

# Workplace Security and Resilience:

How Cisco Security Suites and Microsoft Empower a Stronger Defense Strategy



## The challenges of securing the modern workplace

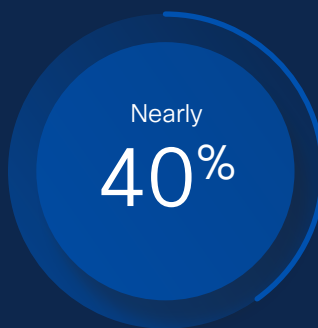
Changes in security strategy can be slow to implement. Even more so if safeguards might impact the end user experience. The struggle of dealing with the realities of hybrid work, half a decade after the coronavirus pandemic, proves it. Especially as we track how attackers make in-roads to sensitive data.

Organizations need solutions that can meet the modern security demands of hybrid workforces while still enabling productivity. To achieve this, security teams need to center efforts around data and people.



100%

of ransomware incidents, accounts did not have multi-factor authentication (MFA) or attacks bypassed MFA.<sup>1</sup>



Nearly  
40%

of incidents involved ransomware, pre-ransomware, and data theft extortion—in which cybercriminals steal and threaten to release victims' files or other data without using any encryption mechanisms.<sup>3</sup>



25%

of incidents involved password spraying and/or brute force attempts to steal valid credentials.<sup>2</sup>



25%

of ransomware incidents involved misconfigured or missing Endpoint Detection and Response (EDR) solutions.<sup>4</sup>

1 Cisco, [Talos IR Trends Q4 2024](#)

2 Cisco, [Talos IR Trends Q3 2024](#)

3 Cisco, [Talos IR Trends Q4 2024](#)

4 Cisco, [Talos IR Trends Q4 2024](#)





## 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—security vulnerabilities are harder to pinpoint and protect against, leaving businesses exposed to threats like ransomware and new, unpredictable attacks. So how can organizations provide seamless, secure access without the luxury of abundant resources or specialized expertise?

Disparate security products guard against individual attack vectors but lack holistic protection. To improve security posture, simplify management, and enhance the user experience, organizations should look to trusted vendors and platform-level integration to achieve the best combination of comprehensive networking, cloud, security, identity, and productivity capabilities.

## Security that unlocks the maximum benefits of Microsoft 365

Microsoft 365 is a massive target for cybercriminals. According to estimates, over a million companies worldwide use Microsoft 365 as an essential for day-to-day business.<sup>5</sup> The productivity and connectivity that Microsoft's product provides makes businesses work better. However, in order to have maximum impact, users, their tools, and data need to be secure. That's why the tech giant includes some "core" security tools within an E3 license:

- **Identity:** Multi-factor authentication (MFA) for cloud applications
- **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.

In this eBook, we will explore the answer to that question and why you should layer Cisco User Protection and Breach Protection Suites 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 is greater than ever before—as is the variety. Prevention-focused anti-virus has been proven ineffective and it is insufficient to stop modern threats. Organizations need Advanced Endpoint Detection and Response (EDR) tools for their ability to perform behavioral-based detection, response and recovery from security incidents.

**Advanced email threats:** Basic protections do not stop threats like malicious QR codes, account take over, and Business Email Compromise (BEC). IC3 reported BEC in all 50 US states and 186 countries.<sup>6</sup>

**Security Service Edge (SSE):** Only having one or some of the security functions that combine to form SSE, such as Zero Trust Network Access (ZTNA), a secure web gateway, or cloud access security brokers, isn't enough when the number of connected identities and devices continues to grow.

**Identity visibility gaps:** To clearly understand the blast radius of an identity-related attack and cut down remediation time, you need insights across the identity ecosystem—not only across applications.

**Contractors/Third parties:** Third-party contracting used to be a niche approach. Today, it's growing in popularity for modern, agile companies. However, it introduces many new edge cases that are accessing an organization's resources and creating identity complexities.

<sup>5</sup> Statista, [Number of companies using Office 365 worldwide as of February 2024](#)

<sup>6</sup> IC3, [Business Email Compromise: The \\$55 Billion Scam](#), September 2024

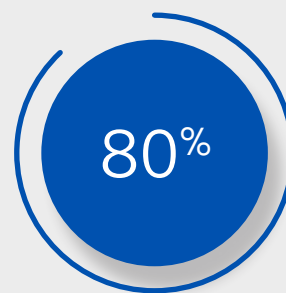




## Zero Trust: Protecting all users and devices to achieve workplace security

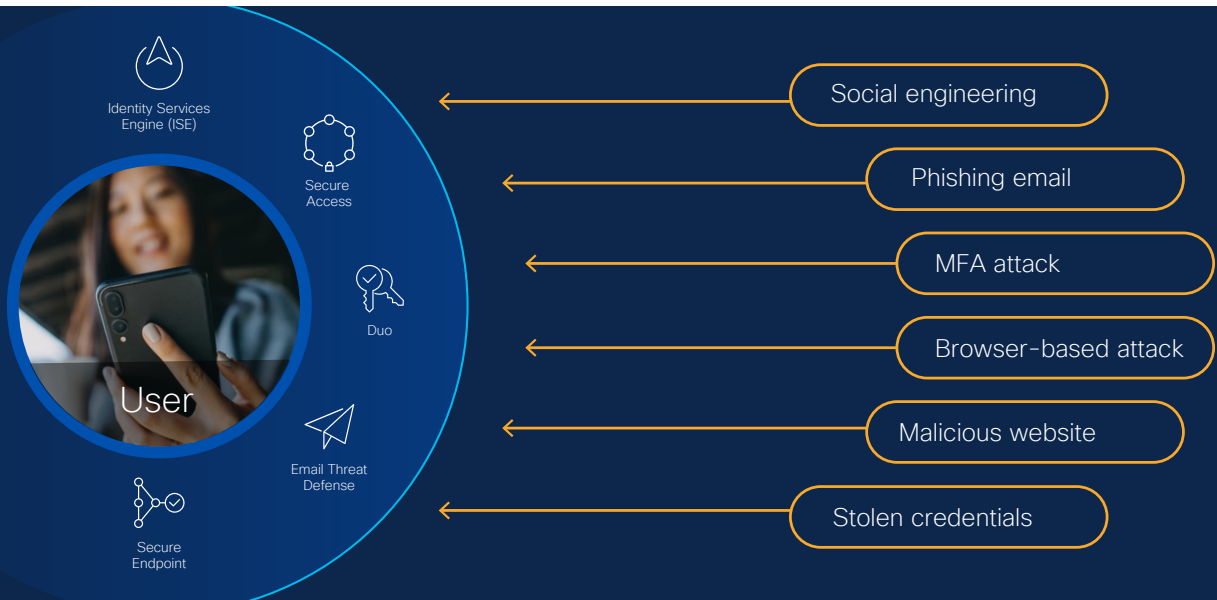
Protecting users has long been a crucial priority to safeguard organizations. That's why companies of all sizes today are asking where they should start or what to do next in their Zero Trust journey.

Zero Trust adoption increases security resilience for organizations at every access decision. The security model evaluates risk and verifies trust continually before granting least-privilege access.



80% of all breaches result from attackers targeting users, including stolen credentials, social engineering, privilege misuse, or user error.<sup>7</sup>

<sup>7</sup> [Cisco Talos Incident Response data 2023-2024](#)



## Frustrate attackers, not users.

Attackers have learned that it's easier to log in than break in. That's why they are accelerating their identity-driven attacks across various operations, with credential theft often being their primary objective.

Organizations need an approach that both continually verifies identities while also keeping users productive inside Microsoft 365, where they spend much of their workday.

Microsoft provides the necessary IT infrastructure for users to get to work, including Windows software and user identities. In order to protect the software, devices, and identities within a Microsoft ecosystem, organizations are implementing Zero Trust strategies. This is essential. We should not presume that if an identity logs in, that it has initiated the session. If that identity is given access to all applications and services after one verification, it could be an entry-point for attack.

More than 86% of respondents in a recent survey shared that their organizations have already begun moving to Zero Trust. The downside is that only 2% have achieved maturity across Zero Trust pillars.<sup>8</sup>

## How will you implement Zero Trust?

While Zero Trust is a strategy, rather than a product that organizations can buy, most organizations prioritize deployment of technologies, such as MFA and ZTNA. These technologies, along with a Zero Trust roadmap, enable organizations to implement protections without harming end user productivity.

<sup>8</sup> Cisco, [Security Outcomes for Zero Trust](#)

## Broad Identity Visibility and Protection

Protecting identities is a top concern across the Microsoft ecosystem and beyond.

Threat actors launching internal attacks from compromised, valid accounts are difficult to detect. Once they compromise an account, they can carry out a variety of malicious activities including, account creation, escalating privileges to gain access to more sensitive information, and launching social engineering attacks, like BEC, against other users on the network.

End users don't care how they authenticate; they just want to get to work. While working towards Zero Trust, organizations often get stuck on how to connect per user, per service, and per application level. There are too many variables. How do you manage all of that and progress in your Zero Trust initiative?

### Correlate identity data. Detect attack patterns.

With Cisco, Identity Intelligence ingests data across your environment, including your identity provider, SaaS applications, HR resources, and more. This allows us to determine potential vulnerabilities like info stealers and attackers who are exploiting software, application, and service vulnerabilities.

Recent attacks have highlighted the dangers of adversaries chaining identity-based attacks. In one case, the actors gained initial access, obtained credentials and implanted web shells on victim networks.

## Is your identity security enough?

Microsoft offers both MFA and conditional access, but do you need more? Based on hundreds of security assessments conducted by Cisco, the answer is likely, "yes." Insights show that even when customers say, for example, that they require all users to have MFA, there are errors in conditional access where it accidentally exempted a group from MFA. Or, unbeknownst to them they have weak forms of MFA with SMS/Telephony in use by a group of users.

## Putting MFA to the test

During a major worldwide sporting event, a red team/blue team exercise included testing of identity protection. Microsoft offers MFA, and base protections, but when the red team was constantly able to get into accounts using compromised identities found on GitHub, the blue team was at a loss. When Cisco used Identity Intelligence along with existing protections, the root cause of the account takeover was able to be identified and stopped.

## Cisco helps you identify your gaps:

Changes in security strategy can be slow to implement. Even more so if safeguards might impact the end user experience. The struggle of dealing with the realities of hybrid work, half a decade after the coronavirus pandemic, proves it. Especially as we track how attackers make in-roads to sensitive data.

- Cross-platform identity context feeds both security posture insights and a dedicated threat detection engine that is optimized and managed by experts.
- Identity posture analysis uncovers vulnerabilities—like MFA misconfigurations, dormant accounts, and overprivileged administrators—that can be proactively resolved.
- Smart detection leverages AI and ML to highlight anomalous and suspicious identity behavior.
- Tools easily allow you to map threats to security frameworks like MITRE ATT&CK and CIS.

40% of incidents bypassing MFA were because of improper MFA implementation.<sup>9</sup>

## Close your identity gaps

Cisco Duo provides flexible authentication options on an extensive set of use cases, to enable seamless access for trusted users and stop attackers from logging in.

The synergy between Identity Intelligence and Duo is clear. Identity Intelligence correlates data to highlight security gaps and risks. Duo then protects those vulnerabilities.

9 Cisco, [Talos IR Trends Q4 2024](#)

Even for the hardest use cases, Cisco Duo is ready to protect.



Broad coverage



Protects legacy use cases like VPN and firewall policies



Phishing resistant authentication



Uses biometric or passwordless authentication to step up the authentication workflow in real time



Risk-based authentication



Evaluates potential threat signals at each login attempt and uses automated responses to block the attacker and secure trusted users



Pair authentication with device trust policies



Verifies device health before granting access



## Comprehensive SSE with Cisco Secure Access

Many organizations struggle to reduce VPN usage and evolve to ZTNA, opting to modernize certain applications while leaving others unchanged. This creates management and user experience headaches, plus security gaps. That's why advancing your Zero Trust strategy, in a way that is built for the real world, is crucial. Cisco helps you make meaningful progress in your Zero Trust journey with SSE capability that comprehensively strengthens your security posture.

### Microsoft recommends third-party SSE

SSE provides an avenue toward consolidating secure access to Microsoft applications, all other internet traffic, and SaaS applications. According to Microsoft's Tech Community Blog, "you can choose to rely on Microsoft Entra Internet Access for the unique security and visibility capabilities for Microsoft 365, while keeping all your other internet traffic and SaaS apps protected by another SSE solution of your choice."<sup>10</sup>



### SSE that's identity aware

To support your productivity applications, Cisco Secure Access consolidates key security technologies into one unified, cloud-delivered platform.

- Close the gap between authentication and access for stronger Zero Trust security.
- Ease the path from VPN to ZTNA with VPNaaS (VPN as a Service) using a single client, single console, and single policy. Protect all apps—even those not ready for ZTNA in a way that's transparent to users.

- One dashboard, one client for integrated Secure Internet Access and Secure Private Access
- Fix performance issues fast—from endpoint to app, and anywhere in between—with integrated digital experience monitoring.

<sup>10</sup> Microsoft, [Microsoft Entra Internet Access: An identity-centric Secure Web Gateway solution](#), September 2023

## Cisco SSE consolidates security functions and enables productivity

By choosing an identity-centric SSE like Cisco's, you can consolidate vendors, enforce policies from a single dashboard and client, and protect Microsoft 365 and your entire environment, while eliminating the need to purchase Microsoft add-ons.

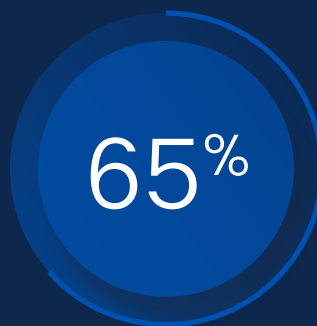
## Protect users and things as they securely connect. Be sure you have:

- ✓ Internet Access
  - ✓ SWG
  - ✓ DLP + CASB
  - ✓ Remote Browser Isolation
  - ✓ FWaaS + IPS
  - ✓ DNS-layer security
- ✓ Private Access
  - ✓ Clientless ZTNA
  - ✓ VPNaaS
  - ✓ Digital Experience Monitoring

## Benefits of consolidation



of customers are seeking to consolidate vendors<sup>11</sup>



Improve posture



Improve security

<sup>11</sup> Source: Gartner, Top Trends in Cybersecurity – Survey analysis. Feb2023 Dionisio Zumerle, John Watts

## 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.

### 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
- Spam protection

### 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 advanced 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) lack threat detection and response capabilities. That's why organizations are adopting EDR to detect and respond to advanced threats quickly.

Malware mutation, polymorphism, fileless malware, and AI-enhanced threats are some reasons why signature-based detections are no longer enough to secure. Organizations need the capability to detect known threats, plus be agile enough to pivot around potential threats that target endpoints.

### Stop threats before they compromise your business

The sooner businesses detect threats, the faster they can recover. Here are three ways Cisco stops threats with powerful EDR capabilities:

1. **Analytics** across the Cisco portfolio supports fast threat decisioning on blocking malware and emerging threats.
2. **Verifies a user's identity** through unified access security, MFA, and contextual user access policies to reveal if users are who they say they are. Since trust is neither binary nor permanent, security health checks constantly evaluate devices for trustworthiness.
3. **Blocks** users from logging into their account on a device if Secure Endpoint identifies malware.

## Level up your endpoint protection

Don't let stealthy threats through. Be sure you have what you need to detect, investigate, and remediate APTs that target your productivity suite.



### 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:

osquery uses the relational data model to represent an endpoint's entire operating system as a high-performance relational database, allowing you to write SQL queries to explore operating systems and device data.



### 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).

## Gain Ultimate Visibility and Control of Every Device on Your Network

The complexity of increasing usage of BYOD devices, work from home, and cloud applications doesn't have to keep you from your Zero Trust goals. Identity Services Engine (ISE) provides the ultimate visibility to every device on the network. It also gives you control to build visibility-based segmentation to support a Zero Trust framework.

As you move along your Zero Trust journey, ISE serves as the policy decision point. It gathers intel from the stack to authenticate users and endpoints, automatically containing threats.

Get a detailed review of every device:

- Snapshot of activity
- Unusual behavior
- Access denials
- And more

How ISE helps organizations follow the principles of least-privileged access and ensure that a device that is connected to the network cannot gain access to sensitive data.



Authenticates and authorizes all devices that connect to the network.



Assigns tags to these devices, including corporate devices, BYOD, and IoT devices, like cameras and printers.



Tags are integrated into Secure Access to enable organizations to create and enforce security policies across devices and users.

## Responsive Breach Protection

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 have access to correlated telemetry across the environment for comprehensive visibility into sophisticated threats—including productivity tools. Cisco XDR correlates data from a wide variety of security tools across network, cloud, email, endpoint, identity, and applications, including Microsoft products like Office 365, Defender, and Entra ID, to improve detection and response.

### 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, with prioritized threats for streamlined investigations.
- Elevate productivity by filtering out the noise, automating tasks, and boosting the output of your limited resources.
- Build resilience with actionable intelligence that closes security gaps and bolsters your defenses.

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

A managed services engagement can help when you are 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 or certified Cisco partners. Additional proactive services to assess your cybersecurity preparedness are also available, including Talos Incident Response, penetration testing, and [security operation assessments](#).





## Complete Your Zero Trust Strategy

Every technology vendor has its own strengths. Bring those capabilities together and organizations have the best of all worlds.

Microsoft 365 and Cisco's User and Breach Protection Suites 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's Suites further bolsters its security features.

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, adaptive, and user-centric solution for both productivity and protection.

### **Protect your identity infrastructure with a free identity security assessment.**

As you focus your security on data and people, and continue along your Zero Trust journey, you will need to first find your security gaps. Cisco offers a free identity security assessment to provide your organizations with a complete view of your security posture.

#### **Outcomes include:**

- A detailed view of all identities and devices logging into your network
- An analysis of your multi-factor authentication usage and adoption
- A snapshot of your total number of inactive accounts

Get started today with a free [identity assessment](#).

