CISCO
SECURE

SECURITY OUTCOMES

study
endpoint

Proven Success Factors for Endpoint Security

Finding success in cybersecurity isn't easy. That's why we embarked on a journey to identify factors that are measurably improving the chances of achieving successful outcomes for organizations around the world. Through an independent research firm, we collected data about 25 organizational security practices and 11 program-level outcomes from over 4,800 IT and security professionals. We published what we learned from analyzing that data in the Security Outcomes Study.

One of the things readers told us they appreciated about the Security Outcomes Study is that it's not a marketing document. It's based on rigorous, independent analysis and completely devoid of mentions of Cisco products. At the same time, we've fielded questions from customers along the lines of "How does [*insert security product*] line up with the practices and outcomes from this study?" We appreciate the interest, and thought that a recent expansion of Cisco Secure Endpoint offered an excellent opportunity to explore this question.

Contents

Bottom Line Up Front

We're going to use data collected from a double-blind survey of thousands of respondents to demonstrate the value of endpoint security solutions in helping organizations build more successful security programs. **Our analysis concludes that Cisco Secure Endpoint contributes in multiple ways to every single program-level objective examined in the Security Outcomes Study.**

As impressive as that statement sounds, we don't expect you to just take it at face value. We'll walk through evidence of security incidents detected by our endpoint sensors and those reported by survey respondents. Next, we'll clearly demonstrate how Cisco Secure Endpoint implements practices from the Security Outcomes Study, as well as how those practices drive measurable outcomes. We hope you'll agree that this makes a defensible and compelling case for the role of endpoint security solutions in modern cybersecurity programs.

Reported Incidents and Losses

Readers of our 2021 Security Outcomes Study may recall that 'avoiding major incidents and losses' was one of the 11 outcomes we examined. Having a major security incident or loss doesn't mean the security program is failing (nor does the absence of them prove success), but it's undoubtedly a top-of-mind metric for organizational leadership. And therefore it's something that deserves serious attention.

All told, 43% of the 4,800 respondents to the study claimed their organization was successful in avoiding major incidents and losses. This, of course, means that the majority said they're struggling to some degree. That statistic isn't entirely unexpected—but it is rather sobering. Here's some additional context presented to participants to help them diagnose where they stand on this important outcome:

> We expect that an organization that's highly successful in achieving this goal has not had a major security incident (of high internal and/or external visibility) in the last couple years. Furthermore, there's no reason to suspect that it's merely a matter of time until a major data loss event occurs. Minor and even moderate incidents are expected, but the question here is whether the organization has and will continue to stay out of the headlines.

The thing to note here is that "struggling" doesn't necessarily mean an organization suffered a major incident or loss. Due to that ambiguity, we also asked a more explicit follow-up question: ***"Has your organization actually had a major security incident or loss in the last two years?"*** Overall, 41% answered in the affirmative, and another 5% weren't sure.

Source: Cisco 2021 Security Outcomes Study

Figure 1: Has your organization had a major security incident or loss in the last two years?

As one might suspect, the answer to this question varies quite a bit around the world. One of the things that sets the Security Outcomes Study apart from others is its impressive global scope. We set survey response targets for 25 countries to ensure adequate samples for statistical comparisons. Those interested in learning how security practices and outcomes differed across regions can download reports specific to Europe, Middle East, Africa and Russia; Asia-Pacific; and The Americas. Here though, we're looking for a global view of major incidents, and Figure 2 delivers on that request.

The reported incident rates in Figure 2 show a sizable spread among countries. Less than a quarter of respondents from Russia said their firms experienced a major cyber event in the last two years, compared to two-thirds of those from Thailand. Beyond that, three additional EMEAR countries boast the lowest rates, and two other Asian countries sit atop the high end of that scale. Representatives from the Americas region are scattered through the middle ranks.

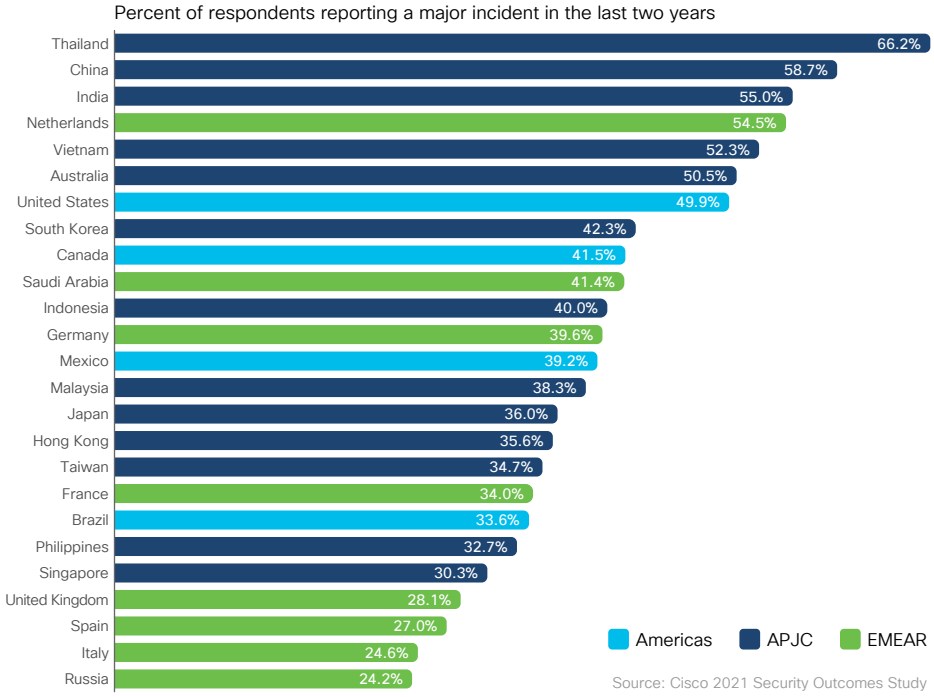


Figure 2: Reported rates of major security incidents by country

As one might suspect, the likelihood of reporting major security incidents also varies quite a bit across industries. Figure 3 reveals that the oft-plagued hospitality and education sectors exhibit the highest rates, with over half of organizations in those sectors reporting major security incidents in the last two years. The energy and public sectors stand on the other end of that spectrum, with purported percentages falling to 26% and 31% respectively.

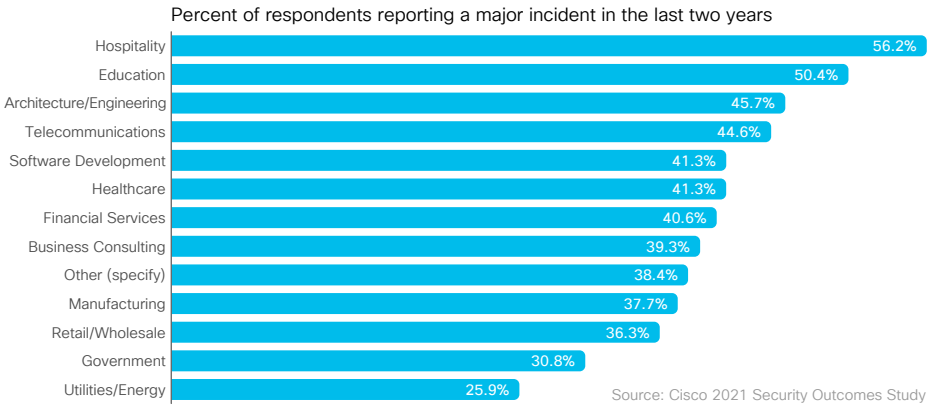


Figure 3: Reported rates of major security incidents by sector

Asking people questions about their organization's history of major cybersecurity incidents and losses helps in understanding perceptions and experiences relevant to managing risk. But it's not the same as detecting events that ***actually*** happened and responding to them on an ongoing basis. Besides, there's a whole host of nasty threats constantly occurring that (thankfully) don't rise to the status of a major incident. We'll go a level deeper by examining actual threats detected by Cisco in the next section.

"When we started using Cisco [Secure Endpoint], we noticed greater visibility, more effective threat hunting and investigation, and faster detection and response."

Suat Celikok
Security Operations Center Manager, Destel/Istanbul Grand Airport

Threats Detected by Cisco Secure Endpoint

Since endpoints (servers, laptops, etc.) are often ground zero for security incidents like those reported in the preceding section, we decided to focus there in our search for objective data on malicious events. Cisco Secure Endpoint leverages a protection lattice composed of several technologies that work in concert. One of those layers is the Indication of Compromise (IOC) feature, which can detect suspicious behaviors observed on endpoints and look for patterns related to malicious activity.

Threats Observed at the Endpoint

The data presented in Figure 4 is aggregated across organizations and covers events detected in the second half of 2020. In keeping with our goal of uncovering significant events, we'll filter our analysis down to critical severity IOCs. While these make up a small portion (under 5%) of the overall IOC-based alerts, they demand immediate attention if observed on an endpoint.

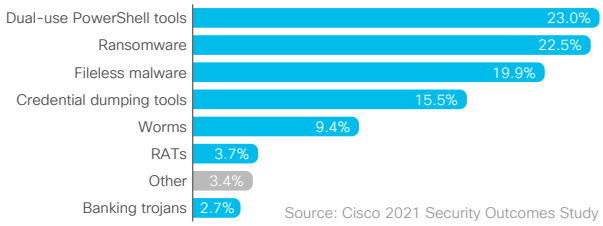


Figure 4: Critical severity IOCs detected by Cisco Secure Endpoint

After sorting the critical IOCs observed, the top category is dual-use tools leveraged for both exploitation and post-exploitation tasks. PowerShell Empire, Cobalt Strike, PowerSploit, and Metasploit are four such tools commonly seen. While many of these tools have legitimate uses, they've been adopted into the attacker toolkit, as well. This tactic of "living off the land" avoids the added risk of detection when deploying foreign tools or code to compromise systems.

Coming in second is ransomware, which was undoubtedly one of the biggest threat trends of 2020. Within our endpoint data and beyond, we observed the widespread adoption of new ways of deploying ransomware on corporate networks, as well as maximizing profits through tactics like big game hunting and double extortion schemes. We won't get into the details here, but those interested should check out Talos' Quarterly Incident Response Trends on this topic.

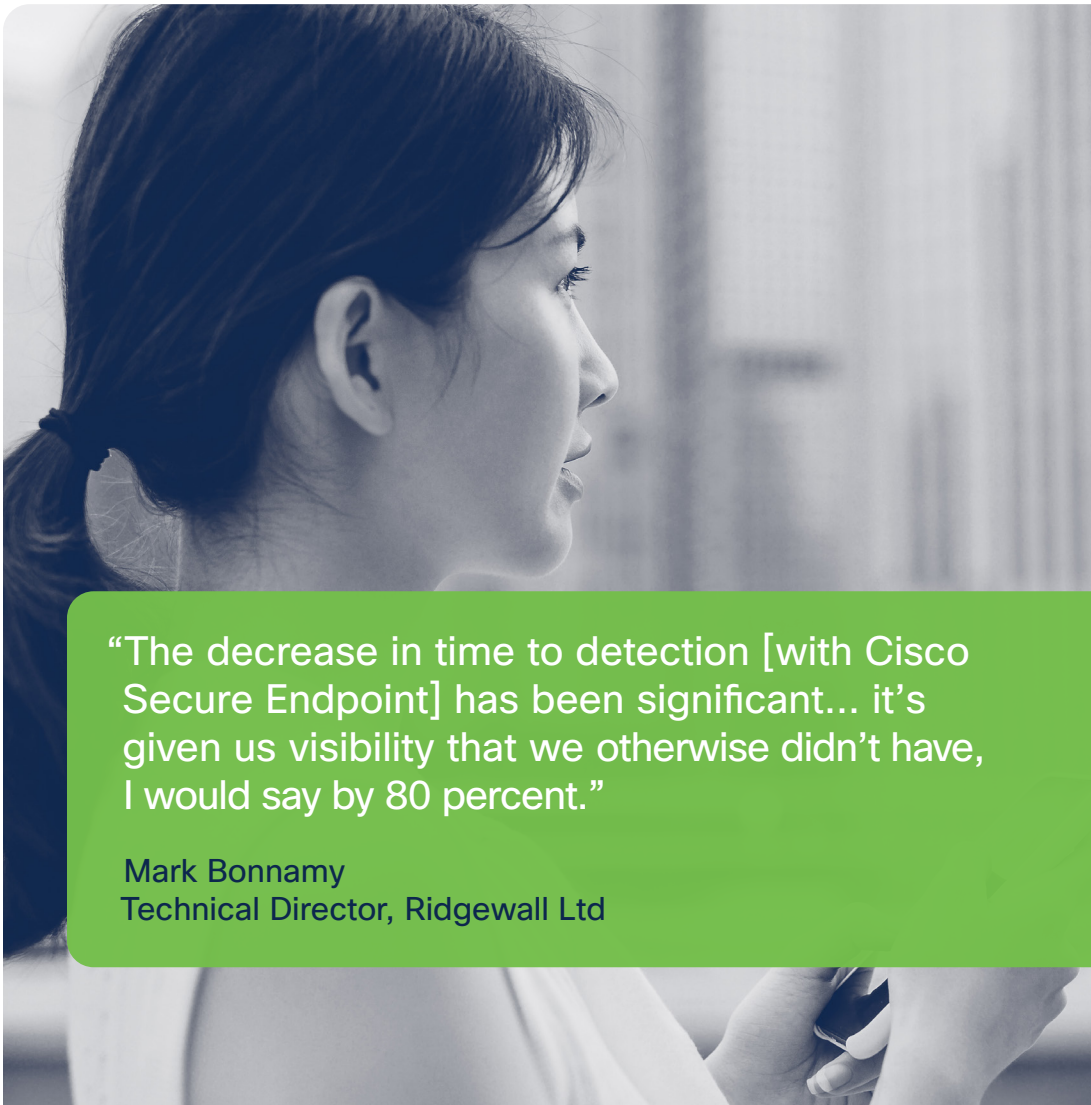
The third most frequently seen IOC group is fileless malware. This type of malware does not use executable files and has no signature for antivirus to detect, making it difficult to identify. Fileless malware often manifests itself via suspicious process injections and registry activity. Common examples of this type of threat include Kovter, Poweliks, Divergent, and Lemon Duck.

Another category of dual-use tools weighs in at #4. Credential dumping is the process used by malicious actors to scrape login credentials from a compromised computer. The most commonly seen of these tools in the second half of 2020 is Mimikatz, which Cisco Secure Endpoint caught dumping credentials from memory.

All told, these first four categories comprise over 80 percent of the critical severity IOCs seen. The remaining 20 percent contains a mix of behaviors known to be carried out by well-known threats like worms, remote access trojans (RATs), and banking trojans, with a mix of various downloaders, wipers, and rootkits rounding out the "Other" category.

Want to know how these stats compare to events detected by Cisco Secure Endpoint during the first half of 2020? Check out this two-part blog series:

- https://blogs.cisco.com/security/threat-landscape-trends-endpoint-security
- https://blogs.cisco.com/security/threat-landscape-trends-endpoint-security-part-2



"The decrease in time to detection [with Cisco Secure Endpoint] has been significant… it's given us visibility that we otherwise didn't have, I would say by 80 percent."

Mark Bonnamy
Technical Director, Ridgewall Ltd

Adversary Tactics Observed at the Endpoint

Another way to look at the IOC data is by using the tactic categories laid out in the MITRE ATT&CK framework. Within Cisco Secure Endpoint, each IOC includes information about the MITRE ATT&CK tactics employed. These tactics can provide context on the objectives of different parts of an attack, such as moving laterally through a network or exfiltrating confidential information.

Multiple tactics can also apply to a single IOC. For example, an IOC that covers a dual-use tool such as PowerShell Empire covers three tactics:

1. Defense Evasion: It can hide its activities from being detected.
2. Execution: It can run further modules to carry out malicious tasks.
3. Credential Access: It can load modules that steal credentials.

With this overlap in mind, let's look at the top MITRE ATT&CK tactics as a percentage of all critical IOCs seen:

MITRE ATT&CK Tactic	% of critical IOCs
Defense Evasion	50%
Execution	42%
Persistence	31%
Impact	22%
Lateral Movement	17%
Credential Access	16%

Table 1: Top MITRE ATT&CK tactics based on critical IOCs detected by Cisco Secure Endpoint

Defense Evasion is the most common tactic and accounts for 50% of critical IOCs seen. That's not at all surprising—what criminal do you know who wants to get caught? Tactics for evading detection are myriad, including bypassing user access controls, hiding evidence, and disabling security mechanisms.

Execution, which involves an adversary attempting to run malicious code, lands at the #2 spot. Most multi-stage attacks involve deploying malware to aid initial access, move laterally in the environment, and maintain persistence. For example, an attacker that has established persistence using a dual-use tool may follow up by downloading and executing a credential dumping tool or ransomware on the compromised computer.

We've just mentioned Persistence and Lateral Movement. These tactics allow attackers to set up shop in your environment and expand their operations. It's worth noting that the relative percentage of detections pertaining to persistence jumps dramatically when viewing critical severity IOCs (because it's a red flag for adversary presence).

Impact encompasses adversaries attempting to manipulate, interrupt, or destroy systems and data. It rose up the rankings over the second half of the year concurrently with the increase in ransomware detections.

Credential Access rounds out the top ATT&CK tactics based on critical IOC detections by Cisco Secure Endpoint. In many ways, this ties to other tactics shown here as threat actors attempt to exploit trust and permissions to accomplish their illicit activities under the radar.

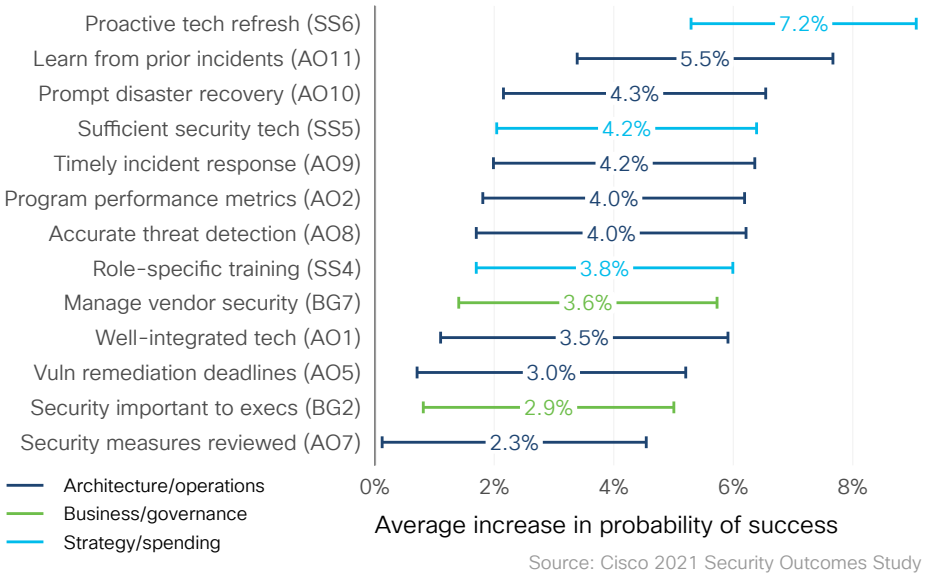
From the detections highlighted above, it should be clear that endpoint security solutions can help mitigate diverse threats that lead to major incidents and losses. Let's keep pulling on that thread and detour back to the Security Outcomes Study to see if it sheds light on other outcomes driven by endpoint security solutions.

Proven Success Factors for Endpoint Security

We mentioned earlier in this report that 43% of survey respondents said their organizations are successful in avoiding major security incidents. That begs the question of what makes those firms succeed when the majority are struggling.

Answering that question is the entire focus of the Security Outcomes Study. We conducted an extensive multivariate analysis of response data to identify security practices that correlate strongly with successful program-level outcomes. Below you'll find a chart from the study listing practices that, according to the data, measurably increased the probability of participants reporting that their firms are avoiding major incidents and losses.

Figure 5 shows the change in probability of overall program success as a range. Read it like this: "A proactive tech refresh strategy increases the chance of successfully avoiding major incidents and losses by roughly 5% to 9%, with an average of 7.2%."

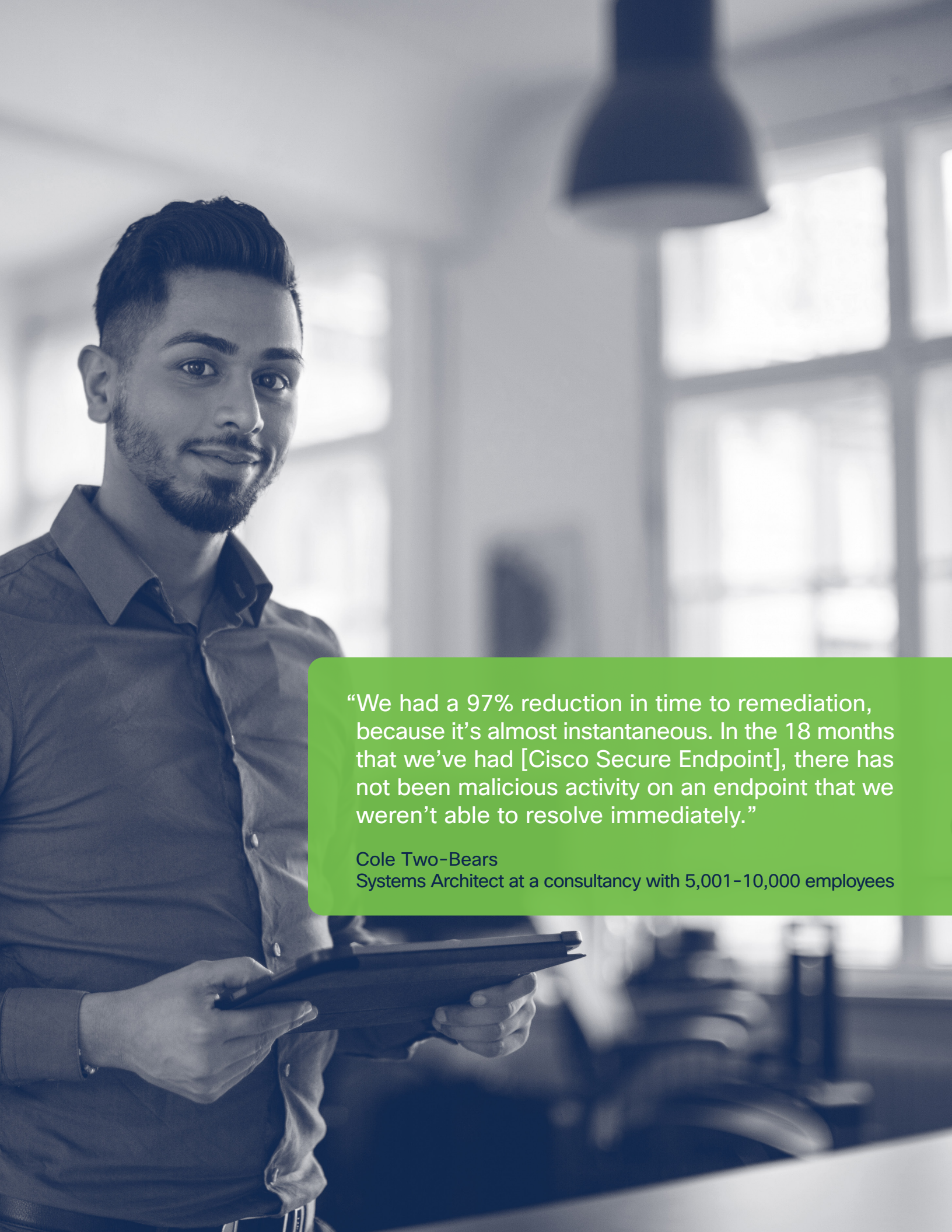


Source: Cisco 2021 Security Outcomes Study

Figure 5: Top security success factors for avoiding major incidents

Figure 5 lists practices from top to bottom based on their strength of correlation with respondents claiming success in avoiding major incidents and losses. You'll find fuller versions of these short labels in the Appendix of the Security Outcomes Study. The bars and values indicate the expected increase in probability of success associated with each practice.

So, as stated above, organizations that pursue a proactive refresh strategy to stay current with the latest and greatest security technologies were, on average, 7.2% more likely to avoid major incidents. That might not sound like much, but you should know by now that there's no silver bullet solution for avoiding major security incidents. Success is found in the combined effect of many practices woven together into a cohesive defense. And you'll accomplish that much faster if everything you weave in contributes to the objective.



"We had a 97% reduction in time to remediation, because it's almost instantaneous. In the 18 months that we've had [Cisco Secure Endpoint], there has not been malicious activity on an endpoint that we weren't able to resolve immediately."

Cole Two-Bears
Systems Architect at a consultancy with 5,001-10,000 employees

Avoiding Incidents with Cisco Secure Endpoint

You've probably noticed that nothing in Figure 5 explicitly states "endpoint security." We just didn't get that specific in the practices we included in the study. Nevertheless, we can't help but see several hints of endpoint features in what's listed there. In the sections that follow, we examine how Cisco Secure Endpoint helps organizations implement these proven practices that help them successfully avoid major security incidents and losses.

Threat Detection and Incident Response

Accurate threat detection and timely incident response are the bread and butter of endpoint security solutions. The ability to identify and mitigate malicious behaviors at the endpoint is crucial for building a comprehensive defense against adversary tactics like those mentioned above. There are several ways in which Cisco Secure Endpoint helps organizations implement these practices.

Cisco Secure Endpoint uses multiple approaches to prevent and detect threats. We demonstrated the utility of IOCs for this purpose in an earlier section. Since IOCs only work for known threats, Cisco Secure Endpoint includes machine learning algorithms that help detect never-before-seen threats at the point of entry. The solution also supports complex queries across all endpoints, and continuously monitors all file activity to detect stealthy malware. Furthermore, the threat hunting capabilities facilitated by Cisco Secure Endpoint help produce high-fidelity alerts.

It's impossible to prevent all threats all the time, so Cisco Secure Endpoint also offers advanced capabilities to investigate and remediate security incidents. Powerful tools like file trajectory and device trajectory use continuous analysis to show the full scope of malicious activity. Cisco Secure Endpoint identifies all affected applications, processes, and systems to pinpoint patient zero, as well as the method and point of entry.

The Advanced Search capability in Cisco Secure Endpoint streamlines security investigations by providing over 200 pre-canned queries, allowing complex inquiries to be run on any or all endpoints. This provides deeper visibility into what happened to an endpoint at the point of compromise, or at any given time, by taking a forensic snapshot of its current state.

When necessary, Cisco Secure Endpoint allows for automated isolation of endpoints that have been compromised to stop threats from spreading and communicating with command-and-control (C&C) hosts on the Internet. The endpoint can then be de-isolated through a single click by the admin or through an unlock code by the user. Throughout this endpoint isolation process, you won't lose the ability to communicate with your trusted resources, including the Cisco cloud servers for file disposition lookups and more.

Sufficient Technology and Proactive Refresh

Beyond those staple Cisco Secure Endpoint features, we also see association with a proactive tech refresh strategy and maintaining sufficient security technologies from Figure 5. We'll start with the latter because it's fundamental to the former. The longer version of this statement posed to survey respondents makes it more clear what we're getting at here: "*Our security program has the technology and tools needed to successfully achieve its mission.*"

Granted, that's pretty vague, but it basically says that adequate technology is an important component of success. Because endpoint security solutions provide visibility and control where other types of security tools cannot, they've become essential technology for defending against advanced threats.

Of course, just deploying a technology (endpoint solutions included) won't remain effective indefinitely due to the evolving nature of cyber threats. That's likely one of the big reasons why respondents who said their firm's tech refresh strategy emphasizes proactive upgrades to best-of-breed IT and security technologies were significantly more likely to avoid major incidents and losses. Conversely, those who indicated that their firms rarely upgrade infrastructure or only do so when things break showed reduced rates of success.

There are numerous ways in which Cisco Secure Endpoint implements a proactive approach to keeping current. IOCs are continually refreshed to maximize detection of known threats. Behavioral analysis and activity patterns are dynamically updated as threats evolve. Machine learning capabilities in Cisco Secure Endpoint are fed by the comprehensive intelligence of Cisco Talos to ensure a better, more accurate model.

Additionally, new endpoint queries are added for the most common use cases like incident investigations, vulnerability and compliance, threat hunting, IT operations, and more. Incident response playbooks are regularly enriched with new hunts and lessons. And don't forget, when it comes to tech refresh, making sure you have the most updated version of Cisco Secure Endpoint allows you to have the latest and greatest defenses against threats.

Prior Incidents and Performance Metrics

The inclusion of 'learn from prior incidents' and 'program performance metrics' in Figure 5 might not elicit thoughts of endpoint security, but there is a connection here too. For example, Cisco Secure Endpoint uses continuous monitoring to correlate new threat information with past history, and automatically quarantines files the moment they start to exhibit familiar malicious behavior. This automated response to the latest threats provides a faster time to detection and greatly reduces the proliferation of malware.

Another example of how Cisco Secure Endpoint uses lessons from the past to fight present battles is found in a highly secure sandboxing environment powered by Cisco Secure Malware Analytics (formerly Threat Grid). This capability analyzes the behavior of suspect files, and records the severity of behaviors, the original file name, screenshots of the malware executing, and sample packet captures. Armed with this information, defenders have a better understanding of what is necessary to contain the outbreak and block future attacks.

Dashboards built into Cisco Secure Endpoint include detailed reporting on detected events, as well as powerful operational response metrics. Events and endpoints are categorized by priority and tied into workflows to track progress during investigations. Tracking detection and response metrics over time offers an excellent way to monitor and improve performance levels.

A Well-Integrated Security Solution

One of the main lessons from the Security Outcomes Study concerns the critical role technology integration plays in building a successful security program. Don't be deceived by this practice landing toward the bottom of Figure 5; we have ample evidence that well-integrated IT and security technologies have myriad benefits.

Take Figure 6, for example. These results come from a question we asked participants in the Security Outcomes Study regarding the primary decision factors organizations used to select from the many security solutions on the market. It's abundantly clear from the chart that organizations strongly desire security solutions that integrate well with their existing infrastructure.

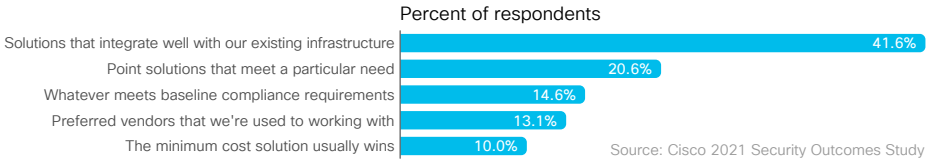


Figure 6: Primary factors driving the selection of security solutions

It's good to know what decision makers value, but their preferences don't always align with what features provide the greatest efficacy for a given purpose. In this case, we were able to test whether the desire for integrated technologies correlated with a measurable reduction in the likelihood of major security incidents. Figure 7 presents the compelling results of that test.

Organizations that typically go with the least costly solution show an incident rate of 58%. By contrast, 36% of those that seek solutions that integrate with their existing infrastructure report major incidents. **Organizations that prioritize integrated solutions were 22% less likely to have reported a major security incident in the last two years!**

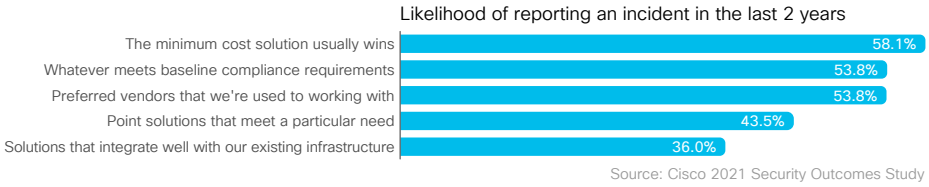
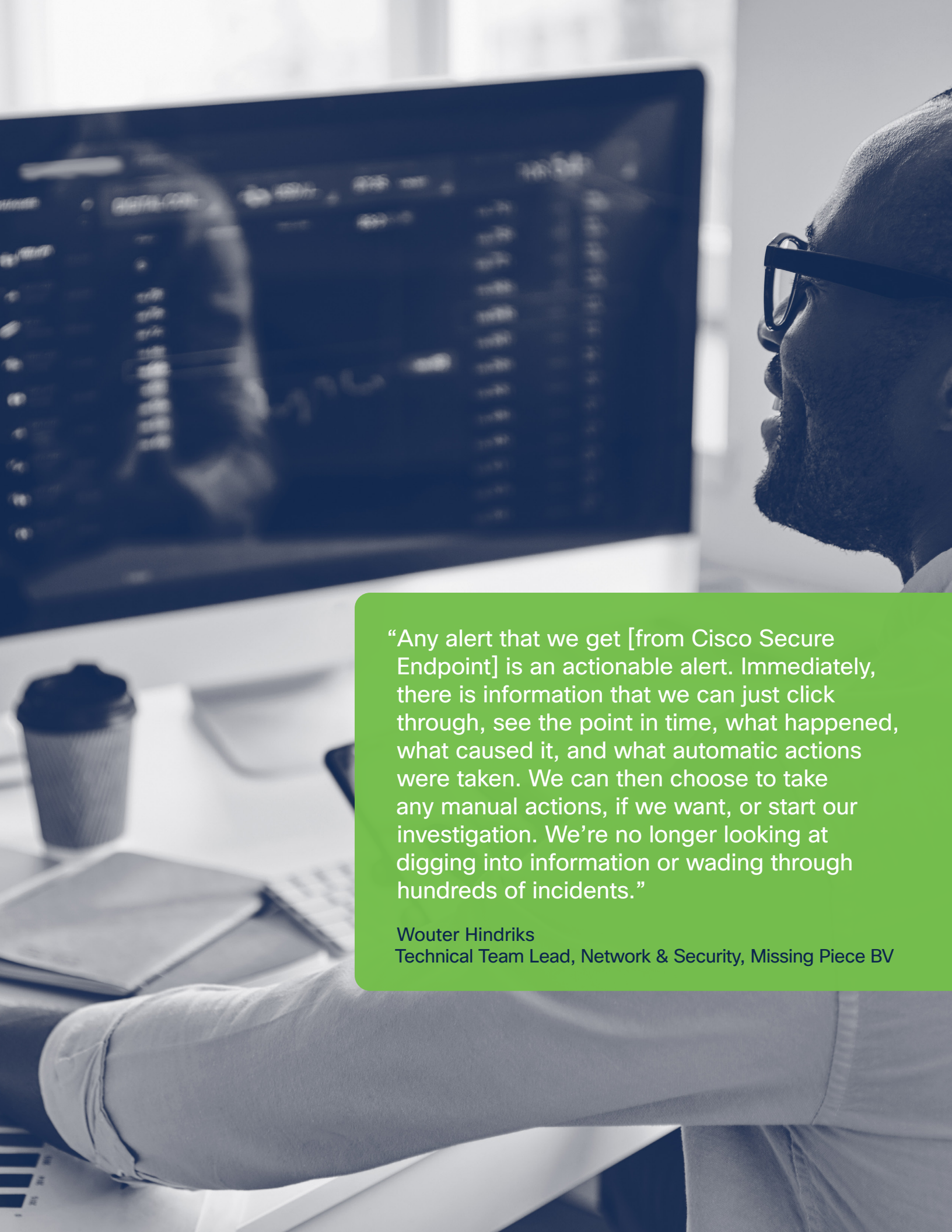


Figure 7: Incident likelihood according to primary factors driving the selection of security solutions

So, what does this have to do with Cisco Secure Endpoint? Glad you asked! Cisco Secure Endpoint is part of Cisco's integrated, platform approach to security known as SecureX. SecureX is included with all Cisco security products, and makes it easier for companies to integrate their endpoint security with other technologies from Cisco and third parties. This allows customers to embrace their existing infrastructure while still transitioning to emerging security solutions such as SASE, Zero Trust, and XDR.



"Any alert that we get [from Cisco Secure Endpoint] is an actionable alert. Immediately, there is information that we can just click through, see the point in time, what happened, what caused it, and what automatic actions were taken. We can then choose to take any manual actions, if we want, or start our investigation. We're no longer looking at digging into information or wading through hundreds of incidents."

Wouter Hindriks
Technical Team Lead, Network & Security, Missing Piece BV

Contribution of Cisco Secure Endpoint to Other Outcomes

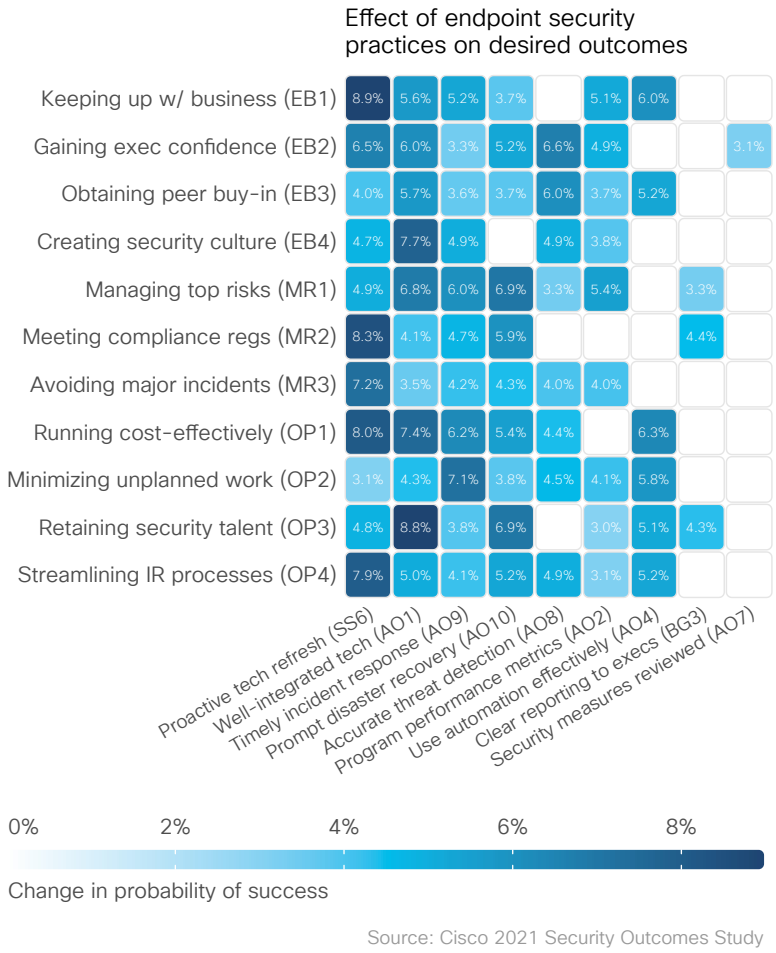
Up to this point, we've talked a lot about major security incidents and how to avoid them. But the Security Outcomes Study examined 10 other outcomes that all combine to create a successful program. The question we'd like to ask in this final section is whether we see any evidence that Cisco Secure Endpoint can help organizations achieve success across these other outcomes.

The first step in answering that question is to create a mapping of the 25 security practices to the features and capabilities of Cisco Secure Endpoint. We started that process in the prior section for practices that the Security Outcomes Study identified as correlating strongly with avoiding security incidents. Completing that mapping process found the following practices to be most closely tied to Cisco Secure Endpoint:

AO1	Our security technologies are well integrated and work effectively together
AO2	Our security program uses performance metrics to drive operational decisions and actions
AO4	We use automation effectively to improve the efficiency of security operations and personnel
AO7	Our security measures are actively monitored and regularly reviewed to verify and maintain their effectiveness
AO8	Our threat detection capabilities provide accurate awareness of potential security events without significant blind spots
AO9	Our incident response capabilities enable timely and effective investigation and remediation of security events
AO10	Our recovery capabilities minimize impact and ensure prompt restoration of assets affected by security incidents
BG3	My organization's top executives receive clear reporting on the activities and effectiveness of the security program
SS6	My organization has a proactive tech refresh strategy of frequent upgrades to best available IT and security technologies

Table 2: Practices from the Security Outcomes Study most closely aligned with capabilities of Cisco Secure Endpoint

With that done, we'll now adapt a visualization used in the Security Outcomes Study to link these practices (and thereby Cisco Secure Endpoint capabilities) to outcomes. Readers of that report may recall a large matrix consisting of all 25 practices and 11 outcomes. If not, there's a slick interactive version of it on the website associated with the study that should refresh your memory. You'll find a version of that matrix in Figure 8 that correlates the practices from Table 2 with the outcomes they help organizations achieve.



Source: Cisco 2021 Security Outcomes Study

Figure 8: Security practices and outcomes most closely aligned with capabilities of Cisco Secure Endpoint

The percentages in Figure 8 mean the same thing as those back in Figure 5. For example, organizations that report having a well-integrated technology stack were, on average, 5.6% more likely to say their security programs are successfully keeping up with the business (top row; second square). The intensity of coloring indicates the strength of correlation between each practice and outcome combination. But don't get too distracted by numbers and shading. **The bigger message here is that we have good reason to conclude that Cisco Secure Endpoint contributes in multiple ways to all 11 security program outcomes from our study.** That's quite an impressive feat!

We shared many tangible examples of how Cisco Secure Endpoint drives organizational success in the outcome of avoiding major incidents and losses, so we won't retread that territory. But we do want to wrap up this report by providing brief justification as to why and how Cisco Secure Endpoint helps achieve the other outcomes in Figure 8.

Enabling Business

As the title implies, this objective focuses on security's mission of supporting and fostering business activities. The outcomes in this category recognize that security doesn't exist for security's sake; it serves the business.

Keeping up with the demands and growth of the business

One recent example of how Cisco Secure Endpoint enables security to keep up with the business can be seen in the transition to remote work environments in the wake of the COVID-19 pandemic. This completely upended the security architecture of many organizations because a large proportion of endpoints suddenly migrated outside the corporate network perimeter. Endpoint security is increasingly the last critical line of defense for remote employees and the devices they use every day. Cisco Secure Endpoint allows organizations to maintain the visibility and protection necessary to safeguard endpoints, thereby helping the business to safely navigate difficult circumstances.

Gaining the confidence and trust of executive leadership

Many C-suite executives view cybersecurity as insurance against their company landing in the headlines for a major breach or business interruption. Those fears may be why practices that ensure threats are accurately detected and effectively handled rise high among factors that correlate with gaining executive confidence. We already discussed how accurate detection and timely incident response are core capabilities of Cisco Secure Endpoint, so we'll move on to the next outcome.

Obtaining buy-in from peers and other organizational units

Security programs often have a tenuous relationship with peer groups across the organization. Sometimes that's due to them having to continually object to other teams' initiatives over security concerns. IT getting burdened with managing the security program's latest tool is another common gripe. Cisco Secure Endpoint offers a salve for this pain point by eliminating complexity through the integrated Cisco SecureX platform. SecureX brings together a wide range of security, networking, and IT tools, and allows these various teams to work together towards common goals from a single platform. This fosters greater collaboration, operational efficiency, and hopefully more willingness from other teams to work closer with security.

Creating a security culture embraced by all employees

We tend to think of culture as merely a reflection of organizational policies or employee mentality, but the data suggests that technology also plays an important role. If you've ever been frustrated by clunky applications or oppressive security controls, you can get a sense of why this is so. We think Cisco Secure Endpoint's maximum coverage via a single agent with minimal footprint makes it easy for all users to operate securely.

Managing Risk

Managing risk is what most people think of when asked about security's primary responsibility. Of course, risk is multi-faceted, which is why we chose to examine three outcomes that each provide a distinct perspective on how companies manage cyber risk. (Just a reminder that the third outcome, avoiding major incidents, is already discussed at length above.)

Managing the top cyber risks to the organization

Managing the top cyber risks depends upon the ability to see them, and that's exactly why security solutions have migrated to the endpoint over the years. They're literally the ending point of most attacks. As demonstrated in our analysis of 2020 threat detections above, Cisco Secure Endpoint offers visibility into today's most insidious and impactful threats.

Meeting regulatory compliance requirements

We mentioned the Advanced Search capability of Cisco Secure Endpoint earlier. It provides numerous ready-to-go queries that can quickly be run across endpoints. Since compliance often comes down to actually doing what you say you're doing, this ability to get a snapshot of the current state or pull the history of any endpoint at any time can greatly assist with the audit process.

Operating Efficiently

Beyond enabling business and managing risk, the ability to operate efficiently often sets great IT programs apart from the good ones. This last set of outcomes addresses cost-effectiveness, executing strategy, talent management, and incident response processes.

Running a cost-effective security program

"You'll have to install another agent" is not something most IT and security managers want to hear. Cisco understood early on that agent fatigue was an issue—thus having a common agent for an Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) is important. That's why we're thrilled to say that Cisco Secure Client – a single agent that unifies user and endpoint protection – reduces agent fatigue, dramatically minimizing the cost of buying, deploying, updating, and managing multiple agents. This greatly boosts endpoint operational efficiency and cost effectiveness.

Minimizing unplanned work and wasted effort

Security incidents are, by definition, unplanned work and tend to generate a lot of wasted effort. The fog of war that pervades the incident response process has a remarkable way of exposing poor planning and ineffective processes. But it doesn't have to be that way. The suite of EDR capabilities bundled into Cisco Secure Endpoint effectively clears away the fog and shores up those plans and processes. It enables security teams to run advanced investigations across all endpoints, and accelerates threat response through automated playbooks and hundreds of preloaded queries.

Recruiting and retaining talented security personnel

It may seem odd that a security solution would have anything to do with talent recruitment and retention, but our research suggests that good tools attract good people. The cybersecurity profession suffers from a high churn rate, and that's made worse when staff feel their time is wasted on mundane tasks. Cisco Secure Endpoint is designed with the analyst in mind and provides an extensive set of capabilities to help them work effectively.

Streamlining incident detection and response processes

With a suite of advanced EDR tools and integrated XDR capabilities (and more) from SecureX, Cisco Secure Endpoint can cut remediation time by up to 97%. With Cisco Secure Client and Secure Endpoint, customers get deeper visibility across their environment from the cloud to the endpoint, enabling faster threat detection and response.

About Cisco Secure Endpoint

In today's dynamic threat landscape, endpoint security is our last line of defense. At the same time, it's easy for security teams to feel overwhelmed when managing more devices, alerts, and threats. That's why at Cisco, we've made it our mission to empower security teams with a simple, integrated approach to achieving more visibility, collaboration, and efficiency.

Cisco Secure Endpoint uses multiple prevention techniques and posture assessments in a single solution to protect against various attack methods and vectors. With user and endpoint security combined, it provides a coordinated defense to fully expose, contain, and resolve threats. And when paired with SecureX, Cisco Secure Endpoint allows security teams to seamlessly integrate endpoint security with their other solutions, enabling complementary technologies to work together for stronger, more automated protection. Not only does this integrated approach improve security efficacy, but it also reduces complexity and boosts productivity.

Learn more about how Cisco solutions can accelerate your success and secure your future at **cisco.com/go/secure**.

Ready for endpoint security that works for you?
Get started with a free trial today.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published May 2021 Endpoint_05_2021

cisco SECURE

CISCO

SECURE

The bridge to possible