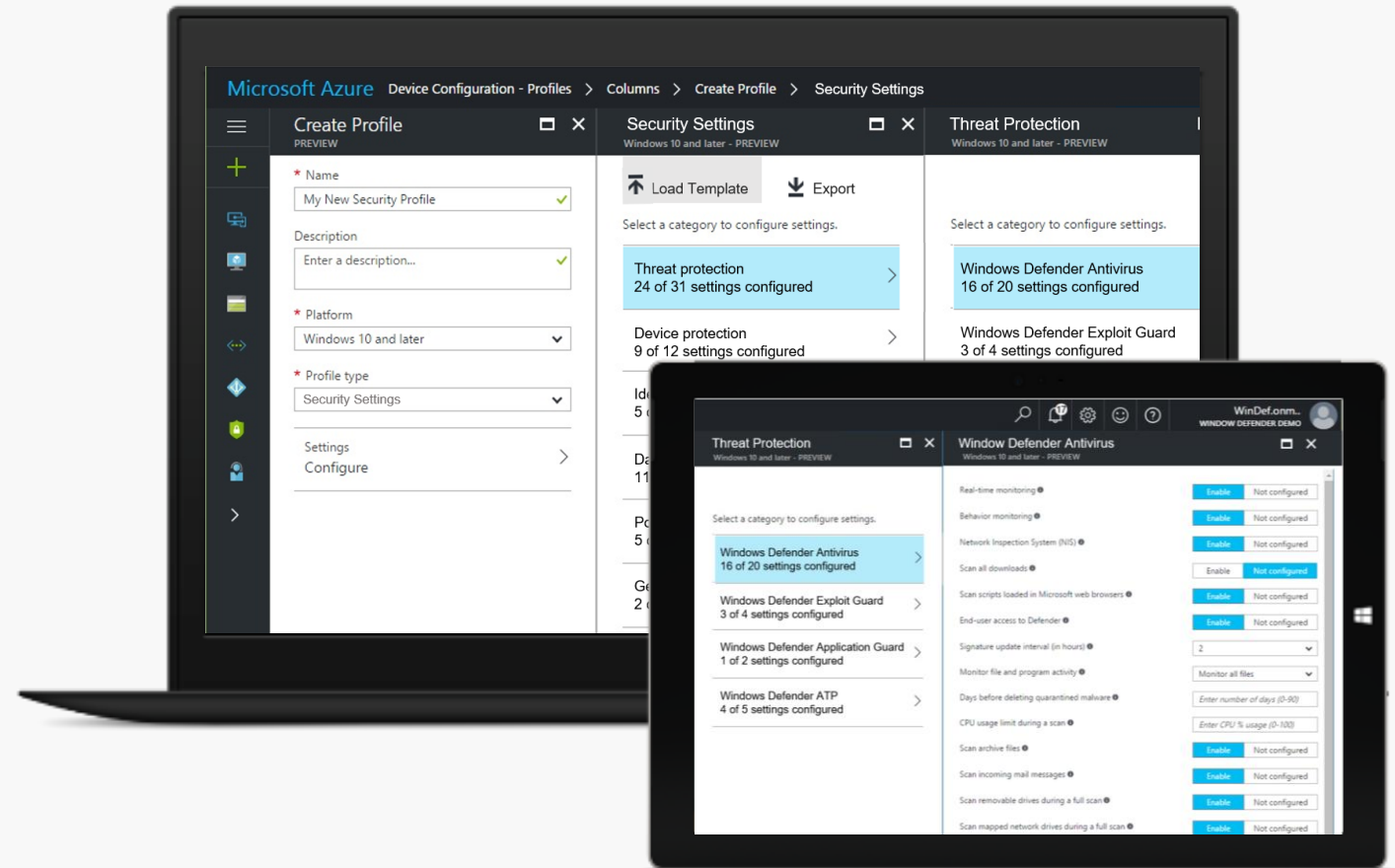# DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR DEVICES

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

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

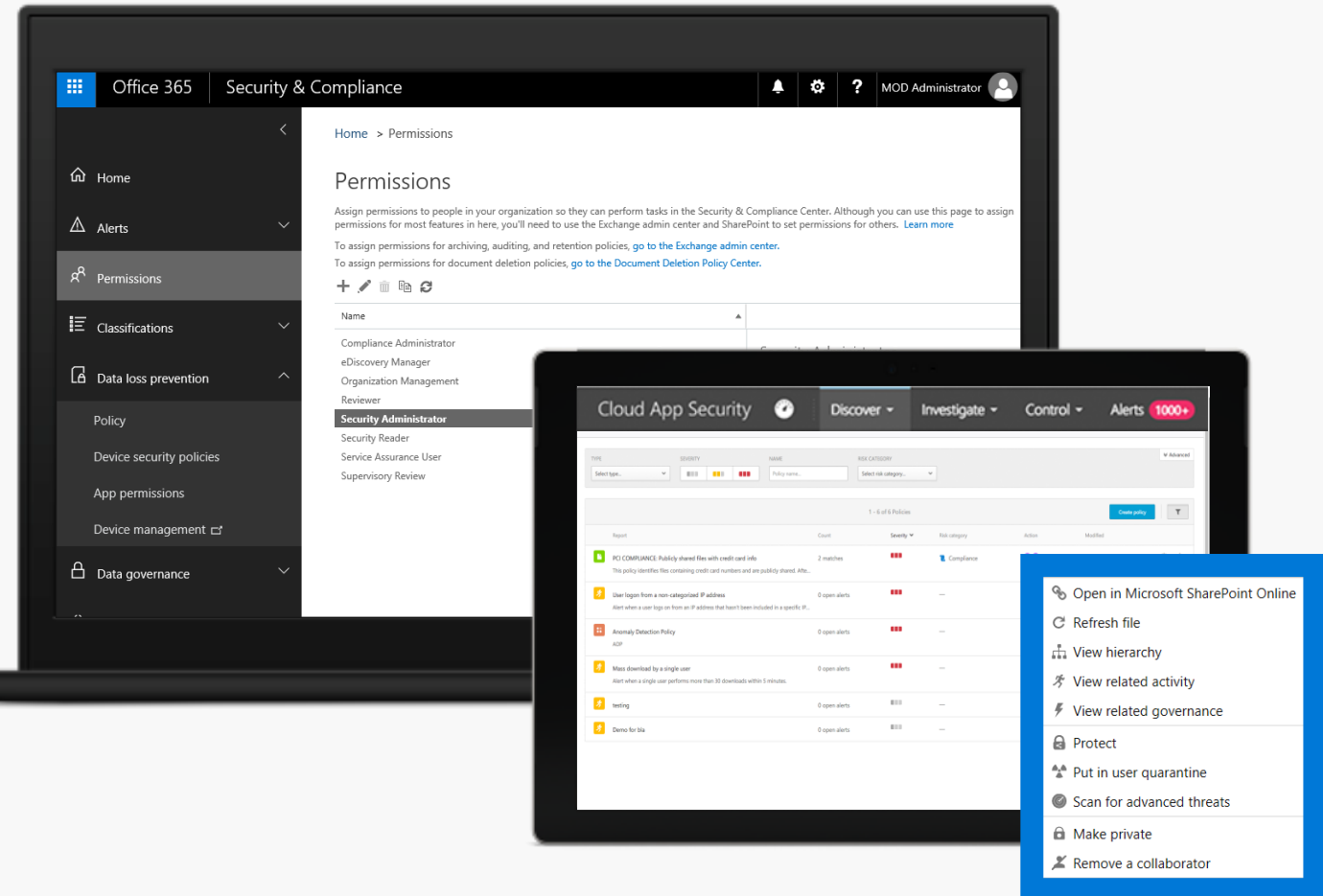# DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR APPS & DATA

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

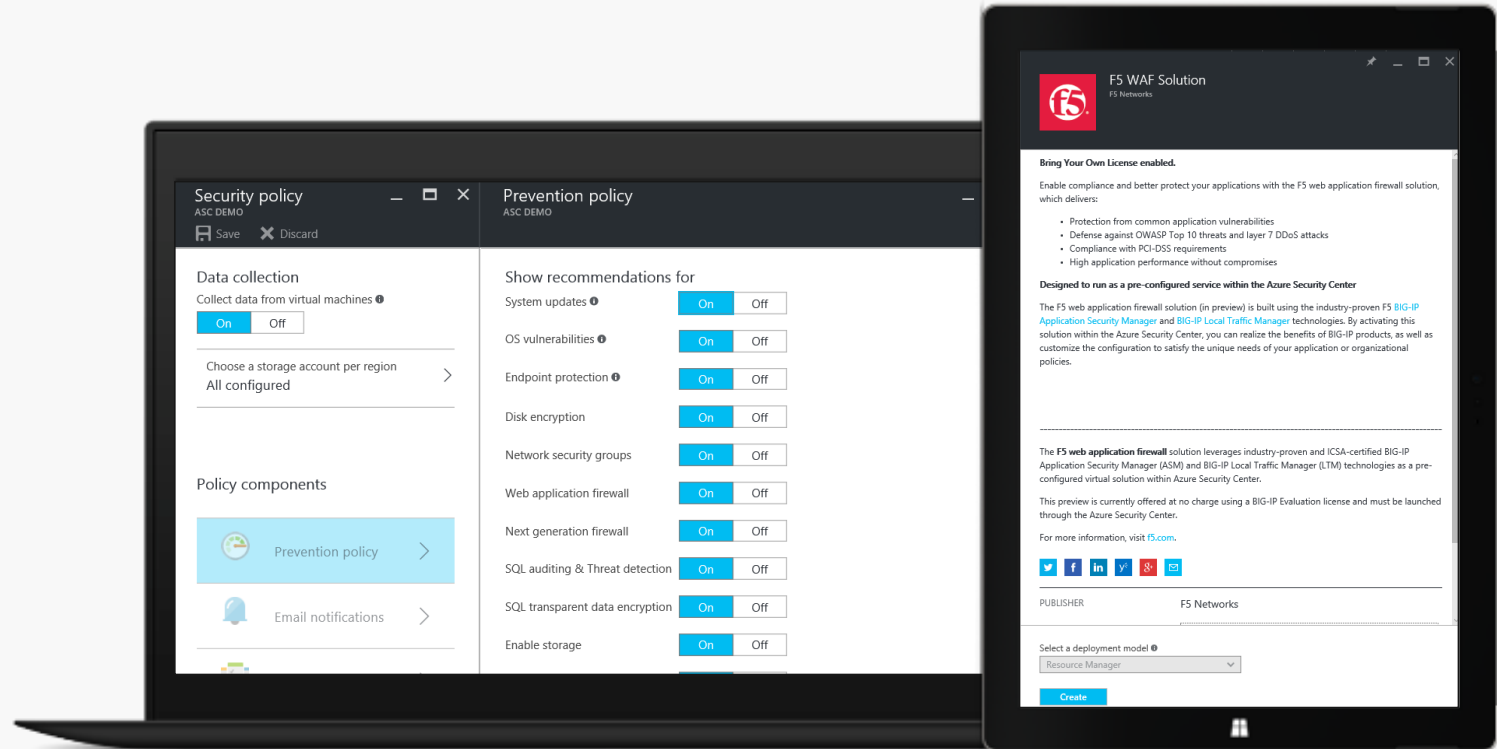# DEFINE CONSISTENT SECURITY POLICIES AND ENABLE CONTROLS FOR WORKLOADS ACROSS HYBRID INFRASTRUCTURE

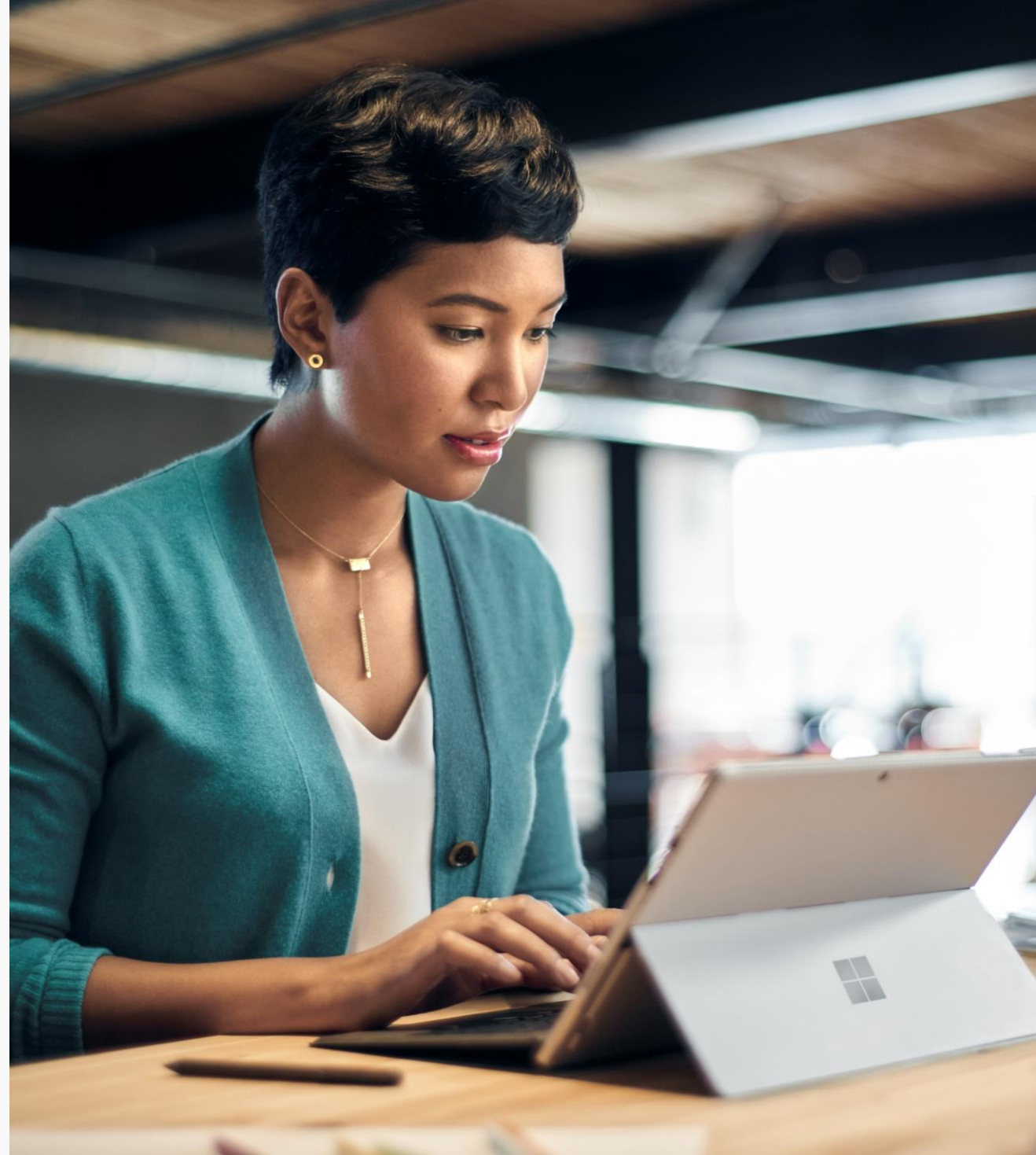**SET SECURITY POLICIES** FOR RESOURCES IN THE CLOUD

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
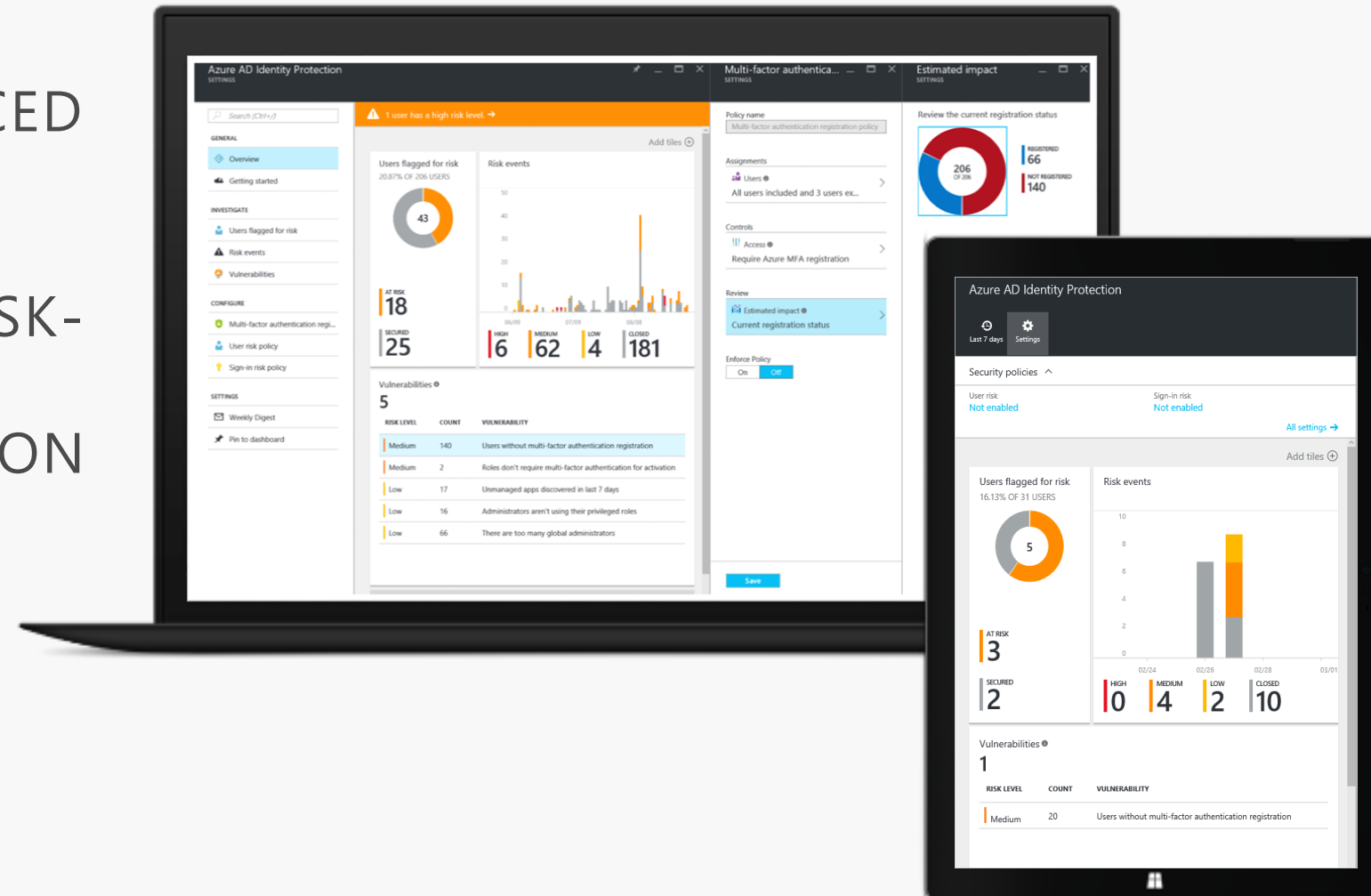
BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR DEVICES
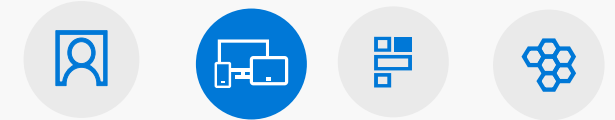
RECOMMENDATIONS DRIVEN BY YOUR ENDPOINTS FOR **ENHANCED SECURITY**

EVERY ALERT COMES WITH RECOMMENDATION FOR **REMEDIATION FOR THREATS AND FUTURE RISKS**

ASSESS **ORGANIZATIONAL SECURITY SCORE** INCLUDING TRENDS OVER TIME
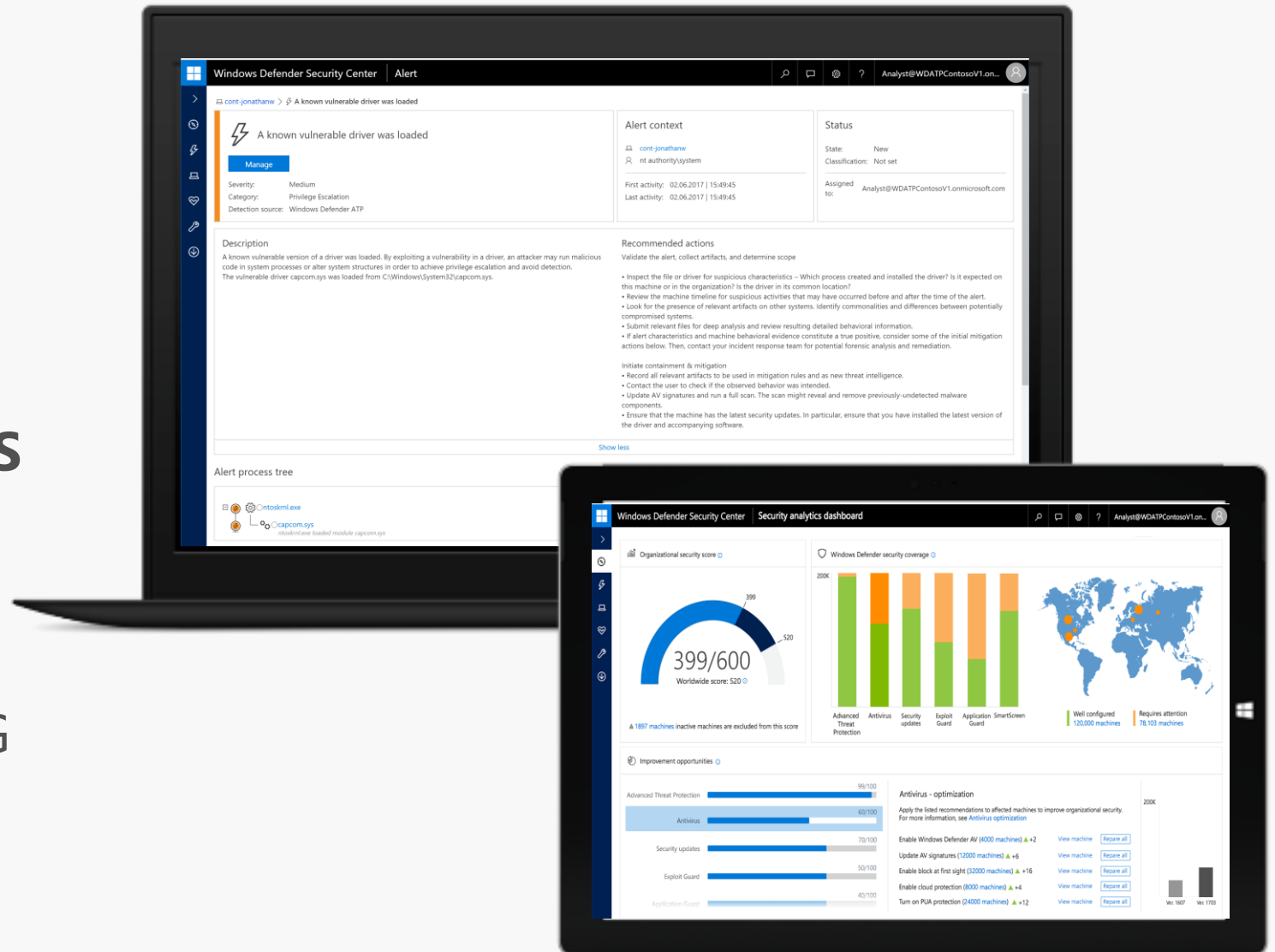
BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR APPS & DATA

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

LEVERAGE THE MOST EFFECTIVE CONTROLS BASED ON BEST PRACTICES AND YOUR GOALS
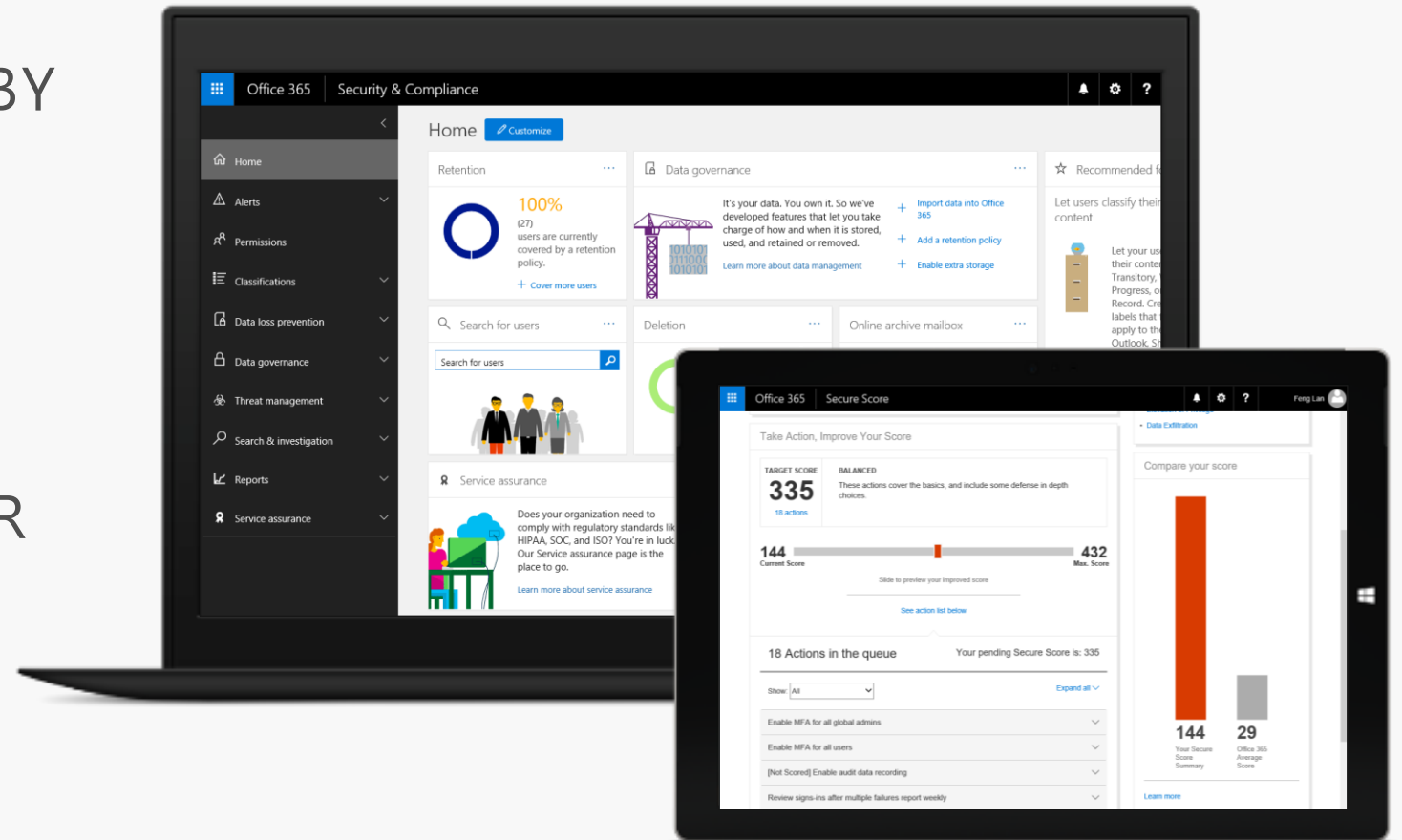
BUILT-IN INTELLIGENCE AND RECOMMENDATIONS FOR WORKLOADS ACROSS HYBRID INFRASTRUCTURE

180+ RECOMMENDED SECURITY CONFIGURATIONS

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

AUTOMATED REMEDIATION WITH PLAYBOOKS
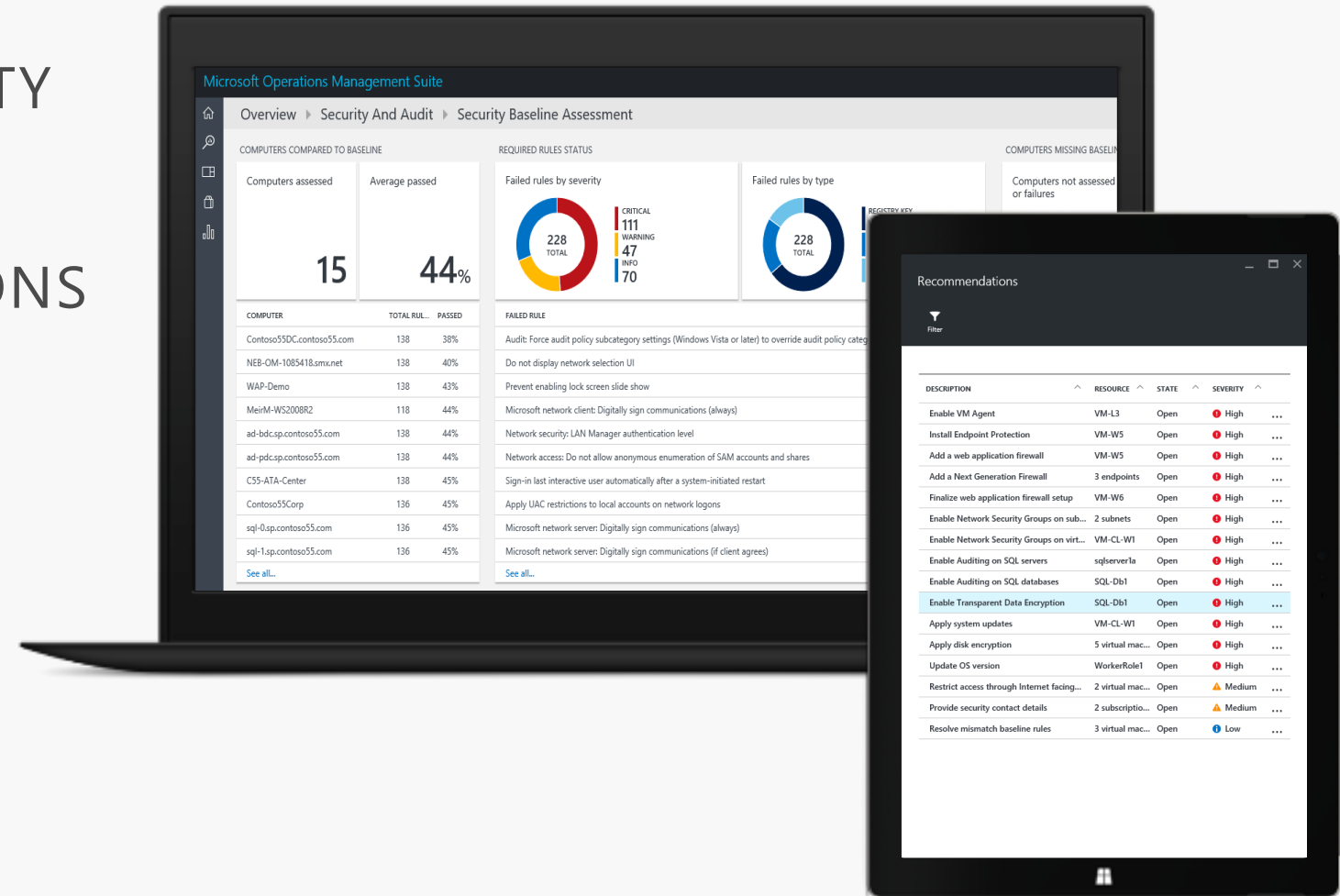
POWERED BY
**INTELLIGENT
SECURITY GRAPH**

IDENTITY

DEVICES

APPS / DATA

INFRASTRUCTURE

Powered by the
Intelligent Security Graph
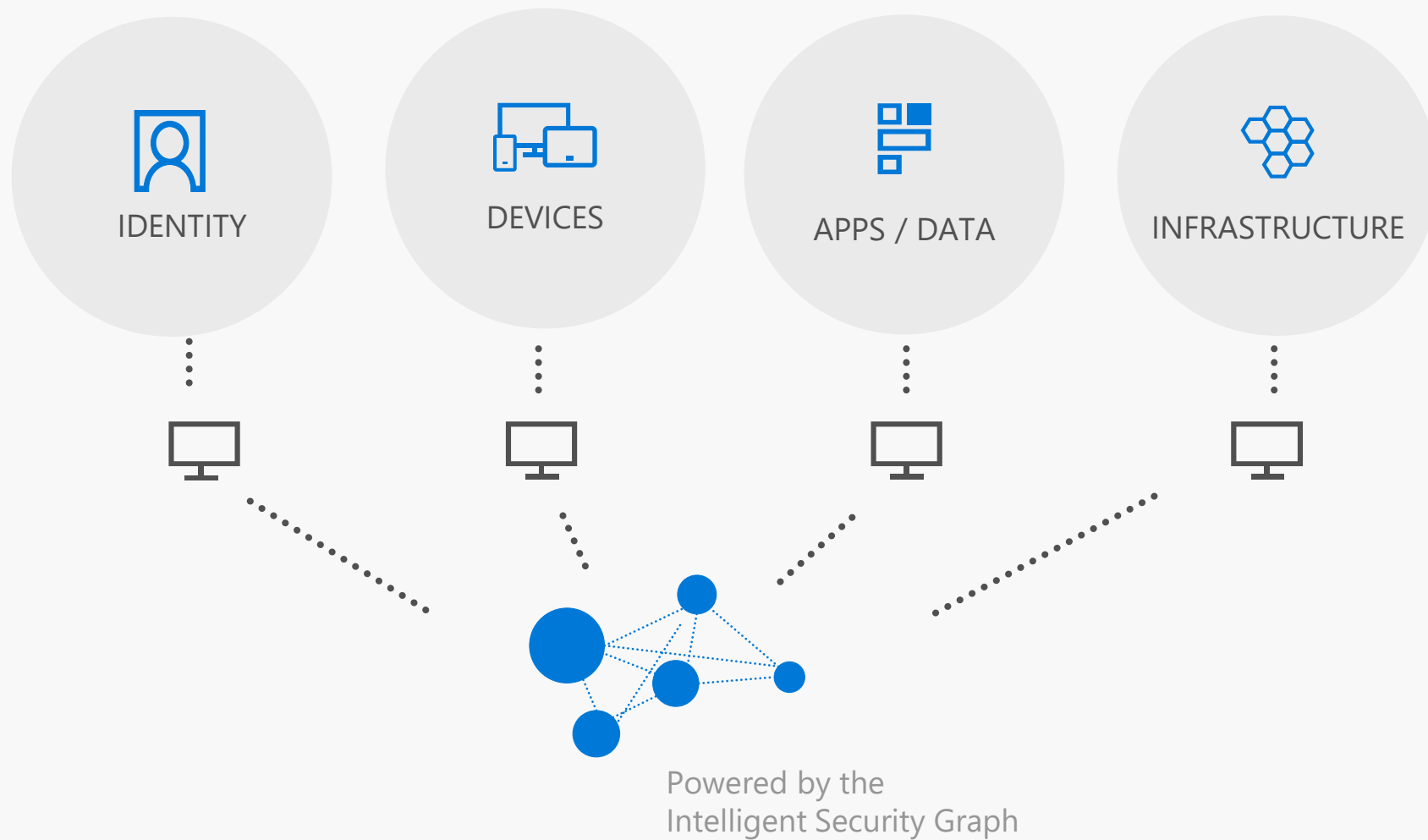
INTELLIGENT SECURITY GRAPH

Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services
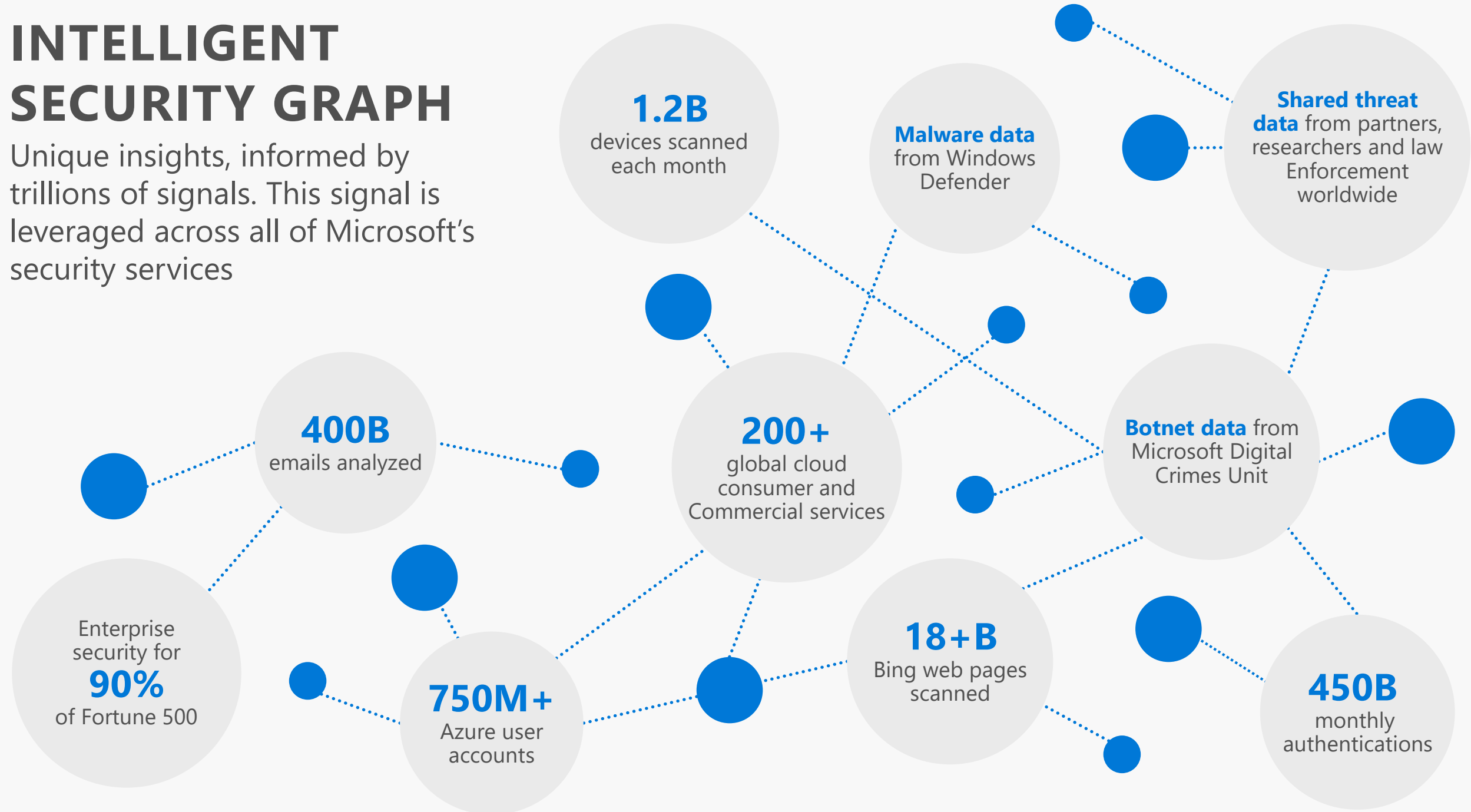
1.2B devices scanned each month

Malware data from Windows Defender

Shared threat data from partners, researchers and law Enforcement worldwide

400B emails analyzed

200+ global cloud consumer and Commercial services

Botnet data from Microsoft Digital Crimes Unit

Enterprise security for **90%** of Fortune 500

750M+ Azure user accounts

18+B Bing web pages scanned
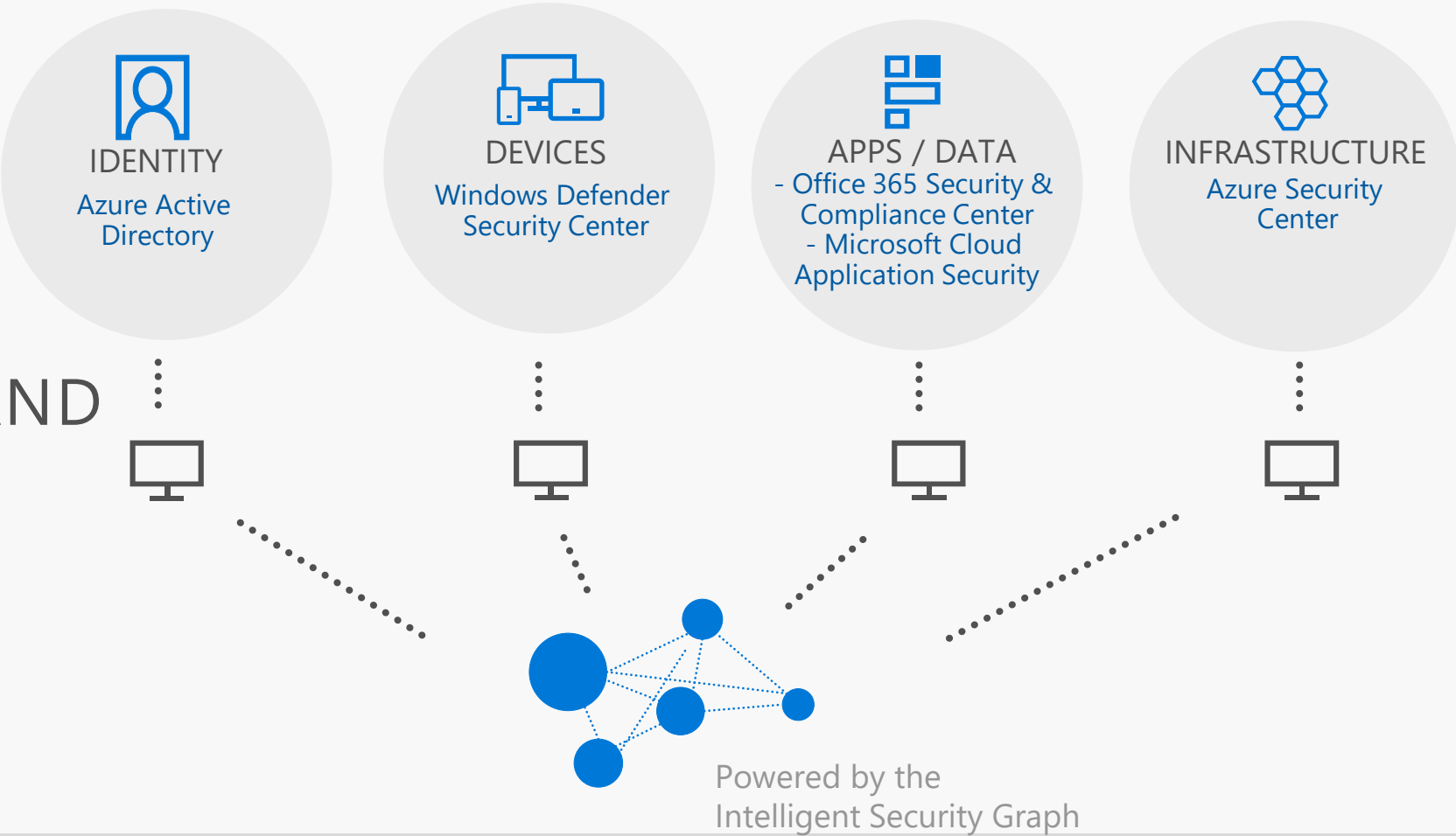
450B monthly authentications

GETTING STARTED:

Use Azure Active Directory to secure identities in your environment

Enable threat management for your devices through Windows Defender Security Center

Manage and control apps and data for your SaaS apps with Office 365 Security and Compliance Center as well as Microsoft Cloud App Security

Consolidate security management for your infrastructure in cloud and on-premises with Azure Security Center

Microsoft

RESOURCES

Identity and Access Management
[Learn more about Azure Active Directory](#)

Security Management for Devices
[Learn more about Windows Defender Security Center](#)

Security Management for Apps & Data
[Learn more about Office 365 Security and Compliance Center](#)

[Overview of Cloud App Security](#)

Security Management for Infrastructure

[Overview of Azure Security Center](#)

OUR SECURITY **OFFERING**

Identity & Access Management

Azure Active Directory

Conditional Access

Windows Hello

Windows Credential Guard

Threat Protection

Advanced Threat Analytics

Windows Defender Advanced Threat Protection

Office 365 Advanced Threat Protection

Office 365 Threat Intelligence

Information Protection

Azure Information Protection

Office 365 Data Loss Prevention

Windows Information Protection

Microsoft Cloud App Security

Office 365 Advanced Security Mgmt

Microsoft Intune

Security Management

Azure Security Center

Office 365 Security & Compliance Center

Windows Defender Security Center

GENERAL DATA PROTECTION REGULATION (GDPR)

- **Enhanced** personal privacy rights

- **Increased** duty for protecting data

- **Mandatory** breach reporting

- **Significant** penalties for non-compliance

HOW YOU GET STARTED:

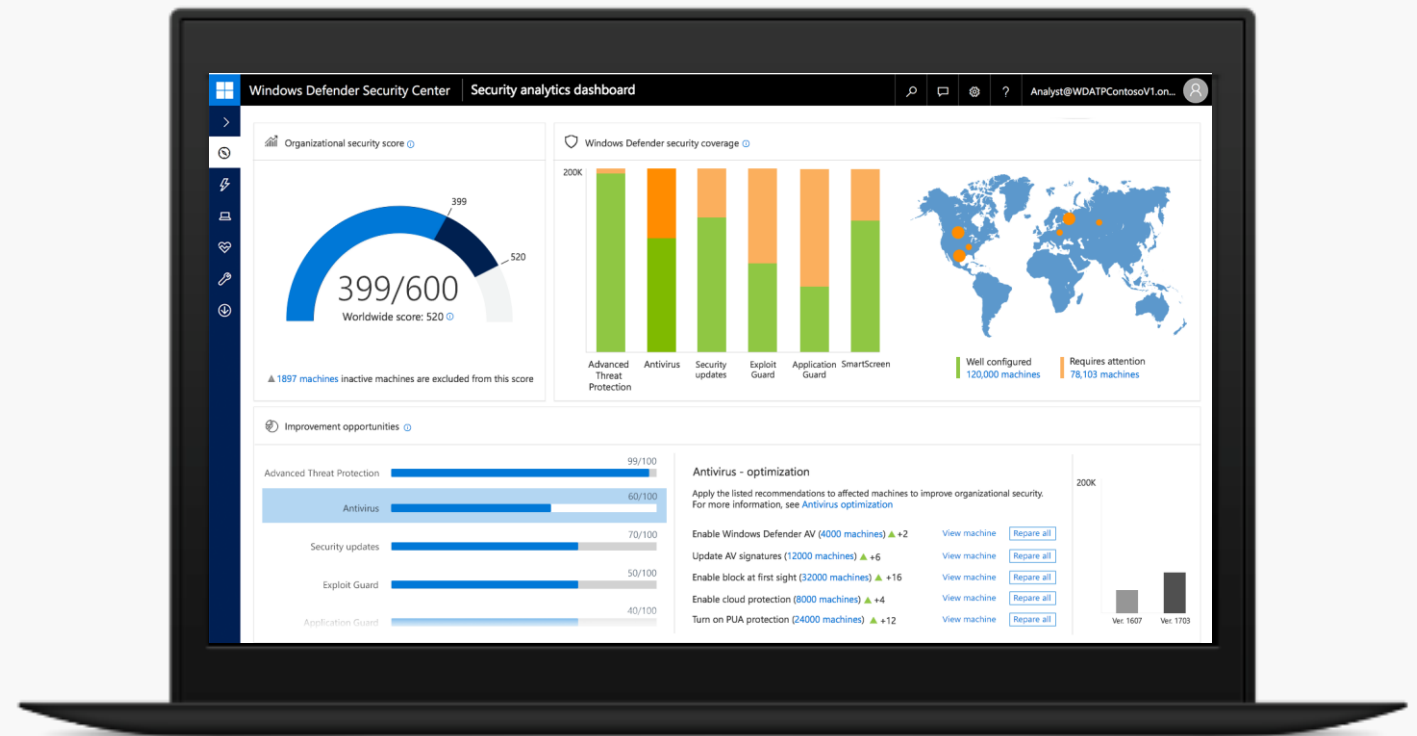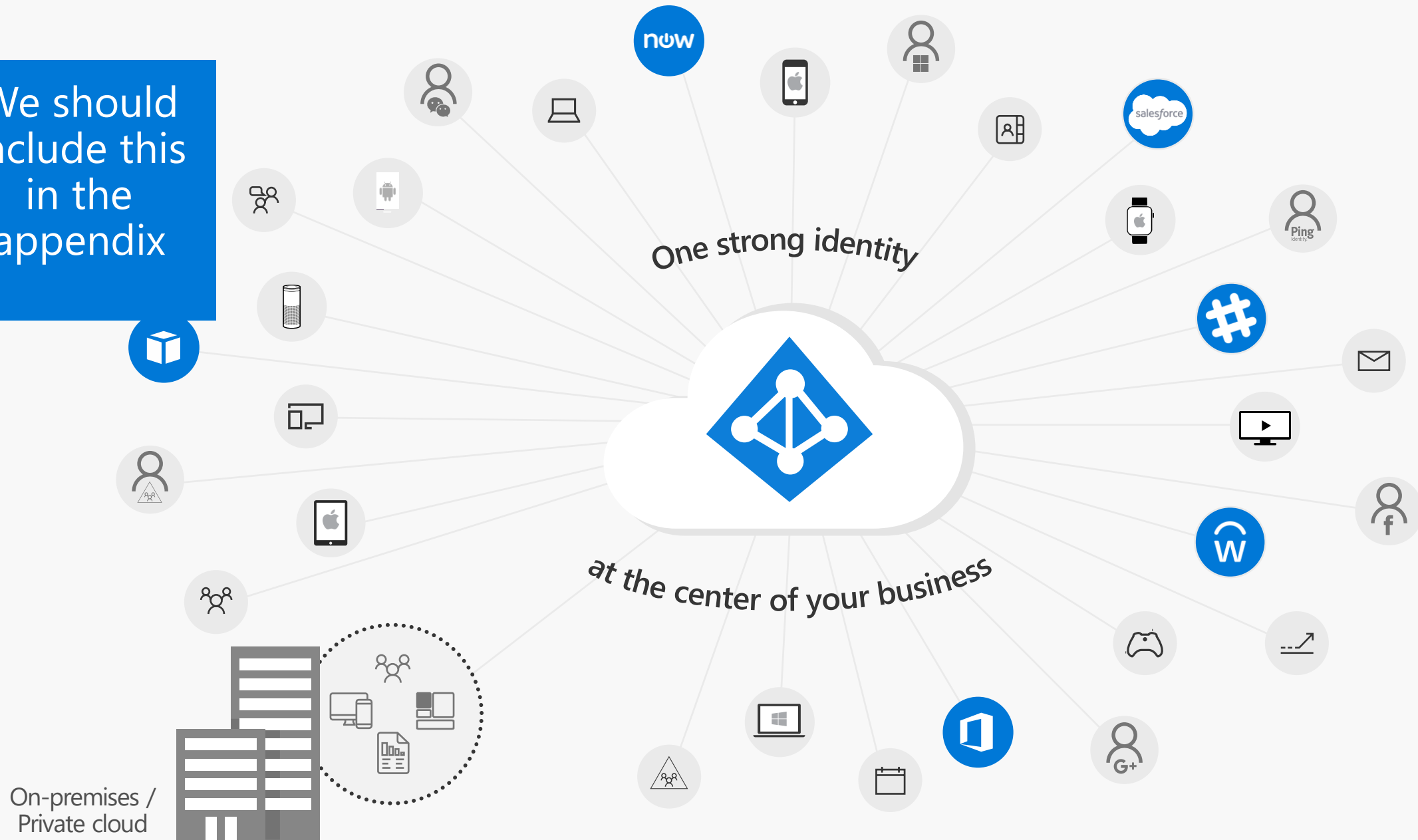| #		
1	**Discover**	Identify what personal data you have and where it resides
2	**Manage**	Govern how personal data is used and accessed
3	**Protect**	Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches
4	**Report**	Keep required documentation, manage data requests and breach notifications

Intelligent Security Graph

PROACTIVELY IDENTIFY & RESOLVE CONFIGURATION ISSUES TO **REDUCE ATTACK SURFACE**

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

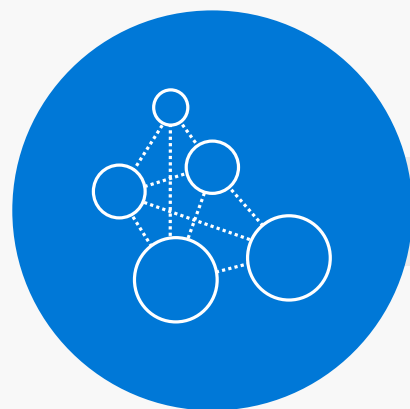RECOMMENDATIONS DRIVEN BY YOUR ENDPOINTS FOR **ENHANCED SECURITY**

Windows Defender Security Center | Security analytics dashboard | Analyst@WDATPContosoV1.on...

Organizational security score

399
399/600
520
Worldwide score: 520

⚠ 1897 machines inactive machines are excluded from this score

Windows Defender security coverage

200K

Advanced Threat Protection | Antivirus | Security updates | Exploit Guard | Application Guard | SmartScreen

Well configured 120,000 machines | Requires attention 78,103 machines

Improvement opportunities

Advanced Threat Protection — 99/100
Antivirus — 60/100
Security updates — 70/100
Exploit Guard — 50/100
Application Guard — 40/100

Antivirus - optimization

Apply the listed recommendations to affected machines to improve organizational security. For more information, see Antivirus optimization.

Enable Windows Defender AV (4000 machines) ▲ +2 | View machine | Repair all
Update AV signatures (12000 machines) ▲ +6 | View machine | Repair all
Enable block at first sight (32000 machines) ▲ +16 | View machine | Repair all
Enable cloud protection (8000 machines) ▲ +4 | View machine | Repair all
Turn on PUA protection (24000 machines) ▲ +12 | View machine | Repair all

200K

Ver. 1607 | Ver. 1703

We should include this in the appendix

One strong identity

at the center of your business

On-premises / Private cloud

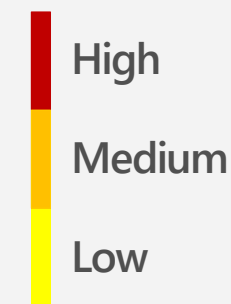# CONTROL AND PROTECT ACCESS
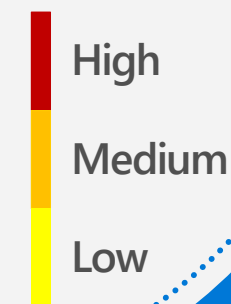
IF

THEN

10TB per day

Privileged user?

Credentials found in public?

Accessing sensitive app?

Unmanaged device?

Malware detected?

IP detected in Botnet?

Impossible travel?

Anonymous client?

User risk

High

Medium

Low

Session risk

High

Medium

Low

Allow access

Require MFA
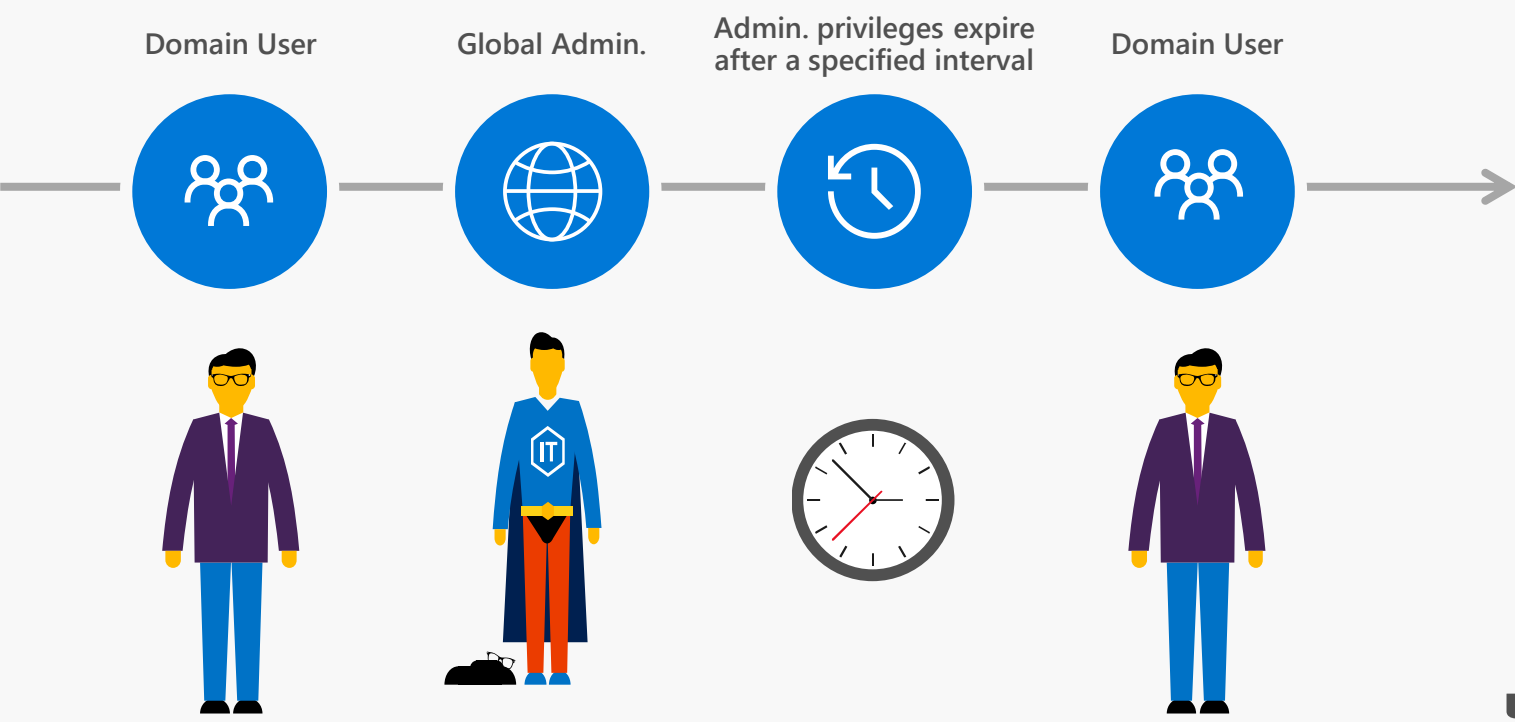
Force password reset

Deny access

Limit access

CONTROL AND PROTECT **PRIVILEGED IDENTITIES**

Enforce on-demand, just-in-time administrative access when needed

Use Alert, Audit Reports and Access Review

Domain User

Global Admin.

Admin. privileges expire after a specified interval

Domain User

GAIN VISIBILITY INTO **CLOUD APPS** USED IN YOUR ENVIRONMENT

GET **RISK ASSESSMENT** AND ON-GOING ANALYTICS