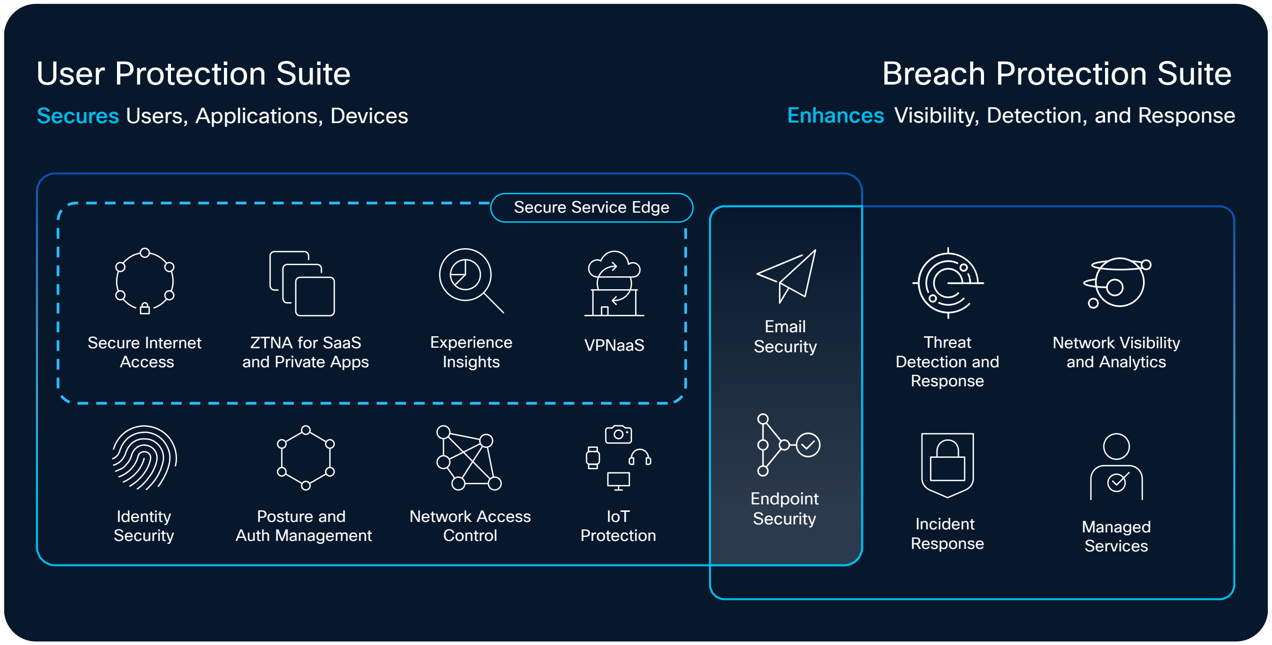
Cisco User and Breach Protection Suite

A stronger security posture: proactive prevention and accelerated detection and response.

Security teams today face a mix of challenges–from sophisticated adversaries to simple, persistent attacks that exploit organizations with lower security maturity. Attackers often target users as the weakest link, using techniques like phishing and credential theft to gain initial access. Identity-based attacks accounted for 60% of incidents in 2024, according to Cisco Talos. Disparate security tools further burden defenders, leading to alert overload, slower response times, and weaker security outcomes.

To help organizations overcome these threats, the Cisco User and Breach Protection Suite delivers a unified, end-to-end approach. It puts users at the center of your security strategy while empowering security teams to accelerate detection and response. By integrating the Cisco security portfolio across endpoint, email, network, identity, firewall, access to applications, and cloud, the suite provides comprehensive protection with simplified management. This unified approach strengthens your security posture – wherever you are in your security journey – while reducing complexity and operational overhead.



User Protection Suite

Secures Users, Applications, Devices

Breach Protection Suite

Enhances Visibility, Detection, and Response

Secure Service Edge

Secure Internet Access

ZTNA for SaaS and Private Apps

Experience Insights

VPNaaS

Identity Security

Posture and Auth Management

Network Access Control

IoT Protection

Email Security

Endpoint Security

Threat Detection and Response

Network Visibility and Analytics

Incident Response

Managed Services

Figure 1. User and Breach Suite Composition

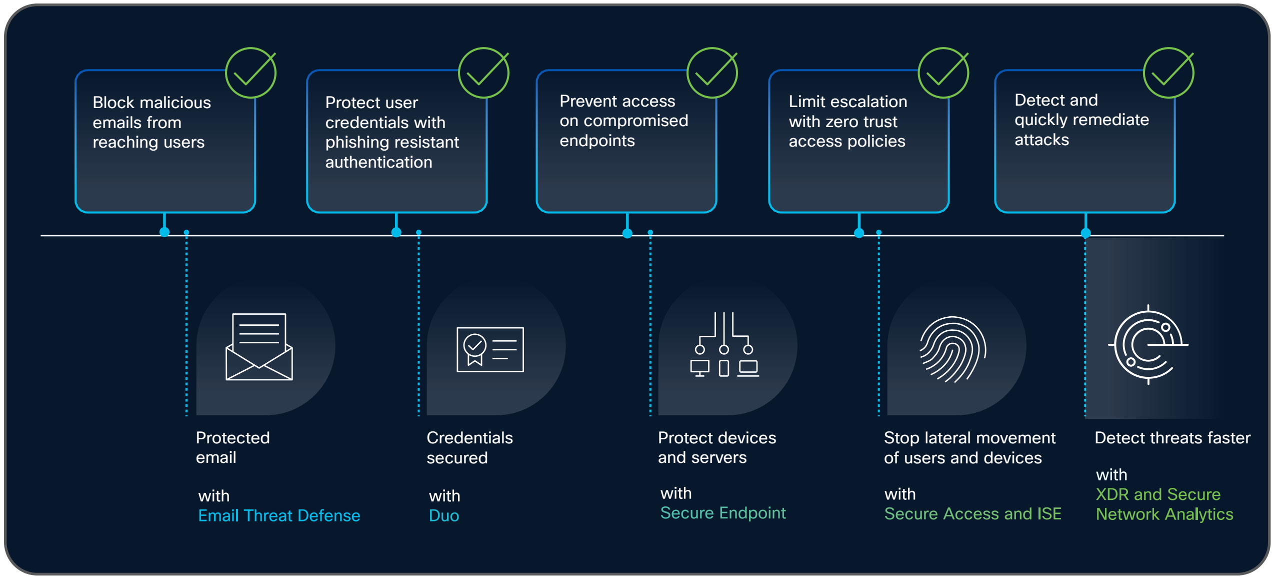
- **Better Efficacy:** Stop threats like ransomware and identity-based attacks like Business Email Compromise with layered protection, high-fidelity telemetry, and AI-driven insights. Integrated products work better together to defend against the evolving threat landscape and provide clear verdicts for decisive action.
- **Better Experiences:** Enable a seamless and secure experience for the hybrid workforce, anywhere. Reduce user friction by simplifying authentication and access. For security teams, streamline investigations, prioritize threats, and simplify management with unified capabilities.
- **Better Economics:** Ease operational burdens and support vendor consolidation by leveraging integrated protection. Combat increasing security complexity and reduce breach risk with a unified approach. Elevate analyst skills through response guidance and automation to enhance efficiency and effectiveness.

Why Cisco? Why suites?

- **Unified, Intelligent Protection:** A cloud-based platform that leverages AI, cross-domain telemetry (including native network visibility), and Cisco Talos threat intelligence for intelligent, integrated protection across your environment.
- **Simplified Security Operations:** Solutions are designed to reduce the burden on your security team by simplifying operations while providing world-class protection. Centralized management and a single agent reduce complexity.
- **Strategic Value & Comprehensive Coverage:** Cisco Security Suites bring together the right tools for comprehensive protection and vendor consolidation, delivering exceptional value for your evolving security needs.

How it works together (Example: Phishing attack)

Attackers frequently target users as the weakest link, often through phishing campaigns. Once an attacker gains access to a valid account, it can take an average of **210 days** to detect a breach, providing ample time for them to escalate privileges, move laterally, and significantly increase the cost and damage of the breach.



Block malicious emails from reaching users
Protect user credentials with phishing resistant authentication
Prevent access on compromised endpoints
Limit escalation with zero trust access policies
Detect and quickly remediate attacks
Protected email
with
Email Threat Defense
Credentials secured
with
Duo
Protect devices and servers
with
Secure Endpoint
Stop lateral movement of users and devices
with
Secure Access and ISE
Detect threats faster
with
XDR and Secure Network Analytics

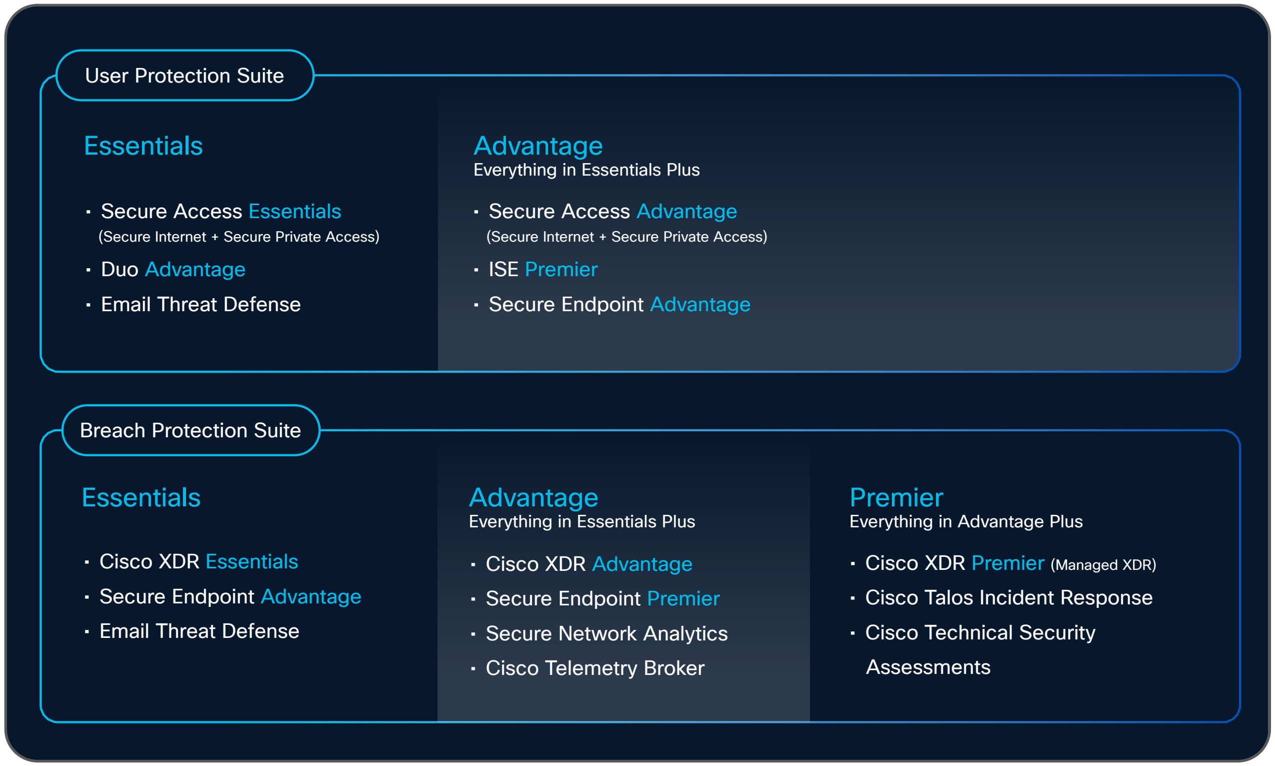
Figure 2. Layered Approach to Security

Consider a common phishing scenario: A user receives a fraudulent email, perhaps disguised as an urgent request from HR to fix an expense report. If they click a malicious link, log into a fake website, and even accept a push notification, an attacker could gain access to their account and begin to move laterally across the network.

Here's how Cisco's User and Breach Protection Suite provides a layered, integrated defense:

- **Secure Email Threat Defense:** Proactively blocks malicious emails (like phishing attempts) from ever reaching the user's inbox, stopping the attack at its first point of entry.
- **Duo:** Even if an email slips through, Duo provides phishing-resistant authentication, protecting user credentials and preventing attackers from logging in, even with stolen passwords.
- **Secure Endpoint:** Should malware be downloaded onto a device, Secure Endpoint detects and blocks it, working together with Duo to prevent fraudulent access attempts.
- **Secure Access/ISE:** If an attacker manages to gain a foothold, Secure Access/ISE enforce zero-trust policies, preventing damage by stopping lateral movement across the network for both users and IoT devices.
- **Cisco XDR:** Acting as the central intelligence hub that natively integrates and correlates data from all these solutions, Cisco XDR provide a unified view of the incident. This comprehensive telemetry allows security teams to prioritize threats, understand the full scope of an attack, and respond rapidly before significant damage occurs.

This integrated approach empowers security teams with full visibility into the attack chain, enabling proactive prevention and accelerated response for improved security outcomes and operational efficiency.



User Protection Suite

Essentials

- Secure Access Essentials
  (Secure Internet + Secure Private Access)
- Duo Advantage
- Email Threat Defense

Advantage
Everything in Essentials Plus

- Secure Access Advantage
  (Secure Internet + Secure Private Access)
- ISE Premier
- Secure Endpoint Advantage

Breach Protection Suite

Essentials

- Cisco XDR Essentials
- Secure Endpoint Advantage
- Email Threat Defense

Advantage
Everything in Essentials Plus

- Cisco XDR Advantage
- Secure Endpoint Premier
- Secure Network Analytics
- Cisco Telemetry Broker

Premier
Everything in Advantage Plus

- Cisco XDR Premier (Managed XDR)
- Cisco Talos Incident Response
- Cisco Technical Security Assessments

Figure 3. Mix and Match Tiers of User & Breach Protection Suite

For more information

Ready to learn more? Connect with a Cisco Security Suites expert today.