WEBINAR

Cyber Insurance

How to Meet the Ever-Increasing Requirements of Cybersecurity Insurance

interlink®
CLOUD ADVISORS

Presenters:

Mike Wilson
Interlink Cloud Advisors
CTO / Vice President

Jimmy Smogor
Interlink Cloud Advisors
Security Practice Lead

Agenda

Cyber Insurance

Microsoft Partner
Microsoft

Gold Cloud Productivity
Gold Cloud Platform
Gold Enterprise Mobility Management
Gold Datacenter
Gold Collaboration and Content
Gold Messaging
Gold Communications
Gold Windows and Devices
Gold Project and Portfolio Management
Gold Small and Midmarket Cloud Solutions
Gold Security

- Welcome/Interlink Overview
- Overview of Cybersecurity Insurance
- Protecting User Identities
- Endpoint Management
- Threat Protection and Response
- Vulnerability Management
- Backup & Disaster Recovery Techniques
- Licensing Options/Assessments
- Q&A

THE INTERLINK ADVANTAGE

SIMPLIFY

We simplify your organization’s interaction with Microsoft

✓Advocate with Microsoft: We know how to navigate their programs, licensing, incentives, and teams on your behalf

✓Consistently in the top 10 of partners worldwide in the usage of Microsoft funding to assist with your pilots, workshops, and deployments

✓**Licensing: multiple certified licensing experts who understand the complex maze of product and program licensing can help you find the best licensing options**

✓Thought leaders: we summarize pertinent industry information to keep our clients educated and informed through our blog, webinars, and regular speaking engagements

EXPERIENCED

We ensure the success of your project

✓Documented, tested, and proven methodologies used in over 5000 implementations

✓Comprehensive assessments which identify challenges in advance, before they impact the project

✓Interlink can accelerate all escalations straight to Microsoft Level III minimizing support frustration

✓**Responsive live answer Service Desk runs 24x7x365 with one-hour service level agreements**

REMOVE RISK

We build security and compliance into every project

- ✓ Architect to satisfy compliance requirements such as CMMC, GDPR, HIPAA, and NIST
- ✓ Processes built to help identify and mitigate security risks
- ✓ We continue to revisit and renew as new compliance and regulations surface
- ✓ We help you understand where risks and vulnerabilities exist and create long-term plans

CREATE BUSINESS VALUE

We drive business value from your technology investments

- ✓ Midmarket focused: we combine the resource availability with the expertise levels that you need to ensure the right fit
- ✓ Build personalized deployment roadmaps to drive long term success
- ✓ Support of our clients budgeting, planning, and C-Suite justification processes, including jointly building ROI and cost justification models
- ✓ Recognized by Microsoft as the top partner for helping our clients adopt their cloud technologies

MICROSOFT EXPERTISE

We have extensive expertise in Microsoft technologies

- ✓ 11 Microsoft Gold Competencies and 9 Advanced Specializations covering Microsoft 365 and Azure
- ✓ All consultants hold certifications from Microsoft
- ✓ Interlink employees badged by Microsoft in recognition of our expertise
- ✓ Deployed more seats of Office 365 in geography in the first three years than any other partner
- ✓ Frequently recognized and awarded by Microsoft – including partner of the year
- ✓ Nationally managed by Microsoft: gains us access to a wide array of resources for clients

Mike Wilson

Interlink Cloud Advisors – CTO / Vice President

- Overview of Cybersecurity Insurance
- Types of Coverage Available

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

- **Interlink can help with how to meet coverage requirements.**

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

- Interlink can help with how to meet coverage requirements.
- Disclaimer: Interlink does not sell insurance and we are not making specific recommendations for you or your business

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

Why Cyber Insurance?

- Breaches are expensive

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

Why Cyber Insurance?

- Breaches are expensive
- **May be required by contract or regulation**

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

Two Primary Scenarios:

- Business Disruption

Cybersecurity Insurance Coverage:

Two Primary Scenarios:

- Business Disruption
  - Ransomware, Virus Activity, etc.

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

Interlink
Cloud
Advisors

Two Primary Scenarios:

- Business Disruption
  - Ransomware, Virus Activity, etc.
- Data Breach

Cybersecurity Insurance Coverage:

Two Primary Scenarios:

- Business Disruption
  - Ransomware, Virus Activity, etc.
- Data Breach
  - Worse for regulated industries (FINRA, HIPAA, FedRAMP, etc.)

Cybersecurity Insurance Coverage:

What is covered?:

- Forensic investigation and response

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

What is covered?:

- Forensic investigation and response
- **Legal expenses**

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

Interlink
Cloud
Advisors

What is covered?:

- Forensic investigation and response
- Legal expenses
- **Notifications**

Cybersecurity Insurance Coverage:

Interlink
Cloud
Advisors

What is covered?:

- Forensic investigation and response
- Legal expenses
- Notifications
- Regulatory defense expenses/fines

Cybersecurity Insurance Coverage:

Interlink
Cloud
Advisors

What is covered?:

- Forensic investigation and response
- Legal expenses
- Notifications
- Regulatory defense expenses/fines
- Cyber extortion (ransom)

Cybersecurity Insurance Coverage:

Interlink
Cloud
Advisors

What is covered?:

- Forensic investigation and response
- Legal expenses
- Notifications
- Regulatory defense expenses/fines
- Cyber extortion (ransom)
- **Business interruption**

Interlink
Cloud
Advisors

Cybersecurity Insurance Coverage:

What is covered?:

- Forensic investigation and response
- Legal expenses
- Notifications
- Regulatory defense expenses/fines
- Cyber extortion (ransom)
- Business interruption
- **Payment fraud**

Cybersecurity Insurance Coverage:

Old Model:

- Fill out a survey, get a price

Cybersecurity Insurance Coverage:

Interlink
Cloud
Advisors

Old Model:

- Fill out a survey, get a price

New Model:

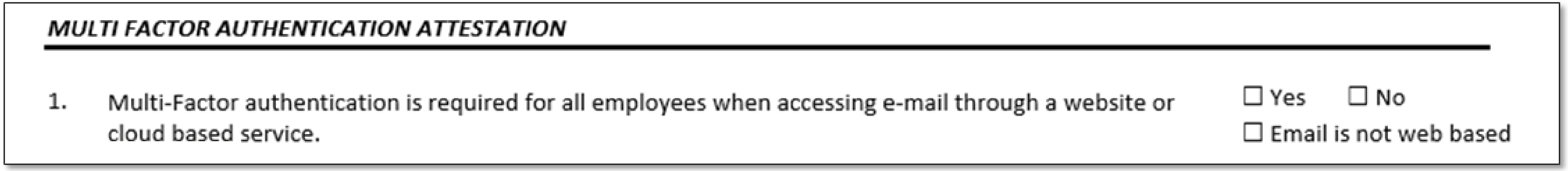
- Prescriptive requirements or discounts for enhanced security

Jimmy Smogor

Interlink Cloud Advisors – Security Practice Lead

- Implementing Strong Identity Protections
- Endpoint Management
- Threat Protection and Response

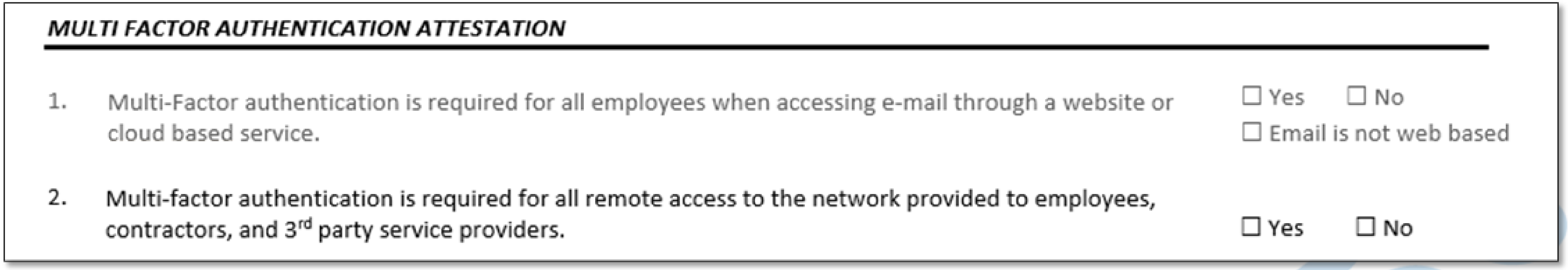
Example of Cyber Insurance Policy:



MULTI FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing e-mail through a website or cloud based service. ☐ Yes ☐ No ☐ Email is not web based

Example of Cyber Insurance Policy:

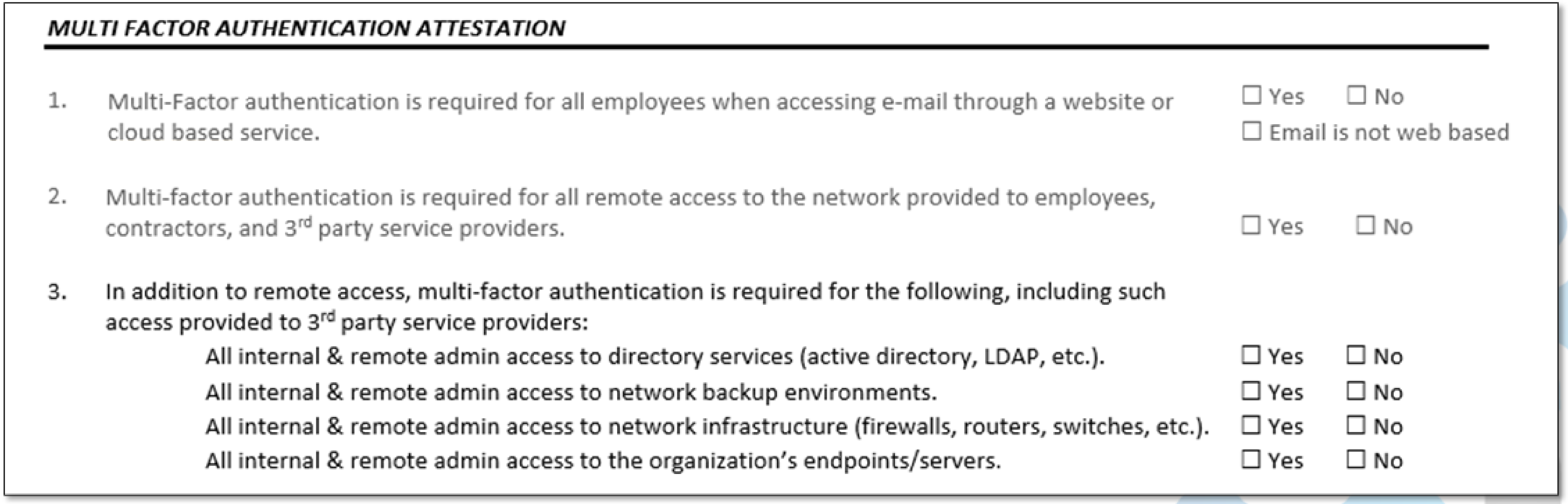


MULTI FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing e-mail through a website or cloud based service. ☐ Yes ☐ No ☐ Email is not web based

2. Multi-factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☐ Yes ☐ No

Example of Cyber Insurance Policy:



MULTI FACTOR AUTHENTICATION ATTESTATION

1. Multi-Factor authentication is required for all employees when accessing e-mail through a website or cloud based service. ☐ Yes ☐ No ☐ Email is not web based

2. Multi-factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers. ☐ Yes ☐ No

3. In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:

All internal & remote admin access to directory services (active directory, LDAP, etc.). ☐ Yes ☐ No

All internal & remote admin access to network backup environments. ☐ Yes ☐ No

All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.). ☐ Yes ☐ No

All internal & remote admin access to the organization's endpoints/servers. ☐ Yes ☐ No

Multi Factor with Azure Conditional Access

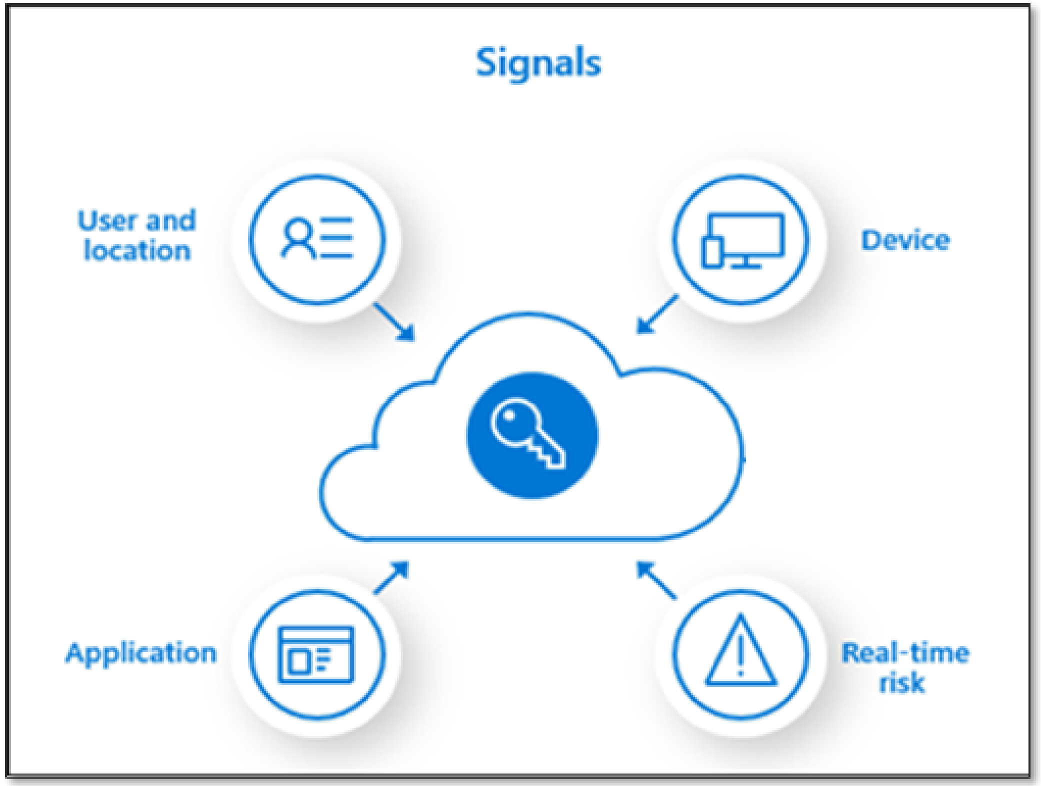
- Use Conditional Access policies to apply the right access controls

Multi Factor with Azure Conditional Access

- Use Conditional Access policies to apply the right access controls
- Keep your organization secure and stay out of your user's way when not needed

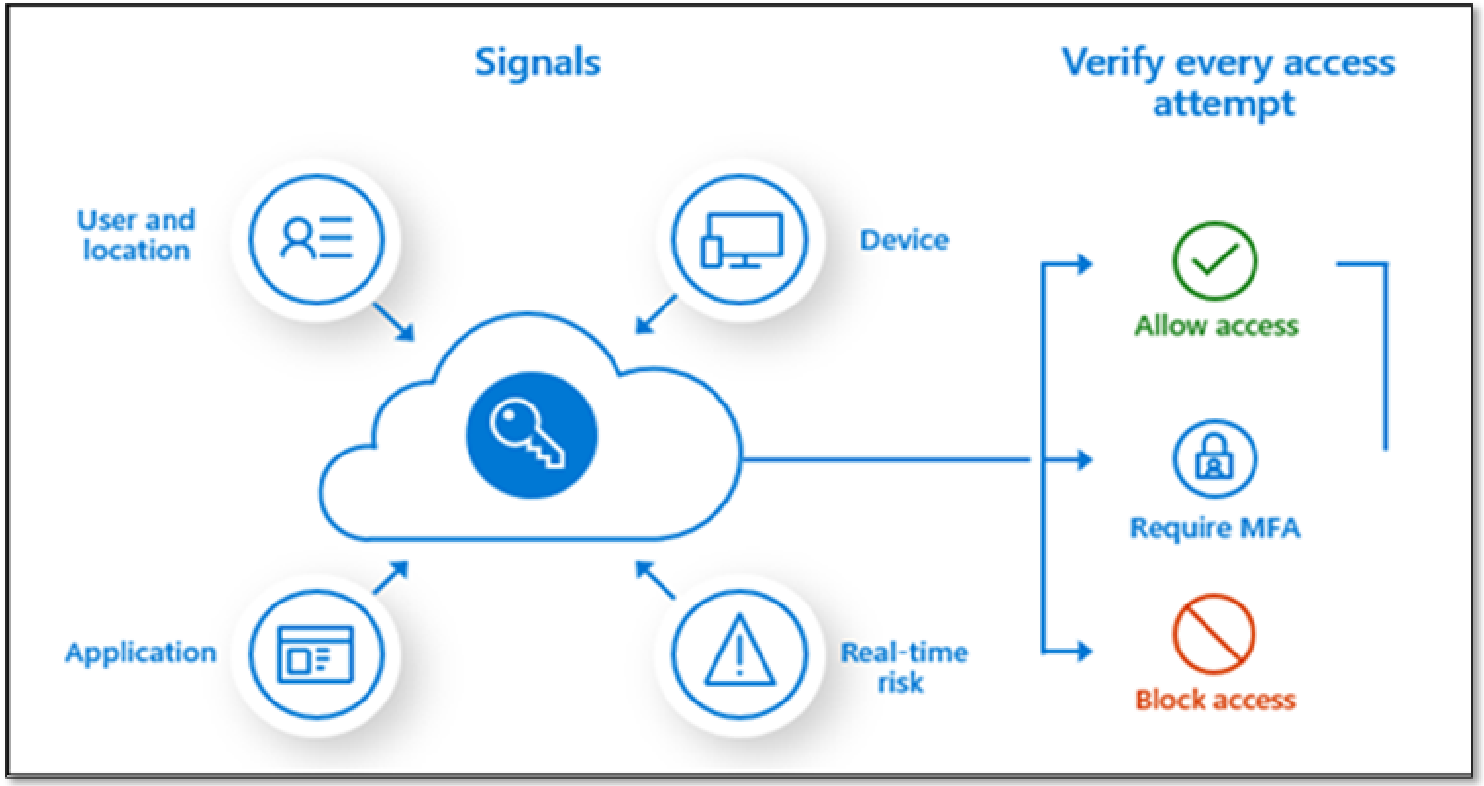
Multi Factor with Azure Conditional Access

- Use Conditional Access policies to apply the right access controls
- Keep your organization secure and stay out of your user's way when not needed



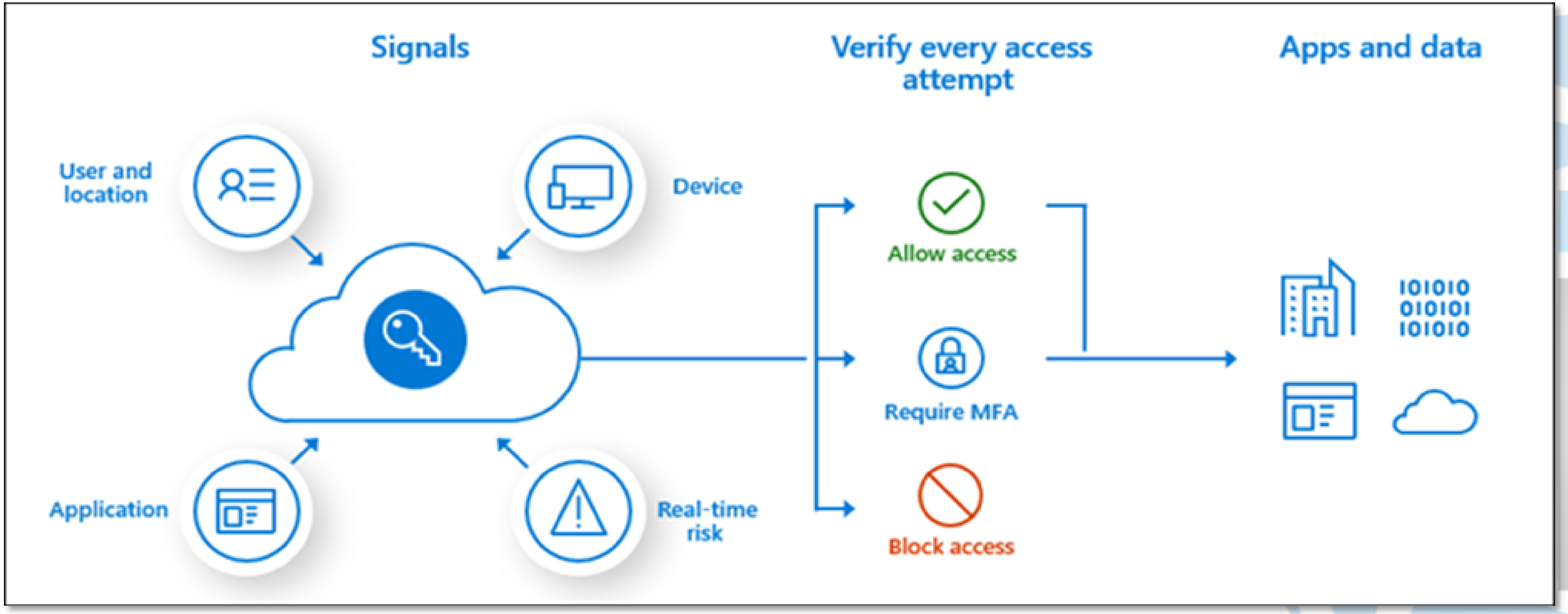
Multi Factor with Azure Conditional Access

- Use Conditional Access policies to apply the right access controls
- Keep your organization secure and stay out of your user's way when not needed

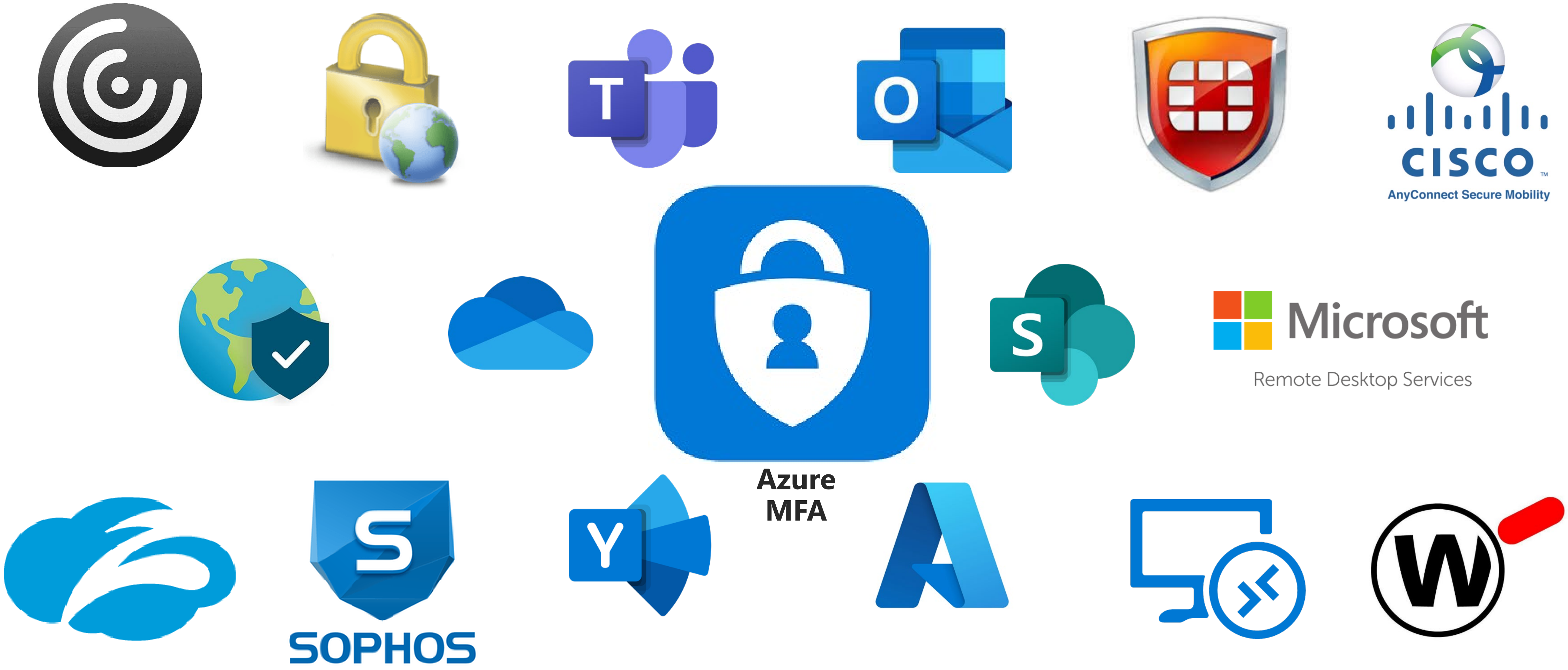


Multi Factor with Azure Conditional Access

- Use Conditional Access policies to apply the right access controls
- Keep your organization secure and stay out of your user's way when not needed

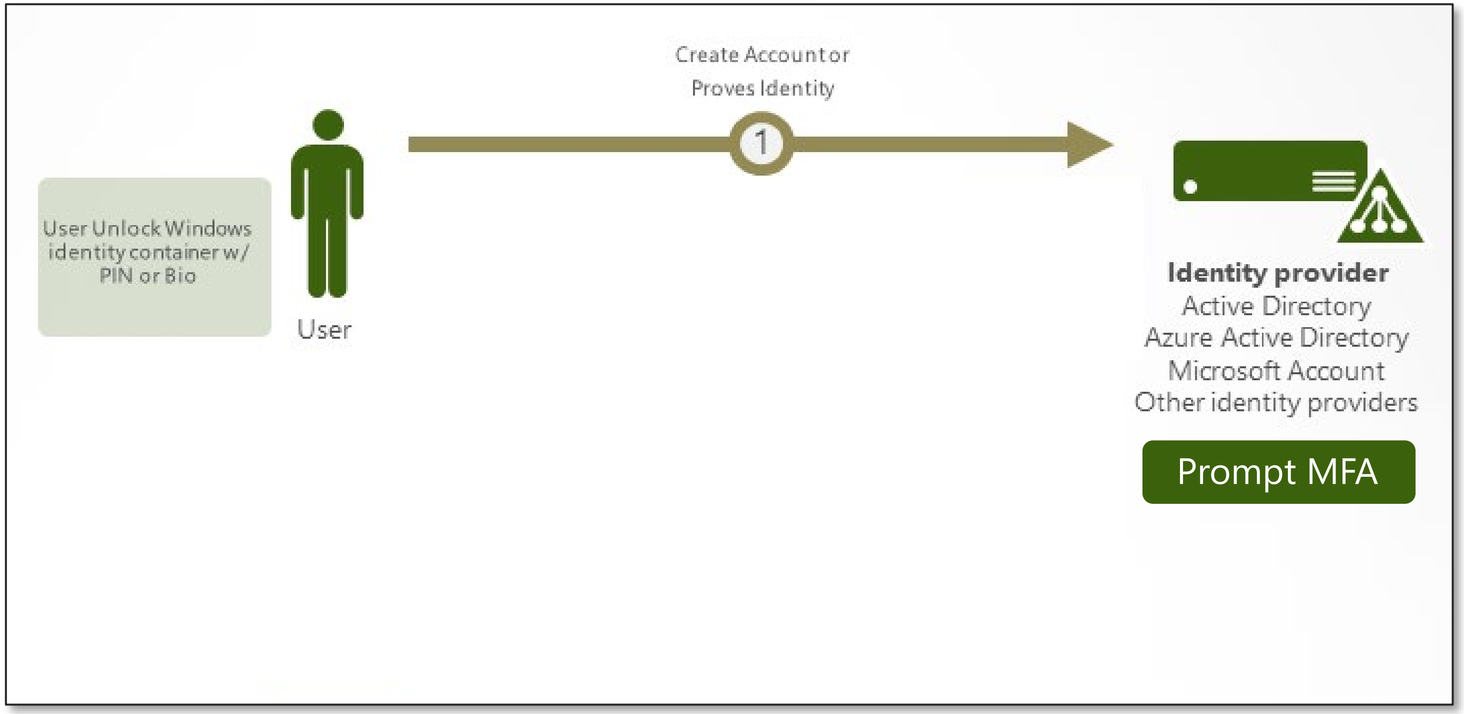


MFA for only Cloud Applications?



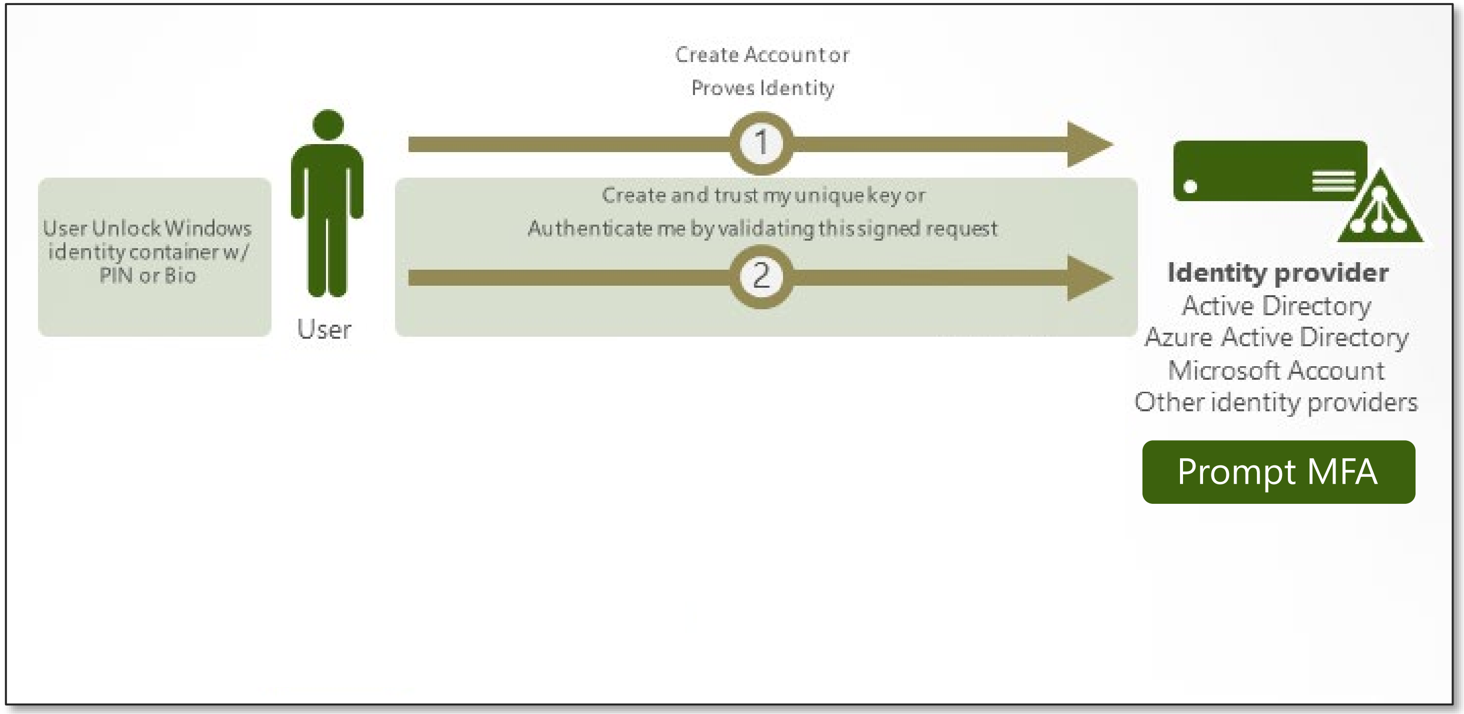
Requirement: MFA at the User Endpoint

- Windows Hello
- Protected & enforced by Azure MFA
- A Hello certificate can only be created after a successful sign in from Azure MFA
- With the correct trusts in place Windows Hello can be a verified authentication method to companies on-premise Active Directory environments
- Single token created per user per device



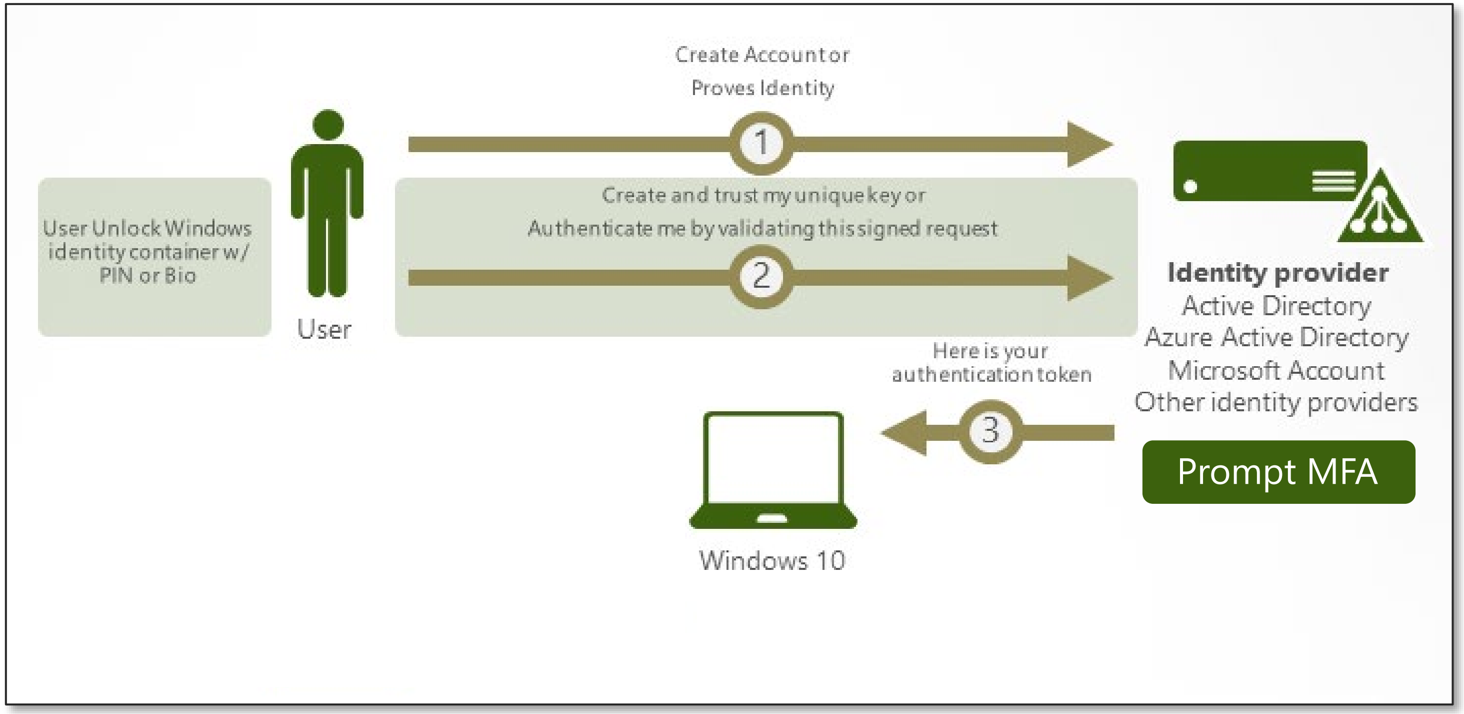
Requirement: MFA at the User Endpoint

- Windows Hello
- Protected & enforced by Azure MFA
- A Hello certificate can only be created after a successful sign in from Azure MFA
- With the correct trusts in place Windows Hello can be a verified authentication method to companies on-premise Active Directory environments
- Single token created per user per device



Requirement: MFA at the User Endpoint

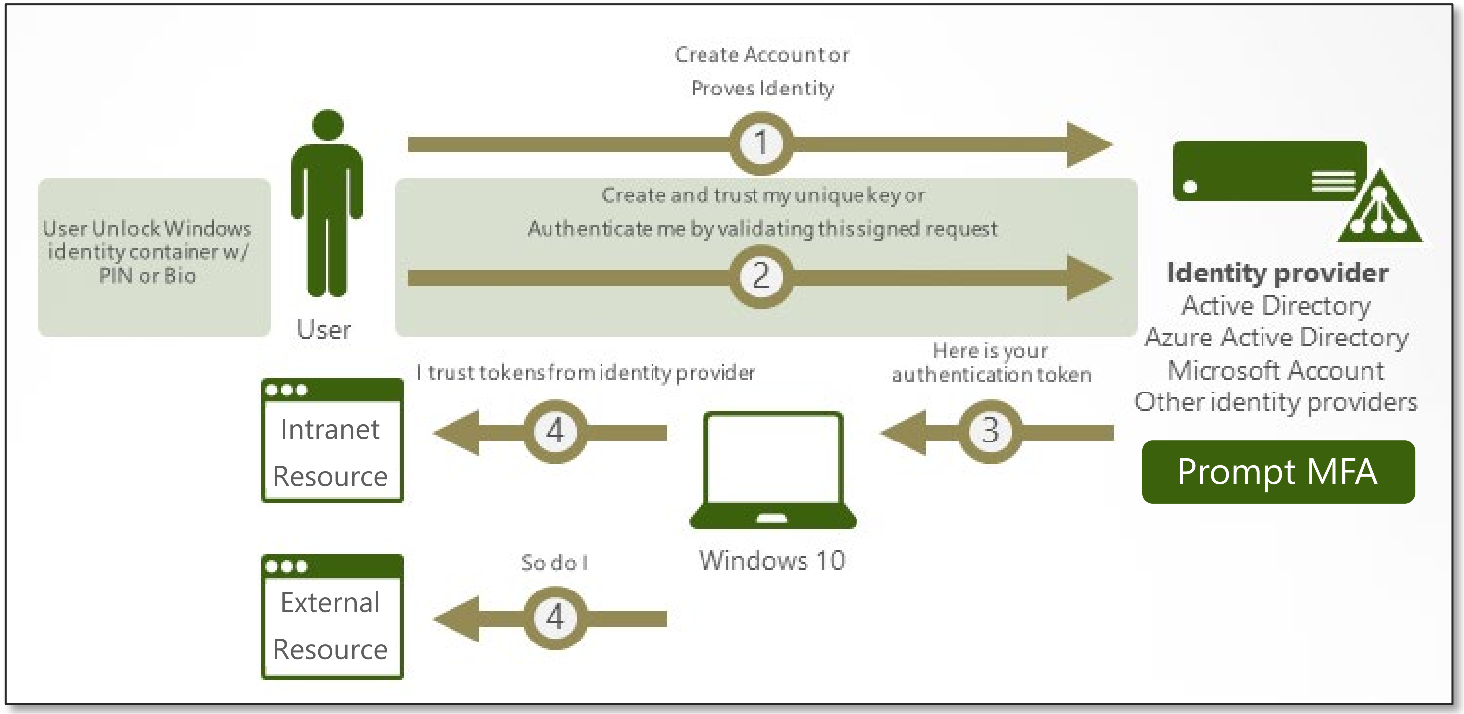
- Windows Hello
- Protected & enforced by Azure MFA
- A Hello certificate can only be created after a successful sign in from Azure MFA
- With the correct trusts in place Windows Hello can be a verified authentication method to companies on-premise Active Directory environments
- Single token created per user per device



Create Account or
Proves Identity
1
User Unlock Windows identity container w/ PIN or Bio
User
Create and trust my unique key or
Authenticate me by validating this signed request
2
Identity provider
Active Directory
Azure Active Directory
Microsoft Account
Other identity providers
Here is your authentication token
3
Prompt MFA
Windows 10

Requirement: MFA at the User Endpoint

- Windows Hello
- Protected & enforced by Azure MFA
- A Hello certificate can only be created after a successful sign in from Azure MFA
- With the correct trusts in place Windows Hello can be a verified authentication method to companies on-premise Active Directory environments
- Single token created per user per device



Create Account or
Proves Identity
1
User Unlock Windows identity container w/ PIN or Bio
User
Create and trust my unique key or
Authenticate me by validating this signed request
2
Identity provider
Active Directory
Azure Active Directory
Microsoft Account
Other identity providers
Prompt MFA
I trust tokens from identity provider
Here is your authentication token
3
4
Intranet Resource
Windows 10
So do I
4
External Resource

Requirement: MFA for Administrator Logons to Directory Services

Interlink Cloud Advisors

- With Azure MFA admins can lock down privileged accounts within a few seconds.

Requirement: MFA for Administrator Logons to Directory Services

Interlink Cloud Advisors

- With Azure MFA admins can lock down privileged accounts within a few seconds.
- How do you require the same requirement for on-premise activities?

Requirement: MFA for Administrator Logons to Directory Services

Smart Cards:

- Require a specific hardware token for completing the user authentication

Requirement: MFA for Administrator Logons to Directory Services

Smart Cards:

- Require a specific hardware token for completing the user authentication
- Smart Cards are far more secure than using a password.

Requirement: MFA for Administrator Logons to Directory Services

Smart Cards:

- Require a specific hardware token for completing the user authentication
- Smart Cards are far more secure than using a password.
  - All require two-factor PIN to unlock

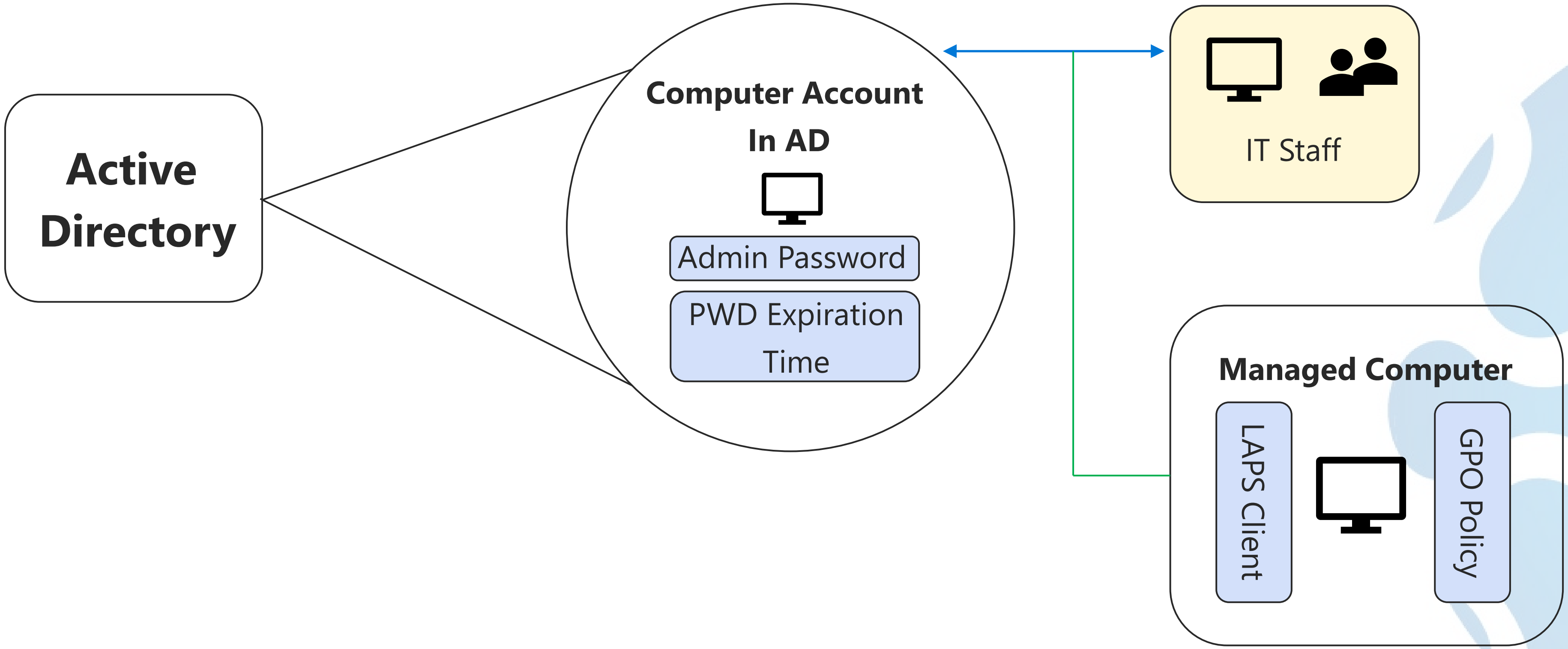
Requirement: MFA for Administrator Logons to Directory Services

Smart Cards:

- Require a specific hardware token for completing the user authentication
- Smart Cards are far more secure than using a password.
  - All require two-factor PIN to unlock
  - Newer cards supporting biometrics

Requirement: Protect Local Administrator Accounts

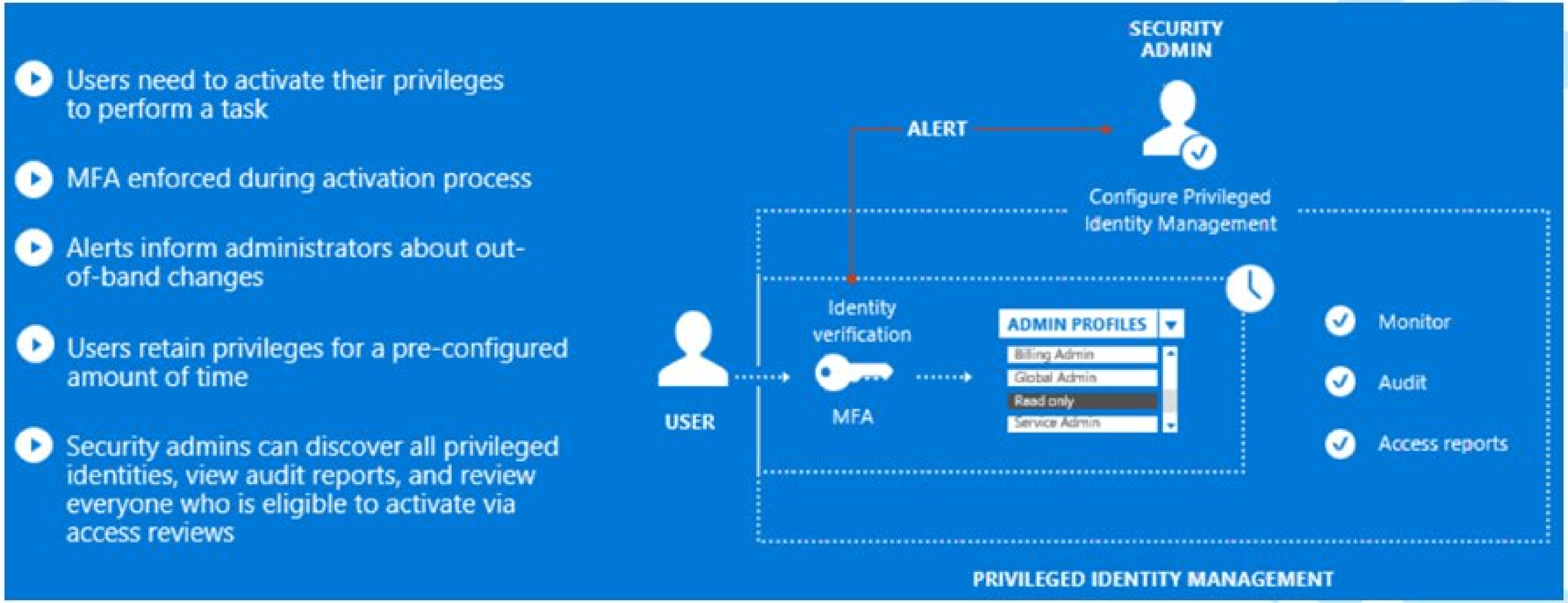
- Local Admin Password Solution (LAPS)
- Targets local administrator accounts on Windows devices
- Automatically rotates passwords for all machines controlled by LAPS



Requirement: Review Administrative Access on a Regular Basis

Azure Privileged Identity Management (PIM)

- Access Reviews
- Conditional Administrators



- Users need to activate their privileges to perform a task
- MFA enforced during activation process
- Alerts inform administrators about out-of-band changes
- Users retain privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports, and review everyone who is eligible to activate via access reviews

Requirement: Encrypt Data on Endpoints

Bitlocker Disk Encryption

Requirement: Encrypt Data on Endpoints

Bitlocker Disk Encryption

- Full drive encryption on Windows 10 systems

Requirement: Encrypt Data on Endpoints

Bitlocker Disk Encryption

- Full drive encryption on Windows 10 systems
- Managed by Microsoft Endpoint Manager (Intune)

Requirement: Encrypt Data on Endpoints

Bitlocker Disk Encryption

- Full drive encryption on Windows 10 systems
- Managed by Microsoft Endpoint Manager (Intune)
- Encryption keys stored in Azure Active Directory

Interlink
Cloud
Advisors

Requirement: Patch Endpoints on a Regular Basis

- Can’t wait for systems to be connected to the network

Interlink
Cloud
Advisors

Requirement: Patch Endpoints on a Regular Basis

- Can’t wait for systems to be connected to the network
- Deploy updates quickly after release

Interlink
Cloud
Advisors

Requirement: Patch Endpoints on a Regular Basis

- Can’t wait for systems to be connected to the network
- Deploy updates quickly after release
- Answer: Endpoint Manager (Intune + SCCM)

Requirement: Strong Email Security

- **Flag external emails**

Requirement: Strong Email Security

- Flag external emails
- **Sandbox for advanced scanning of attachments and embedded links (Defender for O365)**

Requirement: Strong Email Security

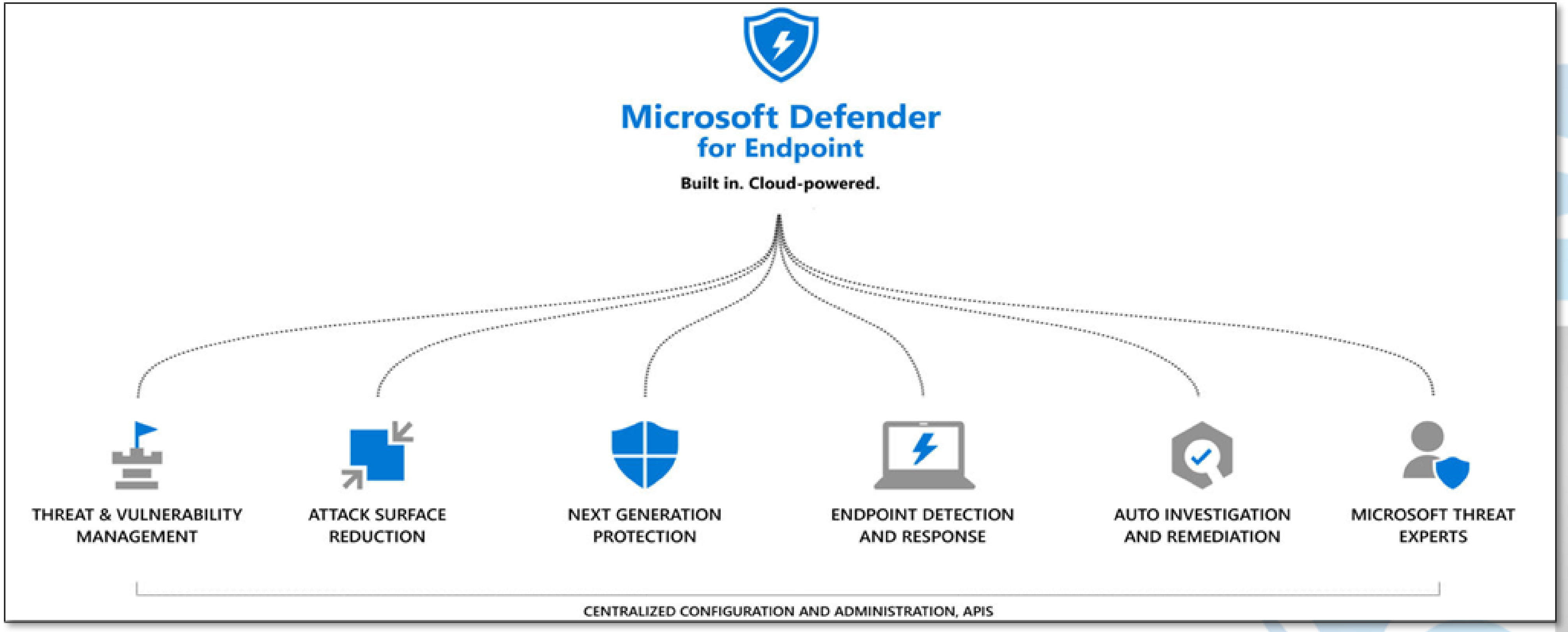
- Flag external emails
- Sandbox for advanced scanning of attachments and embedded links (Defender for O365)
- **Protect against phishing – SPF/DKIM/DMARC**

Requirement: Protect Endpoints with an EDR Tool

Anti-virus is not enough.

Requirement: Protect Endpoints with an EDR Tool

Anti-virus is not enough.



Microsoft Defender for Endpoint

Built in. Cloud-powered.

THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION AND RESPONSE

AUTO INVESTIGATION AND REMEDIATION

MICROSOFT THREAT EXPERTS

CENTRALIZED CONFIGURATION AND ADMINISTRATION, APIS

Requirement: Monitor and Respond to Security Alerts

Monitor:

- Implement Azure Sentinel (SIEM)

Requirement: Monitor and Respond to Security Alerts

Monitor:

- Implement Azure Sentinel (SIEM)
- Aggregate Logs

Requirement: Monitor and Respond to Security Alerts

Monitor:

- Implement Azure Sentinel (SIEM)
- Aggregate Logs
- Extract information from raw data

Requirement: Monitor and Respond to Security Alerts

Monitor:

- Implement Azure Sentinel (SIEM)
- Aggregate Logs
- Extract information from raw data
- Create automated responses for security events

Requirement: Monitor and Respond to Security Alerts

Monitor:

- Implement Azure Sentinel (SIEM)
- Aggregate Logs
- Extract information from raw data
- Create automated responses for security events

Respond:

- Build a SOC or outsource

Requirement: Monitor and Respond to Security Alerts

Monitor:

- Implement Azure Sentinel (SIEM)
- Aggregate Logs
- Extract information from raw data
- Create automated responses for security events

Respond:

- Build a SOC or outsource
- CRITICAL START

CRITICAL START Managed Detection and Response

People

We make your team more efficient and effective. **Your team will only see < 1% of total alerts generated and anything they see will have been investigated and contextualized by our world-class SOC.**

Transparency, your team can see and interact with the exact same portal our SOC analysts use. All of the details of what our SOC is seeing, investigating and doing are available.

Mobile, full fidelity of events and full functionality of response options available via a mobile app on iOS and Android.

Real support, whenever guidance is needed, **our highly trained, tenured, shift-based team** is there 24x7x365.

Process

We stop breaches by resolving every security alert.

We seek to prove good. Leveraging our Trusted Behavior Registry, we orchestrate resolution of known good events.

We simplify the end-to-end security detection and response process.

We contain the blast radius of a threat by **actioning the massive visibility across identity, email, endpoint, cloud and SIEM.**

We handle investigation (what happened, how far did they get, is it stopped) by taking alerts and rationalizing them against standard cybersecurity reasoning and vocabulary.

Technology

We address the challenge of portal fatigue. We focus on the right workflows and the right console data, just in time.

We provide pre-built queries that can take variable input to get the necessary data without the learning curve of KQL.

API's are used to pull additional data reducing investigation times. **We stitch together signal from across each Microsoft Threat Protection solution (identity, email, endpoint, cloud and SIEM) to provide a wholistic correlated view of the events.**

Our access follows the principle of least privilege and is co-managed. We function as an AD Enterprise Application to uphold the standard of least privilege and prevent permission creep (we would never ask for Global Admin).

Mike Wilson

Interlink Cloud Advisors – CTO / Vice President

- Vulnerability Management
- Backups and DR
- Microsoft Licensing
- Microsoft Funding
- Questions

Requirement: Regularly Scan Network for Vulnerabilities

- External Scans

Requirement: Regularly Scan Network for Vulnerabilities

- External Scans
- Internal Scans

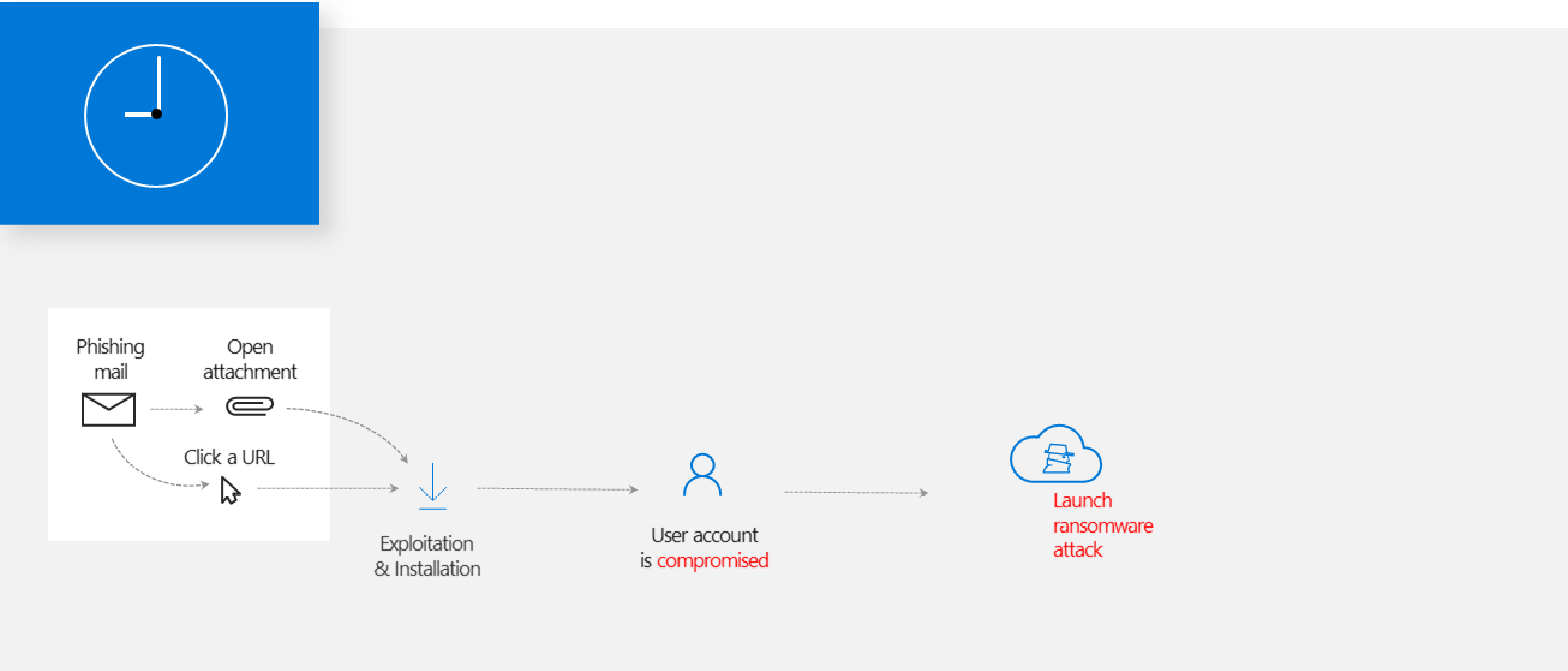
Requirement: Regularly Scan Network for Vulnerabilities

- External Scans
- Internal Scans
- Pen Tests

interlink®
CLOUD ADVISORS

Yes, You Have Backups. Are they good enough?

Anatomy of an Attack – Old Paradigm



Phishing mail

Open attachment

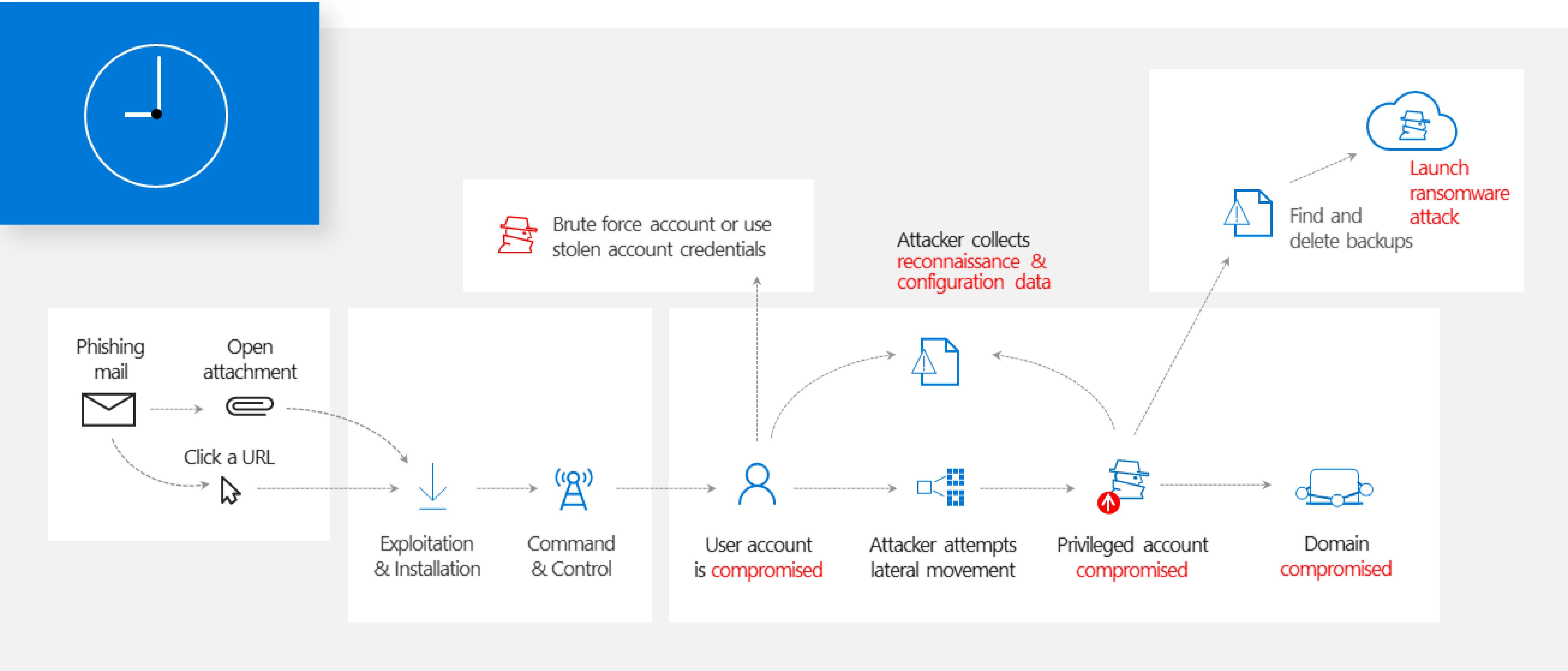
Click a URL

Exploitation & Installation

User account is compromised

Launch ransomware attack

Anatomy of an Attack – New Paradigm


Brute force account or use stolen account credentials
Attacker collects reconnaissance & configuration data
Find and delete backups
Launch ransomware attack
Phishing mail
Open attachment
Click a URL
Exploitation & Installation
Command & Control
User account is compromised
Attacker attempts lateral movement
Privileged account compromised
Domain compromised

Approaching Backups and DR

1. Backups Must be Air-Gapped

Interlink Cloud Advisors

Interlink
Cloud
Advisors

Approaching Backups and DR

1. Backups Must be Air-Gapped
   a. Azure Backup and Azure Site Recovery are cost effective ways to help.

Interlink
Cloud
Advisors

Approaching Backups and DR

1. Backups Must be Air-Gapped
   a. Azure Backup and Azure Site Recovery are cost effective ways to help.
2. Protect the ability to delete backups – these accounts are critical.

Interlink
Cloud
Advisors

Approaching Backups and DR

1. Backups Must be Air-Gapped
   a. Azure Backup and Azure Site Recovery are cost effective ways to help.
2. Protect the ability to delete backups – these accounts are critical.
3. Don’t forget end user desktops – use OneDrive!

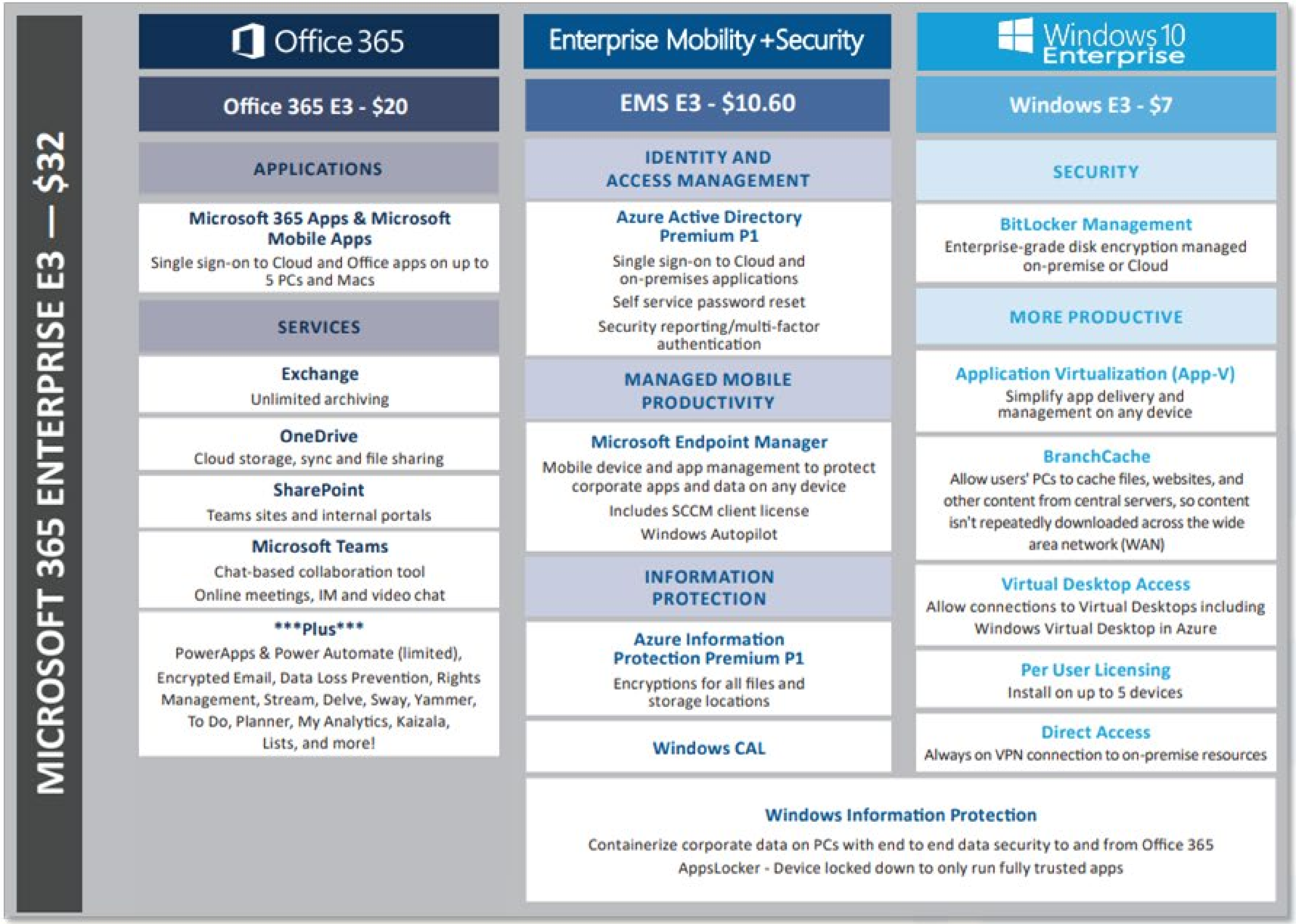
interlink®

CLOUD ADVISORS

Pricing

Cyber Insurance

Microsoft 365 E3



MICROSOFT 365 ENTERPRISE E3 — $32

Office 365

Office 365 E3 - $20

APPLICATIONS

Microsoft 365 Apps & Microsoft Mobile Apps
Single sign-on to Cloud and Office apps on up to 5 PCs and Macs

SERVICES

Exchange
Unlimited archiving

OneDrive
Cloud storage, sync and file sharing

SharePoint
Teams sites and internal portals

Microsoft Teams
Chat-based collaboration tool
Online meetings, IM and video chat

*****Plus*****
PowerApps & Power Automate (limited), Encrypted Email, Data Loss Prevention, Rights Management, Stream, Delve, Sway, Yammer, To Do, Planner, My Analytics, Kaizala, Lists, and more!

Enterprise Mobility + Security

EMS E3 - $10.60

IDENTITY AND ACCESS MANAGEMENT

Azure Active Directory Premium P1
Single sign-on to Cloud and on-premises applications
Self service password reset
Security reporting/multi-factor authentication

MANAGED MOBILE PRODUCTIVITY

Microsoft Endpoint Manager
Mobile device and app management to protect corporate apps and data on any device
Includes SCCM client license
Windows Autopilot

INFORMATION PROTECTION

Azure Information Protection Premium P1
Encryptions for all files and storage locations

Windows CAL

Windows 10 Enterprise

Windows E3 - $7

SECURITY

BitLocker Management
Enterprise-grade disk encryption managed on-premise or Cloud

MORE PRODUCTIVE

Application Virtualization (App-V)
Simplify app delivery and management on any device

BranchCache
Allow users' PCs to cache files, websites, and other content from central servers, so content isn't repeatedly downloaded across the wide area network (WAN)

Virtual Desktop Access
Allow connections to Virtual Desktops including Windows Virtual Desktop in Azure

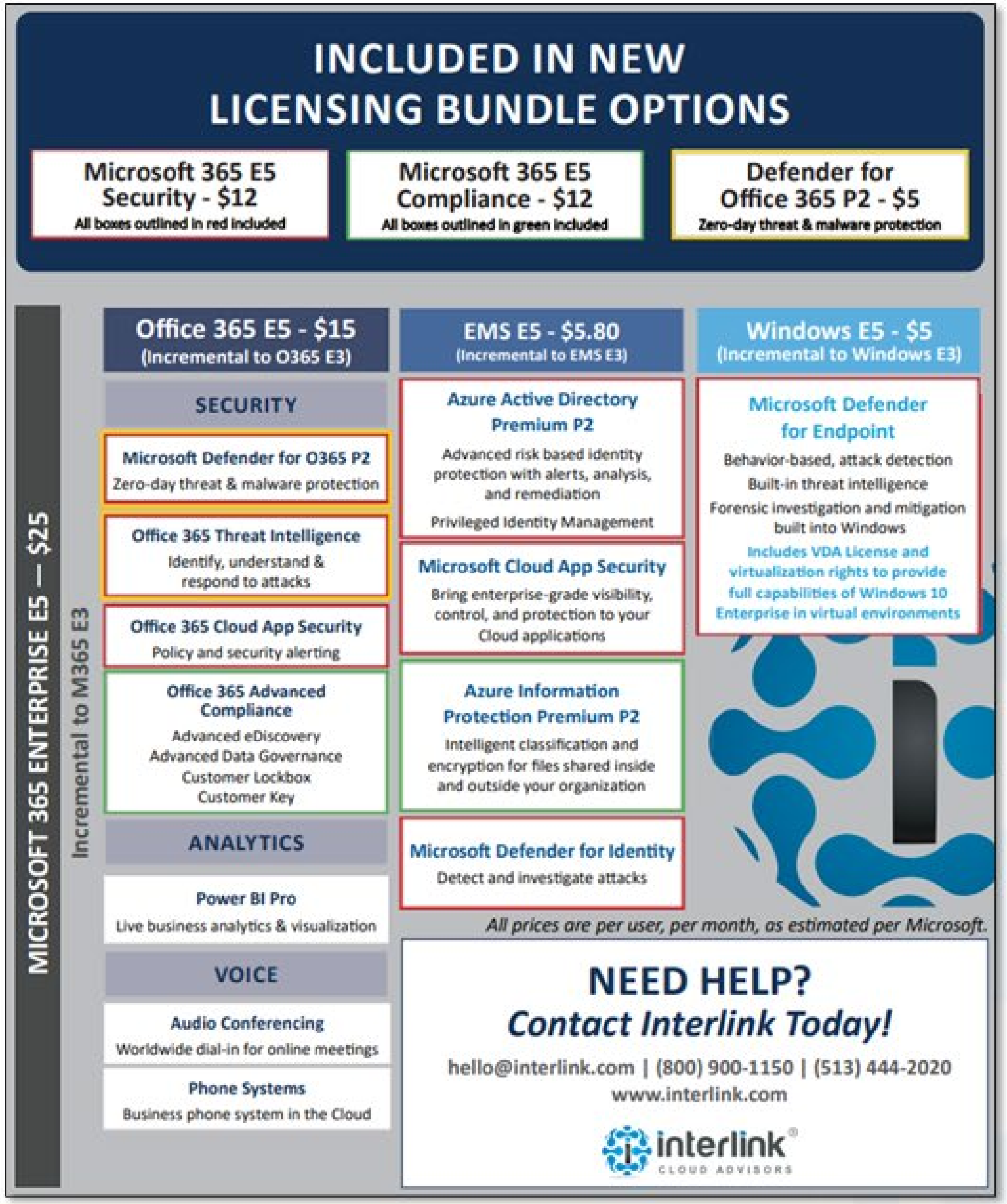
Per User Licensing
Install on up to 5 devices

Direct Access
Always on VPN connection to on-premise resources

Windows Information Protection
Containerize corporate data on PCs with end to end data security to and from Office 365
AppsLocker - Device locked down to only run fully trusted apps

Cyber Insurance

Microsoft 365 E5 Licensing:



INCLUDED IN NEW LICENSING BUNDLE OPTIONS

Microsoft 365 E5 Security - $12
All boxes outlined in red included

Microsoft 365 E5 Compliance - $12
All boxes outlined in green included

Defender for Office 365 P2 - $5
Zero-day threat & malware protection

MICROSOFT 365 ENTERPRISE E5 — $25

Incremental to M365 E3

Office 365 E5 - $15
(Incremental to O365 E3)

SECURITY

Microsoft Defender for O365 P2
Zero-day threat & malware protection

Office 365 Threat Intelligence
Identify, understand & respond to attacks

Office 365 Cloud App Security
Policy and security alerting

Office 365 Advanced Compliance
Advanced eDiscovery
Advanced Data Governance
Customer Lockbox
Customer Key

ANALYTICS

Power BI Pro
Live business analytics & visualization

VOICE

Audio Conferencing
Worldwide dial-in for online meetings

Phone Systems
Business phone system in the Cloud

EMS E5 - $5.80
(Incremental to EMS E3)

Azure Active Directory Premium P2
Advanced risk based identity protection with alerts, analysis, and remediation
Privileged Identity Management

Microsoft Cloud App Security
Bring enterprise-grade visibility, control, and protection to your Cloud applications

Azure Information Protection Premium P2
Intelligent classification and encryption for files shared inside and outside your organization

Microsoft Defender for Identity
Detect and investigate attacks

Windows E5 - $5
(Incremental to Windows E3)

Microsoft Defender for Endpoint
Behavior-based, attack detection
Built-in threat intelligence
Forensic investigation and mitigation built into Windows
Includes VDA License and virtualization rights to provide full capabilities of Windows 10 Enterprise in virtual environments

All prices are per user, per month, as estimated per Microsoft.

NEED HELP?
Contact Interlink Today!
hello@interlink.com | (800) 900-1150 | (513) 444-2020
www.interlink.com

interlink®
CLOUD ADVISORS

Interlink
Cloud
Advisors

Security Energize

THE FOUR MODULES FOR THIS ENGAGEMENT:

Threat Check:

Microsoft 365 security products are used to gain visibility into threats to your Microsoft 365 cloud environment across email, identity, and data in order to better understand, prioritize, and mitigate potential vectors of cyberattacks.

Discovery Session:

This is a standalone module designed for the delivery team to learn about a customer's organization, IT initiatives, security influencer's, and priority/maturity against an array of security capabilities that Microsoft can bring to bear.

Azure Sentinel:

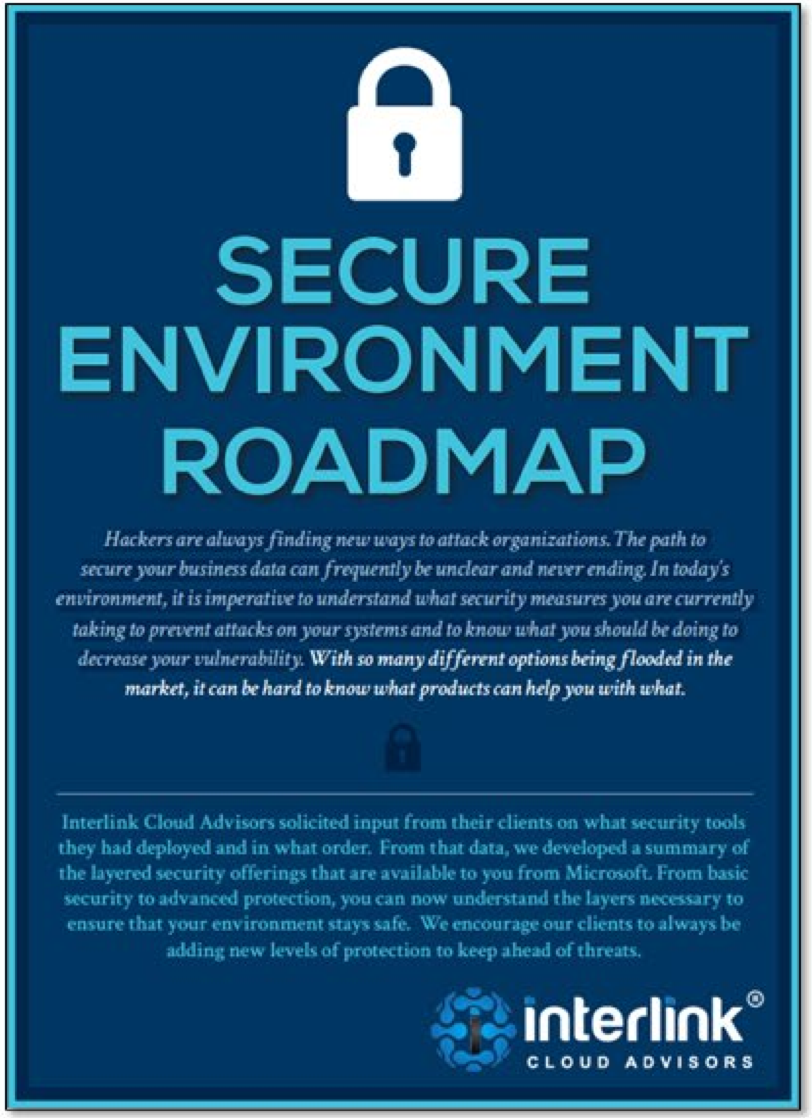
Leverages Azure Sentinel & Microsoft 365 security products to help gain an understanding of Azure Sentinel & gain insights on active threats across on-premises & cloud workloads.

Microsoft Threat Protection:

This is a demonstration of how the security solutions work, including going through key scenarios of an attack kill chain to help you learn how to protect your environment.

Interlink
Cloud
Advisors

Secure Environment Roadmap

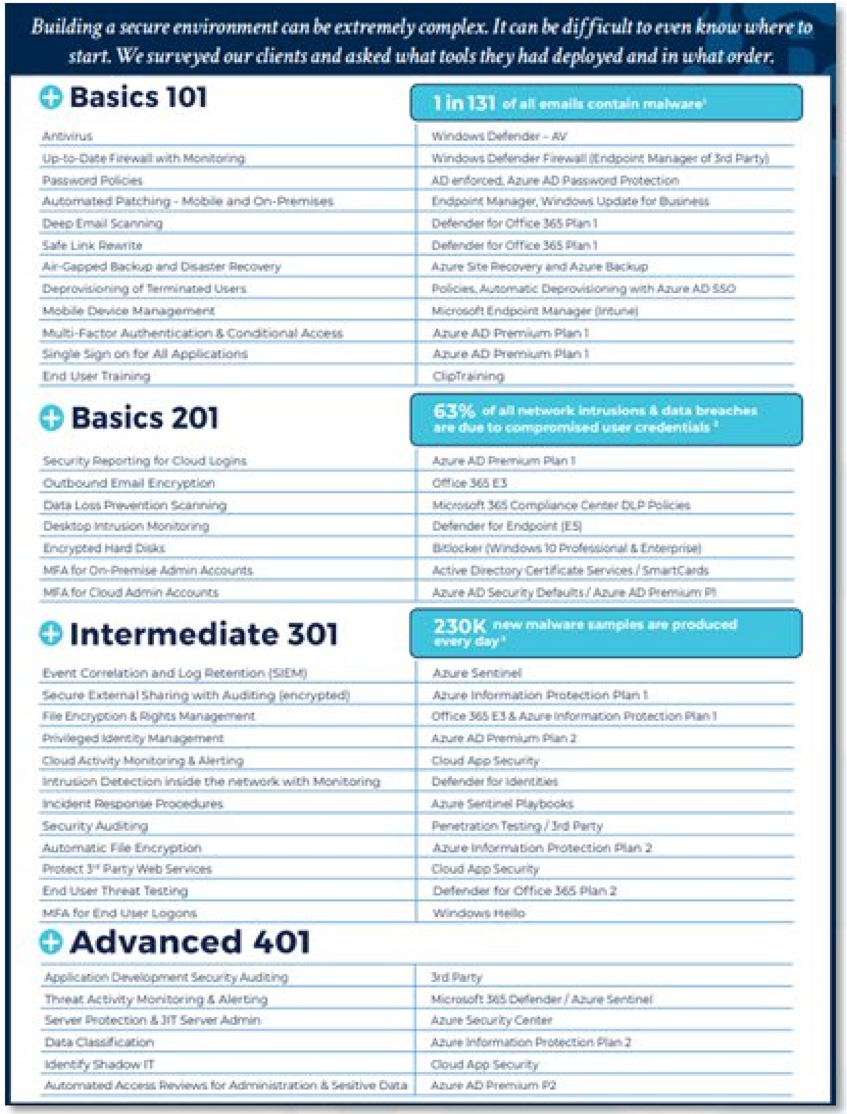


SECURE ENVIRONMENT ROADMAP

Hackers are always finding new ways to attack organizations. The path to secure your business data can frequently be unclear and never ending. In today's environment, it is imperative to understand what security measures you are currently taking to prevent attacks on your systems and to know what you should be doing to decrease your vulnerability. ***With so many different options being flooded in the market, it can be hard to know what products can help you with what.***

Interlink Cloud Advisors solicited input from their clients on what security tools they had deployed and in what order. From that data, we developed a summary of the layered security offerings that are available to you from Microsoft. From basic security to advanced protection, you can now understand the layers necessary to ensure that your environment stays safe. We encourage our clients to always be adding new levels of protection to keep ahead of threats.

interlink®
CLOUD ADVISORS



Building a secure environment can be extremely complex. It can be difficult to even know where to start. We surveyed our clients and asked what tools they had deployed and in what order.

Basics 101

1 in 131 of all emails contain malware[1]

Antivirus	Windows Defender – AV
Up-to-Date Firewall with Monitoring	Windows Defender Firewall (Endpoint Manager of 3rd Party)
Password Policies	AD enforced, Azure AD Password Protection
Automated Patching - Mobile and On-Premises	Endpoint Manager, Windows Update for Business
Deep Email Scanning	Defender for Office 365 Plan 1
Safe Link Rewrite	Defender for Office 365 Plan 1
Air-Gapped Backup and Disaster Recovery	Azure Site Recovery and Azure Backup
Deprovisioning of Terminated Users	Policies, Automatic Deprovisioning with Azure AD SSO
Mobile Device Management	Microsoft Endpoint Manager (Intune)
Multi-Factor Authentication & Conditional Access	Azure AD Premium Plan 1
Single Sign on for All Applications	Azure AD Premium Plan 1
End User Training	ClipTraining

Basics 201

63% of all network intrusions & data breaches are due to compromised user credentials[2]

Security Reporting for Cloud Logins	Azure AD Premium Plan 1
Outbound Email Encryption	Office 365 E3
Data Loss Prevention Scanning	Microsoft 365 Compliance Center DLP Policies
Desktop Intrusion Monitoring	Defender for Endpoint (E5)
Encrypted Hard Disks	Bitlocker (Windows 10 Professional & Enterprise)
MFA for On-Premise Admin Accounts	Active Directory Certificate Services / SmartCards
MFA for Cloud Admin Accounts	Azure AD Security Defaults / Azure AD Premium P1

Intermediate 301

230K new malware samples are produced every day[3]

Event Correlation and Log Retention (SIEM)	Azure Sentinel
Secure External Sharing with Auditing (encrypted)	Azure Information Protection Plan 1
File Encryption & Rights Management	Office 365 E3 & Azure Information Protection Plan 1
Privileged Identity Management	Azure AD Premium Plan 2
Cloud Activity Monitoring & Alerting	Cloud App Security
Intrusion Detection inside the network with Monitoring	Defender for Identities
Incident Response Procedures	Azure Sentinel Playbooks
Security Auditing	Penetration Testing / 3rd Party
Automatic File Encryption	Azure Information Protection Plan 2
Protect 3rd Party Web Services	Cloud App Security
End User Threat Testing	Defender for Office 365 Plan 2
MFA for End User Logons	Windows Hello

Advanced 401

Application Development Security Auditing	3rd Party
Threat Activity Monitoring & Alerting	Microsoft 365 Defender / Azure Sentinel
Server Protection & JIT Server Admin	Azure Security Center
Data Classification	Azure Information Protection Plan 2
Identify Shadow IT	Cloud App Security
Automated Access Reviews for Administration & Sesitive Data	Azure AD Premium P2

Workshops & Assessments

Ask us about Funding!

- Viva and Viva Insights Workshop
- Teams Meetings Workshop Energize
- Teams Apps & Solutions Workshop Energize
- Teams Calling Workshop Energize
- Security Workshop Energize
- Identity Workshop Energize
- And Much More!

Contact Us Today
hello@interlink.com
+1 (513) – 444 – 2020

VIVA AND VIVA INSIGHTS WORKSHOP

interlink CLOUD ADVISORS

Discover how this integrated platform can help digitally reimaging the employee experience to help your people be their best and thrive in the new reality.

In today's world, employees want more flexible remote work options, and meaningful in-person collaboration. Empowering people to thrive in a more flexible work world requires rethinking everything—from how you empower managers, to how you create culture, to how you reimagine the employee experience.

And that's where Microsoft Viva comes in. As your employees are challenged with a growing imbalance between work and life, increased burnout, and decreased wellbeing, and your teams and organization face diminishing social capital, there is an urgent need to digitally reimagine the employee experience.

Discover how Microsoft Viva, an integrated platform built on top of Microsoft Teams, will help your people to be their best, to thrive in the new reality.

TWO WORKSHOPS TO COVER YOUR UNIQUE NEEDS:

Employee Experience with Microsoft Viva:
A three-phase engagement that provides an overview of the Art of the Possible, and deep dives across the Viva suite with Topics, Connections, or Learning.

Employee Experience with Microsoft Viva Insights:
A three-phase engagement that provides an overview of the Art of the Possible, and a deep dive into Viva Insights.

WHAT YOU CAN EXPECT FROM INTERLINK:

- A prioritized list of business scenarios that can be addressed by deploying Microsoft Viva
- Recommended preparation in terms of skills and best practices
- A roadmap outlining potential workstreams and dependencies with clear next steps
- An adoption framework

Contact Interlink Cloud Advisors today to learn more about this engagement and discuss your specific environment!

WORKSHOP FRAMEWORK

Assess
- Gather information on key business scenarios
- Define scope
- Identify business stakeholders
- Introduce Microsoft Viva

Art of the Possible
- Showcase employee experience transformation
- Microsoft Viva overview with selected pathways
- Demos and immersive experiences

Build the Plan
- Build upon your newfound knowledge and pair it with your unique business challenges
- Prioritization of scenarios and next steps built into a plan

ASK US HOW TO GET THIS ENGAGEMENT FUNDED BY MICROSOFT!

Microsoft Partner

interlink CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-890-1730

energize

TEAMS CALLING WORKSHOP

Showcase modern calling capabilities and build a plan to deploy and adopt Microsoft Teams Calling

MICROSOFT TEAMS CALLING WITH PHONE SYSTEM

Now more than ever, businesses need a modern voice solution and phone system capabilities that combine unified communication and teamwork. Calling in Teams provides the features organizations need to deliver seamless, collaborative experiences for employees, business partners and customers. Because the implementation of calling solutions can be complex and involve network remediation, O365 service deployment, telephone number provisioning/porting and device deployment, customers need a partner like Interlink with this highly specialized skillset.

TEAMS CALLING WORKSHOP

Introducing the Teams Calling Workshop – a modular engagement to experience the vision for Microsoft Teams with Phone System capabilities and Advanced Communication scenarios. With extensive solution experience, Interlink will show you the power of Teams Calling for your specific environment. We will discuss the major configuration options, third-party add-ons, hardware options, and licensing scenarios and configurations.

See who is calling you from Microsoft Teams on your mobile device

www.interlink.com/teams-calling-workshop

ASK US HOW TO GET THIS ENGAGEMENT FUNDED BY MICROSOFT!

Microsoft Partner

interlink CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-890-1730

energize

interlink CLOUD ADVISORS

SECURITY WORKSHOP

An immersive experience that brings the Microsoft security vision and capabilities to life.

Are you looking to assess your security landscape and address demanding security goals and challenges?

Interlink's Security Workshop was designed to help you and your organization understand how Microsoft's security capabilities can harden your security posture while providing insight on active threats across on-premises and cloud workloads.

WORKSHOP OBJECTIVES

▶ Discover Threats
Gain visibility into threats to your Microsoft 365 cloud environment across email, identity, and data to better understand, prioritize, and mitigate potential vectors of cyberattacks against your organization.

▶ Understand How to Mitigate Threats
Understand how Microsoft 365 security products can help mitigate and protect against the threats found during the period of this engagement.

▶ Define Security Strategy
Receive an overview security strategy for your security teams and stakeholders.

▶ Accelerate the Security Journey
Get started with trial deployments of Microsoft's Threat Protection and SIEM technologies, which can be transitioned to production.

▶ Define Next Steps
Work together with an Interlink Security Consultant to define a list of next steps based on your needs, objectives, and results from the Security Workshop.

Security is a process of continuous improvement. If you are staying in place, that means you're falling behind. Learn how your organization can accelerate its security journey together with Microsoft.

ASK US HOW TO GET THIS ENGAGEMENT FUNDED BY MICROSOFT!

Microsoft Partner

interlink CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-890-1730

energize

TEAMS MEETINGS AND MEETING ROOMS WORKSHOP

Showcase modern meetings experiences and build a plan to deploy and adopt Microsoft Teams Meetings and Meeting Rooms

DO MORE WITH MICROSOFT TEAMS

Today, organizations rely on teamwork with employees working on twice as many teams as they did just five years ago, and information workers spend 50% more time collaborating with co-workers, outside contractors, suppliers and customers. To succeed, you need collaboration and communication tools that empower your workforce to be more agile, efficient, and secure so they can stay connected.

The way we work has evolved and meeting needs have changed with employees being more mobile and working remotely. In fact, 56% of meetings have at least one remote attendee and 38% of remote attendees join via mobile. Microsoft Teams delivers a unique end-to-end meeting experience that brings back the human element of face-to-face interaction while helping people stay focused before, during and after the meeting.

56%
of meetings have at least one remote attendee

38%
of remote attendees join via mobile

TEAMS MEETINGS AND MEETING ROOMS WORKSHOP

Introducing the Meetings and Meeting Rooms Workshop – a modular engagement to identify and understand business priorities while focusing on specific scenarios that drive meetings culture transformation. With extensive solution experience, Interlink will show you the power of Teams Meetings for your specific environment including, new conferencing functionality, meeting rooms technology, audio conferencing options, and the new Teams Live Events.

www.interlink.com/teams-meetings-workshop

ASK US HOW TO GET THIS ENGAGEMENT FUNDED BY MICROSOFT!

Microsoft Partner

interlink CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-890-1730

energize

interlink CLOUD ADVISORS

IDENTITY SECURITY WORKSHOP

Find Identity Risks, Gain Insight into Your Application Landscape & Improve Your Identity Security Posture

ARE YOU CONCERNED ABOUT SUSPICIOUS USERS AND SIGN-IN BEHAVIOR IN YOUR ENVIRONMENT?

If not, you should be. Microsoft uses machine learning to provide risk scores for 800 million accounts and finds that 300 million login attempts daily come from criminal actors and hackers. They detected 4.6 billion attacks in May of 2018 alone!

Identity is today's gateway to your network and properly controlling it is the key to system security. The growing implementation of Cloud applications, the increased use of personal devices connecting to your network, and the rise of the remote workforce mean that you are no longer able to protect your data behind a four-wall security fortress. The challenge now is securing user identities to ensure you are limiting access to authorized users.

Interlink Energize Identity Security Workshop

Interlink can help with a comprehensive workshop that will show you how to uncover identity risks in your environment, gain insights into your applications, and enhance your identity security posture.

ATTENDING THIS WORKSHOP WILL PROVIDE YOU WITH:

- ✓ A rating of your identity security posture and how it compares to your peers
- ✓ Insights into applications used in your environment including those not sanctioned by your IT department
- ✓ Methods to secure user identities on all devices
- ✓ A deeper understanding of ways to prevent identities from being compromised
- ✓ Ways to reduce costs and improve business agility and security with simplified apps access

ASK US HOW TO GET THIS ENGAGEMENT FUNDED BY MICROSOFT!

Microsoft Partner

interlink CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-890-1730

energize

MICROSOFT TEAMS APPS AND SOLUTIONS WORKSHOP

Get ready to achieve more with Microsoft Teams

SEE WHAT'S POSSIBLE WITH TEAMS

As the hub for teamwork, Microsoft Teams is designed to help companies improve collaboration, boost efficiency, and stay in the flow of work.

Interlink's Teams Apps and Solutions Workshop will provide your business a means to help increase workforce productivity by leveraging the Teams platform for your critical business processes. With extensive solution development experience, our team will work with your organization to understand your environment and identify key business scenarios that could be enhanced by utilizing applications from the 700+ apps available for Teams, along with custom low-code solutions built using Power Automate, Power Apps, Bots, and more.

In this workshop, our Microsoft certified consultants will walk you through the art of the possible, working with you to identify and prioritize key business scenarios to help solve your specific collaboration challenges. During the engagement, we'll also show you how to customize and extend your Teams workspace using the power of automation. Then, we'll design a plan that leverages Teams' platform capabilities to help you move forward.

With industry and technology experience, you can count on Interlink as your trusted partner in your transformation journey.

WORKSHOP DELIVERABLES:

- ✓ Showcase how employees can be more productive in Teams when connected with other data sources
- ✓ Identify and prioritize key use-case scenarios — review of solutions templates available
- ✓ App activation and enablement with governance suggestions
- ✓ Next steps with an adoption kit and success plan

LEARN MORE AT WWW.INTERLINK.COM/TEAMS-APPS-SOLUTIONS-WORKSHOP

Drive Business Results
Through scenarios for increased productivity

Accelerate Outcomes
With ready-to-use apps, plug and play accelerators, and solution options

Enable App Governance
Through guidance on governing Teams apps using policies and controls

ASK US HOW TO GET THIS ENGAGEMENT FUNDED BY MICROSOFT!

Microsoft Partner

interlink CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-890-1730

interlink®
CLOUD ADVISORS

Questions?

Q&A