

IT MANAGERS REGION 9 SEMINAR

Day 1 - Session 5

Microsoft 365 / Azure Security Dashboard

Presenter: Joey Cusimano

STACS

Tuesday, September 22, 2026

Session focus	Microsoft 365 security architecture, Entra ID, MFA, Conditional Access, Intune, Defender, Defender for Endpoint, Azure/Defender for Cloud, Secure Score, vulnerability evidence and recurring SecOps review.
Document style	Detailed organized seminar notes. Discussion is consolidated by subject rather than reproduced as a running transcript.

Key Takeaways

- The session was a practical map of where Microsoft's identity, device, endpoint and cloud security controls live.
- Joey emphasized using the evidence behind a finding - paths, versions, CVEs, registry entries and logs - rather than treating dashboard scores as self-explanatory.
- The recurring SecOps checklist ties the tools together into a repeatable administrative process.

1. Microsoft Cloud Security Terminology

Joey began by separating Microsoft services that are often grouped together in casual conversation. Microsoft 365 is the productivity suite - Outlook, Teams, SharePoint, OneDrive and Office applications. Entra ID, formerly Azure Active Directory, is the identity layer. Intune is the device-management layer. Defender is the security family, and Azure is Microsoft's general cloud-computing platform.

Defender for Cloud focuses on Azure resources and their security posture. Defender for Endpoint is the modern evolution of the Windows endpoint-protection product and reports endpoint security and vulnerability information into Microsoft's centralized security experience.

2. From Traditional On-Premises Management to Cloud Services

The presentation contrasted older on-premises patterns - local Active Directory, local Exchange, Group Policy/SCCM and physical servers - with their cloud equivalents. Entra ID handles cloud identity, Exchange Online handles hosted email, Intune can manage devices and configuration, and Azure can host infrastructure and applications.

This was not presented as meaning every office must immediately abandon on-premises systems. The purpose was to understand where each Microsoft control lives when an office operates a hybrid or cloud-oriented environment.

3. Entra ID, MFA and Conditional Access

Entra ID is where administrators review accounts, authentication and sign-in activity. MFA was presented as a baseline control, but the discussion also addressed the limitations of weak or fatigue-prone MFA methods.

Conditional Access provides more granular enforcement than broad default settings. Policies can consider the user, device, location, application and authentication strength before granting access.

Sign-in logs are an important investigative source because they show successful and failed attempts, device/browser information and geographic indicators that can help identify unusual activity.

4. Intune and Device Management

Intune can enroll and manage Windows PCs and mobile devices, apply configuration, control access and report device state. It can take over some tasks historically performed with Group Policy or local management tools.

For an office considering Intune, the operational question is not simply whether the product exists but which settings should be managed in Intune versus existing Group Policy or other tools. Duplicate/conflicting policy paths can make troubleshooting harder.

5. Defender Portal and Defender for Endpoint

Joey showed the Microsoft Defender portal as a unified security location rather than the old idea of Windows Defender as only a local antivirus program. Defender for Endpoint reports endpoint findings, vulnerabilities, software inventory and security recommendations back to the central portal.

This centralization is particularly useful when an administrator needs to understand whether a finding affects one machine or many and whether the issue is an active executable, an old file or a stale registry entry.

6. Vulnerability Evidence and Software Inventory

The demonstration showed that Defender can provide evidence behind a vulnerability finding, including file paths, software versions, CVE references and sometimes registry information.

That detail matters because simply knowing 'a vulnerability exists' is not enough to remediate it. An administrator may discover that the vulnerable version is a portable copy left in a user folder, an obsolete runtime that another program no longer needs, or a registry artifact from software that was already removed.

Software inventory can also reveal multiple installed versions of frameworks or development tools. The administrator can then determine which version is active and which can safely be removed.

7. Microsoft Graph and PowerShell

Joey discussed Microsoft Graph as the API layer for Microsoft 365 information. Graph can be queried from PowerShell to retrieve data such as sign-in and audit logs without relying entirely on the portal.

This is useful when the portal is slow, when the same investigation must be repeated, or when the administrator wants to filter and export exactly the fields needed for a report.

The examples included selecting specific properties, working with JSON results and producing more readable output for security review.

8. Sign-In Investigation and Location Review

One practical use case is retrieving a user's sign-ins over a defined period and reviewing successful/failed activity, locations and other indicators. The administrator can flag countries or locations that are inconsistent with expected use.

The presentation treated location as an investigative clue rather than proof by itself. Cloud services, VPNs and provider infrastructure can affect the location recorded in logs, so the sign-in needs to be interpreted with the rest of the evidence.

9. Defender for Cloud and Azure Security

Defender for Cloud applies security recommendations and secure-score concepts to Azure-hosted resources such as virtual machines and managed services. Its view is broader than the configuration of a single endpoint because it also considers networking and relationships among cloud resources.

Some recommendations overlap with controls that can be configured through Group Policy, Intune or another management plane. The office needs to decide where the authoritative configuration should live.

10. Secure Score and Achievable Score

Secure Score provides a prioritized list of recommended security improvements. Joey emphasized that the number should not be treated as a permanent grade because Microsoft continually changes recommendations, weighting and product interfaces.

A score can therefore move even when the office did not intentionally weaken security. The useful part is the underlying recommendation list and whether each recommendation is applicable, already addressed another way, or requires an exception.

The discussion of achievable score reinforced that not every recommendation is necessarily appropriate for every environment. The office should understand what is realistically applicable rather than chasing a number without context.

11. Service Accounts and Practical Exceptions

Some Microsoft recommendations assume an interactive user and do not fit automation or service accounts. For example, a service account may not be able to complete an interactive MFA prompt without redesigning the service.

The appropriate response is to understand and document the exception, reduce the account's privileges and exposure where possible, and avoid pretending that a recommendation has been implemented when the application cannot support it.

12. Recurring SecOps Review

Joey closed the material by showing how these tools can be brought into a recurring security-operations review. The purpose is to look for exceptions that otherwise sit unnoticed: vulnerable software, pending updates, devices waiting for restart, unusual sign-ins and unresolved recommendations.

A weekly cadence was demonstrated, but the larger lesson was repeatability. An office can choose another interval as long as the review is performed consistently and findings are tracked to resolution.