CISCO
SECURE

Checklist:

Top 5 tips for CISOs choosing endpoint protection

With the sudden increase of the virtual workforce, the number of vulnerable endpoints has expanded exponentially. This new normal calls for security resilience – the ability to protect the integrity of every aspect of the business and withstand unpredictable threats or changes, and then emerge stronger. And security resilience calls for more than what the past has offered. Organizations must embrace multi-layered endpoint security solutions and the latest technologies, such as unified platforms and extended detection and response (XDR) capabilities, in order to protect their networks.

Below are some great tips for CISOs looking to understand how to choose the right solution for endpoint protection so their security teams can get visibility to defend their networks more effectively, get answers quickly, and automate repetitive manual tasks.

1 Block more effectively

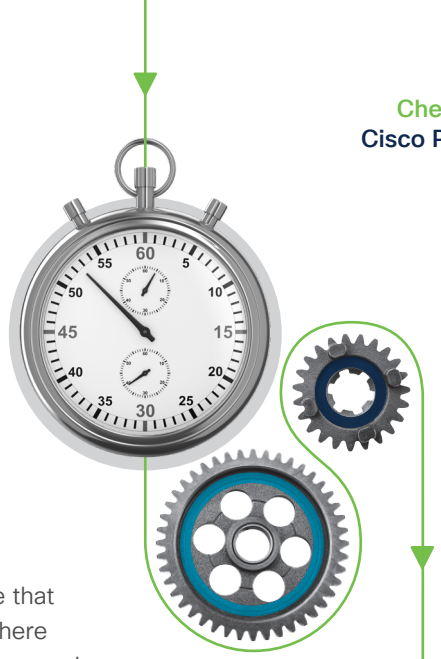
Defending against threats is never a one-time event. To secure networks efficiently, businesses require cloud-delivered endpoint protection to close gaps in the ecosystem and ensure that all security patches are up to date.

Read more about how you can stop threats before you're compromised.

2 See more accurately

Seeing isn't just about looking. It's about knowing what to look for. You need a constantly updated, context-rich malware knowledgebase and robust set of security investigation capabilities so you can understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it in real time.

Read more about advanced threat intelligence as one unified solution.



3 React faster

Automation is key not only to help increase reaction time, but also to ensure that decision makers have the right context. CISOs need a zero-click solution where the tools do the work with automation and orchestration running in the background.

Read more about how to bolster your endpoint detection and response.

4 Make integration work for you

Every company is unique, and has different requirements for effectively securing their network. Organizations need a solution that maximizes the benefits of a built-in platform approach by providing integration, automation, and the ability to orchestrate with existing security investments.

Read more about maximizing the benefits of a built-in platform approach.

5 Harness threat hunting

Why sit back and wait to be attacked when you can go on the offensive? Threat hunting is changing the game, enabling organizations to proactively pursue, discover, and stop cyberthreats in their tracks.

Read more about how you can disrupt attacks before they materialize.

Learn more about Cisco Secure Endpoint ›