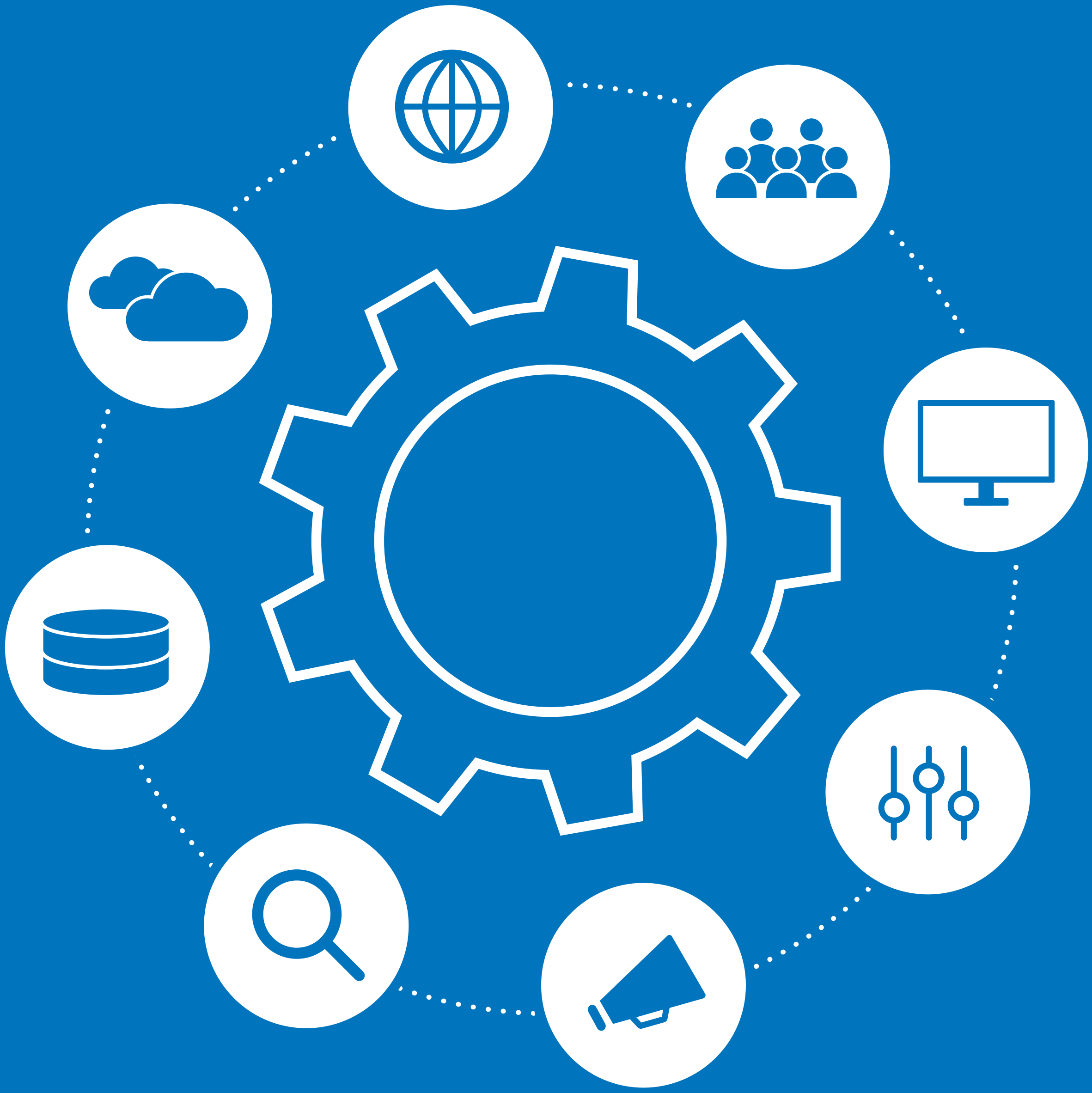
PeerPaper™ Report 2021

EDR: Understanding the SecOps Value of an Ecosystem Approach

Based on real user reviews of Cisco Secure Endpoint



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

Endpoint Detection and Response (EDR) is one of today's great security operations (SecOps) challenges. As devices proliferate and employees increasingly access corporate networks from remote locations, endpoint security managers have to maintain security while juggling the typical resource challenges and competition for analysts' attention. An ecosystem approach, exemplified by the Cisco Secure Endpoint (formerly AMP for Endpoints) solution, offers a number of advantages. As described in real user reviews on IT Central Station, an EDR ecosystem provides integration and SecOps efficiency, along with strong support. The EDR ecosystem also enables faster, simplified investigation and remediation of threats.

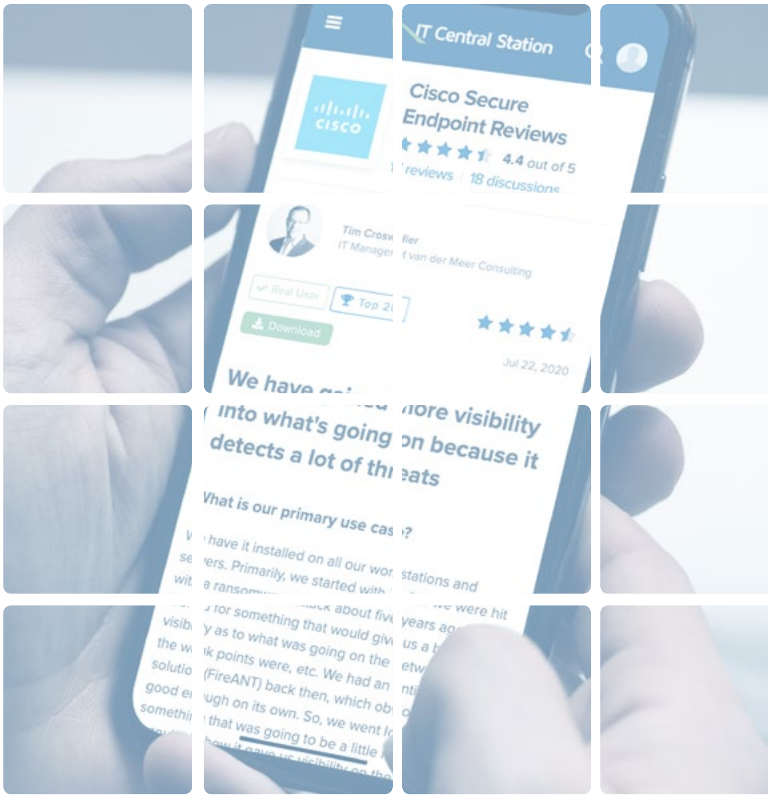
CONTENTS

INTRODUCTION

Protecting endpoints is a serious challenge for security departments. Never an easy workload, Endpoint Detection and Response (EDR) has grown more difficult as device types proliferate and employees are requiring more frequent remote access. Security managers have to defend vulnerable endpoints without affecting their performance and draining their limited resources. As IT Central Station members have discovered, an ecosystem approach, as made possible by the Cisco Secure Endpoint solution [formerly Cisco AMP for Endpoints], helps them with EDR on a variety of levels. The platform and ecosystem mode of EDR drives increased security operations (SecOps) efficiency while enabling faster, more effective threat investigation and remediation. This paper looks at how it all works, based on real user experiences.

Advantages of the platform/ecosystem approach

EDR tends to work better when SecOps teams adopt a platform approach. An EDR ecosystem should make SecOps more efficient by streamlining threat detection and incident remediation. A dedicated platform, such as Cisco Secure Endpoint, makes integration with other systems easier than is possible with point solutions. If cloud hosting for the ecosystem is available, that amplifies the benefits of the platform approach.



SecOps efficiency

Success in SecOps has a lot to do with getting maximum productivity out of personnel. This can happen when a team has the right policies and tools. As a Systems Architect at a consultancy with more than 5,000 employees explained, the biggest lesson he learned from using Secure Endpoint was, “How impactful proper tool utilization in an organization can be to the overall efficiency.”

The CIO at Per Mar Security Services, a security firm with over 1,000 employees, described how Cisco Secure Endpoint enables his team to see a threat once and block it everywhere, across all endpoints and their entire security platform. This makes the team more productive. He further said, “If one piece of bad malware gets through, the entire network will self-heal. It makes us more efficient. Standardizing on one pane of glass is the dream that you’re after.”

A Technical Team Lead Network & Security at Missing Piece BV, a small tech services company, offered another example of efficiency through Cisco Secure Endpoint. He said, “Orbital helps us with investigation, especially if there’s been an incident on one machine, and I want to know, ‘Are there other machines in my environment with the same type of modifications.’ It’s just a click away. I don’t have to leave the Orbital or Secure Endpoint to do the incident investigation. Thus, I don't have to pivot to another solution to check the event logs or files on the endpoints, and not having to leave the tool is very efficient."

As a result of this capability, he shared that his technicians are doing more meaningful tasks. He revealed, "They can just do their threat hunting and incident response without having to find tools that can do the things already built into Secure Endpoint and Threat Response."

Integration across security systems and beyond

EDR solutions need to be able to work in concert with other security tools. For this reason, integration potential in the EDR platform approach has a great deal of appeal. "I find the integration to be valuable," said Missing Piece's Technical Team Lead. "Cisco Email Security, Threat Response, and firewall are all completely integrated with this solution. It's very easy to connect your firewall or Email Security appliance with Secure Endpoint to get visibility within Threat Response. On Cisco's end, we have had no trouble integrating. You go to the menu, and say, 'I want to integrate this kind of device.' Then, it basically shows you which buttons to click to integrate. It has been very easy." Figure 1 offers a simple reference architecture for this scenario.

> “
> It's very easy to connect your firewall or Email Security appliance with Secure Endpoint...

For a Security Officer at a small healthcare company, what mattered was how "Cisco is standing up so much stuff right now." He said, "This solution interfaces with Talos Intelligence, Threat Grid, Threat Response, and SecureX. All of these things are integrating together and a lot of stuff is now starting to happen automatically."

He shared, for instance, that if a threat is detected, it is automatically interfacing with

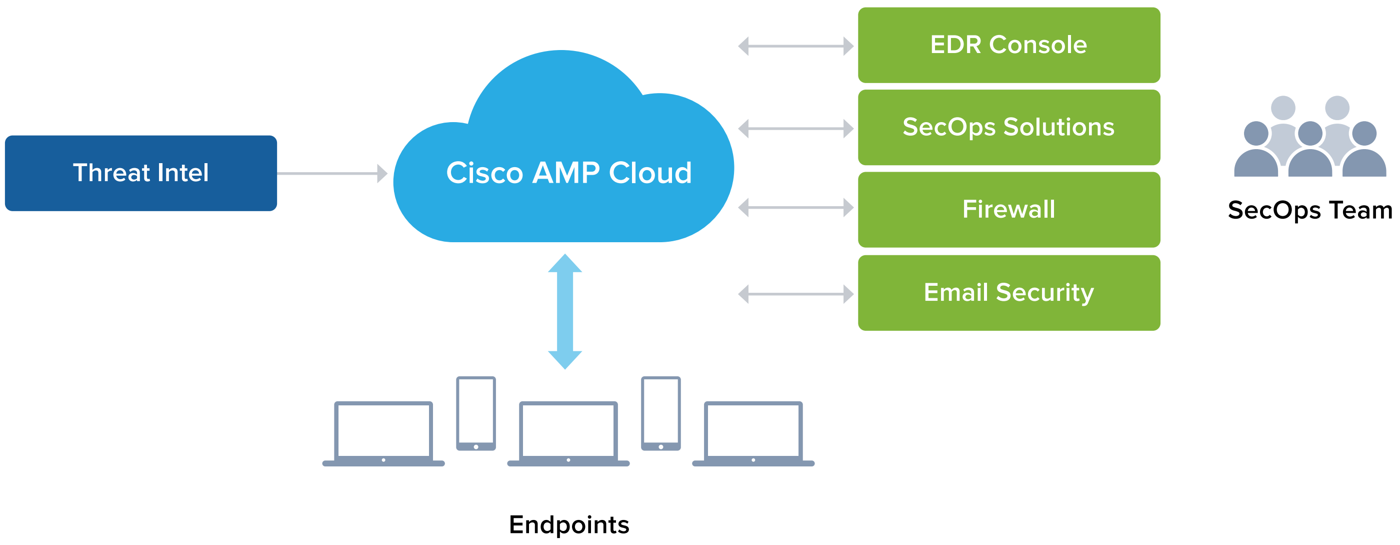


Figure 1 - Integration of threat intel, firewall and more into the cloud EDR platform.

Talos Intelligence to figure out what that threat is and the hash value of whatever file that is. “If it thinks it’s suspicious,” he added, “it automatically submits it to Threat Grid, which detonates the file in the sandbox, but also in the cloud, and returns a report saying whether the file, or whatever it is, is an actual threat/incident. Then, it remediates and quarantines it, and you find out about it later. It’s doing a lot of stuff in the background as the integration with other tools increases.”

Other notable comments about integration included:

- “The most valuable features of this solution are the IPS and the integration with ISE.” - Network Administrator at Lili Valley Foundation, a healthcare company with over 1,000 employees
- “The solution’s integration capabilities are excellent. It’s one of the best features.” - System Architect at COMPASS IT Solutions & Services Pvt.Ltd., a small tech services company
- “Because we do have the Email Security appliance and it is integrated with Threat Response, we have everything tied together. With SecureX, we are able to pull all those applications into one pane for visibility and maintenance. This greatly maximizes our security operations.” - Systems Architect at a consultancy with more than 5,000 employees

Cloud hosting and its suitability for remote work

IT Central Station members perceive cloud hosting to be a source of advantage for the platform approach to EDR. As Missing Piece’s Technical Team Lead observed, “I don’t have to worry about the console, the amount of data, or the back-end, as that is all being handled by the cloud. Therefore, I can scale as much as I want, as long as I have enough licenses. The visibility has increased a lot because all the heavy work is being done in the cloud.” This helped his team during the work-from-home period of the last year.

The Per Mar Security Services CIO similarly noted, “The fact that the solution offers cloud-delivered endpoint protection simplifies our security operations. We don’t have to worry about updates or signature updates. It takes care of itself in the background, so it frees my guys up to do more meaningful work.”

> “
> **The visibility has increased a lot because all the heavy work is being done in the cloud.**

Cloud features stood out to the healthcare Security Officer. With the cloud, he saw that it doesn’t matter if a device is located inside or outside the network environment. With today’s remote work trend, this is helpful because users don’t have to be VPNed into the environment for Secure Endpoint to work. He said, “Secure Endpoint will work anywhere in the world, as long as it has an internet connection. You get protection and reporting with it. No matter where the device is, Secure Endpoint has still got coverage on it and is protecting it. You still have the ability to manage and remediate things. The cloud feature is the magic bullet. This is what makes the solution a valuable tool as far as I’m concerned.”

The cloud gives an IT Manager at van der Meer Consulting, a small construction company, visibility with minimal intrusion. He related, “We don’t have an on-premise sort of interaction with it, though. It’s just a connector that sits on the workstations and servers, then interacts with the workstations or servers through to the cloud.

It has very minimal impact on us in terms of performance.” A Deputy GM at Oregon Systems, a small tech services company, simply stated, “The most important thing is that they’re cloud-based, highly scalable and highly integrated.”

Quality of support

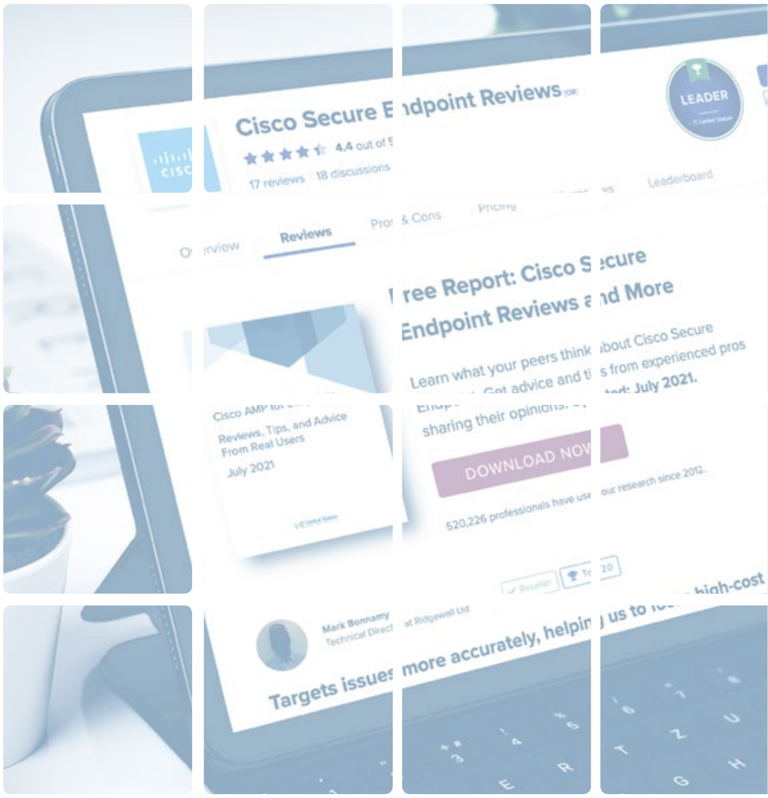
EDR system owners need strong support from vendors. The platform/ecosystem approach to EDR makes this more likely to occur. There are fewer vendors and fewer of the kind of inter-system complications that can impede good support in best-of-breed EDR environments. A Solution Architect / Presales Engineer at a comms service provider with over 1,000 employees spoke to this issue when he said, “We were previously using Check Point Sandblast Agent. We switched because it wasn’t as stable as this one. We had some problems with it and we needed to contact their support and it wasn’t so good. I would get tough questions from my clients so eventually I told them that we would look into other solutions.”

> “
>
> **The technical support has always been fantastic,.. Cisco TAC has been very helpful.**

“The technical support has always been fantastic,” said a System Architect at COMPASS IT Solutions & Services Pvt. Ltd., a small tech services company. “It has never been a disappointing experience to be very frank. Cisco TAC has been very helpful. I worked in the presales team as well, so there is Partner Plus which has always been favored in terms of providing us with solution-based documents as well as presentations to take to our customers.” Per Mar Security Services’ CIO concurred, saying, “Their tech support, overall, is best-in-class. If you ever have a question, TAC gets the answer for you and helps you work through the solutions.”

Faster, simpler investigations and threat remediation

The platform/ecosystem approach to EDR also has appeal in its ability to speed up and simplify investigations and remediate threats. Users of Cisco Secure Endpoint have found that the solution enables them to mitigate threats before they cause serious problems. The solution provides a high level of endpoint visibility, while also easily scaling and securing endpoints through ease of use.


Cisco Secure Endpoint Reviews
LEADER
17 reviews | 18 discussions
Reviews
Leaderboard
Free Report: Cisco Secure Endpoint Reviews and More
DOWNLOAD NOW
Targets issues more accurately, helping us to

Mitigating threats before they become problems

As experienced SecOps professionals know, the best time to mitigate a threat is before it takes root in one's infrastructure. IT Central Station members shared their experiences with Cisco Secure Endpoint's capabilities in this area. As the Technical Team Lead at Missing Piece put it, "With Cisco Secure Endpoint, you get the possibility to proactively go hunting for threats and find them before they become a problem."

In his case, Cisco Threat Response takes the intelligence from all available different solutions, then combines it with sources, like VirusTotal, and includes general information that Cisco has available on those threats. He elaborated, saying, "If I see a file somewhere, I can with one click

> **With Cisco Secure Endpoint, you get the possibility to proactively go hunting for threats...**

go from my Secure Endpoint console to Cisco Threat Response, and there it will be enriched, saying, 'We have already seen this piece of software two months ago in Japan. This is what we thought of it. We did an automatic analysis on it. These are the indicators on this piece of software being either malicious or benign.' With Threat Response, it is very easy to go from what's happening on my environment to what's happening in the world."

"Secure Endpoint intersects with a bunch of other Cisco tools, such as Threat Grid, Threat Response, and Talos Intelligence to identify threats, then automatically quarantine or remove them," remarked the healthcare Security Officer. "It also gives you the ability to isolate endpoints to prevent further spread of any sort of malware, like a virus that might infect other machines. It gives you great detail, a timeline, and continuity of events leading up to whatever the incident is, and then, after. This helps you understand and nail down what the threat is and how to fix it."

Achieving a high state of endpoint visibility

EDR users need to know what's going on in with their endpoints. Visibility is essential. A platform/ecosystem approach delivers this capability, as the Per Mar Security Services CIO found. He said, "For the endpoint, Cisco gives us good clarity about what our endpoints are actually doing. So when we get bad actors into the network, we get quick visibility into which devices are compromised."

He further commented, "Secure Endpoint feeds into that whole Threat Grid for us. We're able to see hashes, and the like, all the way down to the client and we get that visibility because of Secure Endpoint. As Secure Endpoint reports back into the Threat Grid, we can see the hashes running on the actual endpoint, and whether they are malicious, and what those things have done. If malware has infected a certain laptop, we get all the forensic evidence around that laptop and, if it's jumped, where that bad stuff has jumped to and what it's done. All that visibility is possible because of Secure Endpoint."

> “
> **...when we get bad actors into the network, we get quick visibility into which devices are compromised.**

A Technical Director at Ridgewall Ltd, a small wholesaler/distributor, acknowledged the value of Cisco Secure Endpoint's ability to look across the estate. He shared, "If somebody has been compromised, the question always is: How has it affected other devices in the network? Cisco Secure Endpoint gives you a very neat view of that." An Application Manager at Huntington Bancshares Incorporated, a financial services firm with over 10,000 employees, put it this way: "Identity and access management capability within the console allows administrators the ability to drill down user visibility on a role based access control, limiting access to policies, groups, exclusions, and other controls. The visibility, dashboard and the navigations gives pretty decent insights into threats, IOCs and endpoint events to help with proactive monitoring."

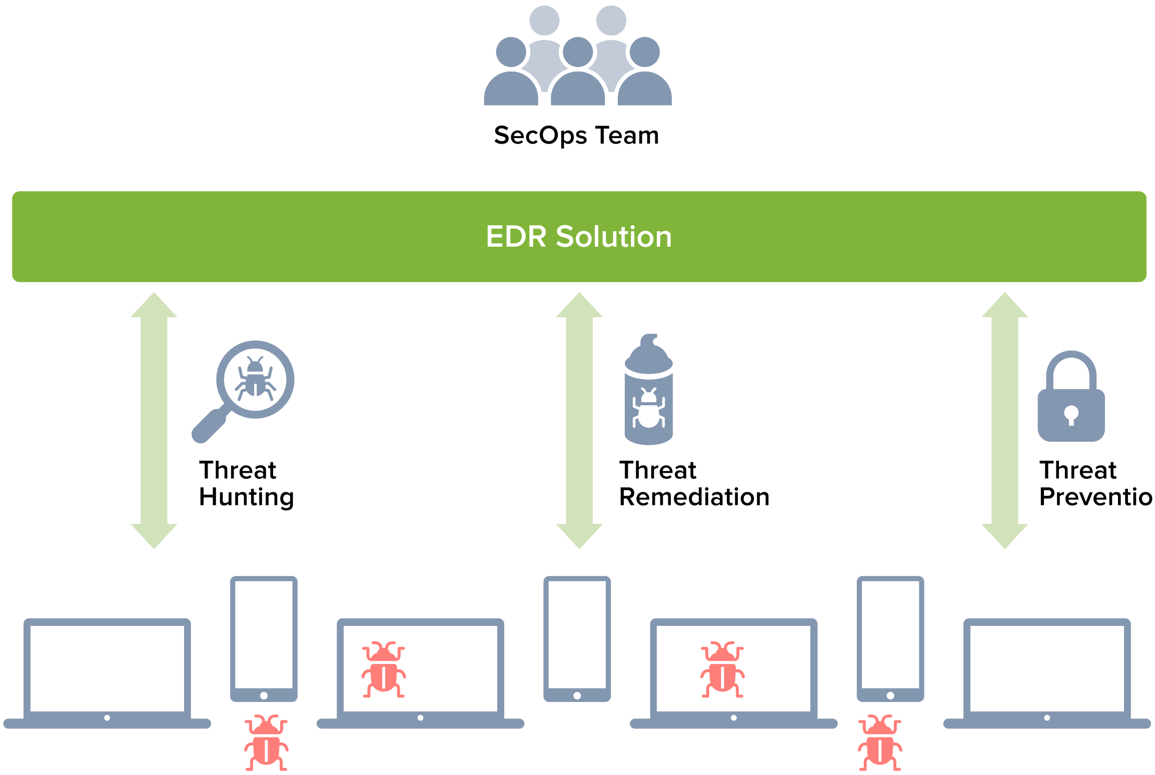
Remediating endpoint security problems more quickly

If there is a security incident involving an endpoint, fast detection and remediation is critical for protecting the endpoint as well as for stopping the attacker from moving further into the network. A Network Security Engineer at a tech services company with over 1,000 employees addressed this concern when he said, "With every protection software, there are issues, because it takes time to detect the malware, but Cisco is very fast in detection compared to other products."

The Technical Director at Ridgewall similarly noted, "The decrease in time to detection has been significant. It's very hard to put a percentage to it because, before it, we were often blissfully unaware that devices had a problem at all. It's given us visibility and we are much more effective. I'm guessing in terms of what it saves time-wise, because it's given us visibility that we otherwise didn't have, but I would say 80 percent."

The CIO at Per Mar Security Services was also able to quantify the benefit, saying, "Secure Endpoint has decreased our time to detection and to remediate, without a doubt. It's gone down by 100 percent. We're able to detect, real-time, bad or malicious software and mitigate it, not quite in real-time but pretty darn close." This user compared the outcome with the situation prior to deploying Cisco Secure Endpoint. Then, he said, there was no time measurement. He added, "I'm comfortable saying it has sped things up considerably. Now, we're only chasing real threats."

> "
> **The decrease in time to detection has been significant. It's given us visibility and we are much more effective.**



An EDR platform enables threat hunting, threat remediation and threat prevention to occur simultaneous through a single solution.

The IT Manager at van der Meer Consulting offered an example that represents a common fear among SecOps professionals. He related, "Because I was able to get on top of our ransomware attack fairly quickly, I was able to restore stuff from backups. Disruption is time, and we are a time-based business." He even suggested a quantitative assessment of the experience, explaining "If we had 100 technical people at X amount of dollars per hour charge-out rate, then that gives us an hourly cost as a very rudimentary way of working out hourly cost. Therefore, if we're down for half a day, or even a day, then we can very quickly work out how many dollars we will lose every time we get taken down by this type of attack."

Scaling and securing endpoints efficiently through ease of use

Ease of use also matters when it comes to implementing effective, efficient EDR. Ease of use translates into scalability, which is necessary for organizations that are growing or adding new devices to EDR protection. The CEO of Oriental Weavers, a manufacturing company with over 10,000 employees, said, "It is stable, easy to scale and I like the price. I guess it's easy to scale, because I started a project with the requirements and when I needed to move forward to scale it up, it's been so easy. We currently have around 50 users."

> **"The ease of implementation is a very valuable aspect of the solution. It's also very user-friendly.**

"A solution that's easy to implement, is highly scalable and is extremely user-friendly," is how Oregon Systems' Deputy GM described Cisco Secure Endpoint. "The ease of implementation is a very valuable aspect of the solution. It's also very user-friendly. The initial setup was straightforward. We're well-versed in the solution, so for us, it was easy." The Per Mar Security Services CIO, describing his company as a "baby user," with only 800 endpoints, nonetheless pointed out that his initial setup was straightforward. With Cisco's Quick Start Guide, they got those 800 devices out to 30 offices in just two weeks.

CONCLUSION

As security professionals rise to the challenges of endpoint protection, they are finding the platform/ecosystem approach, especially one with cloud hosting, to be beneficial. A platform that offers ease of use and straightforward integration with related security systems can improve EDR and SecOps efficiency. These outcomes were validated by reviews of Cisco Secure Endpoint by IT Central Station members. They also revealed that the Cisco Secure Endpoint solution helped them get better – and faster – at investigating and remediating endpoint threats. In some cases, they were able to block threats before they took root and caused problems. With a sound EDR platform, SecOps teams are poised to maintain a strong endpoint defense even as requirements and threats continue to evolve in the future.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT CISCO

Cisco is a multinational technology conglomerate that develops, manufactures, and sells networking hardware, software, telecommunications equipment, and other high-tech services and products. Founded by a husband-and-wife team who pioneered the concept of a local area network (LAN) to connect geographically dispersed computers, the company's mission remains to connect the unconnected and create a world of potential.

The Cisco Secure Endpoint (formerly AMP for Endpoints) cloud solution delivers robust protection, detection, and response to threats to your endpoints and networks – aiming to reduce remediation time for security professionals by as much as 85%.