Microsoft's Recommendations for Mature Configuration Management for Microsoft 365

Microsoft on the Risk of Tenant Misconfigurations:

Cybercriminals leverage misconfigurations when executing data breaches. Without dedicated configuration management, there is no way to detect when your Microsoft 365 security configurations are mistakenly or purposefully changed.

According to Microsoft's Digital Defense team:

- 40% of ransomware attacks exploited Entra Misconfigurations[1]
- 30% drop in quality of Microsoft threat detection when Defender is misconfigured[2]
- 300% increase in device compromise if Microsoft Intune is not properly configured[3]

Having a way to detect when configurations drift from your ideal state will massively enhance your cybersecurity efforts and help your hard-working security teams move on to other critical cybersecurity tasks.

What Microsoft Recommends:

MICROSOFT RECOMMENDS A ROBUST CONFIGURATION CHANGE MANAGEMENT PROCESS:

Microsoft recommends that all customers find a way to introduce mature configuration change management processes:

"It is critical that alterations to the intended configuration of a Microsoft tenant are subject to robust configuration change management processes." [4]

Implementing configuration change management in Microsoft 365 requires organizations to set up Dev and Test tenants that precisely replicate the configurations of their Production tenants.

This requires HUGE operational overhead without the ability to deploy consistent configurations across multiple tenants.

MICROSOFT RECOMMENDS SECURITY CONFIGURATION BASELINING:

Microsoft recommends that all customers find a way to baseline their configurations so that they can deploy them securely across multiple tenants, and detect drift:

"Adhere to security configuration baselines and best practices when deploying and maintaining identity systems, such as Entra ID infrastructure." [5]

Microsoft report that 43% of attacks are the result of “insecure Entra ID configuration” – something that can only be detected with a built-for-purpose configuration management tool.

MICROSOFT RECOMMENDS COREVIEW FOR THEIR CUSTOMERS:

Microsoft has recommended that customers consider CoreView as a solution to strengthen the security of their Entra configurations.

CoreView also works closely with the Microsoft solutions team who recommend us to customers who are concerned about security and governance in their tenant. For more information, you can see details about our partnership practice here.

CoreView is now an AI Microsoft Azure Cloud Partner, listed on the learn.microsoft list of approved SaaS vendors, and available for purchase on the Azure Marketplace.

[1] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[2] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[3] https://www.microsoft.com/en-us/security/blog/2022/08/22/cyber-signals-defend-against-the-new-ransomware-landscape/

[4] https://learn.microsoft.com/en-us/entra/architecture/recover-from-misconfigurations

[5] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023