Microsoft 365 Security, Compliance, and Identity Concepts

Security Concepts & Methodologies for Microsoft 365

Vlad Catrinescu

Microsoft MVP

@vladcatrinescu https://VladTalksTech.com

Overview

Cloud Computing: Who Secures What?

Common Security Threats

Zero Trust Methodology

Cloud Computing: Who Secures What?

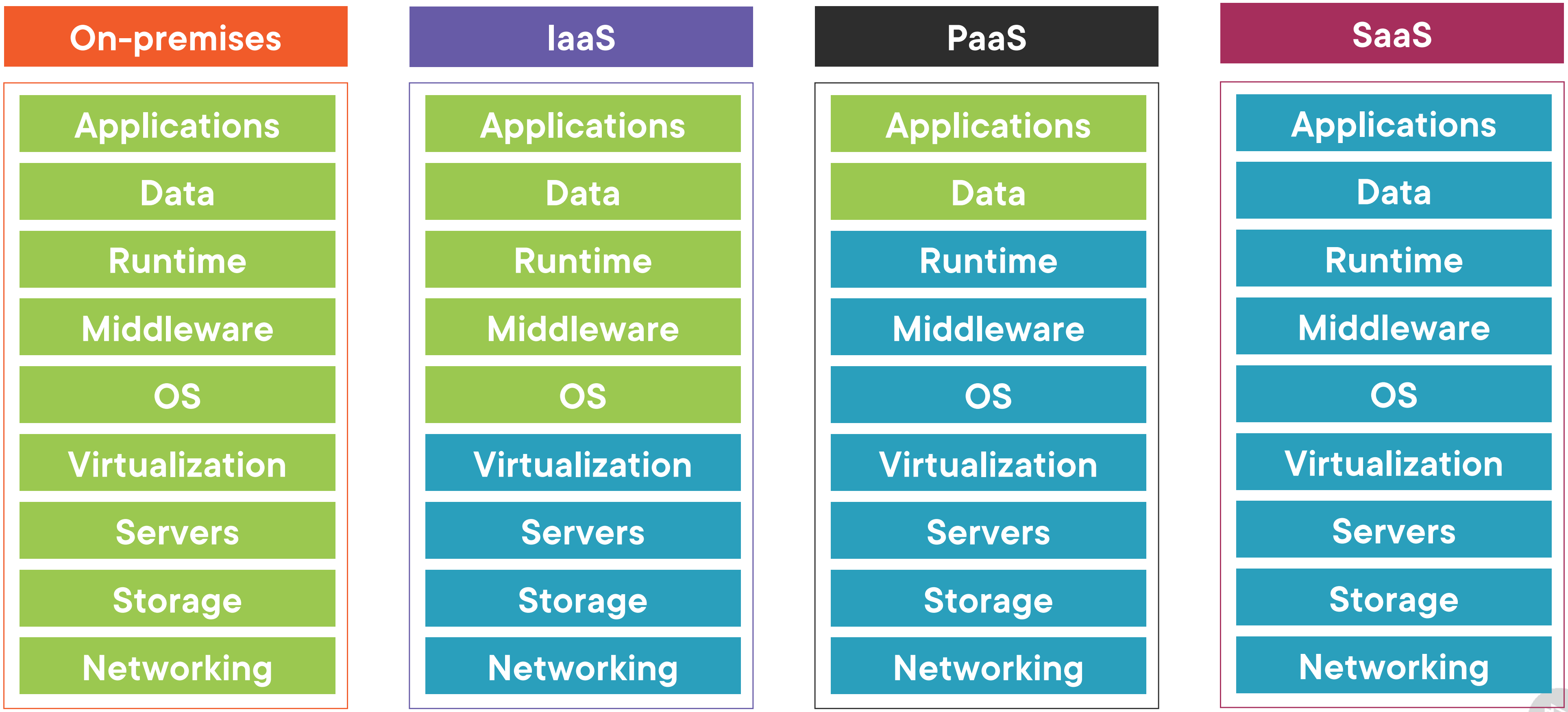
Types of Cloud Computing Services

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Types of Cloud Computing Services



On-premises	IaaS	PaaS	SaaS
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications
🟩 Data	🟩 Data	🟩 Data	🟦 Data
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Middleware	🟩 Middleware	🟦 Middleware	🟦 Middleware
🟩 OS	🟩 OS	🟦 OS	🟦 OS
🟩 Virtualization	🟦 Virtualization	🟦 Virtualization	🟦 Virtualization
🟩 Servers	🟦 Servers	🟦 Servers	🟦 Servers
🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking

🟩 You manage

🟦 Managed by vendor

Most Companies Use Products from Each Service Type

IaaS

- Azure Compute (Virtual Machines)
- Azure Storage

PaaS

- Azure Logic Apps
- Azure Functions
- Azure Web Apps
- Azure Automation

SaaS

- SharePoint
- OneDrive for Business
- Microsoft Teams

Security in the Cloud Is a Partnership

The cloud provider operates and secures

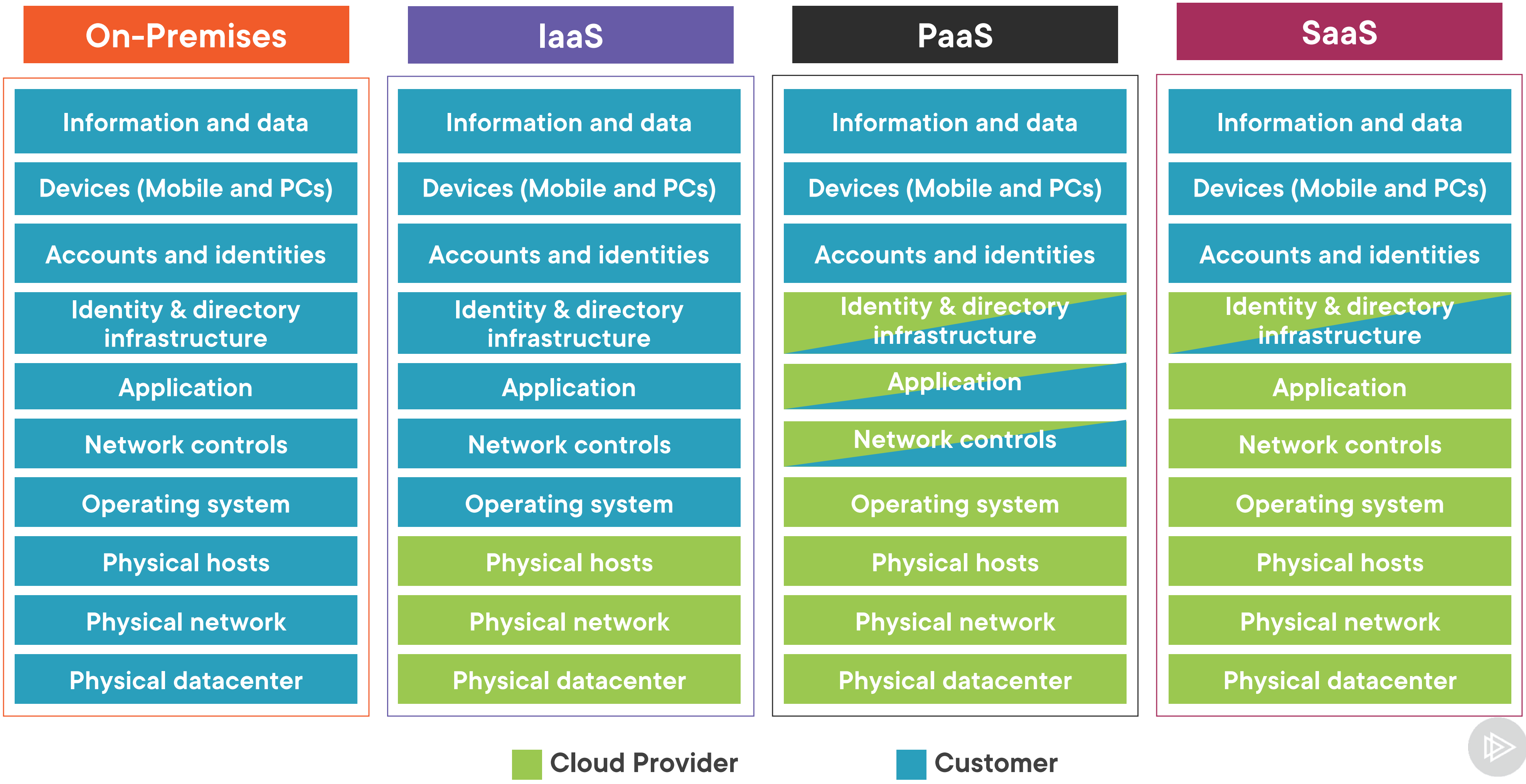
- The base infrastructure
- Host operating system layers

You control and secure

- Identities
- Additional application settings (ex: MFA)

The responsibilities and controls for the security of applications and networks vary by the service type

Who Secures What? – The Shared Responsibility Model



	On-Premises	IaaS	PaaS	SaaS
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity & directory infrastructure	🟦	🟦	🟩/🟦	🟩/🟦
Application	🟦	🟦	🟩/🟦	🟩
Network controls	🟦	🟦	🟩/🟦	🟩
Operating system	🟦	🟦	🟩	🟩
Physical hosts	🟦	🟩	🟩	🟩
Physical network	🟦	🟩	🟩	🟩
Physical datacenter	🟦	🟩	🟩	🟩

🟩 Cloud Provider

🟦 Customer

It’s your duty to know what your security responsibilities are for each type of workload you leverage in the cloud

Common Security Threats

Common Security Threats

Data Breach

Disruptive attacks

Dictionary attack
aka Brute Force Attack

Ransomware

Worms

Coin Miners
aka Cryptojacking

Data Breach

A data breach is when data is stolen

- Personal data

Can result in identity attacks

- Phishing / Spear Phishing
- Tech support scams

Dictionary Attacks

Also called *Brute Force Attack*

Common Identity attack

Hacker attempts by trying a large number of known passwords

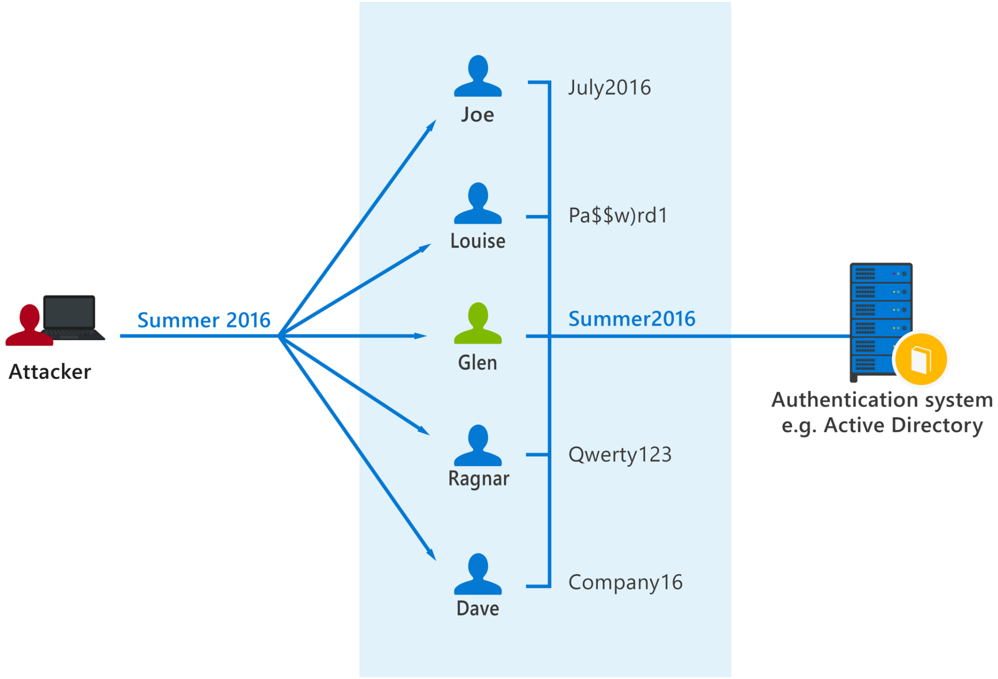
- Each password is automatically tested against a known username

Password Spray

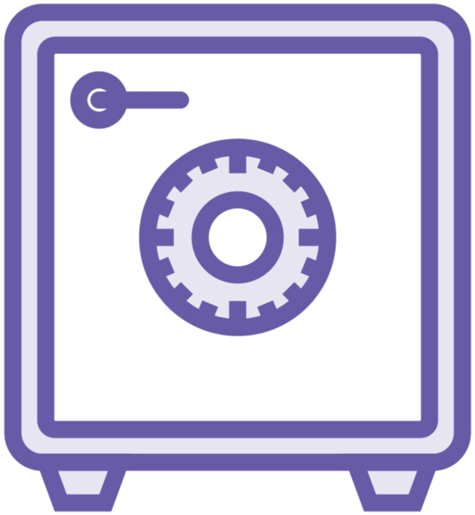
Identity Attack

Submit a small number of known weakest password to all accounts in an organization

Limited number of tries in order to avoid detection thresholds



Ransomware



Type of malware that encrypts files and folders

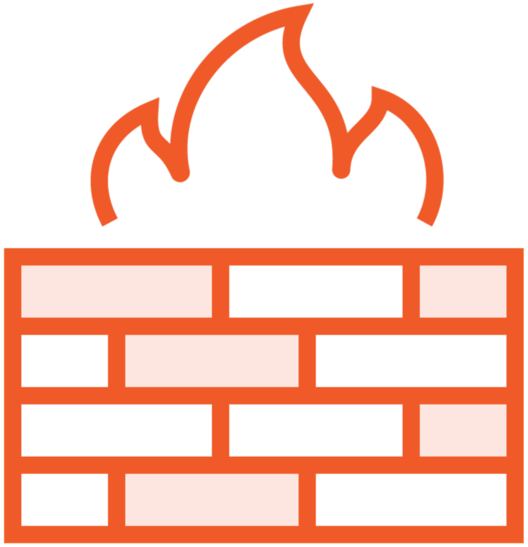
Ransomware attempts to extort money from victims in exchange for the decryption key

- Usually in cryptocurrency

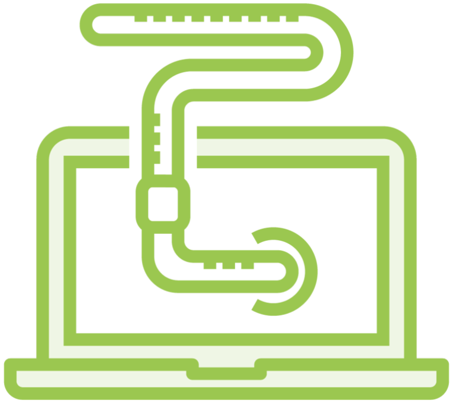
Disruptive Attacks

Distributed Denial of Service (DDoS) attack

- Exhaust an application / server / service resources by flooding it with traffic
- Renders the target unavailable to legitimate users



Worms



Type of malware that can copy itself

Spreads through a network by exploiting vulnerabilities

Can spread trough multiple ways

- E-mail attachments
- Text messages
- Removable drives

Coin Miners (Cryptojacking)

Affected computer mines for Cryptocurrency currency for the hacker

Affected computers only notice a decrease in performance

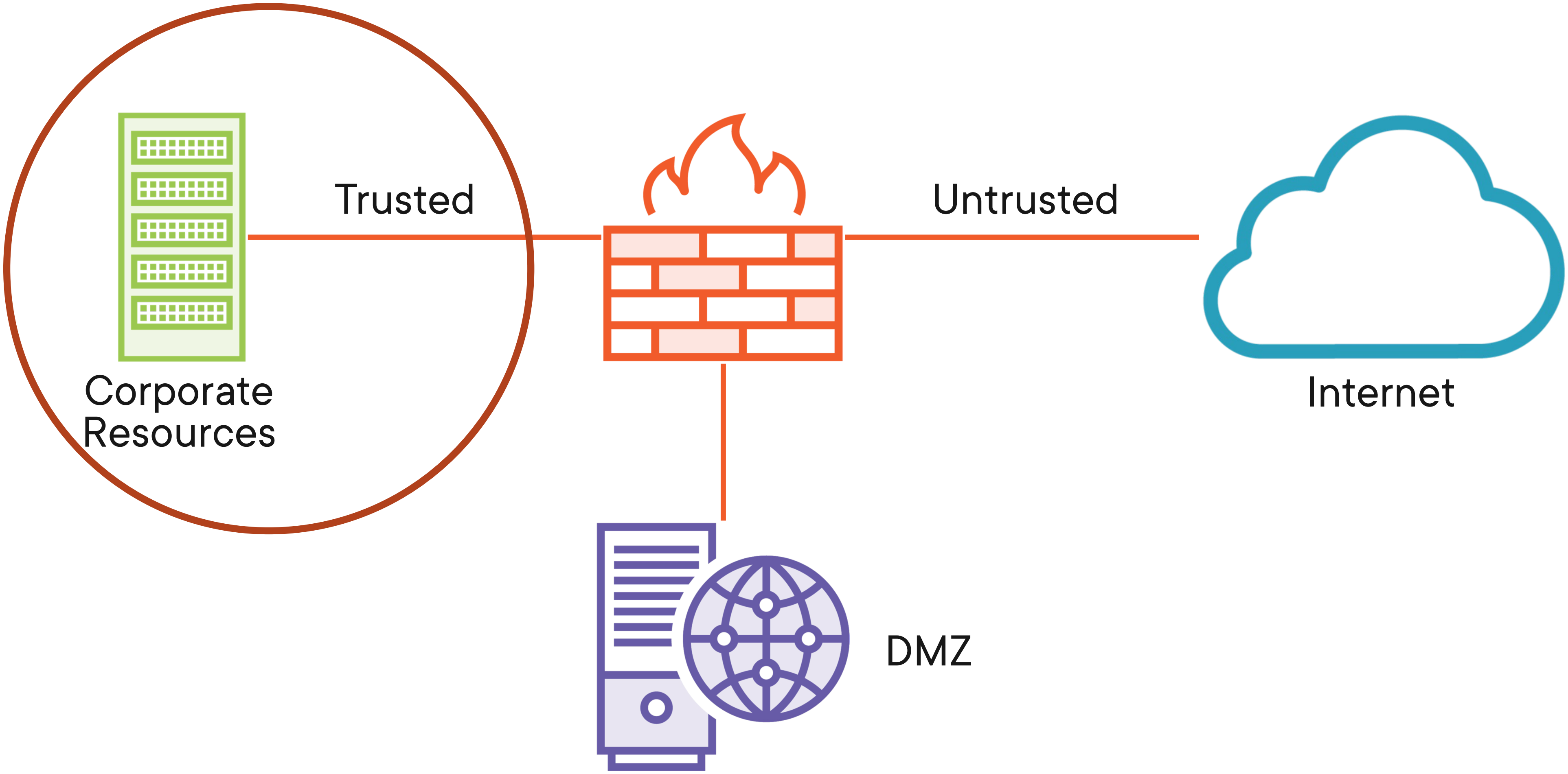
Zero Trust Methodology

Zero Trust

Zero Trust is a cybersecurity model with a very simple premise: eliminate the concept of “trust” from your network.

https://www.techradar.com/features/zero-trust-the-strategic-approach-to-stop-data-breaches

Traditional Network Design



The Corporate Perimeter Has Changed

Cloud Technology

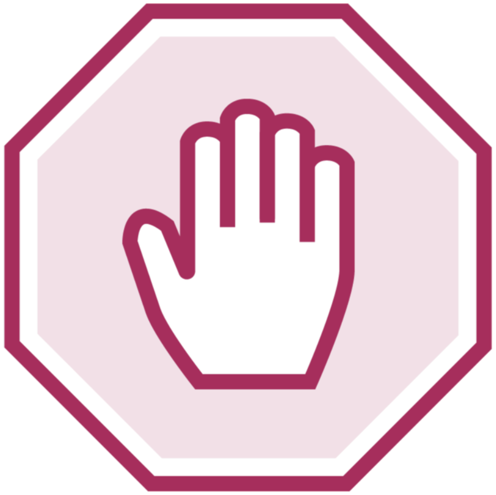
Mobile Workforce

Bad actors and threats have evolved

Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

NIST SP 800-207

Zero Trust Guiding Principles

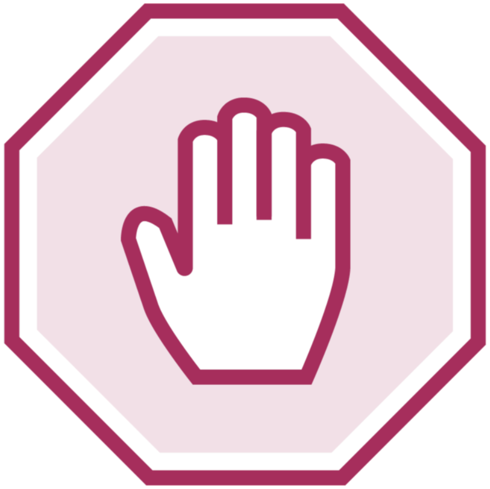


Verify Explicitly

Least Privileged Access

Assume Breach

Verify Explicitly



Authenticate and authorize based on available data points

- User identity
- Location
- Device
- Service
- Data anomalies

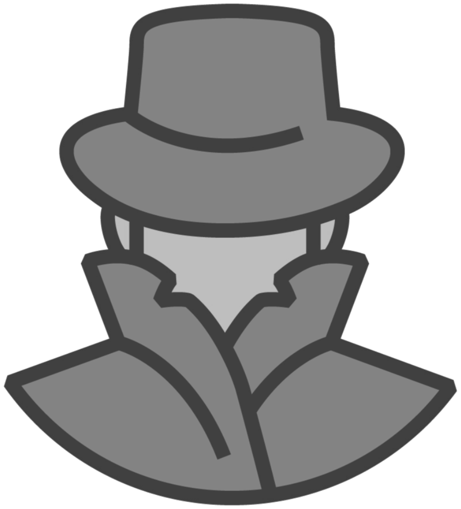
Least Privileged Access

Limit users with Just-in-time and just-enough access

- JIT/JEA

Risk-Based Adaptive Policies

Assume Breach



Segment access by network, user, devices, and application

Use encryption to protect data

Use analytics to get visibility

Zero Trust Foundational Pillars

Identities	Devices	Applications
Data	Infrastructure	Networks

Conclusion

Shared Responsibility Model

- Different responsibilities depending on cloud service type
- Some responsibilities are **always** retained by the customer!
  - Information and data
  - Devices
  - Accounts and identities

Common threats in the cloud

Zero Trust Methodology

- Verify explicitly
- Least privileged access
- Assume breach

Up Next:

Identity and Access Management Solutions for Microsoft 365

Course Update

Microsoft Product Renames

Vlad Catrinescu

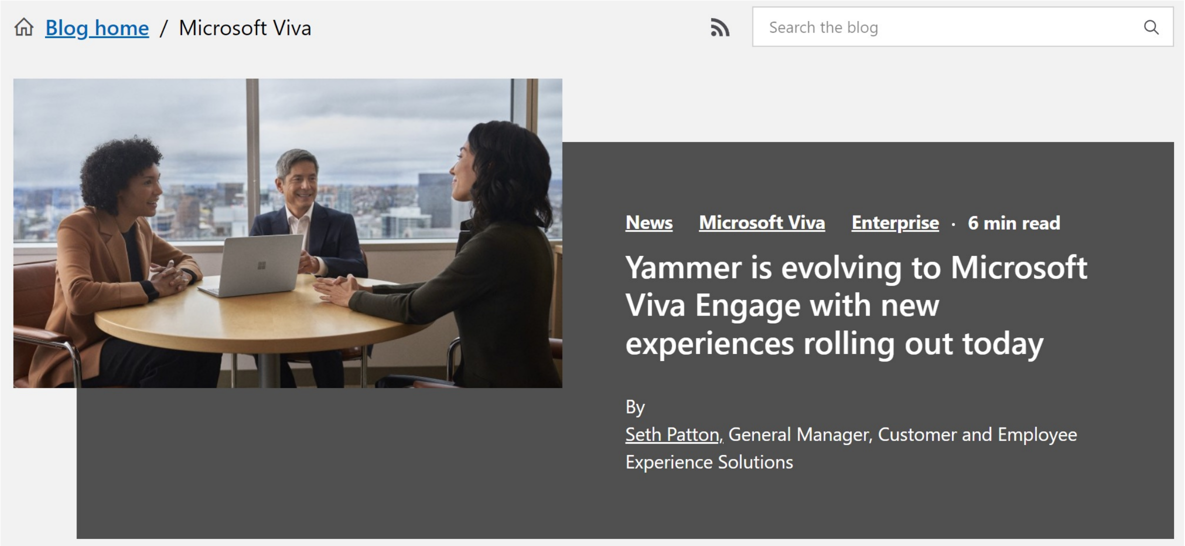
Microsoft MVP

@vladcatrinescu https://VladTalksTech.com

Yammer is Now Viva Engage

Yammer is now called Microsoft Viva Engage

Same purpose and goal inside Microsoft 365

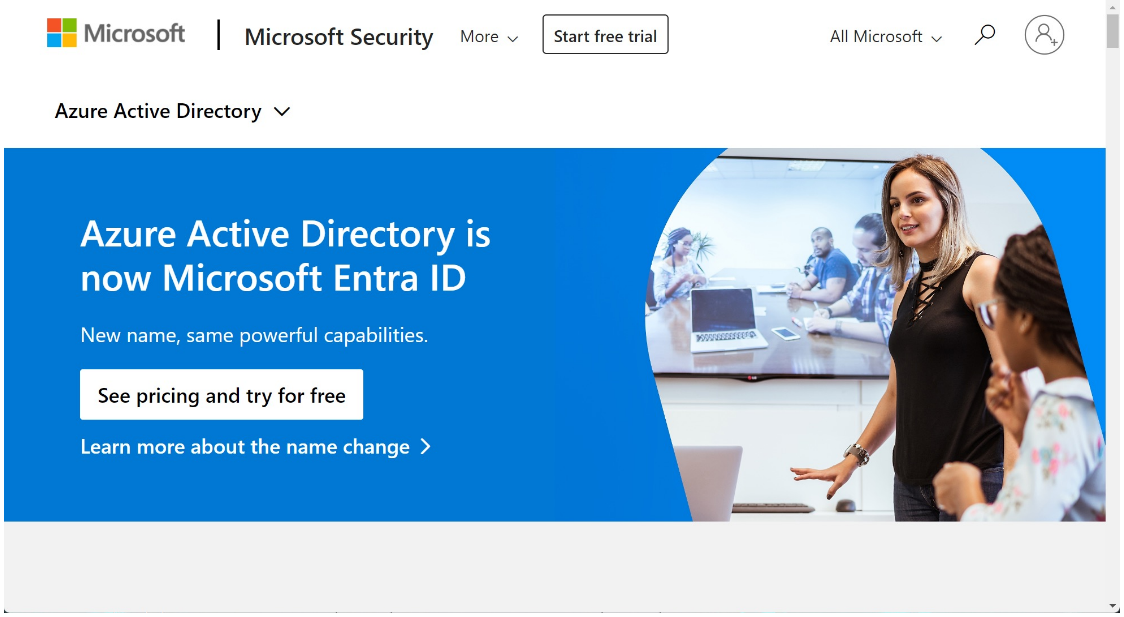


Blog home / Microsoft Viva

News Microsoft Viva Enterprise · 6 min read

Yammer is evolving to Microsoft Viva Engage with new experiences rolling out today

By
Seth Patton, General Manager, Customer and Employee Experience Solutions



Microsoft | Microsoft Security More Start free trial All Microsoft

Azure Active Directory

Azure Active Directory is now Microsoft Entra ID

New name, same powerful capabilities.

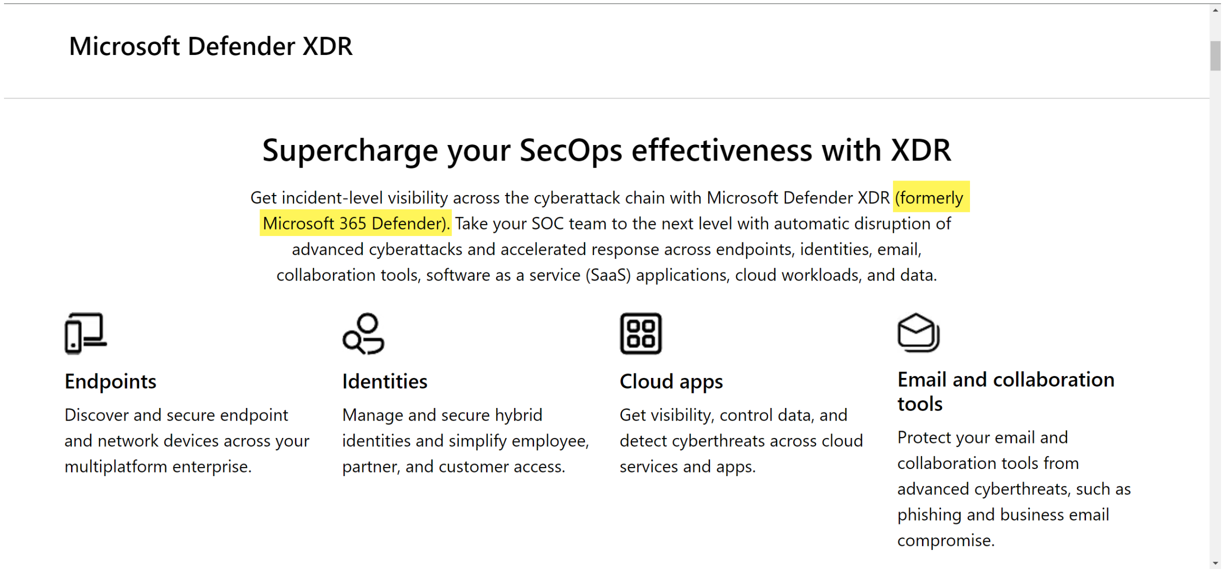
See pricing and try for free
Learn more about the name change >

Azure Active Directory is now Microsoft Entra ID

New name, same powerful capabilities!

Microsoft 365 Defender is now Microsoft Defender XDR

Name for Defender products inside the suite did not change



Microsoft Defender XDR

Supercharge your SecOps effectiveness with XDR

Get incident-level visibility across the cyberattack chain with Microsoft Defender XDR (formerly Microsoft 365 Defender). Take your SOC team to the next level with automatic disruption of advanced cyberattacks and accelerated response across endpoints, identities, email, collaboration tools, software as a service (SaaS) applications, cloud workloads, and data.

Endpoints

Discover and secure endpoint and network devices across your multiplatform enterprise.

Identities

Manage and secure hybrid identities and simplify employee, partner, and customer access.

Cloud apps

Get visibility, control data, and detect cyberthreats across cloud services and apps.

Email and collaboration tools

Protect your email and collaboration tools from advanced cyberthreats, such as phishing and business email compromise.

Name Changes Impact

The product name changes have no impact on the features you will learn in this course

Many internal and external resources might still use the old names of the products