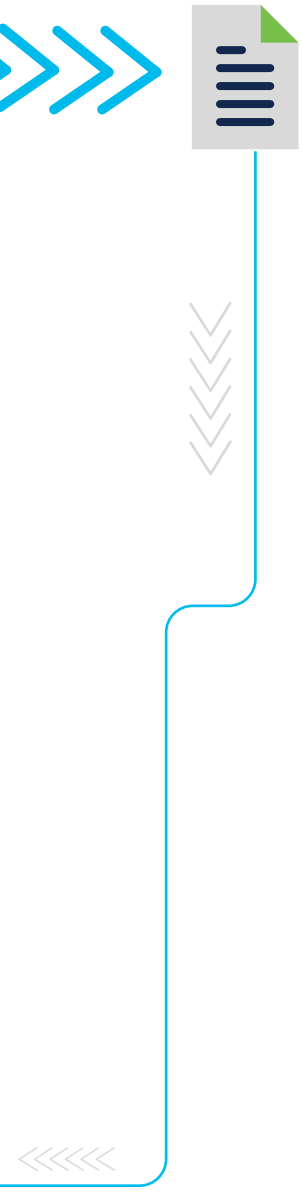
CISCO
SECURE

Cisco Secure Endpoint Buyer's Guide

Rethinking your endpoint security strategy

Contents



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?

Organizations are making massive investments in resilience since disruption is happening faster than ever.

Today's CISOs are facing unprecedented challenges which make it difficult to anticipate and prepare for the next wave of threats. This includes:

- A continuously changing threat landscape.
- A lack of visibility due to disparate point products that don't communicate with each other and fire off unnecessary alerts.
- Difficulty prioritizing security alerts and identifying the most critical threats that can cause the most damage.

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.

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. 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.

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. · Next-gen antivirus to automatically diagnose and block malicious threats · Fileless malware and ransomware protection · Behavioral protection and machine learning techniques · Complete visibility from the network edge to the endpoint · Real-time global intelligence	Quickly detects and responds to threats once compromised. · Dwell time reduction to detect, remediate, and minimize impact fast · Query the endpoint with any question and get answers in real time · Built-in threat hunting to proactively identify threats · Determine Indicators of Compromise (IoCs) through MITRE ATT&CK mapping · 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.

How to get even more long-term value

Cisco surveyed 100 IT and security leaders on the Gartner Peer Insights platform who are part of the endpoint security evaluation process to understand their level of security maturity and their perspective on the future of endpoint security.

Key Insights:

- Many organizations are employing EDR and XDR capabilities, but few have reached full maturity.
- Organizations are looking for integrated platforms that support hybrid workforces while simplifying vendor management.
- In anticipation of the ever-increasing threat landscape, organizations are looking for highly integrated and automated endpoint security solutions.
- Organizations want future-proof endpoint security solutions that bolster their security resilience.

Secure the endpoint and extend control further

Unify user and endpoint protection to secure your remote workers

Secure Endpoint is fueled by Talos Threat Intelligence Enables predictable, effective, and rapid responses to security breaches

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.

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

EDR

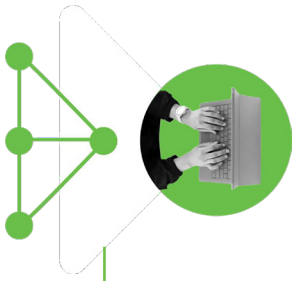
Integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities

- Advanced capabilities to detect and investigate security incidents to remediate endpoints quickly
- We deliver an always-on solution that can be completely managed
- Threat hunting, and integrated risk-based vulnerability management from Kenna Security

MDR for Endpoint

Combines human and machine power to reduce EDR tasks and times. And combines a first and last line of defense to secure devices

- We do the heavy lifting of securing your endpoints
- We detect and respond to threats in minutes, not hours
- We investigate every threat and prioritize the most critical ones



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.

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.

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

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

Learn more today

Read the GPI 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