BDO

Microsoft

Demystify
WEBCAST SERIES

Demystify
Microsoft E5 Security

FEBRUARY 19, 2025

BDO DIGITAL

With You Today

STEVE COMBS
Cyber Managing Director,
BDO Digital

713-576-3417
scombs@bdo.com

Learning Objectives

1 **Understand the core components**

- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint and Server
- Microsoft Entra ID
  (formerly Azure Active Directory)
- Microsoft Sentinel

2 **Understand the suite's features, benefits, and integration capabilities**

3 **Gain visibility into threat prevention and mitigation strategies**

4 **Develop a prioritized roadmap for deploying Microsoft security solutions**

5 **Collaborate with IT and business leaders to align on security initiatives**

Demystify
WEBCAST SERIES

Security Posture

Today’s Challenges

Top Human-Operated Ransomware Concerns

Companies that have policy to pay Ransom related to breach	47%	Policy and tools are implemented in many cases to pay bitcoin to offshore attackers
Ransomware attacks have been rapidly increased	73%	Global companies surveyed by Statista(2).
Recovering from a ransomware attack is costly	$1.85M	Recovering from a ransomware attack cost businesses $1.85 million on average in 2021(3).

1. CFO.com from late 2023
2. Statista 2023
3. Ransomware Statistics, Trends and Facts for 2023 and Beyond

The Increasingly Complex State of Cybersecurity

The cybercrime economy continues to democratize tooling and services

Attacks like ransomware are increasingly targeted

Attack surface is expanding, and attackers are adapting quickly

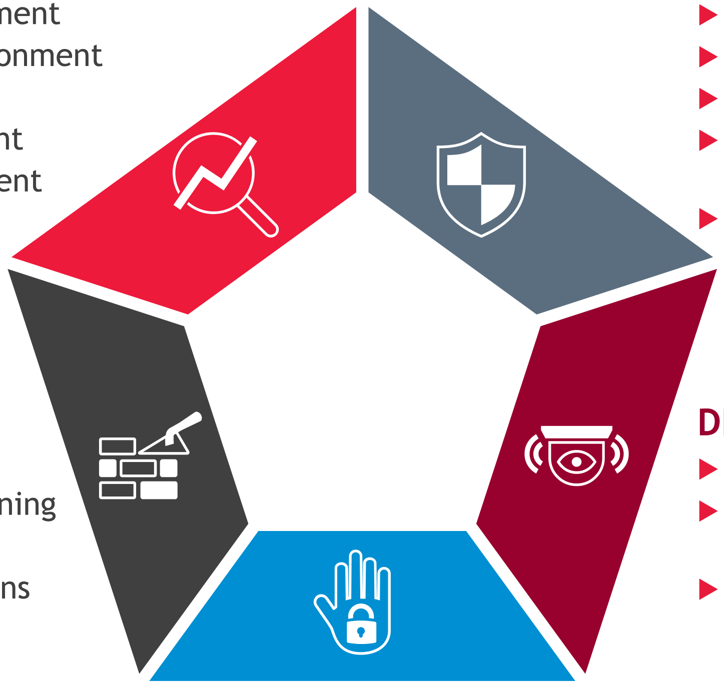
Complex security tooling is costly, inefficient, and lacks integration

Cyber Core Components

Each segment to the right has one or more of the following components

- Policy/Standard
- Procedure
- Technical controls
- Tools
- Business Process
- People

CYBERSECURITY FRAMEWORK OVERVIEW



IDENTIFY

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Awareness Control
- Awareness And Training
- Data Security
- Info Protection And Procedures Maintenance
- Protective Technology

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvement

RECOVER

- Recovery Planning
- Improvements
- Communications

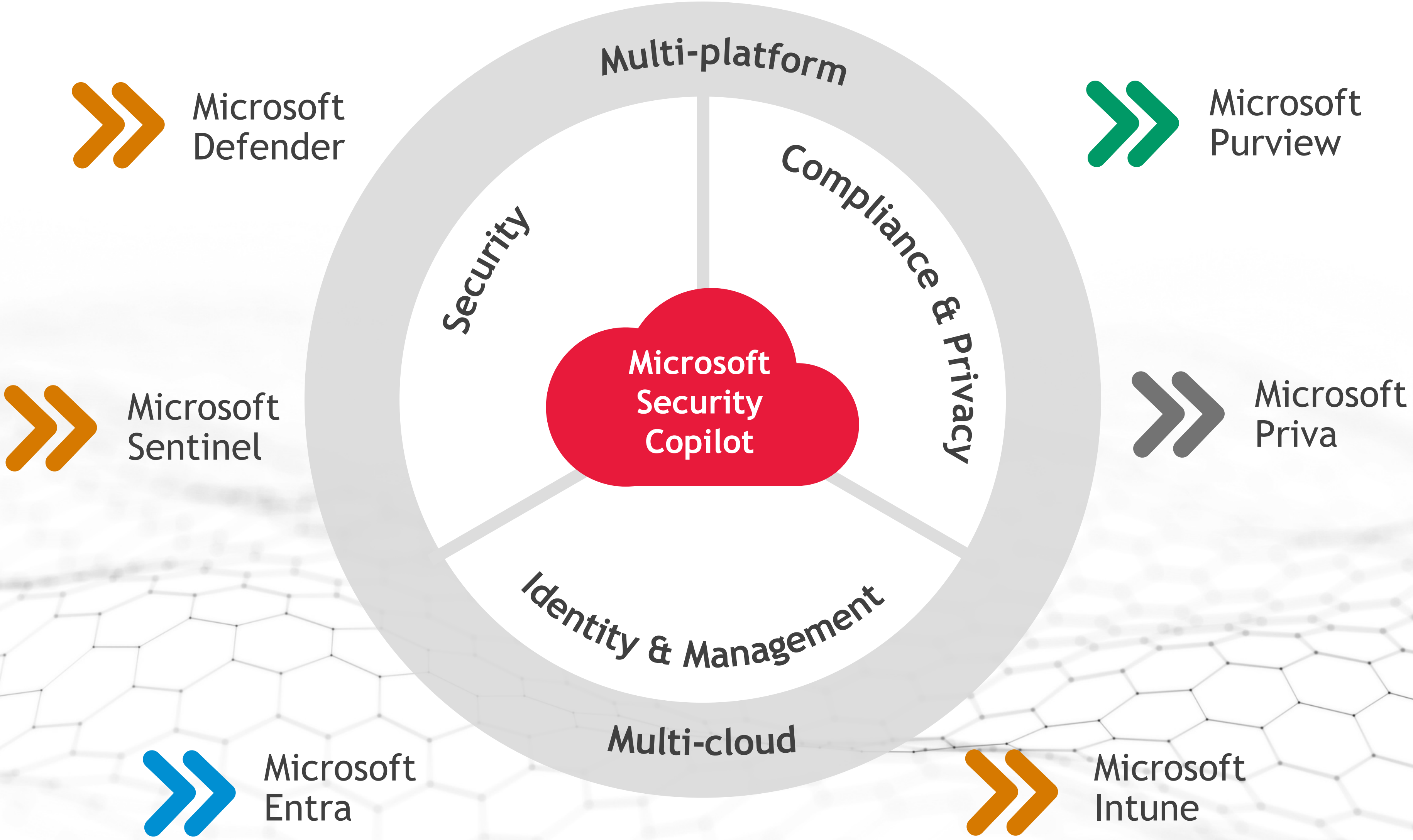
Demystify
WEBCAST SERIES

Overview

Security Approach

Security Portfolio

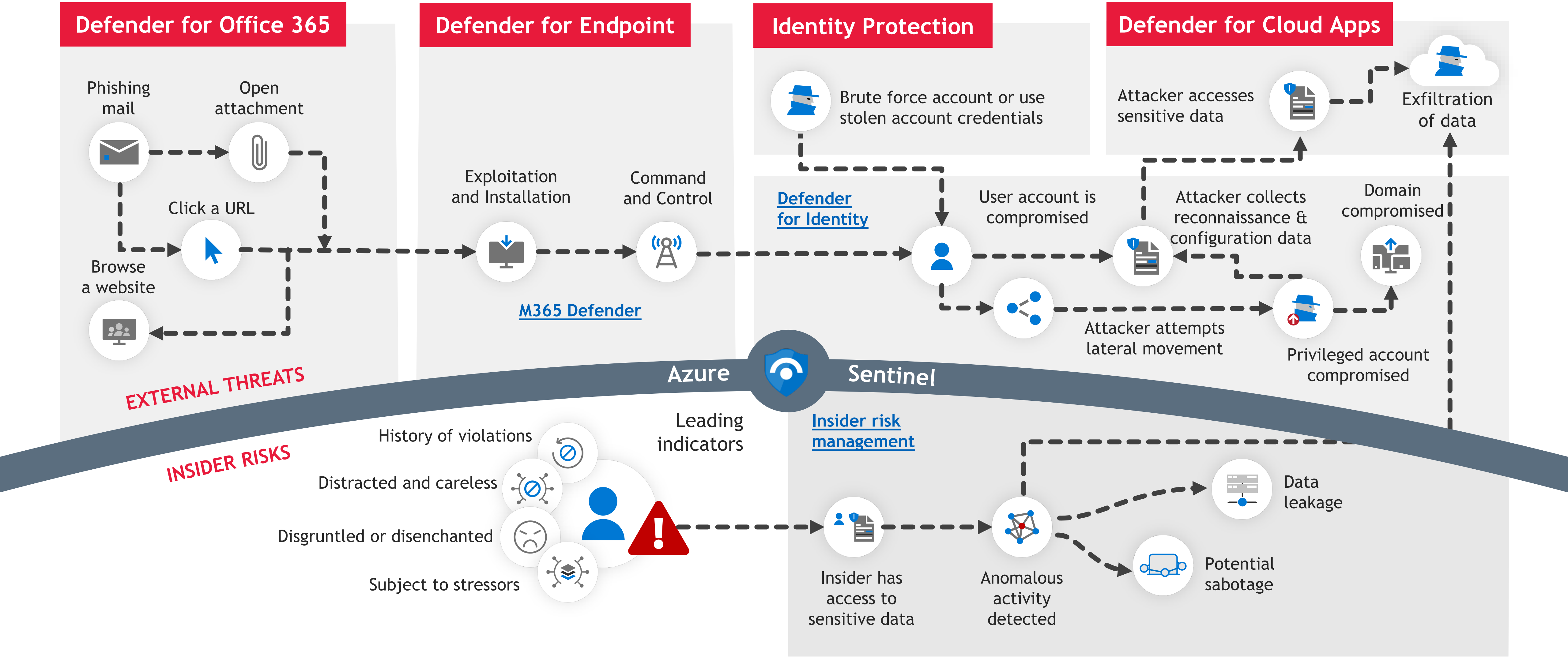
Six product families integrating over 50 product categories



MDR SOLUTIONS

THREAT PROTECTION

Protection Across the Attack Chain: Insider and External Threats



Demystify
WEBCAST SERIES

Email Protection

BDO

Why Microsoft Defender for Office 365 Stands Out

With **a holistic approach** that seamlessly blends advanced protection, rapid response, seamless extended detection and response (XDR) integration, and user-empowerment, Microsoft Defender for Office 365 provides a **uniquely unified defense strategy** against cyberthreats

Automatic attack disruption

Proactive security with powerful features like advanced threat hunting and Zero-Auto-Purge (ZAP) that neutralizes threats before sensitive data is compromised

Streamlined automated response

Automated workflows, processes, and tooling enables SecOps teams to respond quickly and effectively to identified attacks, drastically reducing remediation time

Unified security coverage with XDR

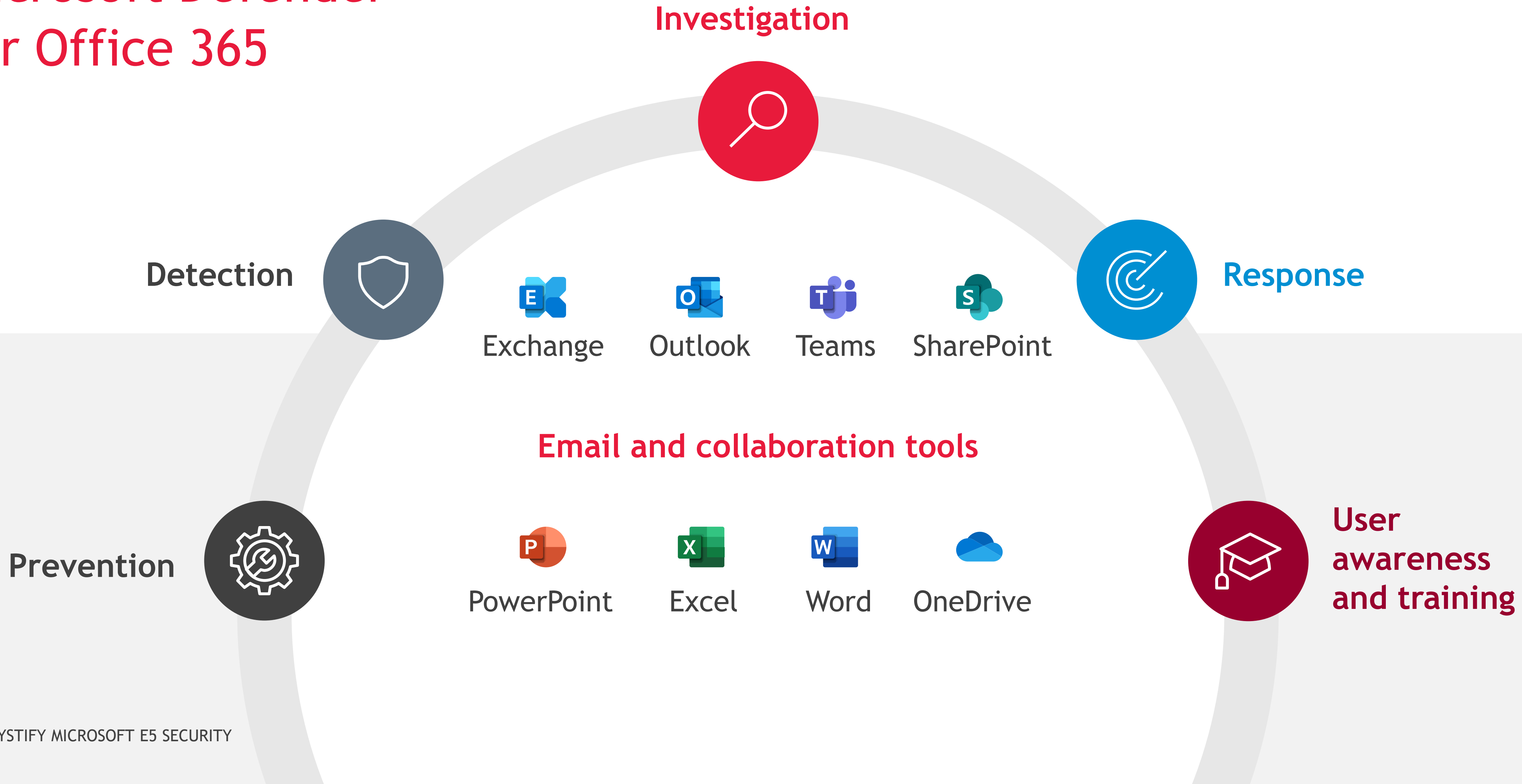
By integrating seamlessly with the broader Microsoft XDR portfolio, eliminate the security gaps created from using a patchwork of different products, with comprehensive protection across platforms beyond email

Empower end-user resilience

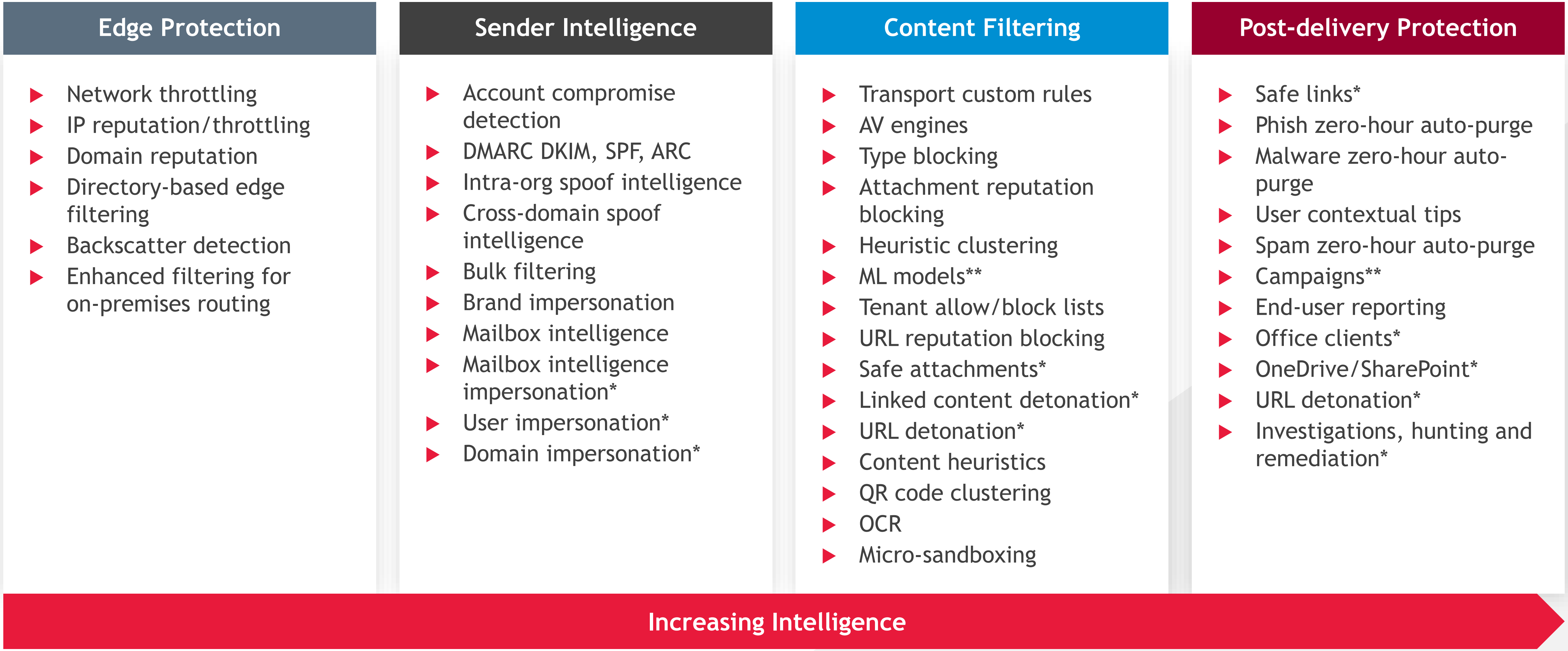
With awareness features like Attack Simulation Training, organizations can equip users with the knowledge to identify and report threats, transforming them into robust security assets

SECURE COMMUNICATION ACROSS PLATFORMS WITH:

Microsoft Defender for Office 365



Multi-Layered Protection Stack



Edge Protection

- Network throttling
- IP reputation/throttling
- Domain reputation
- Directory-based edge filtering
- Backscatter detection
- Enhanced filtering for on-premises routing

Sender Intelligence

- Account compromise detection
- DMARC DKIM, SPF, ARC
- Intra-org spoof intelligence
- Cross-domain spoof intelligence
- Bulk filtering
- Brand impersonation
- Mailbox intelligence
- Mailbox intelligence impersonation*
- User impersonation*
- Domain impersonation*

Content Filtering

- Transport custom rules
- AV engines
- Type blocking
- Attachment reputation blocking
- Heuristic clustering
- ML models**
- Tenant allow/block lists
- URL reputation blocking
- Safe attachments*
- Linked content detonation*
- URL detonation*
- Content heuristics
- QR code clustering
- OCR
- Micro-sandboxing

Post-delivery Protection

- Safe links*
- Phish zero-hour auto-purge
- Malware zero-hour auto-purge
- User contextual tips
- Spam zero-hour auto-purge
- Campaigns**
- End-user reporting
- Office clients*
- OneDrive/SharePoint*
- URL detonation*
- Investigations, hunting and remediation*

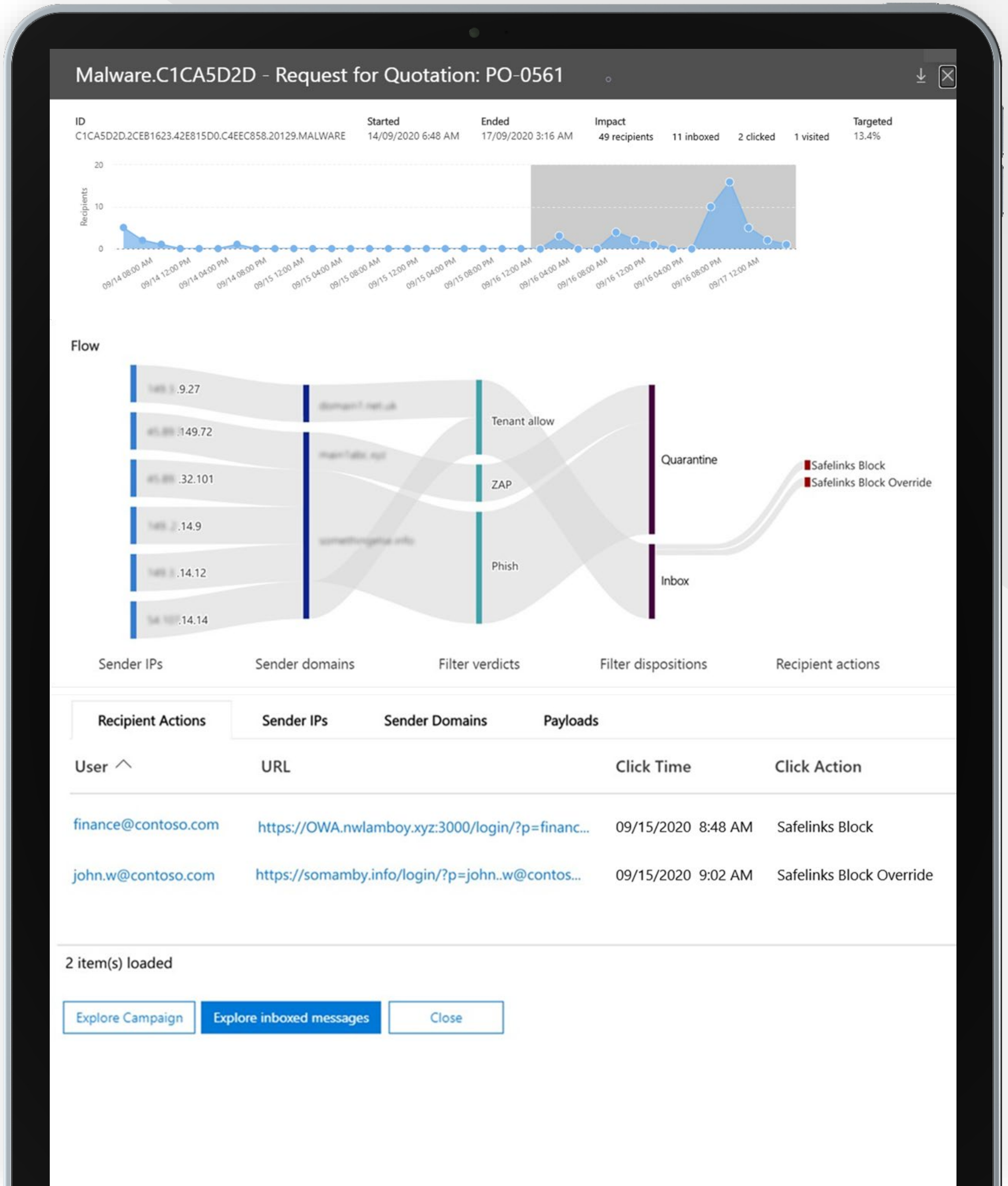
Increasing Intelligence

*Components unique to Microsoft Defender for Office 365

** Enhanced/additional items unique to Microsoft Defender for Office 365

Detection

- With our signal strength and our industry-leading AI to correlate data across Microsoft 365 and detect attacks as they happen in real-time
- Microsoft Defender for Office 365 uses vast data to detect email and collaboration anomalies in Microsoft 365 with advanced and adaptive algorithms
- These algorithms can identify evolving threat tactics with high accuracy, alert your security teams, and automatically restrict the activities of these accounts



Malware.C1CA5D2D - Request for Quotation: PO-0561

ID	Started	Ended	Impact				Targeted
C1CA5D2D.2CEB1623.42E815D0.C4EEC858.20129.MALWARE	14/09/2020 6:48 AM	17/09/2020 3:16 AM	49 recipients	11 inboxed	2 clicked	1 visited	13.4%

User	URL	Click Time	Click Action
finance@contoso.com	https://OWA.nwlamboy.xyz:3000/login/?p=financ...	09/15/2020 8:48 AM	Safelinks Block
john.w@contoso.com	https://somamby.info/login/?p=john..w@contos...	09/15/2020 9:02 AM	Safelinks Block Override

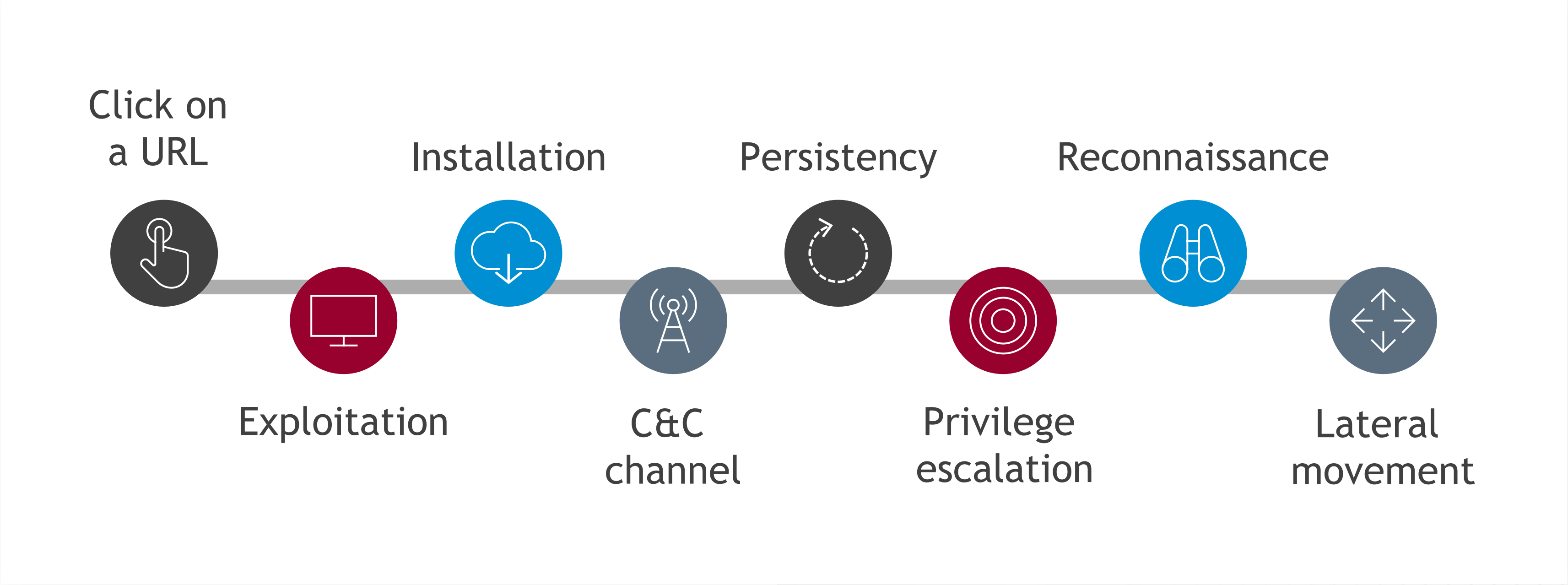
2 item(s) loaded

Endpoint Protection

Entra ID and Defender

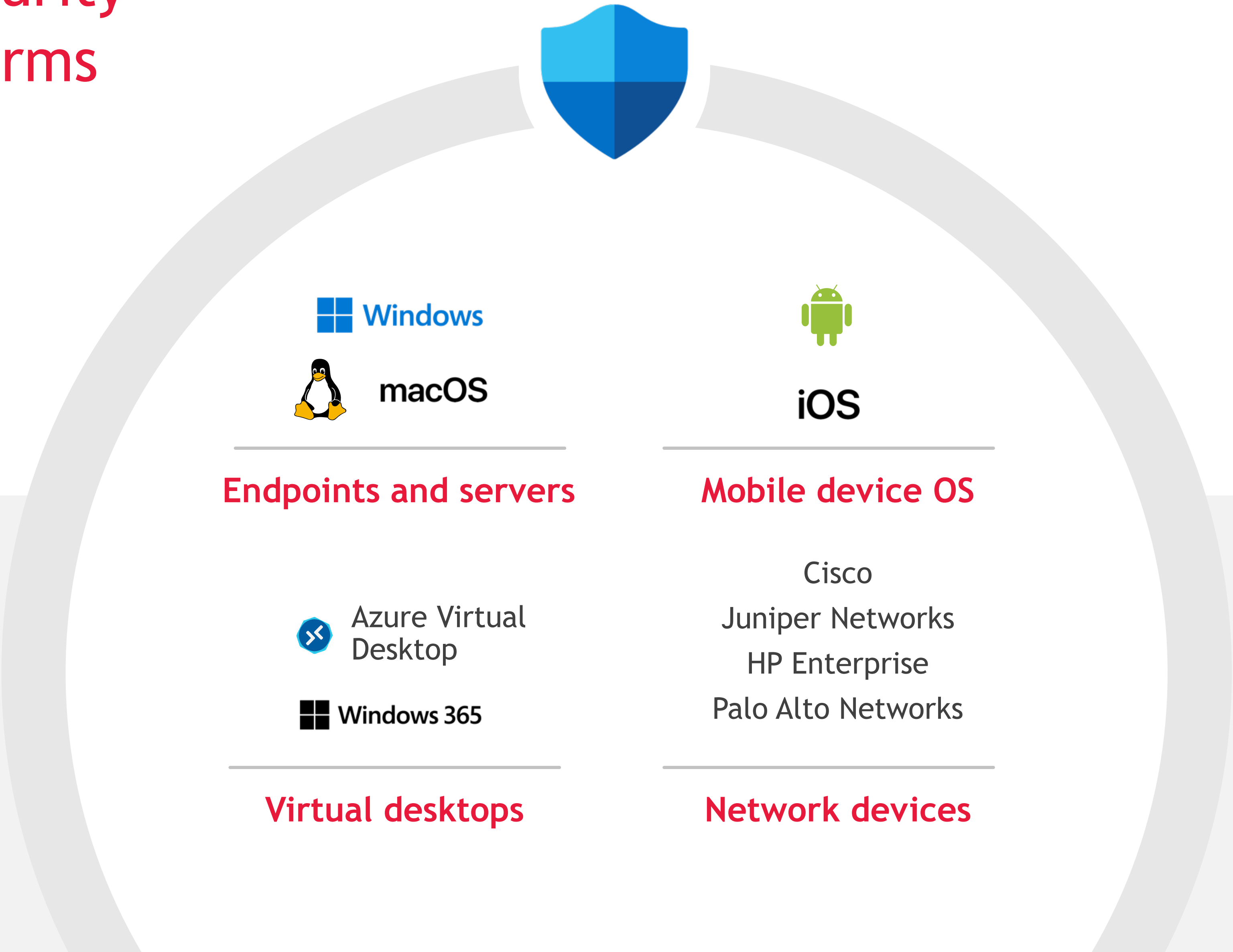
Key Customer Pain Points

As attacks become more complex and multi-staged, it's difficult to make sense of the threats detected.



- 46% of compromised systems had no malware on them
- Following an advanced attack across the network and different sensors can be challenging
- Collecting evidence and alerts, even from one infected device, can be a long time-consuming process
- Living off the land - attackers use evasion-techniques

Delivering Endpoint Security Across Platforms



Windows

macOS

Endpoints and servers

iOS

Mobile device OS

Azure Virtual Desktop

Windows 365

Virtual desktops

Cisco

Juniper Networks

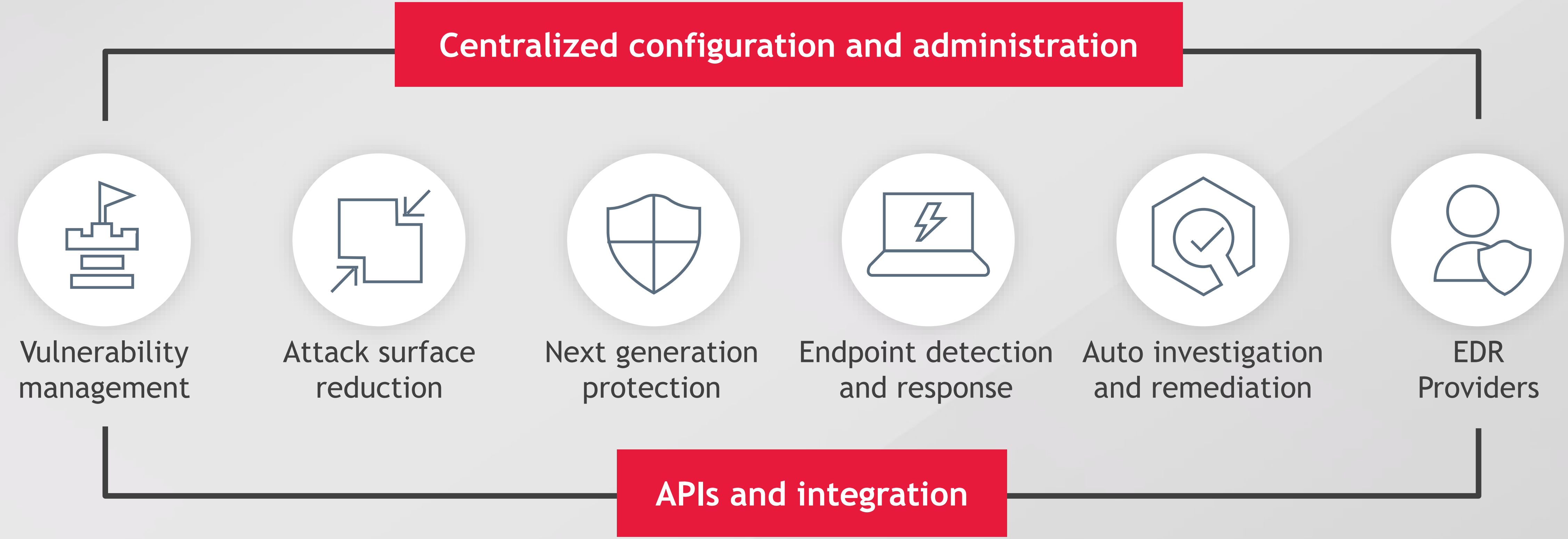
HP Enterprise

Palo Alto Networks

Network devices

Microsoft Defender for Endpoint

THREATS ARE NO MATCH



Centralized configuration and administration

Vulnerability management

Attack surface reduction

Next generation protection

Endpoint detection and response

Auto investigation and remediation

EDR Providers

APIs and integration

Attack Surface Reduction

RESIST ATTACKS AND EXPLOITATIONS

- HW-based isolation
- Application control
- Exploit protection
- Network protection
- Controlled folder access
- Device control
- Web protection
- Ransomware protection

- Isolate access to untrusted sites
- Isolate access to untrusted Office files
- Host intrusion prevention
- Exploit mitigation
- Ransomware protection for your files
- Block traffic to low reputation destinations
- Protect your legacy applications
- Only allow trusted applications to run

Microsoft Defender For Endpoint Next Generation Protection Engines

Metadata-based ML
Stops new threats quickly by analyzing metadata

Behavior-based ML
Identifies new threats with process trees and suspicious behavior sequences

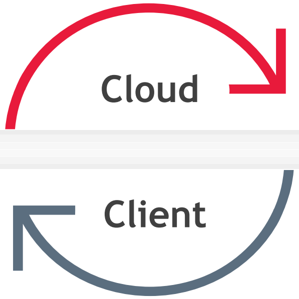
AMSI-paired ML
Detects fileless and in-memory attacks using paired client and cloud ML models

File classification ML
Detects new malware by running multi-class, deep neural network classifiers

Detonation-based ML
Catches new malware by detonating unknown files

Reputation ML
Catches threats with bad reputation, whether direct or by association

Smart rules
Blocks threats using expert-written rules



ML
Spots new and unknown threats using client-based ML models

Behavior monitoring
Identifies malicious behavior, including suspicious runtime sequence

Memory scanning
Detects malicious code running in memory

AMSI integration
Detects fileless and in-memory attacks

Heuristics
Catches malware variants or new strains with similar characteristics

Emulation
Evaluates files based on how they would behave when run

Network monitoring
Catches malicious network activities

Demystify

WEBCAST SERIES

Advanced Identity

Identities Are a Prime Target for Bad Actors

More than **4,000 password attacks per second** increasing the risk of compromised accounts.

Token replay attacks have doubled since 2023, with an average of **11 detections per 100,000** active users in Microsoft Entra ID Protection.

66% of attack paths involve insecure identity credentials.

Sources: Microsoft 2024 State of Multicloud security report

Identity and Network Access Solution Areas

Establish Zero Trust access controls

- Identity and Access Management (IAM)

Secure access for your employees

- Zero Trust Network Access
- Secure Web Gateway
- Identity Governance and Administration
- Identity Protection
- Identity Verification

Secure access for customers/partners

- Customer/ External IAM

Secure access in any cloud

- Cloud Infrastructure Entitlements Management
- Workload IAM

Accelerate with Generative AI capabilities and skills

Formula For Success: Unified Zero Trust User Access

Unify conditional access

For all resources across identity, endpoint, and network

Ensure least privilege access

To any app or resource, including AI

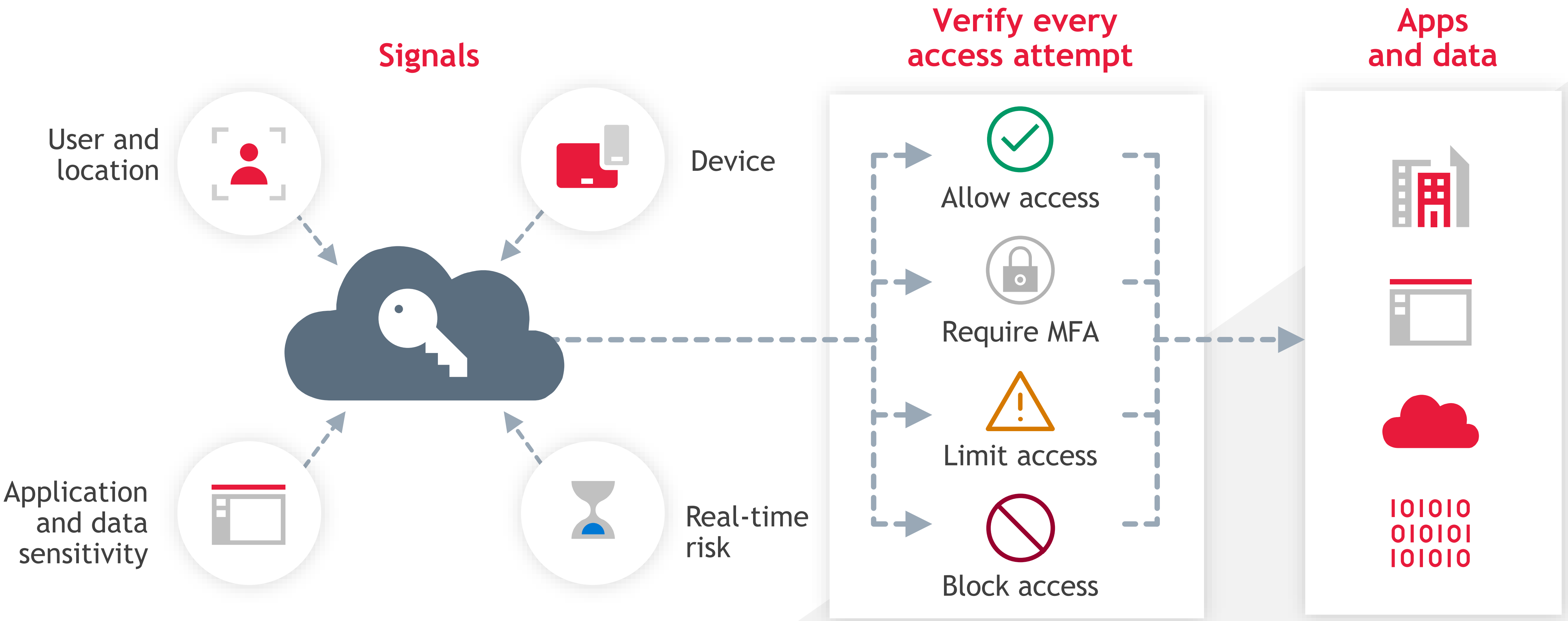
Improve the user experience

For remote, from home and in-office work

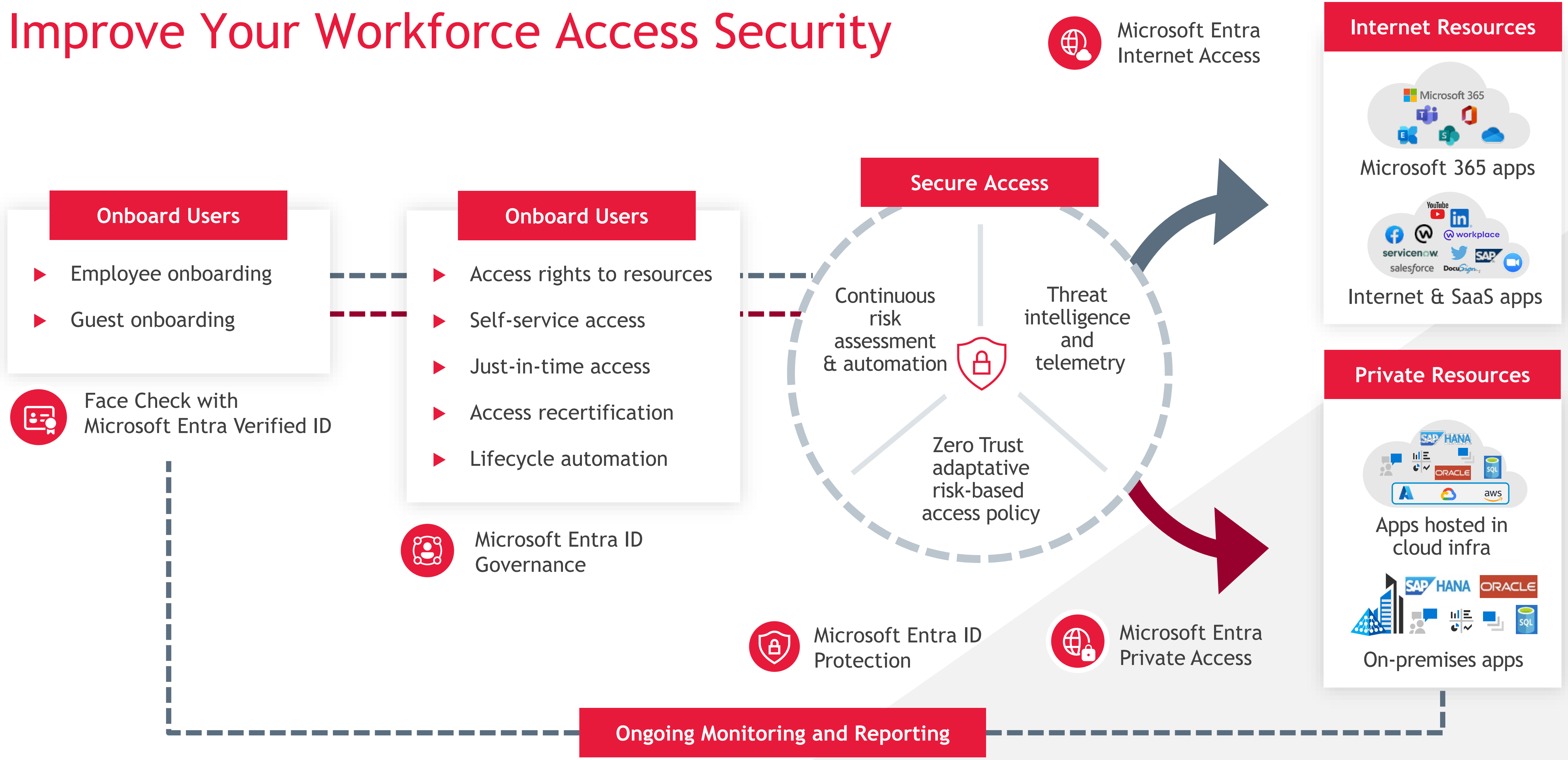
Reduce on-premises security solutions

Retire and minimize dependencies on legacy security solutions

Control Access with Smart Policies and Risk Assessments



Improve Your Workforce Access Security



Onboard Users

- Employee onboarding
- Guest onboarding

Face Check with Microsoft Entra Verified ID

Onboard Users

- Access rights to resources
- Self-service access
- Just-in-time access
- Access recertification
- Lifecycle automation

Microsoft Entra ID Governance

Secure Access

Continuous risk assessment & automation

Threat intelligence and telemetry

Zero Trust adaptative risk-based access policy

Microsoft Entra ID Protection

Microsoft Entra Internet Access

Microsoft Entra Private Access

Internet Resources

Microsoft 365 apps

Internet & SaaS apps

Private Resources

Apps hosted in cloud infra

On-premises apps

Ongoing Monitoring and Reporting

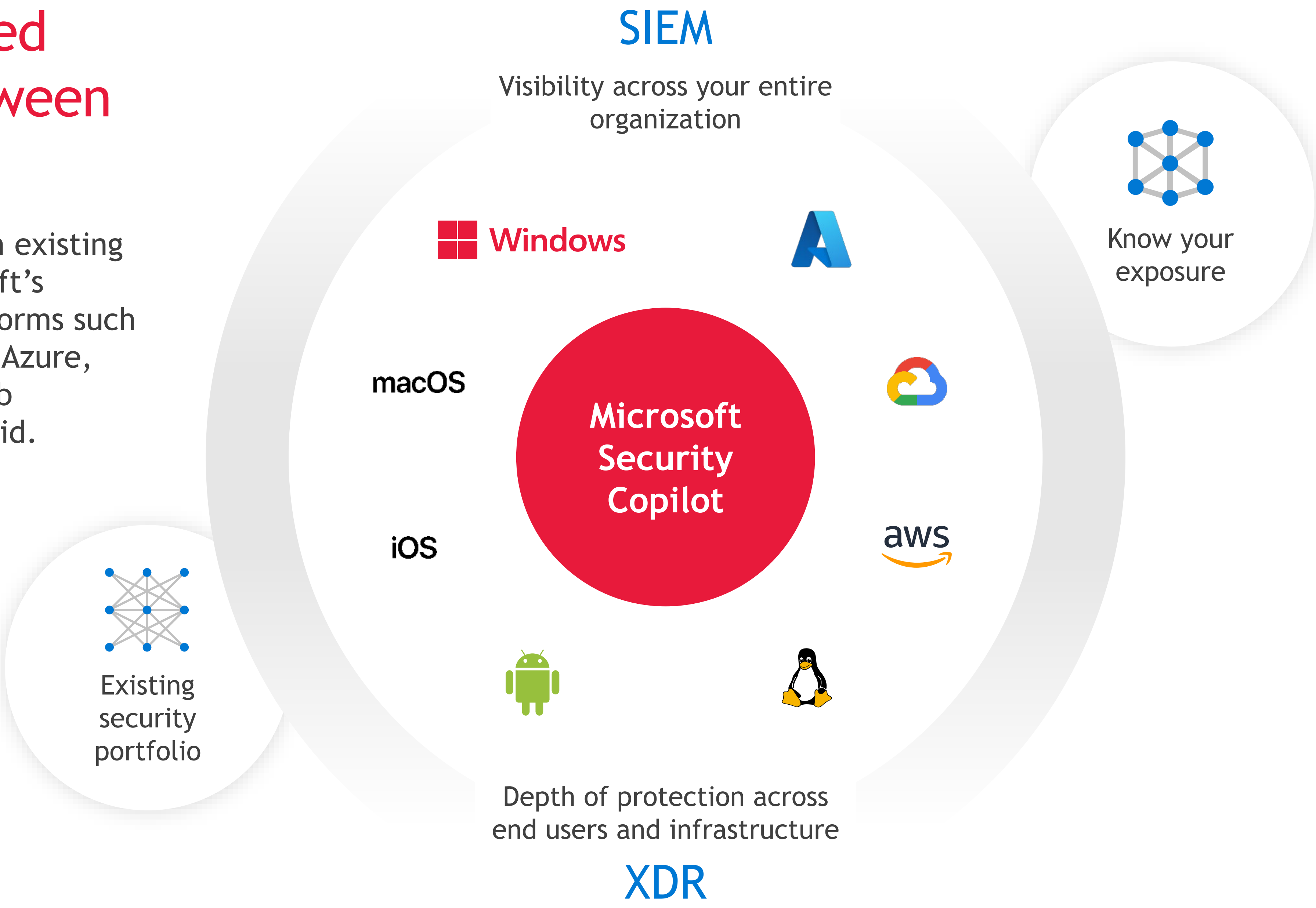
Demystify
WEBCAST SERIES

Security Operations

BDO

A Fully Integrated Experience Between SIEM and XDR

SIEM + XDR integrates with existing security portfolio, Microsoft's ecosystem and other platforms such as, macOS, iOS, Windows, Azure, Google Cloud, Amazon Web Services, Linux, and Android.


SIEM
Visibility across your entire organization
Windows
macOS
iOS
Microsoft Security Copilot
aws
Know your exposure
Existing security portfolio
Depth of protection across end users and infrastructure
XDR

A Unified Security Operations Platform

Begin triage in Microsoft Sentinel

- Assess incidents with prioritized view of all security incidents
- Understand initial scope of incident with all relevant alerts
- Close false positives

Start investigation in Microsoft Defender XDR

- See attack sequence, investigate malicious entities
- Review self-healing investigation and other remediation actions
- Add preventative measures

Complete broader investigation in Microsoft Sentinel

- Dig into any additional alerts related to incident
- Record evidence for incident management
- Leave comments for team members
- Add custom measures

Resolve incident in Microsoft Sentinel

- Perform final remediation actions with predefined playbooks (or manual if needed)
- Close incident

Benefits

Automate response with built-in response and preconfigured playbooks

Prevent repeat attacks with automated posture recommendations

Coordinate response across multiple domains, regardless of architecture

Free security teams to focus on critical threats, regardless of domain

Reduce organizational complexity, save on operational and tooling costs

Protecting the Entire Organization

Remediate issues across your security data sources with a cloud-based SIEM enriched by generative AI

Enable rapid response with XDR-prioritized incidents

- **Individual alerts correlated into single incidents** to uncover the entire kill chain
- **Unified investigation and response experience** across multiple domains
- **Multiple-platform support** for endpoints, identities, and thousands of third- party apps
- **Near real-time custom detections** for a faster response to custom queries

Disrupt advanced attacks at machine speed

- **Identifies** ransomware and other attack scenarios, as well as assets controlled by the attacker
- **Automatically isolates** infected devices and suspends compromised accounts
- **Reduces the overall cost of an attack** by stopping lateral movement
- **Leaves the security operations center (SOC) team in full control** of investigating and remediating

Unify security and identity access management

- Secure adaptive access helps **prevent identity attacks** before they happen
- **Combines** information from all identity sources into a single view, in context.
- **Prevents identity attacks before they happen** with secure conditional access policies from Microsoft
  Entra ID

Microsoft Defender XDR

LET US HELP YOU BUILD A UNIFIED DEFENSE WITH XDR

Cross-domain Security

On-prem and Cloud Identities

Endpoints and IoT

Email and collaboration

Cloud apps

Compliance

Enable rapid response with XDR-prioritized incidents

Disrupt advanced attacks at machine speed

Unify security and identity access management

Built-in preventative controls and posture management

Microsoft Sentinel

SIMPLIFY YOUR DEFENSE AGAINST MODERN THREATS

Empowering the SOC with next-gen SIEM

- Get **unlimited cloud speed** and **scale**
- **Level up** with **Microsoft Intelligence**
- **Detect** and **respond** efficiently
- **Protect your entire digital estate**
- **Native integration** with Microsoft XDR

Powered by the cloud and AI

- Cloud scale protection
- Analytics powered by built-in user entity and behavior analytics and machine learning
- Integrated threat intelligence
- Automated detection, investigation and remediation
- Proactive threat hunting
- Ecosystem integration

Comprehensive capabilities

Demystify

WEBCAST SERIES

Next Steps

Review Microsoft's Cybersecurity Reference Architecture

Microsoft

Cybersecurity Reference Architectures

End to End Security Architecture

Diagrams & References

People

Roles and Risk Management

Artificial Intelligence (AI) and Security

Threat Environment

Ransomware/Extortion, Data Theft, and more

Attack Chain Coverage

Zero Trust

Security Modernization with Zero Trust Principles

Zero Trust Adaptive Access

Security Service Edge (SSE)

Journey

Privileged Access

Development / DevSecOps

Enabling Security & Business Goals

Security Operations

(SecOps/SOC)

Microsoft Security Capabilities

Multi-Cloud & Cross-Platform

Microsoft 365 E5

Build Slide

Role Mapping

Infrastructure

Multi-cloud, cross-platform, native controls

Patch Modernization

Operational Technology (OT)

Industrial Control Systems

Device Types

aka.ms/MCRA | aka.ms/MCRA-videos | December 2023

Slide notes have speaker notes & change history

Microsoft 365 Zero Trust Workshop

Discover gaps in your current Microsoft 365 security posture and receive a customized roadmap with actionable steps to elevate your Zero Trust maturity.

What is Zero Trust?

Zero Trust is a security strategy designed to enhance your security posture by reducing risk and complexity as well as improving your compliance and governance. It's based on three core principals:

- **Verify Explicitly:** Access to a resource should always be validated to ensure they are who they say they are.
- **Use Least Privilege Access:** Only the permissions essential should be granted and only as they're needed.
- **Assume Compromise:** Attacks are inevitable, build you environment to minimize access when it is.

What to Expect

This assessment consists of an automated discovery tool and three workshops covering Identity, Devices, and Data in your Microsoft 365 environment. With each workshop the BDO team will lead you through an interactive session where we'll discuss the capabilities and current state of each area. The assessment will provide a detailed report that outlines the current state of the organization's Zero Trust maturity and delivers a roadmap for improvement.

APPROACHES AND OUTCOMES

Operate your technology stack in confidence, knowing that your security program and investments are working for you.

Identity - Understand best practices for identity verification. Includes strategies for securing identities, enforcing strong authentication methods, and managing access controls.

Devices - Review the current state of device compliance, including paths to secure devices, enforce compliance policies, and manage device access controls.

Data - Review capabilities for securing sensitive information, enforcing data governance policies, and managing data access controls.

Audience Insights

❓ Would you like to receive follow up information from today's session and potentially discuss your AI needs with BDO?

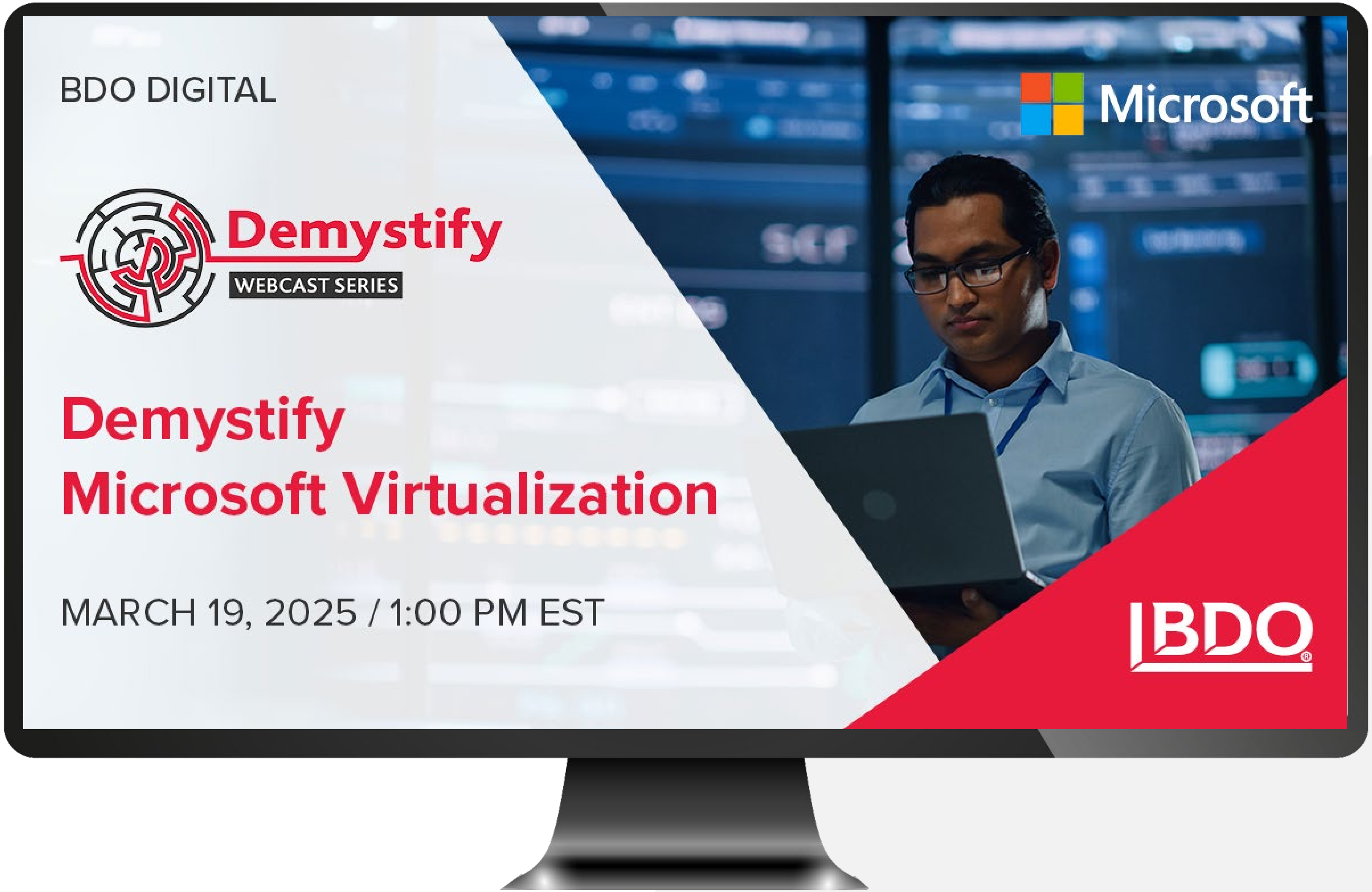
Select your answer
in the panel to the right

Demystify
WEBCAST SERIES

Thank You

BDO

Join Us for the Next Webcast



BDO DIGITAL

Demystify
WEBCAST SERIES

Demystify Microsoft Virtualization

MARCH 19, 2025 / 1:00 PM EST

Microsoft

BDO

BDO Digital, LLC is a Delaware limited liability company, and a wholly-owned subsidiary of BDO USA, P.C.
For more information on BDO Digital, LLC please visit: www.bdodigital.com.

About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C, a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.