Meetup

Microsoft Azure User Community

Azure Cloud Security

NOVEMBER 2023

Azure Security – Overview

What will we discuss

- Architecture
- Security Tools - in Azure and M365
- Security Operations: A day in the life of..
- Ransomware Preparedness
- Other Topics and Q&A

Architecture

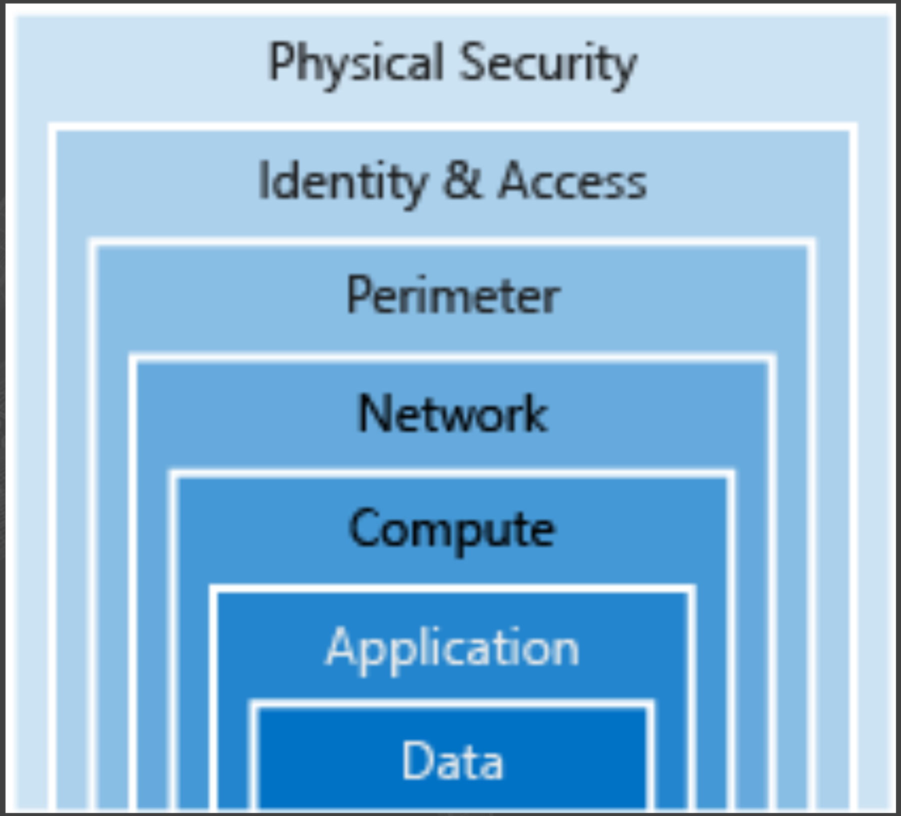
Azure Security – What is there to protect?

Security Defense Objectives

A defense in depth discussion about the security related features in Azure and M365

During this presentation I'll focus on Azure/M365 security topics that many organizations are applying.

What is your focus? One or more of these? →



Azure and Microsoft 365 Security: The Big Picture

Key security related areas in M365:

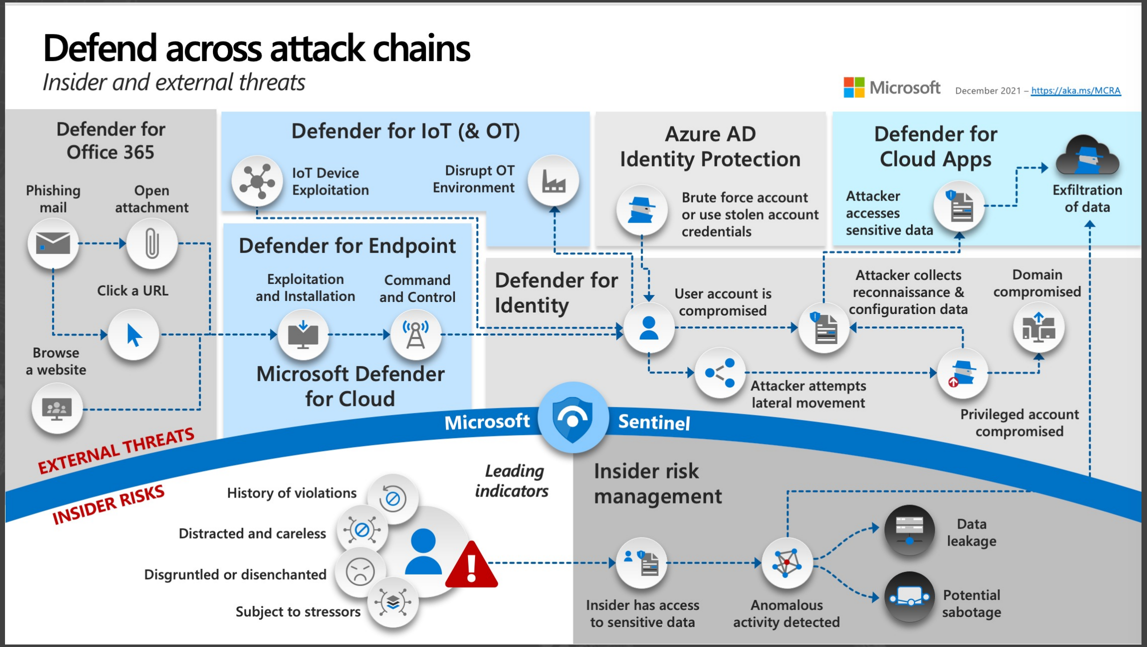
- Endpoints (EDR)
- Email (phishing protection)
- Cloud apps (CASB)

Key areas in Azure:

- Azure Entra (Identity)
- Defender for Cloud (Cloud Posture – CSPM)
- Sentinel (SIEM)

MCRA – Microsoft Cybersecurity Reference Architecture

Reference: https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra



Defend across attack chains

Insider and external threats

Microsoft December 2021 – https://aka.ms/MCRA

Frameworks for Cloud Security

Cloud Adoption Framework for Azure (CAF)

Well Architected Framework (WAF)

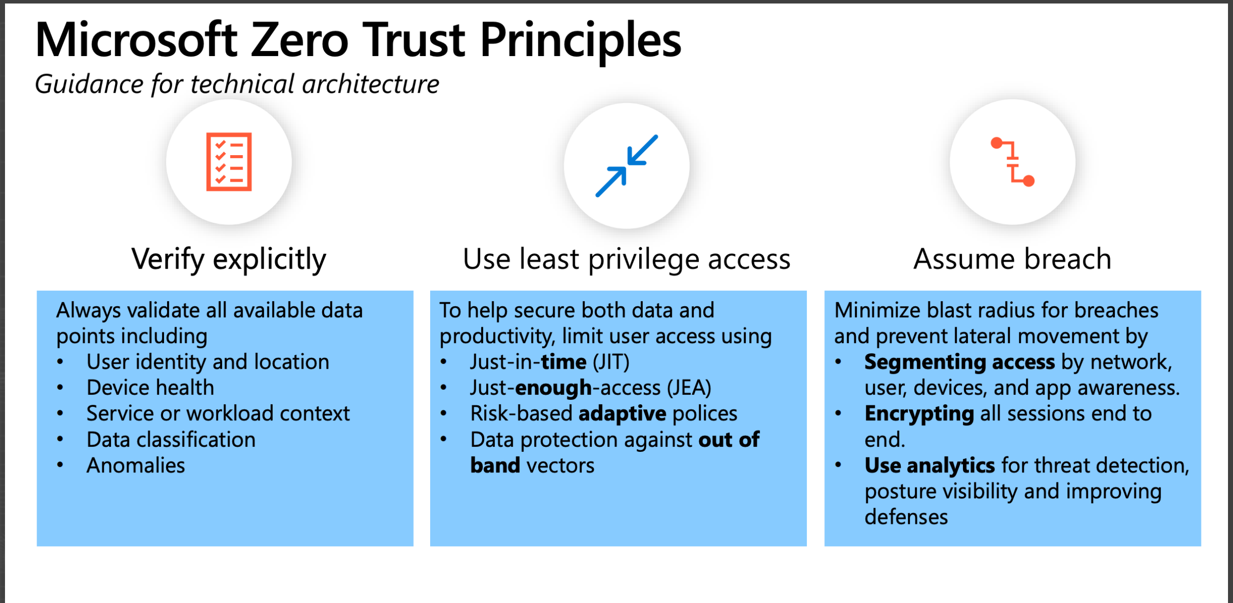
Pillars: Reliability, Security, Cost, Ops, Performance

- Sub-Topics for each Pillar:
  - Quick Links
  - Checklists
  - Trade-offs
- Workloads – VM, IoT, DB, etc
- Service Guides – details, by pillar, for each service type.
- Assessment:
  - https://learn.microsoft.com/en-us/assessments/azure-architecture-review/

Zero Trust – with RaMP

RaMP – Rapid Adoption Modernization Plan

- **Deploy the following security protections first:**
  - Identity
  - Endpoints
  - Apps
  - Networks
- **Protect Data**
  - Prepare Ransomware Readiness
- **Modernize security operations**
  - SIEM/SOAR/AI



Microsoft Zero Trust Principles

Guidance for technical architecture

Verify explicitly

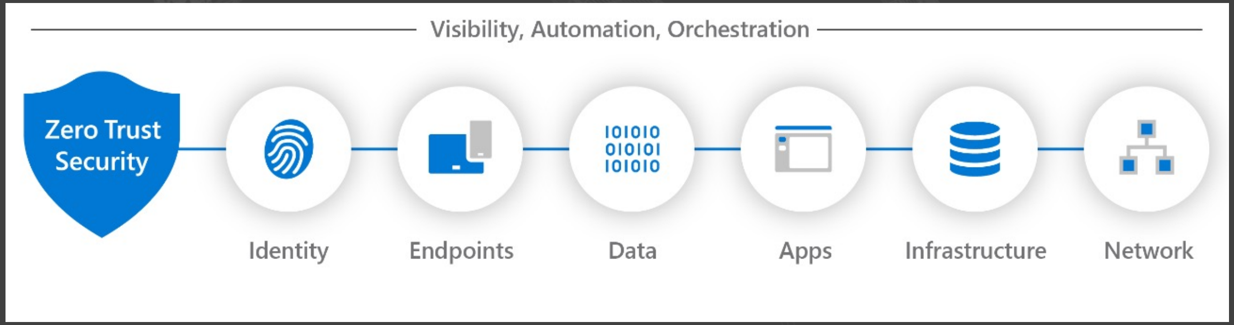
Always validate all available data points including
- User identity and location
- Device health
- Service or workload context
- Data classification
- Anomalies

Use least privilege access

To help secure both data and productivity, limit user access using
- Just-in-**time** (JIT)
- Just-**enough**-access (JEA)
- Risk-based **adaptive** polices
- Data protection against **out of band** vectors

Assume breach

Minimize blast radius for breaches and prevent lateral movement by
- **Segmenting access** by network, user, devices, and app awareness.
- **Encrypting** all sessions end to end.
- **Use analytics** for threat detection, posture visibility and improving defenses



Visibility, Automation, Orchestration

Zero Trust Security

Identity

Endpoints

Data

Apps

Infrastructure

Network

The Tools

Security Monitoring in Azure and Microsoft 365

A look at Microsoft Defender solutions and Sentinel

- Defender for Cloud
- Defender for Cloud Apps
- Defender for Endpoints
- Defender for Server
- Defender for Storage
- Defender for Identity
- Defender for IoT/OT
- Defender for Containers

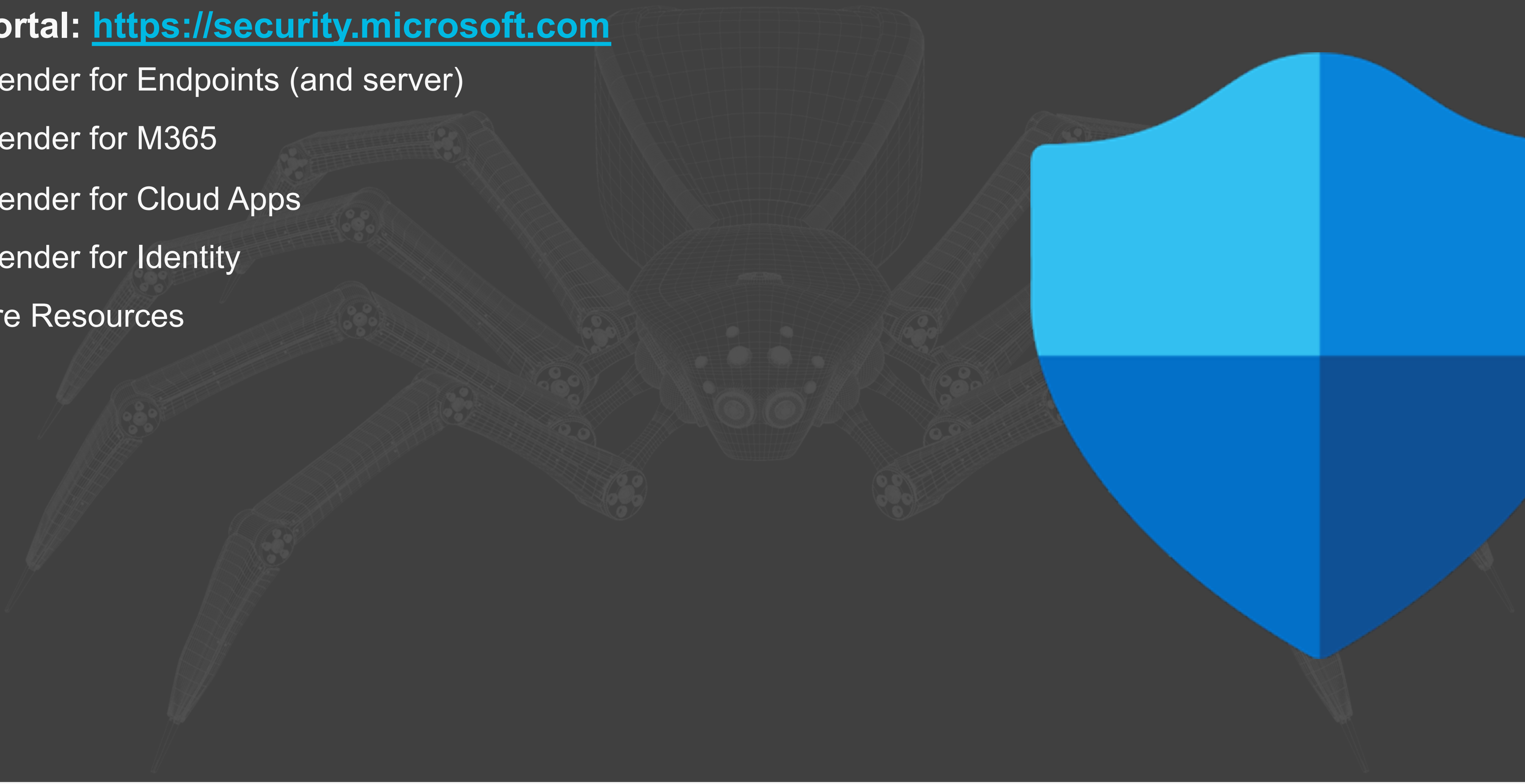
Microsoft Cloud Security: A world of portals

- Azure: https://portal.azure.com
- M365: https://security.microsoft.com
- Compliance (Purview) https://compliance.microsoft.com
- Entra: https://entra.microsoft.com
- Intune: https://intune.microsoft.com

The M365 Security Portal

M365 Portal: https://security.microsoft.com

- Defender for Endpoints (and server)
- Defender for M365
- Defender for Cloud Apps
- Defender for Identity
- More Resources



The Azure Portal

Entra Portal: https://portal.microsoft.com

- Azure Entra ID (formally Azure AD)
  - Security: Conditional Access
  - Security: Identity Protection
  - Security: Risky Users
  - Governance: Access Reviews
  - External Identities – B2B, B2C
  - App Registrations

What security features do you use in Azure Entra ID?

The Entra Portal

Entra Portal: https://entra.microsoft.com

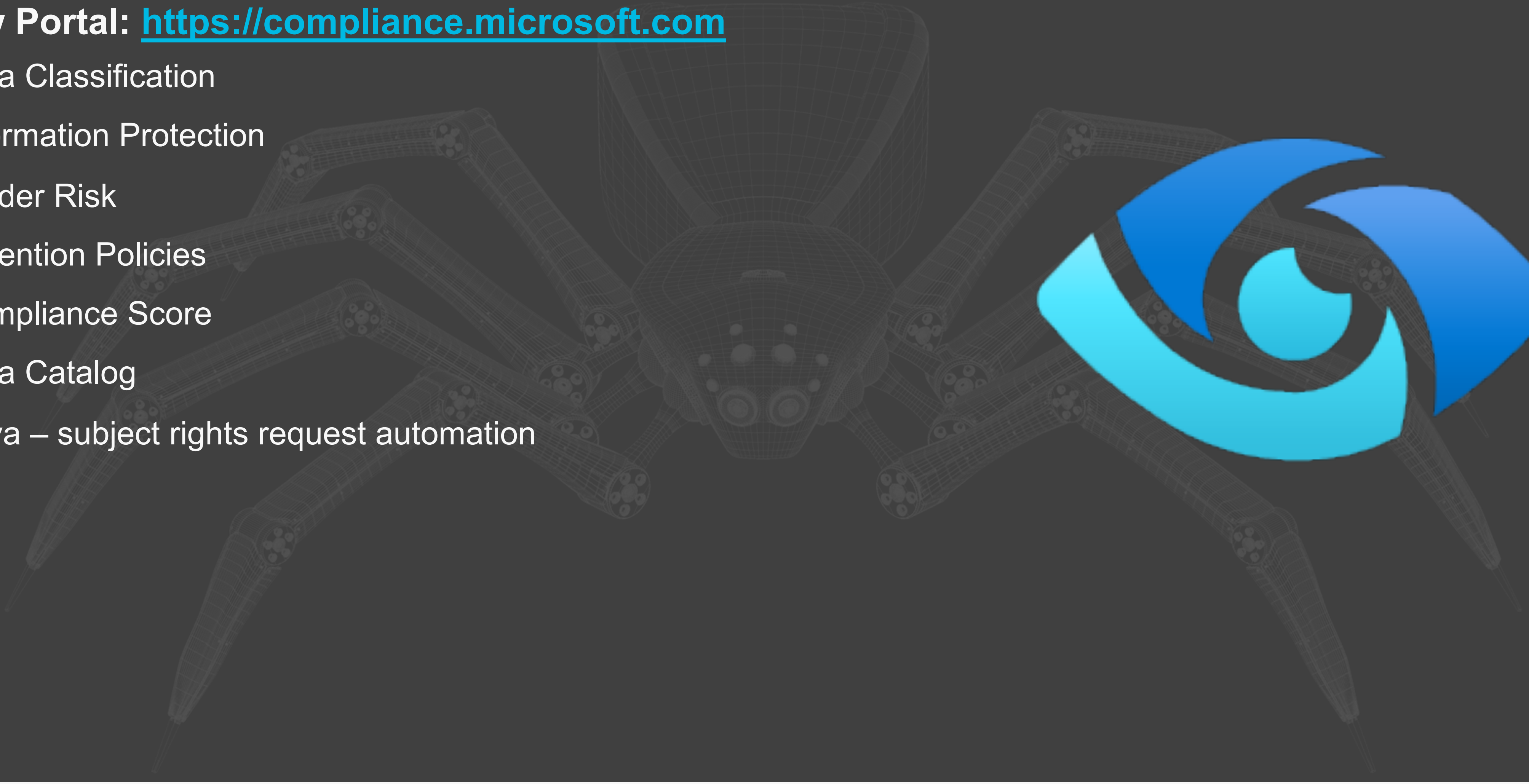
- Permissions Management (CIEM)
- Workload ID
- ID Governance
- Verified ID
- Private Access (SASE)

Note: many organizations do not have a license for the Entra portal features

The Purview Portal

Purview Portal: https://compliance.microsoft.com

- Data Classification
- Information Protection
- Insider Risk
- Retention Policies
- Compliance Score
- Data Catalog
- Priva – subject rights request automation



Security Operations: A Day in the Life Of..

Security Operations

A day in the life of a Security Operator in Azure/M365

1. Check Sentinel Alerts
2. Check Defender Alerts
3. (Optional: Security Copilot)
4. Defender for Threat Intelligence
5. Defender for Cloud – Recommendations and Secure Score
    1. Attack Path Review
6. M365 Defender – Recommendations and Secure Score
7. Purview – Alerts and Secure Score
8. Access Review (weekly?)
9. EASM Review

Ransomware Preparedness

Ransomware Defenses

Microsoft Best Practices for Ransomware Preparedness

- Prepare: Backups, versioning, immutable storage
  - Data Protection – Encrypt your data so it can't be stolen
- Limit Scope of Damage
  - Segmentation – Limit lateral movement
  - Restrict privileged access – PIM, conditional access
  - Improve security – follow Secure Score recommendations

DaRT – Microsoft's Detection and Response Team

- DaRTs Recommendations for Ransomware Incident Response
  - Assess: Identify the cause
  - Determine impact: what line of business is affected
  - Recover: Determine the steps to recover

Other Topics and Q&A

Common Pitfalls When Using Azure/M365 Security

Ad-hoc Architecture – CAF, WAF, MCRA

Inventory Management

- No easy button for inventory/assets

Cloud Security Posture Management (CSPM)

- Often enabled and forgotten. Policies aren't added

Landing Zones

- For building repeatable foundations

Cost Management

- VERY easy to lose track of costs

Access Reviews and PIM

- Controls over user access are slack

Certifications and Training

AZ104: Azure Admin

AZ500: Azure Security Engineer

SC100: Microsoft CyberSecurity Architect

Ninja Training and Microsoft Learn

- Google “Microsoft Ninja”

Where to Learn More about Microsoft Security

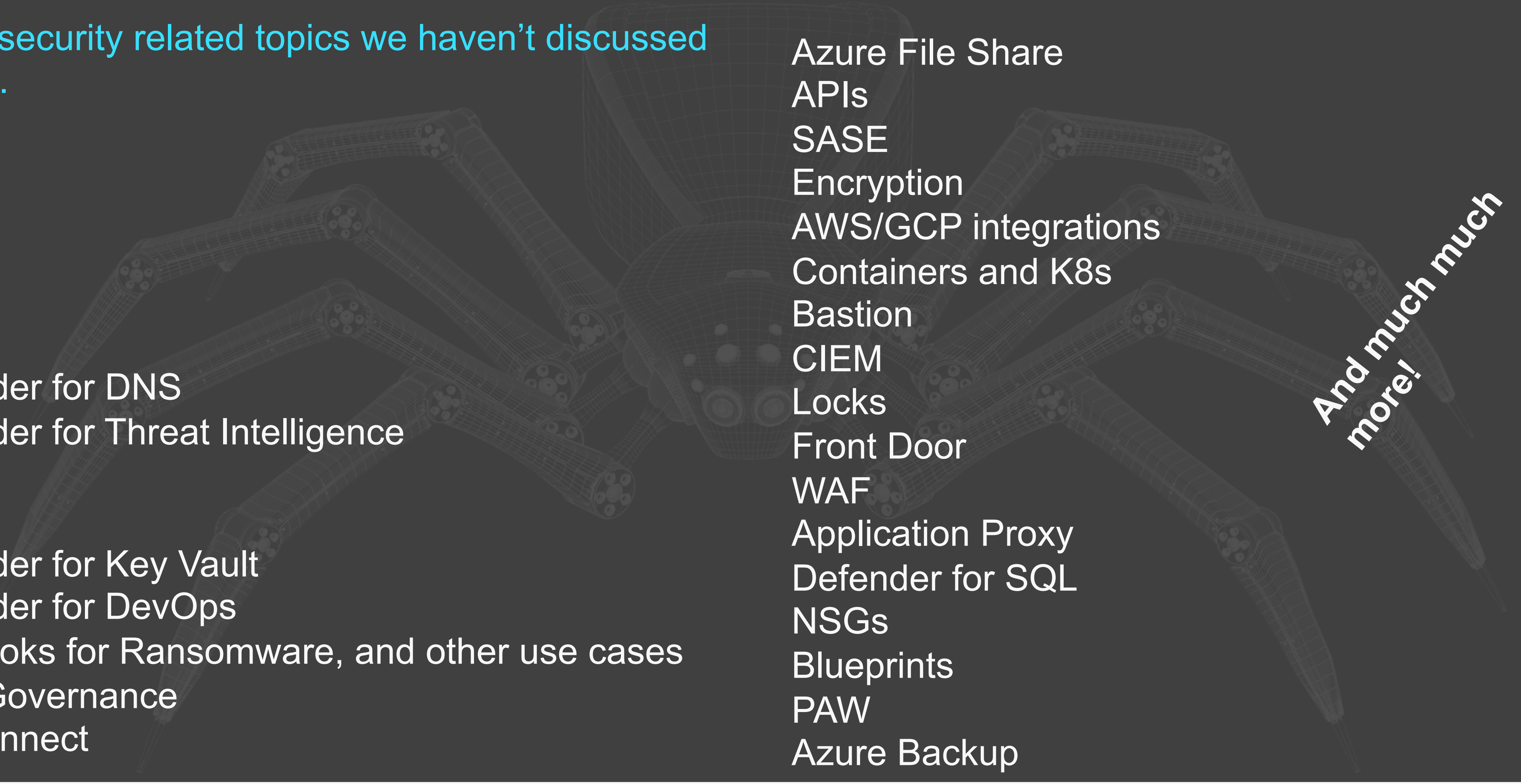
Continue learning with Microsoft Learn

https://learn.microsoft.com

Azure Well Architected Framework
https://learn.microsoft.com/en-us/azure/well-architected/

John Savill – Microsoft Architecture videos
https://onboardtoazure.com/

Questions?



Some security related topics we haven't discussed today...

PIM
PAM
JIT
IAM
RBAC
Defender for DNS
Defender for Threat Intelligence
ARM
KQL
Defender for Key Vault
Defender for DevOps
Runbooks for Ransomware, and other use cases
Data Governance
AD Connect

Azure File Share
APIs
SASE
Encryption
AWS/GCP integrations
Containers and K8s
Bastion
CIEM
Locks
Front Door
WAF
Application Proxy
Defender for SQL
NSGs
Blueprints
PAW
Azure Backup

And much much more!

References

Portals

https://portal.azure.com
https://security.microsoft.com
https://compliance.microsoft.com
https://entra.microsoft.com
https://intune.microsoft.com

Architecture

https://learn.microsoft.com/en-us/assessments/azure-architecture-review/
ttps://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

Zero Trust

https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust
https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

Ransomware Preparedness

https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-prepare
https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/
https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-dart-ransomware-approach?source=recommendations

Thank You