Cisco Security Suites & Microsoft E3:E5 – Better Together

Partner
https://cs.co/1page

Microsoft E3 provides basic security features including multi-factor authentication (MFA) for cloud apps, AV protection with Defender for Endpoint, and basic phishing and spam filtering for email. This level of security is often insufficient for many organizations' overall security posture, leaving gaps that require additional protection.

Benefits:

Enhance your security with Cisco Suites: Layering the Cisco Suites on top of an existing Microsoft E3 solution can maximize the value of existing security investments and fortify your organization against advanced threats.

- **Zero Trust Access:** Cisco Secure Access, a Security Service Edge (SSE) solution includes Secure Internet Access with Secure Private Application Access.
- **Email Security:** Cisco Secure Email Threat Defense (ETD) maximizes your email security investment by augmenting your Microsoft environment with threat protection.
- **Device Access Control:** Cisco Identity Services Engine (ISE) authenticates and authorizes all devices that connect to the network.

Benefits of Consolidation: Reduced spend, Reduced security personnel, Simplified procurement, Improved Security, Improve posture.

Conversation Starters:

- How are you handling threat detection across your network, endpoints, email, and cloud environments?
- How are you currently using Microsoft 365 (E3/E5) for productivity and security?
- Have you identified any applications or use cases where Microsoft’s built-in security falls short, creating a need for additional solutions?
- Are you relying solely on Microsoft's built-in antispam and antimalware, or are you looking for additional layers of protection?

Identify an Opportunity:

- Understand where the customer is at in their Microsoft journey – did they just purchase, or do they have an upcoming renewal?
- What tools within their MS suite is the organization actively utilizing vs. what is shelfware?
- Organizations struggle to integrate or implement various point products.
- Key areas to listen for: identity, endpoint, email, XDR.
- Identify where your customer sees a weakness in the Microsoft solutions.

Cisco Protection Suites vs E3 & E5:

	Capabilities:	User & Breach Prot. Suites	MS E3	MS E5
Identity Security	Basic MFA	✓	✓	✓
	Phishing resistant MFA	✓	Requires Windows Hello	Requires Windows Hello
	Identity visibility (ISPM & ITDR)	✓		Microsoft Data Only
	Machine Identity (IoT)	✓		
Secure Service Edge	Secure Internet + Secure Private Access (ZTNA + VPNaaS)	✓		
	Digital Experience Monitoring	✓		
	CASB / DLP	✓		✓
	Network Access Control (NAC)	✓		
Threat Prevention	Email spam filter, anti-malware, volume phishing detection	✓	✓	✓
	Email obfuscation detection (URLs, QR Codes)	✓		✓
	Business Email Compromise Detection (BEC)	✓		No Internal Scanning
	Basic endpoint malware detection (AV)	✓	✓	✓
Threat Detection	Endpoint Detection & Response (EDR)	✓		✓
	Advanced malware detection, behavioral analysis	✓		✓
	Extended Detection & Response (XDR)	✓		No Network Detections
	Network Detection & Response (NDR)	✓		

Email Threat Defense vs E3 & E5:

	Capabilities:	Email Threat Defense	MS365 E3	MS365 E5
Basic (Core) Email Security	SPAM Detection	✓	✓	✓
	Malware Detection (AV)	✓	✓	✓
	Malware Behavioral Analysis (Sandboxing)	✓		
	Malicious URLs Detection	✓		✓
	Malicious URLs Sandboxing	✓		
	Anti-Phishing Policies	✓		✓
	Phishing Detection	✓		✓
Advanced Threat	Advanced Threat Analytics	✓		✓
	Obfuscated URLs, QR Codes and File Detection	✓		✓
	Scam Detection	✓		✓
	Business Email Compromise Detection	✓		✓
	User Impersonation Detection	✓		✓
AI and Machine Learning	Natural Language Processing (NLP)	✓		✓
	Behavioral Analysis Models	✓		✓
	Phishing Detection Models	✓		✓
	Impersonation Detection Models	✓		✓
	Relationship Graphs	✓		✓
Threat Resp.	Manual Message Remediation	✓		
	Automated Investigation and Response	✓		✓

Resources:

User/Breach Suite & MS Call Guide
Cisco & Microsoft Better Together
Advanced Threat Protection for MS365
Cisco Security Suites + MSFT E3:E5