Microsoft Security

Protecting Microsoft 365 Data
Kyndryl-MS-Veeam

Mayo 08, 2024.
Buenos Aires, Argentina

Santiago Cavanna
CISO Microsoft SSA
SCavanna@Microsoft.com

Security is a defining challenge of our times. The expanding threat of cyberattacks has never been more challenging or more complex.

Satya Nadella
Microsoft, Chief Executive Officer

There is no absolute security!

- Connectivity means remote access and visibility is a double edge sword.
- Given enough time and resources to a group of brilliant but devious hackers, any security system can be broken.
- It’s a rat-race and a bumpy ride, and the best one can do is to stay ahead of the bad guys by a step or two.

End to End Security Architecture

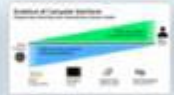
Diagrams & References

Microsoft

Cybersecurity Reference Architectures

People

Roles and Risk Management



Artificial Intelligence (AI) and Security

Threat Environment

Ransomware/Extortion, Data Theft, and more

Attack Chain Coverage

Zero Trust

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

Apply Zero Trust principles

Key changes across security disciplines

All elements informed by threat and business intelligence, assisted by security engineering/automation

Business Enablement

Security Disciplines	Assume Compromise *General strategy shift from 'assume safe network'*	Verify Explicitly *Reduce attack surface and exposure to risk*	Least Privileged *Reduce blast radius both proactive and reactively*
Access Control	**Adaptive Access** Risk-based polices Always make security decisions using all available data points, including identity, location, device health, resource, data classification, and anomalies.	**Just-in-time & Just-enough-access (JIT/JEA)** **Secure Access Service Edge (SASE)** **Cloud Infrastructure Entitlement Management (CIEM)** **Micro-segmentation**	
Security Operations	**Automated threat response** **End to end visibility (SIEM)**	**Asset–centric detection and response (XDR)** Classify assets and apply controls per asset type and classification (CA policies, encryption, monitoring, detection, response etc.)	**Privileged Access Workstations (PAWs)** *For SOC Analysts, IT Admins, and business critical assets*
Asset Protection	**Asset-centric protections**		**Dependency/impact analysis** *backups, service accounts and privileges that control other systems/services, etc.*
Innovation Security	**Threat modelling**	**DevSecOps and CI/CD process integration** *of best practices (Static and dynamic analysis, etc.)*	
Security Governance	**Posture Management** *Continuous improvement* of security posture and standards/policies	**Continuous Monitoring** *of security posture*	*Enablement* → **Hygiene Remediation** Patching, configuration, process updates, etc.

Security Adoption Framework

Align security to business scenarios using initiatives that progressively get closer to full 'Zero Trust'

Business Scenarios
Guiding North Star

1 - I want people to do their job securely from anywhere

2 - I want to minimize business damage from security incidents

3 - I want to identify and protect critical business assets

4 - I want to proactively meet regulatory requirements

5 - I want to have confidence in my security posture and programs

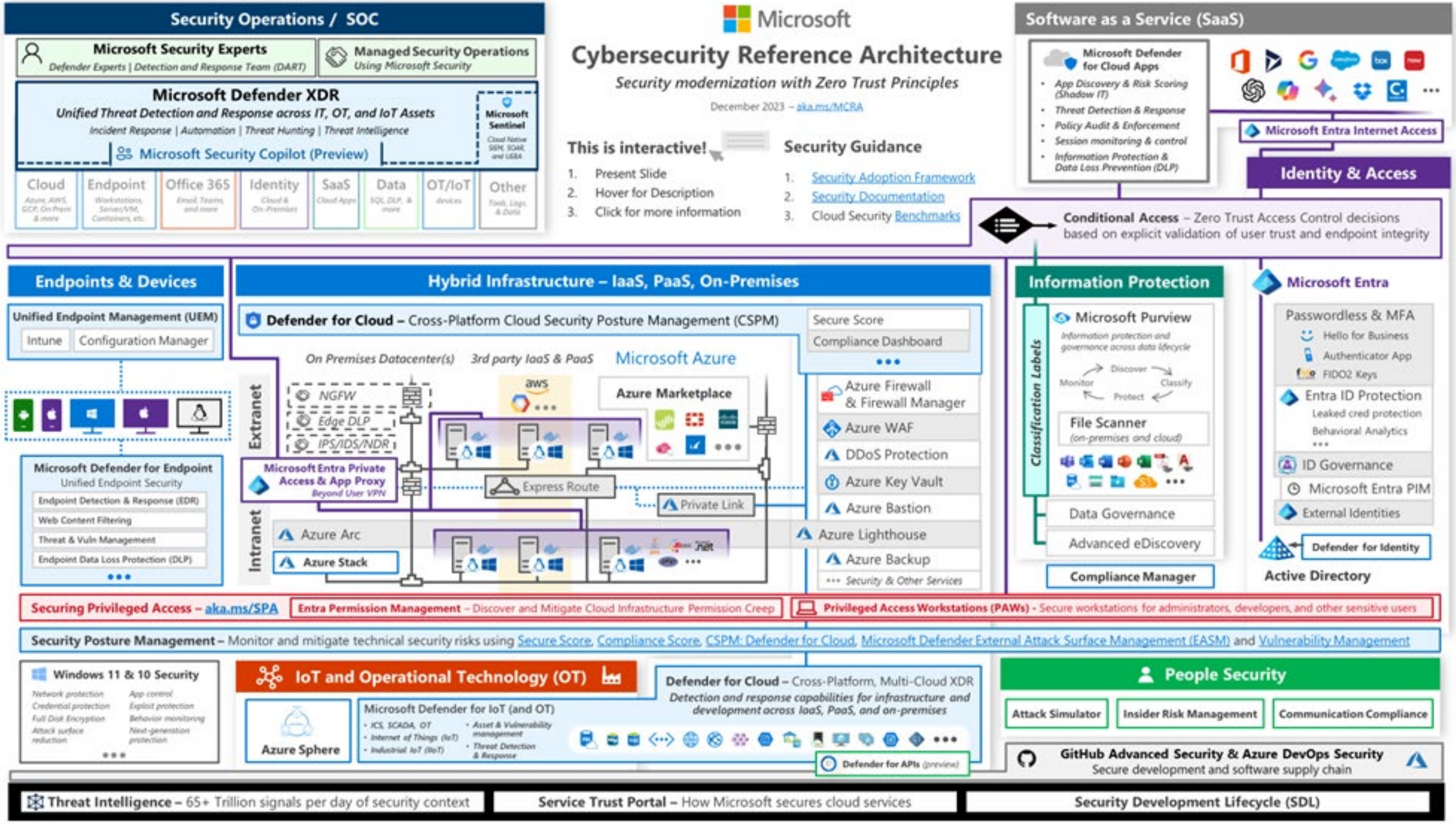
1. Strategic Framework

End to End Strategy, Architecture, and Operating Model

2. Strategic initiatives

Clearly defined architecture and implementation plans

- Security Hygiene: Backup and Patching
- Secure Identities and Access
- Modern Security Operations
- Infrastructure and Development
- Data Security & Governance, Risk, Compliance (GRC)
- OT and IoT Security


Security Operations / SOC
Microsoft Security Experts
Defender Experts | Detection and Response Team (DART)
Managed Security Operations
Using Microsoft Security
Microsoft Defender XDR
Unified Threat Detection and Response across IT, OT, and IoT Assets
Incident Response | Automation | Threat Hunting | Threat Intelligence
Microsoft Security Copilot (Preview)
Microsoft Sentinel
Cloud Native SIEM, SOAR, and UEBA
Cloud
Azure, AWS, GCP, On Prem & more
Endpoint
Workstations, Servers/VM, Containers, etc.
Office 365
Email, Teams, and more
Identity
Cloud & On-Premises
SaaS
Cloud Apps
Data
SQL, DLP, & more
OT/IoT
devices
Other
Tools, Logs, & Data
Microsoft
Cybersecurity Reference Architecture
Security modernization with Zero Trust Principles
December 2023 – aka.ms/MCRA
This is interactive!
1. Present Slide
2. Hover for Description
3. Click for more information
Security Guidance
1. Security Adoption Framework
2. Security Documentation
3. Cloud Security Benchmarks
Software as a Service (SaaS)
Microsoft Defender for Cloud Apps
App Discovery & Risk Scoring (Shadow IT)
Threat Detection & Response
Policy Audit & Enforcement
Session monitoring & control
Information Protection & Data Loss Prevention (DLP)
Microsoft Entra Internet Access
Identity & Access
Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity
Endpoints & Devices
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
Defender for Cloud – 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/NDR
Microsoft Entra Private Access & App Proxy
Beyond User VPN
Azure Marketplace
Express Route
Private Link
Intranet
Azure Arc
Azure Stack
Azure Firewall & Firewall Manager
Azure WAF
DDoS Protection
Azure Key Vault
Azure Bastion
Azure Lighthouse
Azure Backup
Security & Other Services
Information Protection
Microsoft Purview
Information protection and governance across data lifecycle
Discover
Classify
Protect
Monitor
Classification Labels
File Scanner
(on-premises and cloud)
Data Governance
Advanced eDiscovery
Compliance Manager
Microsoft Entra
Passwordless & MFA
Hello for Business
Authenticator App
FIDO2 Keys
Entra ID Protection
Leaked cred protection
Behavioral Analytics
ID Governance
Microsoft Entra PIM
External Identities
Defender for Identity
Active Directory
Securing Privileged Access – aka.ms/SPA
Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep
Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users
Security Posture Management – Monitor and mitigate technical security risks using Secure Score, Compliance Score, CSPM: Defender for Cloud, Microsoft Defender External Attack Surface Management (EASM) and Vulnerability Management
Windows 11 & 10 Security
Network protection
Credential protection
Full Disk Encryption
Attack surface reduction
App control
Exploit protection
Behavior monitoring
Next-generation protection
IoT and Operational Technology (OT)
Azure Sphere
Microsoft Defender for IoT (and OT)
ICS, SCADA, OT
Internet of Things (IoT)
Industrial IoT (IIoT)
Asset & Vulnerability management
Threat Detection & Response
Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises
Defender for APIs (preview)
People Security
Attack Simulator
Insider Risk Management
Communication Compliance
GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain
Threat Intelligence – 65+ Trillion signals per day of security context
Service Trust Portal – How Microsoft secures cloud services
Security Development Lifecycle (SDL)

Learn | Discover | Product documentation | Development languages | Topics | Sign in

Azure | Products | Architecture | Develop | Learn Azure | Troubleshooting | Resources | Portal | Free account

Filter by title

- Fundamentals Documentation
- Overview
- Shared responsibility
- Security posture management
- Detect and mitigate threats
  - Protect against ransomware and extortion

Learn / Azure / Security / Fundamentals /

Backup and restore plan to protect against ransomware

Article • 08/29/2023 • 8 contributors

Feedback

In this article

Additional resources

Training

Module

Prevent ransomware and extortion-based attacks - Training

Prevention against ransomware is essential because such an attack can lead to major disruption for you or your business. In this module, you'll learn about best practice...

Documentation

FAQ - Protect backups from Ransomware with Azure Backup - Azure Backup

In this article, discover answers to protect backups from ransomware with Azure Backup.

Azure features & resources that help you protect, detect, and respond

Azure features & resources that help you protect, detect, and respond

Ransomware protection in Azure

Ransomware protection in Azure

Show 5 more

Learn | Discover | Product documentation | Development languages | Topics | Sign in

Azure | Products | Architecture | Develop | Learn Azure | Troubleshooting | Resources | Portal | Free account

Filter by title

- Fundamentals Documentation
- Overview
- Shared responsibility
  - Shared responsibility in the cloud
  - AI shared responsibility model
- Security posture management
- Detect and mitigate threats
- Securing workloads in Azure
- Azure platform and infrastructure
- Identity management
- Network security
- IaaS security
- Data security, encryption, and storage
- Application
- Monitoring, auditing, and operations
- Resources

Learn / Azure / Security / Fundamentals /

Shared responsibility in the cloud

Article • 09/29/2023 • 4 contributors

Feedback

In this article

- Division of responsibility
- Cloud security advantages
- Next step

As you consider and evaluate public cloud services, it's critical to understand the shared responsibility model and which security tasks the cloud provider handles and which tasks you handle. The workload responsibilities vary depending on whether the workload is hosted on Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or in an on-premises datacenter.

Division of responsibility

In an on-premises datacenter, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft. The following diagram illustrates the areas of responsibility between you and Microsoft, according to the type of deployment of your stack.

	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■

Additional resources

Training

Module

Design cloud solutions for the public sector - Training

Introduction to the stakes and options for implementing Azure to safeguard public sector data.

Certification

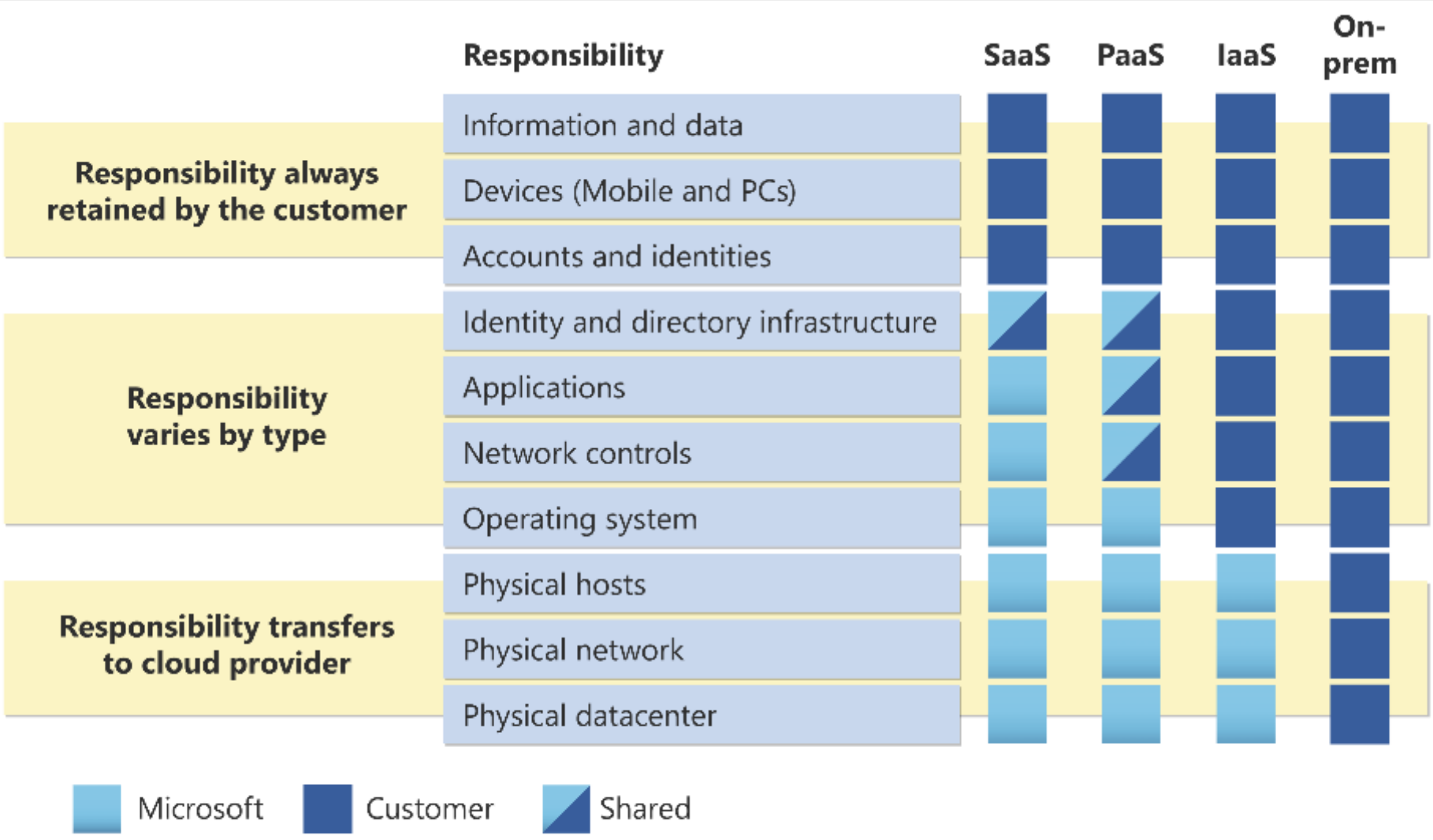
Microsoft Certified: Azure Security Engineer Associate - Certifications

Demonstrate the skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities.

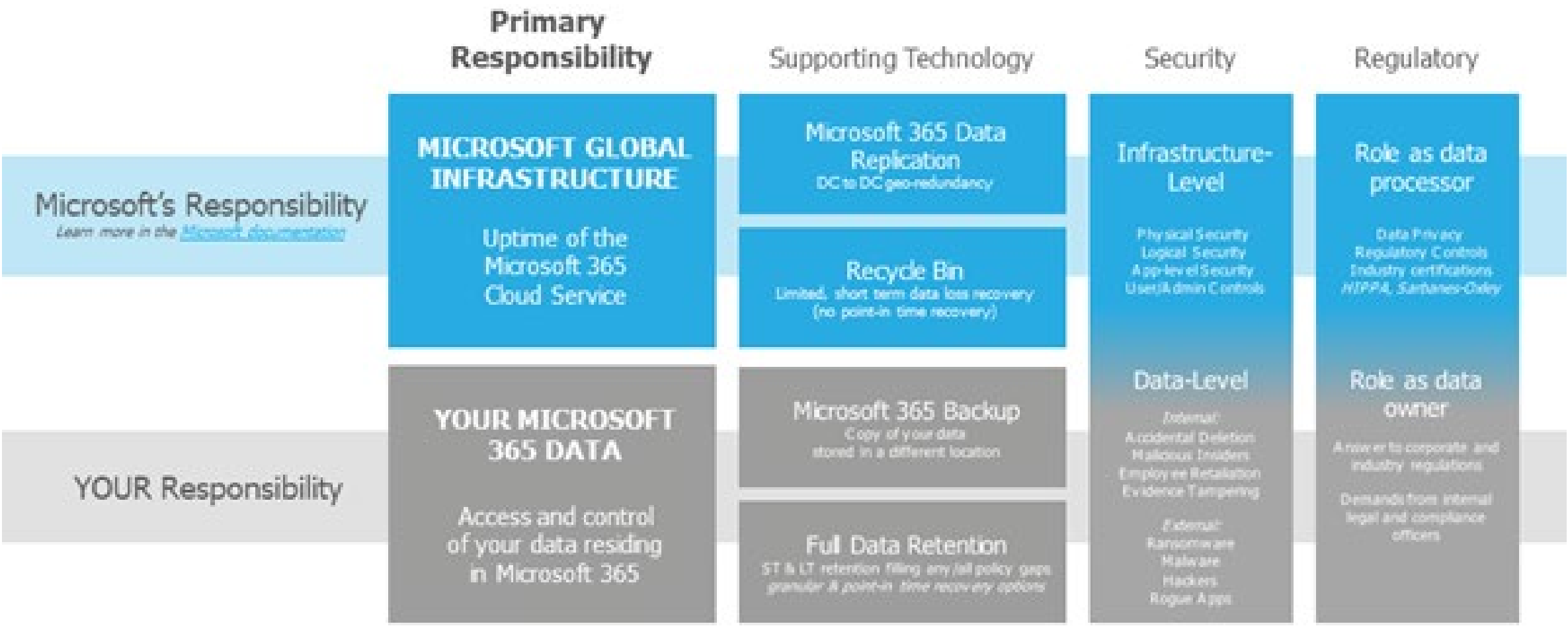
[Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn]

[Azure backup and restore plan to protect against ransomware | Microsoft Learn]

Division of responsibility

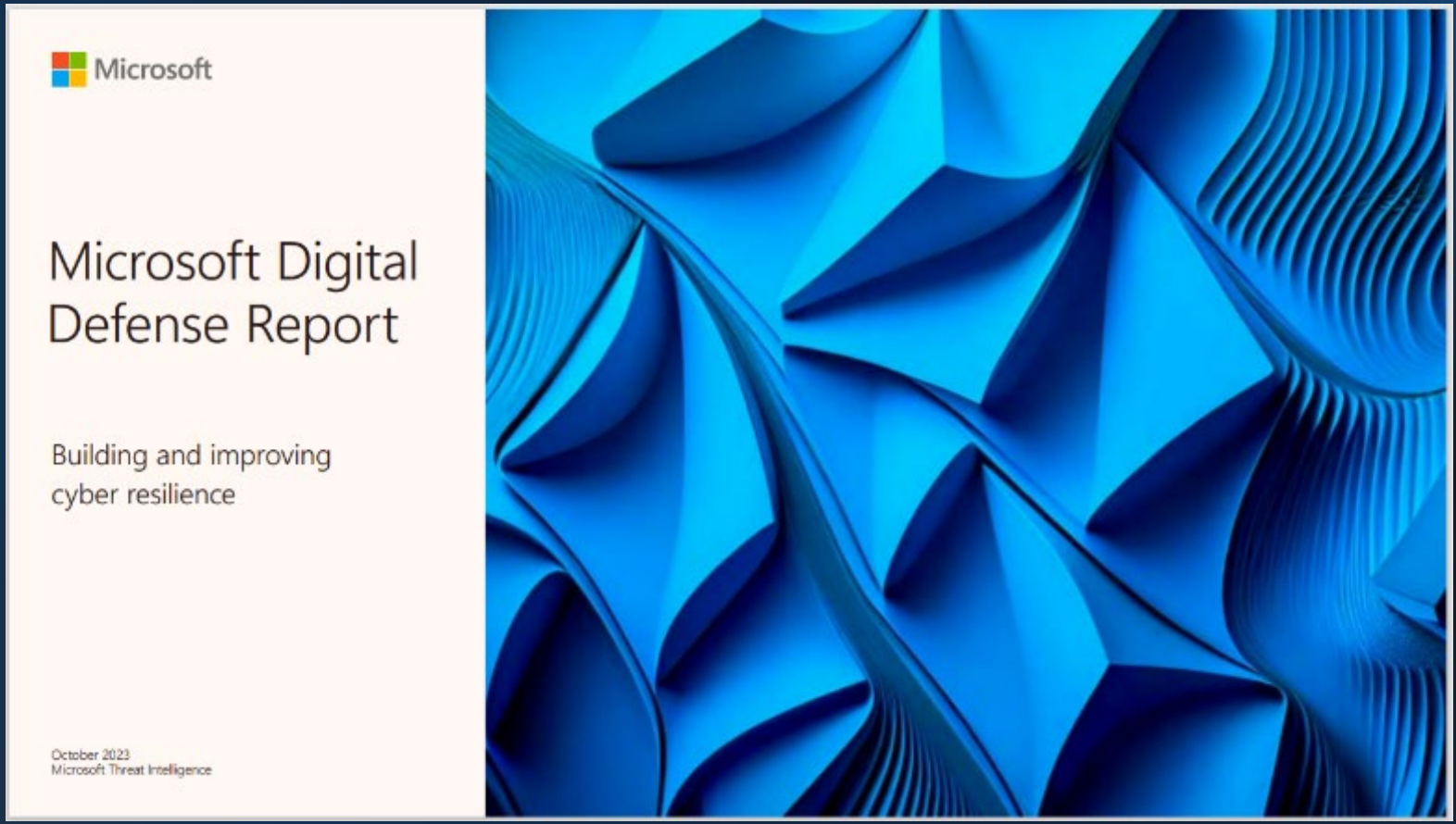


The Microsoft 365 Shared Responsibility Model



[The Microsoft 365 Shared Responsibility Model | Veeam]

Microsoft Digital Defense Report (MDDR)



https://aka.ms/MDDR

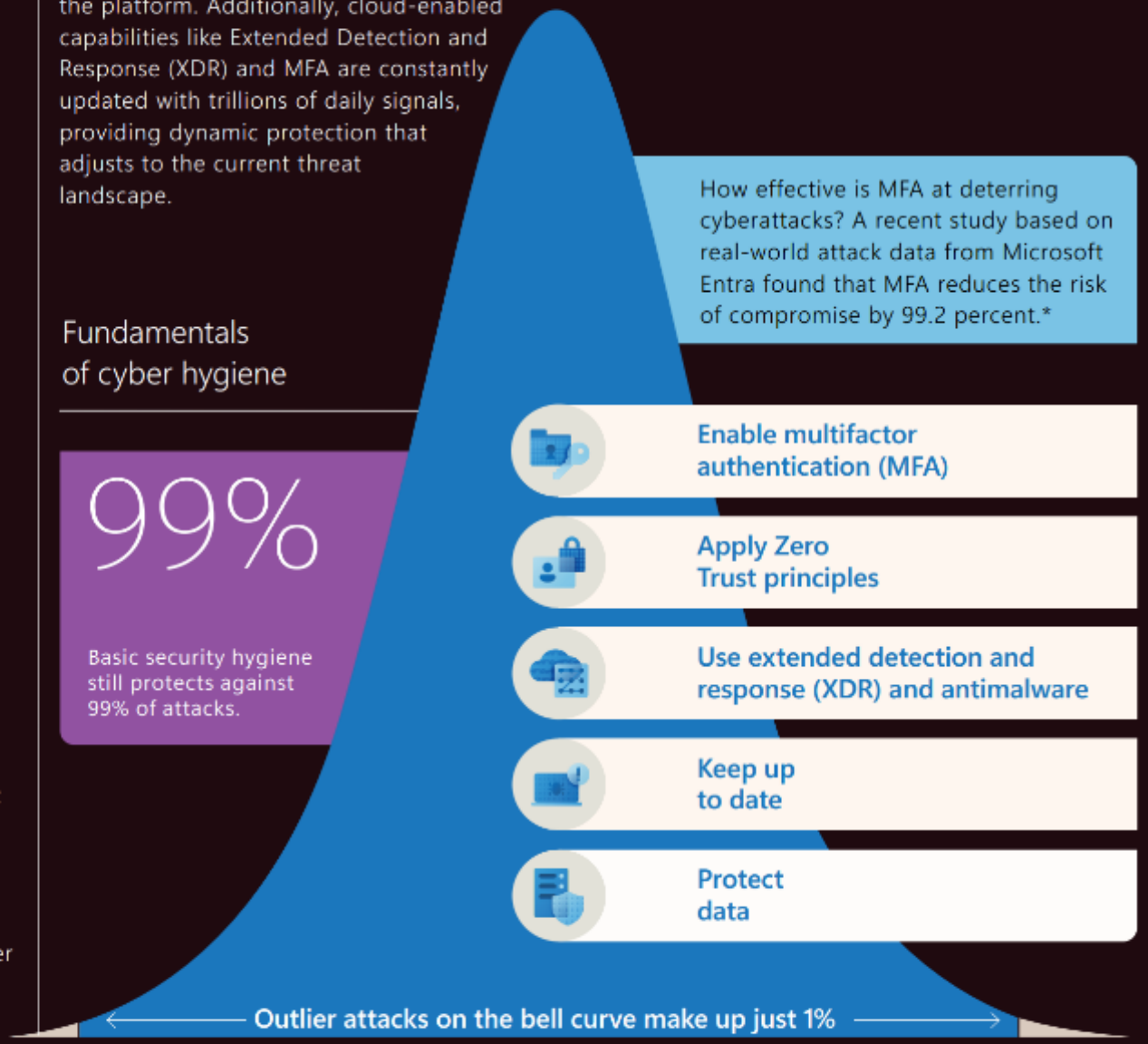
How can we protect against 99% of attacks?

While we explore many dimensions of the cyber threat landscape in this report, there is one crucial point we must emphasize across them all: the vast majority of successful cyberattacks could be thwarted by implementing a few fundamental security hygiene practices.

By adhering to these minimum-security standards, it is possible to protect against over 99 percent of attacks:

1. **Enable multifactor authentication (MFA):** This protects against compromised user passwords and helps to provide extra resilience for identities.
2. **Apply Zero Trust principles:** The cornerstone of any resilience plan is to limit the impact of an attack on an organization. These principles are:
   - Explicitly verify. Ensure users and devices are in a good state before allowing access to resources.
   - Use least privilege access. Allow only the privilege that is needed for access to a resource and no more.
   - Assume breach. Assume system defenses have been breached and systems may be compromised. This means constantly monitoring the environment for possible attack.
3. **Use extended detection and response (XDR) and antimalware:** Implement software to detect and automatically block attacks and provide insights to the security operations software. Monitoring insights from threat detection systems is essential to being able to respond to threats in a timely fashion.
4. **Keep up to date:** Unpatched and out-of-date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.
5. **Protect data:** Knowing your important data, where it is located, and whether the right defenses are implemented is crucial to implementing the appropriate protection.

Hyperscale cloud makes it easier to implement fundamental security practices by either enabling them by default or abstracting the need for customers to implement them. With software as a service (SaaS) and platform as a service (PaaS) solutions, the cloud provider takes responsibility for keeping up with patch management. Implementing security solutions like MFA or Zero Trust principles is simpler with hyperscale cloud because these capabilities are already built into the platform. Additionally, cloud-enabled capabilities like Extended Detection and Response (XDR) and MFA are constantly updated with trillions of daily signals, providing dynamic protection that adjusts to the current threat landscape.



*Source: https://arxiv.org/abs/2305.00945

Microsoft

Microsoft Security

Protecting Microsoft 365 Data

Santiago Cavanna
CISO Microsoft SSA
SCavanna@Microsoft.com

INVITACIÓN EXCLUSIVA

kyndryl / Microsoft

Protecting Microsoft 365 Data

An overview of strategies for securing Microsoft 365 data

Miércoles 8 de Mayo | 9.30 hs
Kyndryl Argentina
Hipólito Yrigoyen 2149, Martínez
Estacionamiento incluido

Regístrese aquí →

Con la participación especial de veeam