Cisco Secure Endpoint

Cisco Secure Endpoint Buyer's Guide

Rethinking your endpoint security strategy

Introduction

There's a reason most organizations revisit their endpoint security strategy every year. Because the endpoint is your frontline, and your adversaries keep finding new ways to penetrate it. If the threats keep growing, why wouldn't your security?

When most of the workforce went remote in 2020 it changed how we think about the frontline.

In a race to secure remote work, organizations turned to zero trust, secure access service edge (SASE) and extended detection and response (XDR). How we secure the endpoint became a key factor in these broader initiatives. It's no longer limited to threats in isolation, it's now guiding the future of work.

Remote work is here to stay, hybrid or otherwise. In this guide, learn how to ensure your endpoint security strategy meets your needs for today with an eye for what's coming tomorrow.

Cisco Secure Endpoint

Securing the endpoint for a hybrid future

The scope of the endpoint broadened in 2020 as a surge in remote work led to new devices on the network and new vulnerabilities.

With this sudden shift, the endpoint was used as a foot in the door to higher value assets. And when the attack surface grows, security teams need to expand visibility across all control points: endpoint, email, network, and cloud.

But gaining visibility without taking on more complexity is no simple task.

In the wake of the pandemic zero trust, SASE and XDR offered new ways to strengthen security and make individual tools work better together as part of a security platform.

At the same time, organizations have been shifting to a platform approach to security as it provides more functionality and efficiencies without the need to compromise visibility or control.

Because the endpoint provides visibility into user behaviors and root cause it plays a more critical role in zero trust, SASE and XDR initiatives.

Each approach enables secure remote work—and you should secure your endpoint with these broader goals in mind.

Cisco Secure Endpoint

Basic requirements your endpoint security provider should deliver

You can think about the foundational requirements for endpoint security in two parts: the endpoint protection platform (EPP) and endpoint detection and response (EDR).

The EPP blocks threats automatically while the EDR handles the ones that slip through.

Endpoint protection platform (EPP)	Endpoint detection and response (EDR)
Prevents the most common attacks before they reach your endpoints.	Quickly detects and responds to threats once compromised.
▸ Next-gen antivirus to automatically diagnose and block malicious threats	▸ Dwell time reduction to detect, remediate, and minimize impact fast
▸ Fileless malware and ransomware protection	▸ Query the endpoint with any question and get answers in real time
▸ Behavioral protection and machine learning techniques	▸ Built-in threat hunting to proactively identify threats
▸ Complete visibility from the network edge to the endpoint	▸ Determine indicators of compromise (IoCs) through MITRE ATT&CK mapping
▸ Real-time global intelligence	▸ Efficacy and accuracy to minimize noise from false positives

These are the key capabilities you should demand from your security provider.

But you don't have to accumulate an excessive number of licenses and disparate tools to achieve all the above, there's a simpler way to get this level of security and more.

Cisco Secure Endpoint

How to get even more long-term value

According to ESG research, most organizations are now planning to replace their current endpoint security solutions within the next year, with 67% desiring a comprehensive endpoint security software suite from a single vendor[1]. This shift to platform coincides with an increased adoption in zero trust, SASE and XDR that enables secure remote work and other desired business outcomes.

Architect your endpoint security to work with a broad array of security controls on an integrated platform and align to other IT initiatives.

Secure the endpoint and extend control further:

Unify user and endpoint protection to secure your remote workers

Combine endpoint security with secure access control for zero trust

Embed endpoint security in your next SASE initiative

Extend detection and response across endpoint, email, network and cloud

Aligning the endpoint to the future of work

The nature of work has changed and with it the requirements for endpoint security.

We now need to rethink the traditional ways we've secured the endpoint with broader goals in mind. Align your endpoint security strategy to meet the business requirements of the top industry mega-trends by including these core capabilities as part of your selection criteria.

Zero Trust

Verify identity at a granular level for applications, services and data

- Ensure trusted access for users through multi-factor authentication (MFA)
- Protect users and network against threats with device posture checks
- Maintain trusted access from any device or location with continuous visibility

SASE

Provide secure direct-to-cloud access to applications more efficiently

- Combine a first and last line of defense to secure devices
- Monitor behavioral patterns on applications and check for malicious activity
- Stop advanced threats that avoid typical detection tools

XDR

Integrate security data across all control points to gain visibility into more advanced threats

- Accelerate time to detection and reduce dwell time
- Focus on the right alerts for investigation and cut through the noise
- Understand root cause by running complex queries on all endpoints

Why Cisco

The role of the endpoint has grown and so should the level of protection you expect.

At Cisco, we deliver a platform to modernize the security stack so you can get more functionality with less effort.

Whether you're looking to secure your remote workforce or planning your next IT initiative, we can secure your endpoint with all these capabilities and more on our built-in SecureX platform.

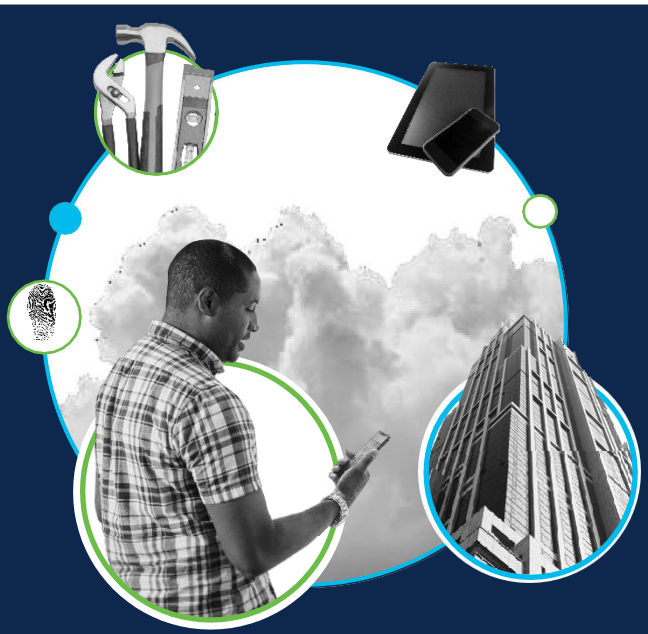
We've been a leader in zero trust and endpoint security for years. We offer the most complete, integrated SASE architecture. And we deliver the broadest XDR capabilities on the market because we've built detection and response into every element of the Cisco Secure portfolio.

We are the first vendor to unify user and device protection: combining MFA with device posture checks and endpoint security in one integrated solution.

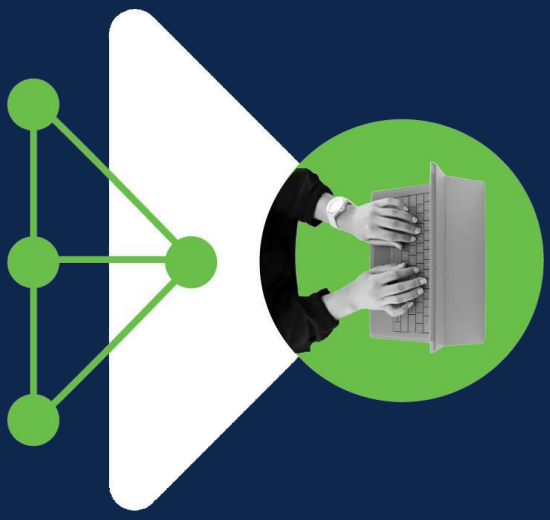
It's time to rethink your endpoint security strategy. Make the right choice and choose Cisco.

SecureX

We work hard behind the scenes to make security feel seamless for you. Through the Cisco SecureX platform you can manage detection and response across your entire security infrastructure. You canprotect everywhere with a single platform—and leverage the unrivaled breadth of intelligence from Cisco Talos which spans the entire Cisco Secure portfolio.



Cisco Secure Endpoint



Learn more today

Read the ESG white paper

Start a 30-day free trial of Cisco Secure Endpoint

Contact a sales representative

Get in touch to see how Cisco can help you meet your security needs.

Contact us

[1]*ESG white paper, Reimagining Endpoint Security, July 2020*