Microsoft Security

Microsoft Security Briefing for Partners

Woody Walton
7/21/2021
Director, Partner Technology Strategy
Microsoft | US Global Partner Solutions

Our new reality intensifies security challenges

How to drive operational resiliency while strengthening cybersecurity?

Threat detection and response across multiple clouds/platforms

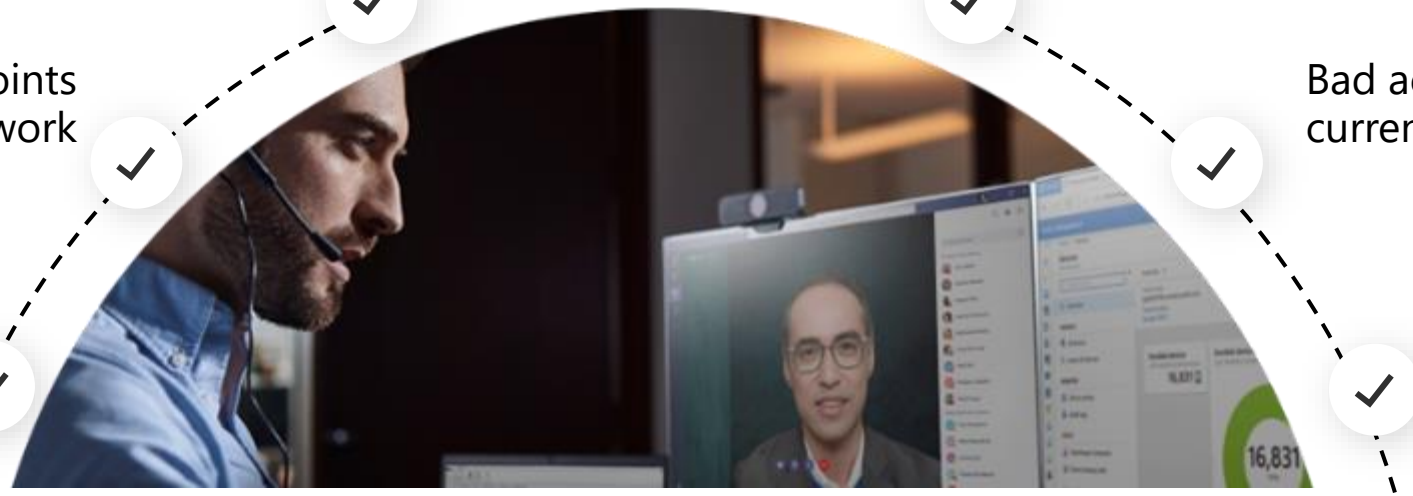
Difficulty rolling out new security controls

Increase in diversity of endpoints accessing the network

Bad actors exploiting current vulnerabilities

Need to support all users in hybrid work

Current networks not optimized to prevent lateral movements



What to expect in 2021 and the next few years...

~~Users are employees~~	→	Employees, partners, customers, bots
~~Corporate managed devices~~	→	Bring your own devices and IoT (OT)
~~On-premises apps~~	→	Explosion of cloud (SaaS) apps
~~Business driving IT~~	→	Technology driving the business
~~Corp network and firewall~~	→	Expanding Perimeters
~~Traditional log collection~~	→	Explosion of signal (identity, data, infrastructure, devices)

Zero Trust

Never Trust, Always Verify

A modern approach to security which treats every access attempt as if it’s originating from an untrusted network, user and device.

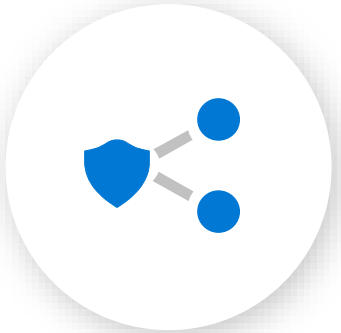
Securing your organization with Zero Trust

Verify **explicitly** | Use **least-privileged access** | Assume **breach**

Microsoft Security

Protect everything

Simplify the complex



Catch what others miss

Grow your future

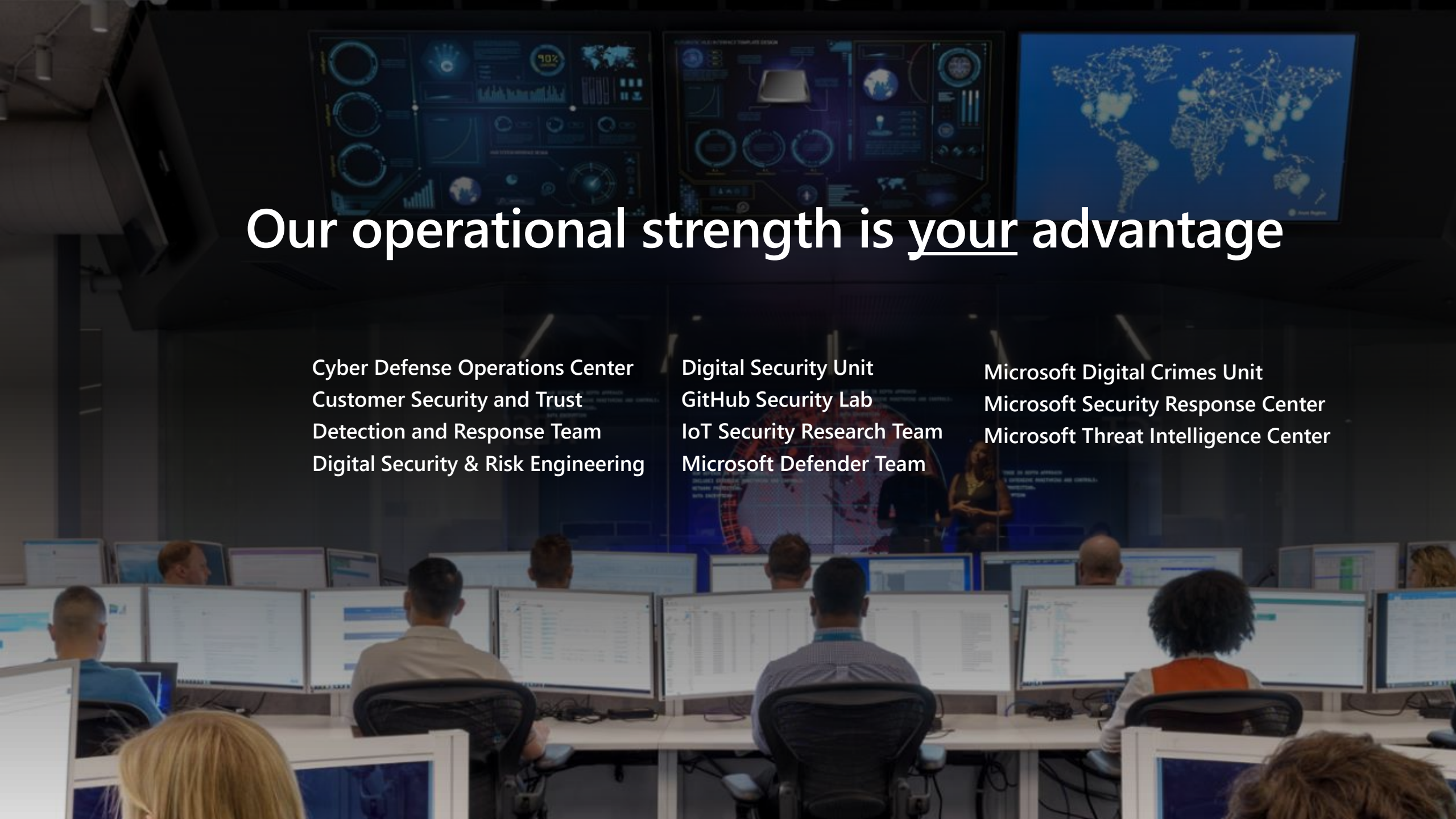
Microsoft's end-to-end security

Integrate up to 40 categories

Endpoint detection and response
Endpoint protection platform
Forensic tools
Intrusion prevention system
Threat vulnerability management
Anti-phishing
User and entity behavior analytics
Threat intelligence feeds
App and browser isolation
Attachment sandboxing
Application control
End-user training
Network firewall (URL detonation)
Host firewall
Secure email gateway
Security assessment
SIEM
SOAR
Cloud access security broker
Cloud workload protection platform
Cloud security posture management
Incident response services
DDOS protection
IoT protection

Data discovery
Data classification
Data loss prevention
Insider risk management
Database security
Information and messaging encryption
Device encryption
Encrypted cloud storage
Secrets management

Identity governance
Active directory
Mobile application management
Mobile device management



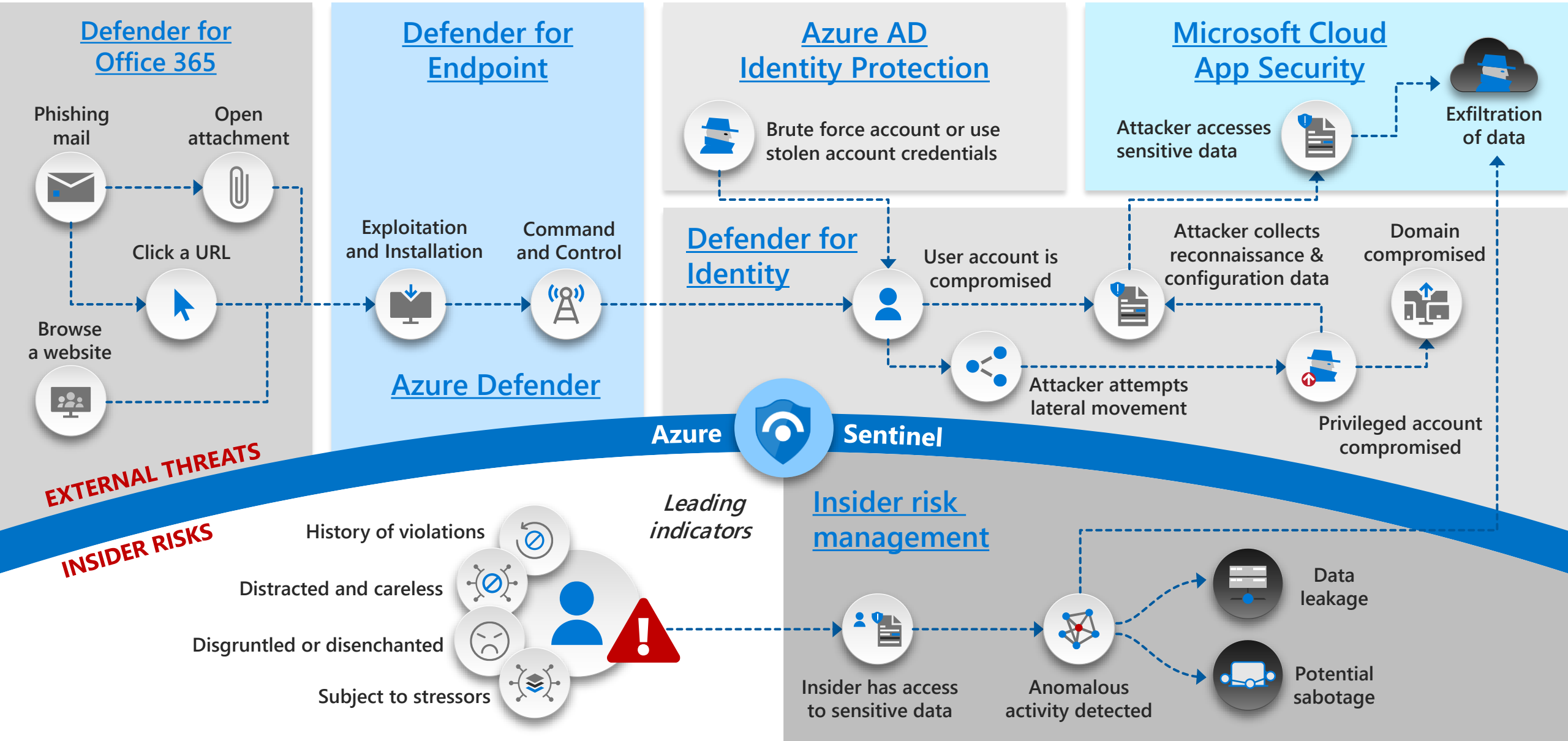
Our operational strength is your advantage

Cyber Defense Operations Center
Customer Security and Trust
Detection and Response Team
Digital Security & Risk Engineering

Digital Security Unit
GitHub Security Lab
IoT Security Research Team
Microsoft Defender Team

Microsoft Digital Crimes Unit
Microsoft Security Response Center
Microsoft Threat Intelligence Center

Protection across the attack chain – insider and external threats



Microsoft Intelligent Security Association

- 130+ Independent software vendors and managed security service providers that have integrated their solutions to better defend against a world of increasing threats.

http://aka.ms/MISA

Microsoft Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

April 2021 – https://aka.ms/MCRA

Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

Azure Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Azure *& 3rd party clouds* | Endpoint *& Server/VM* | Office 365 *Email and Apps* | Identity *Cloud & On-Premises* | SaaS *Microsoft Cloud App Security* | *Other Tools, Logs, and Data Sources*

Microsoft Defender – Extended Detection and Response (XDR)

Azure Defender — *Microsoft 365 Defender*

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

This is interactive!

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

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF

Software as a Service (SaaS)

Microsoft Cloud App Security

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune | Configuration Manager

Microsoft Defender for Endpoint
Unified Endpoint Security
- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Azure Security Center – Cross-Platform Cloud Security Posture Management (CSPM)

Secure Score | Compliance Dashboard

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

Extranet: NGFW | Edge DLP | IPS/IDS | Azure AD App Proxy *Beyond User VPN*

Intranet: Azure Arc | Azure Stack

Express Route | Private Link

Azure Marketplace

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- *Security & Other Services*

Information Protection

Classification Labels

- Azure Purview
- Microsoft Information Protection (MIP): Discover, Classify, Protect, Monitor
- File Scanner *(on-premises and cloud)*
- Data Governance
- Advanced eDiscovery

Compliance Manager

Azure Active Directory

Passwordless & MFA
- Hello for Business
- Authenticator App
- FIDO2 Keys

Identity Protection
- Leaked cred protection
- Behavioral Analytics

Azure AD PIM

Identity Governance

Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 Security

Network protection | *App control*
Credential protection | *Exploit protection*
Full Disk Encryption | *Behavior monitoring*
Attack surface reduction | *Next-generation protection*

IoT and Operational Technology (OT)

Azure Sphere

Azure Defender for IoT
- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Azure Defender – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

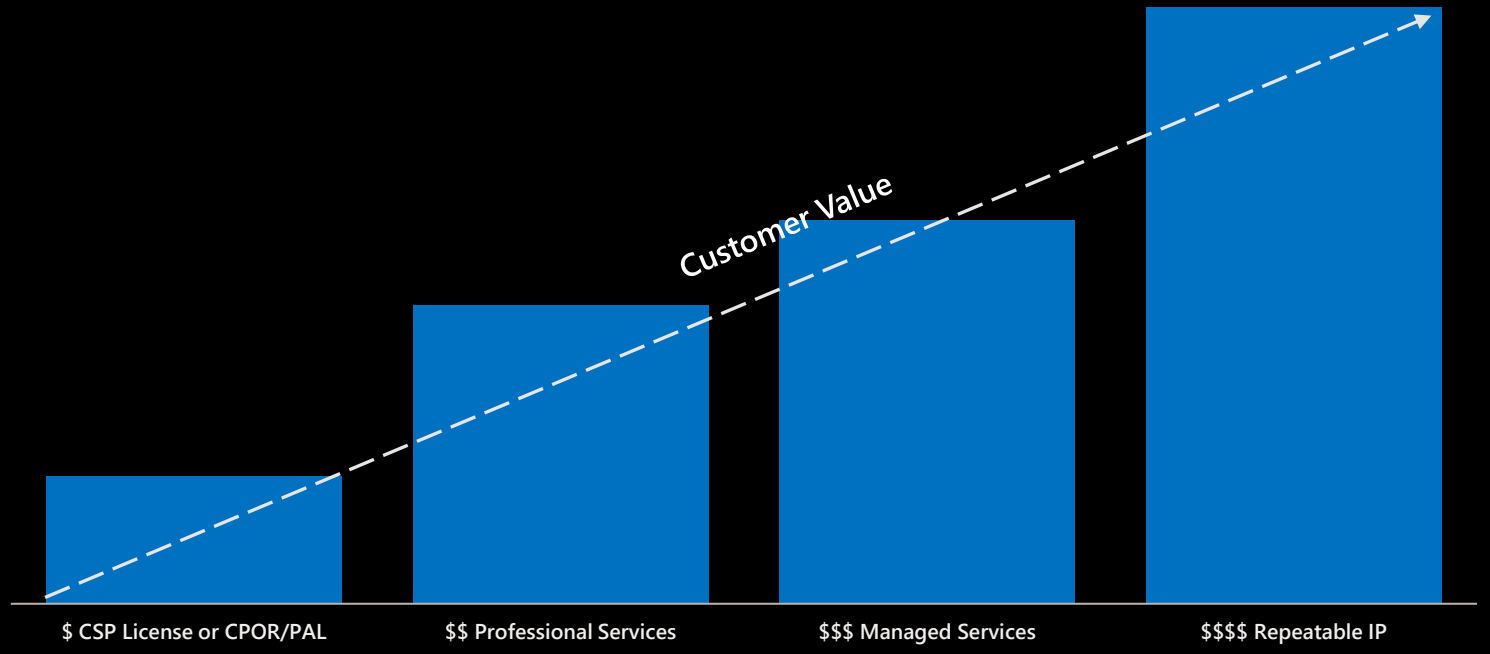
GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

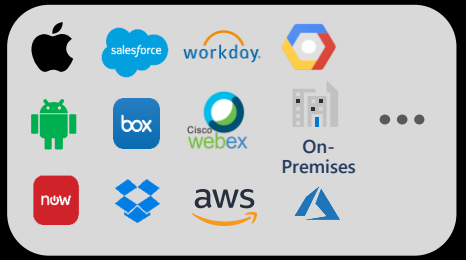
Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Partner Opportunity w/ Security, Compliance and Identity



Extends across Microsoft & Non-Microsoft platforms



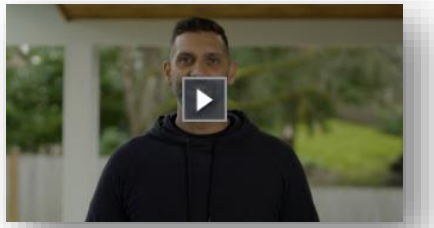
[More Information on Partner Opportunity]

Next Steps and Resources

Inspire content @ https://myinspire.microsoft.com

Learn more about Microsoft Security, Compliance and Identity (SCI)

Security for All



Manage risk and secure information across your environment

Our identity vision and roadmap for strengthening Zero Trust defenses in the era of hybrid work

Microsoft Security's roadmap for defending against advanced threats

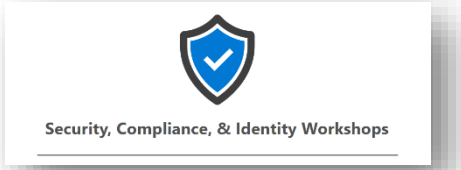
Zero Trust - The proactive approach to cybersecurity

Build capability and capacity in Microsoft SCI

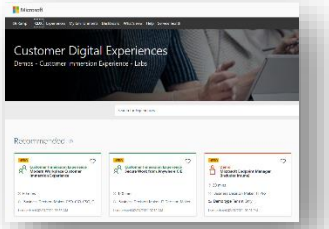
Security Practice Development Playbook

Secure Remote Work Practice Development Playbook

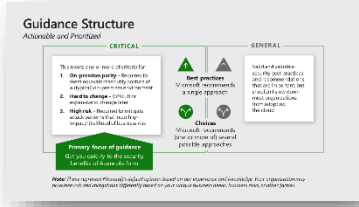
Enablement & Skill Guide



SCI Cloud Accelerator Workshops



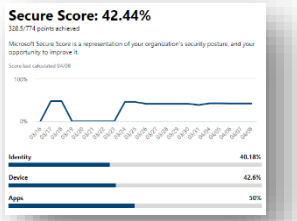
SCI Customer Demos



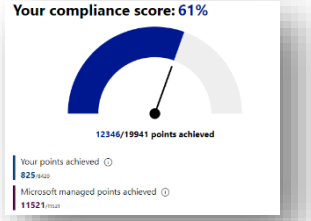
Microsoft Security Best Practices

Strengthen your security and compliance posture

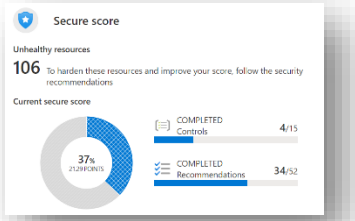
Microsoft 365 Secure Score



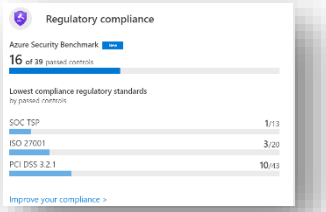
Microsoft 365 Compliance Score



Azure Security Center Secure Score



Azure Security Center Regulatory Compliance



Azure Active Directory Identity Secure Score

Microsoft