Cisco and Microsoft 365: Making Them Better Together

Secure the Modern Workplace with Cisco Security Suites

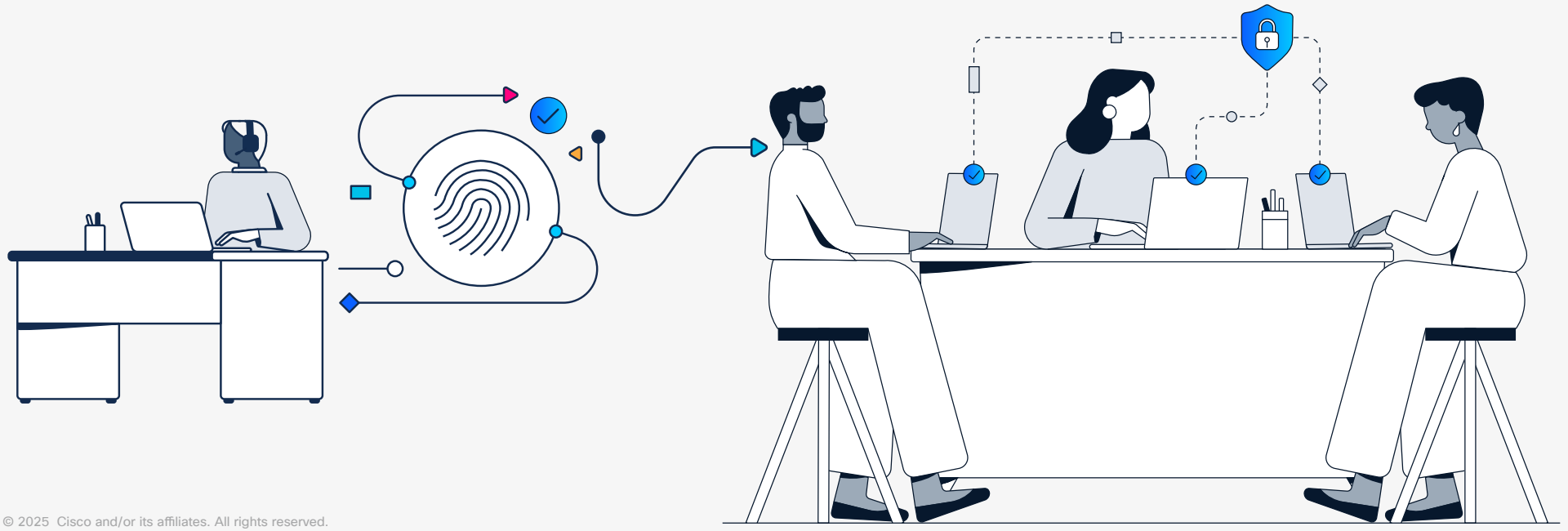
Challenges with securing the modern workplace

The way we work is changing. Organizations today are complex ecosystems with a mixture of remote and hybrid workers and diverse users, applications, AI, and devices. While these environments foster productivity, they can also be difficult to protect, leading to gaps in the attack surface, exposing organizations to ransomware and other unknown vulnerabilities, leaving organizations susceptible to an evolving threat landscape.

Organizations are faced with a difficult challenge: enable seamless and secure access, with limited budget, resources, and talent. That means investing in proactive protections for users, making progress on a zero-trust strategy, and implementing strong Extended Detection and Response (XDR) capabilities to protect against breaches while balancing financial considerations.

To add to these challenges, organizations are also struggling to manage disparate products that guard against individual attack vectors but fail to provide holistic protection. Therefore, to improve security posture, simplify management, and enhance user experience, organizations are looking to trusted vendors and platform-level integration and performance. For many organizations, this means leveraging both Cisco and Microsoft 365 for comprehensive networking, cloud, security, identity, and productivity capabilities.

For Cisco, this includes solutions from both the User Protection Suite and the Breach Protection Suite, including Cisco's Secure Access, Duo, XDR, and more.



Microsoft 365: IT infrastructure and productivity solution

The Microsoft E3/G3 solutions website notes: “connect and empower every employee across your organization with a Microsoft 365 solution that enhances productivity and drives innovation.” Organizations purchase E3/G3 licenses for many reasons. The most common is to provide the tools required to keep a business running. These include:

- **Identity Management:** Entra ID and Active Directory are used as the main identity provider (IdP) to store user information.
- **Device Management:** Organizations using Windows machines require Windows software to operate.
- **Email Security:** Microsoft 365 provides enterprise email solutions.

Because Microsoft wants to ensure their solutions are protected, they include some core security tools within an E3/G3 license.

- **Identity:** Multi-Factor Authentication (MFA) for cloud applications.
- **Devices:** Anti-Virus protection with Defender for Endpoint P1.
- **Email:** Basic phishing and spam filter.

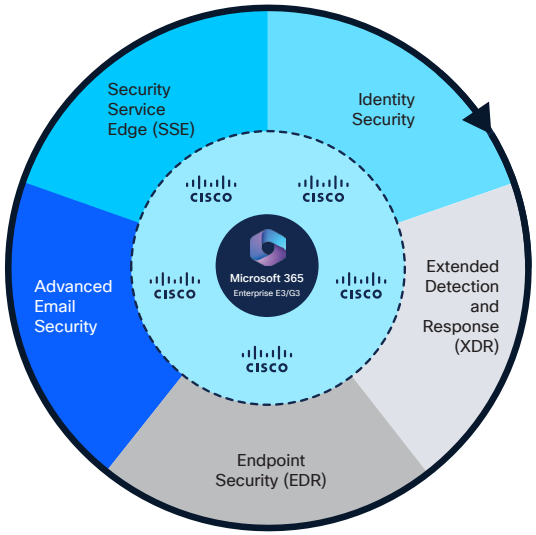
Microsoft’s tools are essential for day-to-day business operations, but if your organization is looking to execute a robust zero trust strategy with full threat visibility across your environment, that’s where Cisco comes in.

Enhance your security with Cisco Suites

Layering the Cisco User Protection and Breach Protection Suites on top of your existing Microsoft E3/G3 solutions can maximize the value of your existing security investments and fortify your organization against advanced threats.

Proactive user protection

- **Identity security:**
  - Cisco Identity Intelligence ingests data across your environment, including your identity provider, SaaS applications, HR resources, and more to determine potential vulnerabilities. Duo provides security first identity and access management capabilities, including phishing resistant authentication options on an extensive set of use cases, to enable seamless access for trusted users and stop attackers from logging in.
- **Zero trust access:**
  - Cisco Secure Access, a comprehensive Security Service Edge (SSE) solution includes Secure Internet Access with Secure Private Application Access. An integrated VPN-as-a-Service and Zero Trust Network Access (ZTNA) client and policies enables organizations to adopt Zero Trust Access on their timeline.
- **Email Security:**
  - Cisco Secure Email Threat Defense maximizes your email security investment by augmenting your Microsoft environment with comprehensive threat protection. Deployed in minutes, Email Threat Defense sits behind your gateway to detect and block dangerous emails including malicious QR codes, Business Email Compromise (BEC), and other advanced threats.



- **Endpoint detection and response:**
  - Secure Endpoint's Endpoint Detection and Response solution provides analytics across the Cisco portfolio to block malware and emerging threats. Working with Duo, it ensures only healthy devices can access corporate resources and prevents access when a threat is detected.
- **Device access control:**
  - Cisco Identity Services Engine (ISE) authenticates and authorizes all devices that connect to the network. ISE assigns tags to these devices, including corporate devices, BYOD, and IoT devices, like cameras and printers. Those tags are integrated in Secure Access to enable organizations to make security policies across their Cisco solutions.

Responsive breach protection

- **Email security:**
  - Secure Email Threat Defense is integrated with Cisco XDR and makes use of the user as an asset for correlation. All threat verdicts from Email Threat Defense are a part of Cisco XDR's incident attack chains.
- **Endpoint detection and response:**
  - Secure Endpoint, the native EDR for Cisco XDR, enhances security by enabling faster detection through shared incident generation, enhancing asset context with detailed endpoint information, prioritizing threats using extensive MITRE TTP mapping, and expediting investigations with the XDR ribbon and pivot menu. Additionally, it accelerates response with powerful workflows available through XDR automation.
- **XDR solution:**
  - Cisco XDR is a network-led, open Extended Detection and Response (XDR) solution that detects, prioritizes, and remediates threats to simplify security operations. It integrates with the Cisco Security portfolio, third-party offerings, and Microsoft products such as Defender, Intune, and Entra ID, to provide comprehensive visibility and holistic threat management.

Make Progress on your security maturity journey

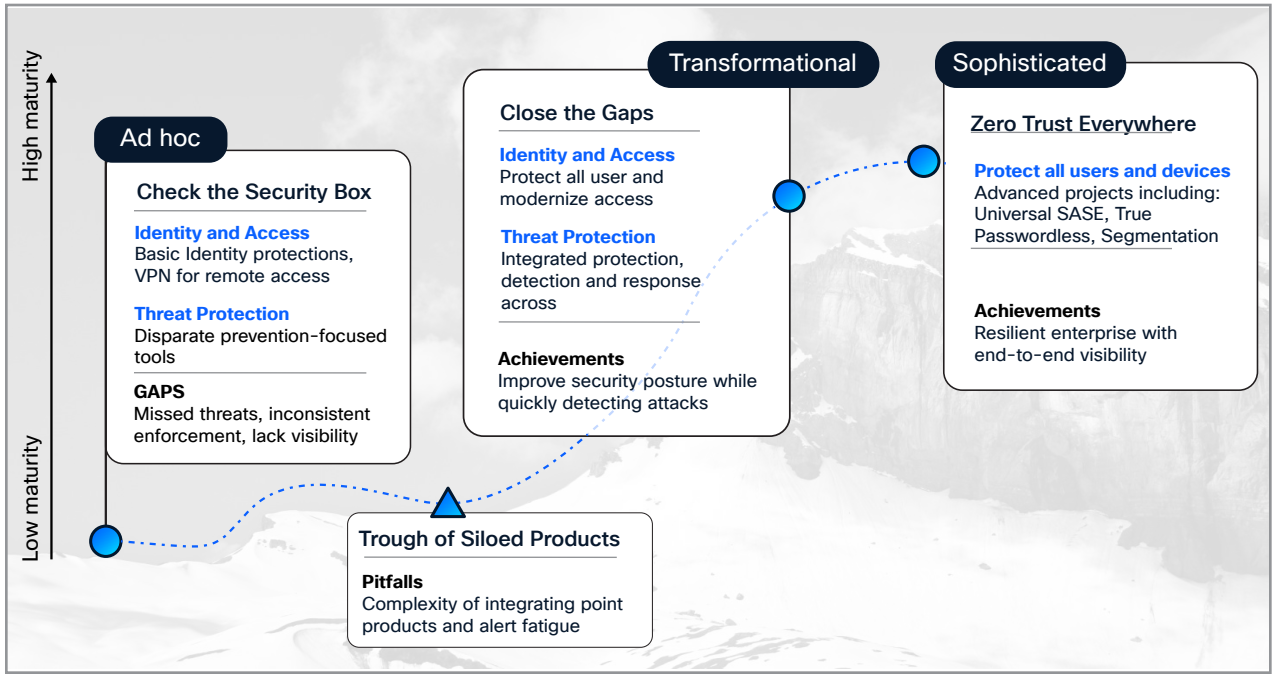
Organizations that are looking to improve security maturity with zero trust programs frequently hit roadblocks. According to Gartner, "**by 2028 30% of organizations will abandon zero-trust programs due to budget constraints, cultural resistance, and vendor product value.**" (Gartner, Inc., Predicts 2025: Scaling Zero-Trust Technology and Resilience, Charanpal Bhogal, Wayne Hankins, Manuel Acosta, John Watts, March 21 2025).

For many organizations, the ultimate goal of implementing zero trust programs is to achieve cyber resiliency. While the attackers will never be eliminated, organizations can minimize the damage, ensure quick recovery, and bounce back to normal operations. However, for organizations that face challenges outlined by Gartner, they might fall back to "check the box" security to meet basic compliance requirements, and stall on the promise of security maturity.

Cisco can support those organizations with a platform approach to eliminate the complexities of integration, ensure consistent policy enforcement, and improve visibility into the environment. By consolidating point solutions down to Cisco's security platform, organizations benefit from an integrated solution and expert guided on-boarding services to rapidly operationalize the solutions.

As a result, organizations can close security gaps, and the security team can gain the breathing room it needs to tackle more advanced and strategic projects. Cisco does this by enabling advanced identity protection (including phishing-resistant MFA and identity posture visibility), modernizing access (such as VPN-as-a-service and ZTNA), and correlating data across endpoints, networks, and the cloud to reduce alert fatigue and enhance detection and response.

Example of security maturity journey



Begin your suite investment

Begin your Suite investment

Mix and match tiers of User + Breach Protection Suite to fit your needs

User Protection Suite

Essentials	Advantage Everything in Essentials Plus
• Secure Access **Essentials** (Secure Internet + Secure Private Access) • Duo **Advantage** • Email Threat Defense	• Secure Access **Advantage** (Secure Internet + Secure Private Access) • ISE **Premier** • Secure Endpoint **Advantage**

Breach Protection Suite

Essentials	Advantage Everything in Essentials Plus	Premier Everything in Essentials Plus
• Cisco XDR **Essentials** • Secure Endpoint **Advantage** • Email Threat Defense	• Cisco XDR **Advantage** • Secure Endpoint **Premier** • Secure Network Analytics • Cisco Telemetry Broker	• Cisco XDR **Premier** (Managed XDR) • Cisco Talos Incident Response • Cisco Technical Security Assessments

Cisco Services

In addition to Cisco products, services help Cisco partner with your organization to scope out deployment, plan your roadmap, and help your organization achieve your security goals. Through enhanced or premium services, you get a dedicated Customer Success Specialist to bring in technical experts and help guide you through best practices.

Cisco Support services for Security Software comparison

	Software Support Enhanced	Software Support Premium
Access: 24x7 access to Cisco TAC for software support	●	●
Response: Service response objective for severity 1 and 2 cases	30 minutes	15 minutes
Updates: Software updates for supported product	●	●
Tools: Knowledgebase and online access to resources, support tools, and product info	●	●
TAC engineer: Primary point of contact accountable for solution issue: single product, multi-product, and multi-vendor support coordination	●	●
Onboarding: Welcome email, kickoff and technical discovery meetings, best practices, Smart Account and Smart Licensing activation, configuration, deployment, and migration guidance	●	●
Technical adoption: Ongoing guidance for customer IT help desks, software feature adoption guidance, software update consultation, periodic configuration reviews	●	●
Designated service management: Cisco expert supports products in your environment, provides design and sizing guidance, and assists with managing the lifecycle		●
Incident and escalation management: Assigned expert owns severe issues until resolution		●
Reviews: Periodic business and technical reviews		●

C22-4861650-01 09/25