Cloud Security Posture Management (CSPM)

With the move to the cloud from on-prem, it is becoming more difficult for any IT dept to know if data, assets, and resources are as protected as they used to be. Misconfiguration makes it rife for attackers to exploit.

CSPM assesses your systems and automatically alerts staff in IT when vulnerabilities are found. It uses:

- **Zero Trust-based access control**: Considers active threat level during access control decisions.
- **Real-time risk scoring**: Provides visibility into top risks
- **Treat and Vulnerability Management (TVM)**: Shows holistic view of orgs attack surface and integrates it into ops and engineering decision making
- **Discover risks**: To understand ata exposeure of enterprise intellectual property
- **Technical policy**: Apply guardrails to audit and enforce orgs standards and policies to systems
- **Threat modeling systems and architectures**: Used alongside other specific apps

MS Defender for Cloud

A tool for CSPM and threat protection. Fills 3 vital needs:

- Continuously assess
- Secure
- Defend

Visibility and hardening recommendations

Central feature is "secure score". MS Defender for Cloud assesses resources, subscriptions, and the org on an ongoing basis for sec issues. Any findings then get weighted and combined into a single score - grouped into sec controls.

Cloud workload protection (CWP)

Through CWP capabilities, MS Defender for Cloud is able to detect and respolve threates to resources, workloads, and services.

Enhanced security of Microsoft Defender for Cloud

MS Defender for Cloud is offered in two modes:

- Free: enabled for free on all Azure subscriptions. It provides the security score and related features (sec policy, continuous sec assessment, actionable sec rec)
- Enhanced Security: extends capabilities of Free to workloads running in Azure, hybrid, or other cloud platforms. CWP are delivered via integrated MS Defender plans specific to resources in your subscriptions.

Defender Plans

For servers: adds threat detection for Win/Linux machines

For App Service: identifies attacks targeting apps running over app service

For storage: detects potentially harmful activity on your Azure Storage accounts

For SQL: secures your databases and their data wherever located

For Kubernetes: provides cloud-native Kubernetes sec env hardening.

For container registries: protects all Azure Resource Manager based registries in your sub

For Key Vault: advanced threat protection for Azure Key Vault

For Resource Manager: automatically monitors resource management operations in your org

For DNS: additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.

For open source relational protections: threat protections for FOSS relational DBs

Enhanced Sec Features

Endpoint Detection and Response: MS Defender for servers includes MS Defender for Endpoint for endpoint detection and response (EDR)

Vuln scanning for VM, container regsitries, and SQL resources: easily deploy scanner to all your machines. Remediate any findings within MS Defender for Cloud

Multi-cloud sec: Connect accounts from AWS and GCP to protect resources and workloads on those platforms

Hybrid sec: Unified view across all on-prem and cloud workloads

Threat protection alerts: monitor networks, machines and cloud services for incoming attacks and post breach activity

Track compliance: MS Defender for Cloud assesses hybrid cloud environment to analyse risk factors according to controls and best practices in Azure Security Benchmark.

Access and application controls: Block malware and other unwated applications via ML powered recommendations.

Azure Security Benchmark & Sec Baselines for Azure

MS has found that using security benchmarks can help orgs quickly secure their cloud deployments and reduce risks. The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations. You can find the sheet on GitHub: [Azure Security Benchmark V3](SecurityBenchmarks/Azure Security Benchmark/3.0 at master · MicrosoftDocs/SecurityBenchmarks · GitHub)

Some key points of ASB V3 are:

- ASB ID - Every line item in the ASB has an identifier mapped to a recommendation
- Control domain - ASB control domains include network security, data protection, identity management, priviledged access, incident response, and endpoint security as a few examples
- Mapping to industry frameworks - ASB recommendations map to pre-existing ones such as Center for Internet Security (CIS), National Institute of Standards and Technology (NSIT), and Payment Card Industry Data Security Standards (PCI DSS)
- Recommendations - each one captures specific functionality associated with the control domain area and is itself a control. The Network Security control domain has NS-1 through 10.

Security Baselines

Security baselines for Azure apply guidance from the ASB to the specific service which it's defined. As an example, the sec baseline for Azure AD applies guidance from the ASB V2 to Azure AD. Each Azure Sec Baseline includes the following:

- Azure ID - the ASB ID that maps to the recommendation
- Azure control - content is grouped by control domain area
- Benchmark recc - maps to recc for associated ASB ID

- Customer guidance - rationale for recc links to guidance on how to implement it
- Responsibility: Who is responsible for implementing control? Customer MS, or shared?
- MS Defender for Cloud - does MS Defender for Cloud monitor the control?
-