Workplace Security & Resilience:

Strengthening Security with Cisco Breach Protection Suite and Microsoft 365

The challenges of securing the modern workplace

Identifying and stopping the most complex and damaging threats has become increasingly challenging. More sophisticated threats can overwhelm security operations teams that don't have the advanced capabilities to re-mediate threats quickly and accurately.

Nearly 40% of incidents
involve ransomware, pre-ransomware, and data theft extortion

25% of ransomware incidents
involve misconfigured or missing Endpoint Detection and Response (EDR) solutions.

Organizations need solutions that collect and correlate data and telemetry across multiple sources – network, cloud, endpoint, email, identity, and applications – to provide unified visibility and deep context into advanced threats.

Do you know your security gaps?

Organizations today operate as intricate networks of users, devices, data, and applications, all interconnected in ways that drive innovation and efficiency.

With that complexity comes a heightened risk that threats are harder to pinpoint and defend against, leaving businesses exposed to ransomware and new, unpredictable attacks.

Disparate security products guard against individual attack vectors but lack holistic protection

To improve security posture, simplify management, and enhance threat protection, organizations should look to trusted vendors and platform-level integration to achieve the best combination of comprehensive networking, cloud, security, and productivity capabilities.

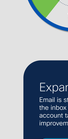
Security that unlocks the maximum benefits of Microsoft 365

Microsoft 365 is a massive target for cybercriminals with over a million organizations worldwide using it as an essential solution for their day-to-day operations. The productivity and connectivity that Microsoft 365 provides makes businesses work better. However, organizations need to secure their users, their tools, and their data to get the maximum impact.

Some "core" security tools are included within an E3 license:

Devices:
Anti-Virus protection with Defender for Endpoint P1

Email:
Basic phishing and spam filter



But is this basic security sufficient for an organization's overall security posture? For many organizations, security gaps remain, requiring additional protection.

Let's explore the answer to that question and look at the reasons you should layer Cisco Breach Protection Suite on top of your existing Microsoft 365 license.

Why you need additional protections to go with your Microsoft investment:

Vulnerable endpoints:

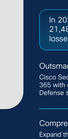
The amount of endpoints are greater than ever before–as is the variety. Prevention-focused anti-virus has proven ineffective and is insufficient to stop modern threats. Organizations need advanced Endpoint Detection and Response (EDR) tools for behavioral-based detection, response, and recovery from security threats.

Advanced email threats:

Basic protections do not stop threats like advanced spear phishing, account take over, and Business Email Compromise (BEC). IC3 reported BEC in all 50 US states and 186 countries.[1]

Multi-vector Threats:

Multi-vector threats target organizations through a combination of attack surfaces – including endpoints, email, networks, identities, clouds, apps and more – making them harder to detect and contain. Security teams often struggle to connect the dots across siloed tools, leading to delayed response times and missed threats



Platform security that increases simplicity and reduces costs.

Cisco Breach Protection Suite provides a comprehensive cybersecurity solution that enhances detection and response capabilities by unifying visibility, prioritizing and contextualizing threats, and empowering analysts to achieve new levels of efficiency.

Expansive Protection for Outlook

Email is still one of the top threat vectors. Protecting the inbox against phishing, BEC internal threats, and account takeover should be at the top of every security improvement to-do list.

In 2023, the IC3 received 21,489 BEC complaints with adjusted losses greater than 2.9 billion.[2]

Outsmart email threats with Secure Email Threat Defense

Cisco Secure Email Threat Defense maximizes your email security investment by augmenting Microsoft 365 with comprehensive, AI powered advanced threat protection. Deployed in minutes, Email Threat Defense sits behind your gateway to detect and block dangerous and damaging threats.

Comprehensive email protection

Expand the scope of your defenses to identify malicious techniques and rapidly search for and remediate threats.

Key capabilities:

Sophisticated AI-led detectors

File reputation and analysis

Sender reputation

URL reputation

Content scanning

Relationship graphs

Move to complete visibility and protection for all messages

Secure Email Threat Defense has complete visibility of inbound, outbound, and internal messages.

Using numerous AI models, it can:

- Uncover known, emerging, and targeted threats with sophisticated, AI powered threat detection capabilities.
- Identify malicious techniques and gain context for specific business risks.
- Rapidly search for dangerous threats and remediate all threat instances in real time.
- Utilize searchable threat telemetry to categorize threats and understand which parts of your organization are most vulnerable to attack.

Cisco XDR natively integrates telemetry from Cisco Secure Email Threat Defense and utilizes user accounts as an asset for correlation. All threat verdicts from Email Threat Defense are a part of Cisco XDR's incident attack chains.

Advanced Endpoint Protection, Detection and Response Across Control Points

Traditional anti-virus and endpoint protection platforms (EPP) often fall short in providing comprehensive threat detection and response. Organizations are increasingly turning to Endpoint Detection and Response (EDR) solutions to quickly identify and counteract sophisticated threats.

With evolving threats such as malware mutation, polymorphism, fileless malware and AI-enhanced attacks, signature-based detections are no longer sufficient for robust security. Organizations need advanced capabilities to detect known threats and adaptively respond to new and emerging threats targeting endpoints.

Stop threats before they compromise your business

The sooner businesses detect threats, the faster they can recover. Cisco Secure Endpoint offers powerful EDR capabilities to counteract threats effectively:

1. Advanced Analytics: Leverages analytics across the Cisco portfolio to make informed decisions on blocking both known and emerging threats.
2. Dynamic Threat Response: Continuously evaluates and adapts device security postures to ensure the highest level of trustworthiness, reducing the risk of breaches.
3. Proactive Threat Blocking: Automatically prevents device access if malware is detected, stopping potential breaches before they occur.

Memory Randomization

Dynamically changes system configurations and attributes to confuse attackers, essentially making the target "move" to avoid being hit. Doing so makes it significantly harder for adversaries to identify and exploit vulnerabilities.

Orbital Queries & Scripts

Utilize advanced querying to gain in-depth insights and visibility into endpoint activities, enabling rapid identification and response to potential threats.

Talos Advanced Threat Hunting & Threat Intel

Intelligence gathered from continuously analyzed malware and threat actor groups helps to uncover new types of threats and create behavioral and forensic profiles for emerging risks, known as Indicators of Compromise (IoCs).

Fast, Effective Threat Detection and Response

Focusing on attacks that target Microsoft 365 isn't enough. With a narrow view, you could miss signs of an attack. Organizations need a simplified approach to security operations where security teams can effectively detect, investigate, and remediate threats across their entire environment.

Cisco XDR gives you comprehensive visibility into sophisticated threats by seamlessly integrating with Microsoft products like Office 365, Defender, and Entra ID, as well as a wide variety of Cisco and third-party security tools across network, endpoint, identity, cloud, email, applications, and more.

This unified view of threats helps you focus on the most critical attacks and quickly understand complex connected attacks that span multiple threat vectors. Moreover, built-in automation, AI-driven remediation, and robust orchestration capabilities in Cisco XDR help you automate repetitive tasks, quickly mitigate threats, and improve security analyst productivity across your environment.

With Cisco XDR, your organization will:

Detect the most sophisticated threats in multi-vendor and multi-vector environments with enriched incidents, asset insights, and threat intelligence.

Act on what truly matters, faster and with more accuracy, with prioritized threats for streamlined investigations.

Elevate productivity by filtering out the noise, automating manual tasks, and boosting the efficiency of your security team.

Short on capacity or expertise? Realize the power of Cisco XDR faster.

A managed services engagement can help when you're short on capacity or expertise to plan, deploy, and provide 24x7 security monitoring, detection, and response based on Cisco XDR.

Managed Detection and Response (MDR) is backed by an elite team of Cisco security experts and certified Cisco partners. Additional proactive services to assess your cybersecurity preparedness are also available, including Talos Incident Response, penetration testing, and security operation assessments.

Complement Office 365 with Comprehensive Defense

Microsoft 365 and Cisco Breach Protection Suite complement each other seamlessly, enhancing overall security and productivity for businesses. While Microsoft 365 offers powerful cloud-based collaboration tools like email, file sharing, and document management, Cisco Breach Protection Suite further bolsters its security capabilities.

Security is continually evolving. Together, Cisco and Microsoft create a robust security environment that prevents and responds to attacks quickly and consolidates for easier management. In combination, the technologies provide organizations with a comprehensive and adaptive solution for both productivity and cybersecurity.

Read more about the ways Cisco and Microsoft are better together.

1. https://www.ic3.gov/PSA/2024/PSA240911
2. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf