Enterprise Strategy Group™ by TechTarget

ECONOMIC VALIDATION

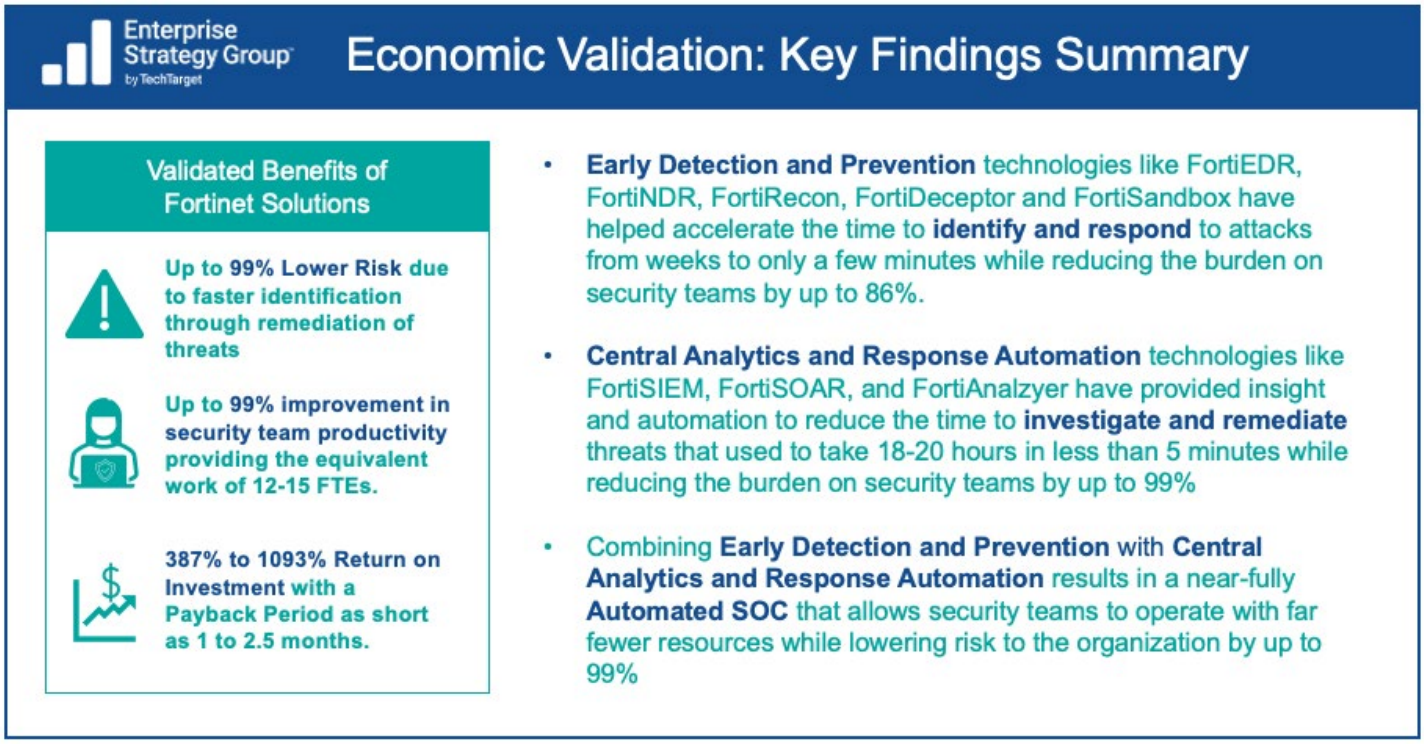
The Quantified Benefits of Fortinet Security Operations Solutions

Improved Security Team Operational Efficiency and Reduced Risk to the Organization, Each by Up to 99%

Aviv Kaufmann, Practice Director and Principal Economic Validation Analyst
Enterprise Strategy Group

July 2023

Contents



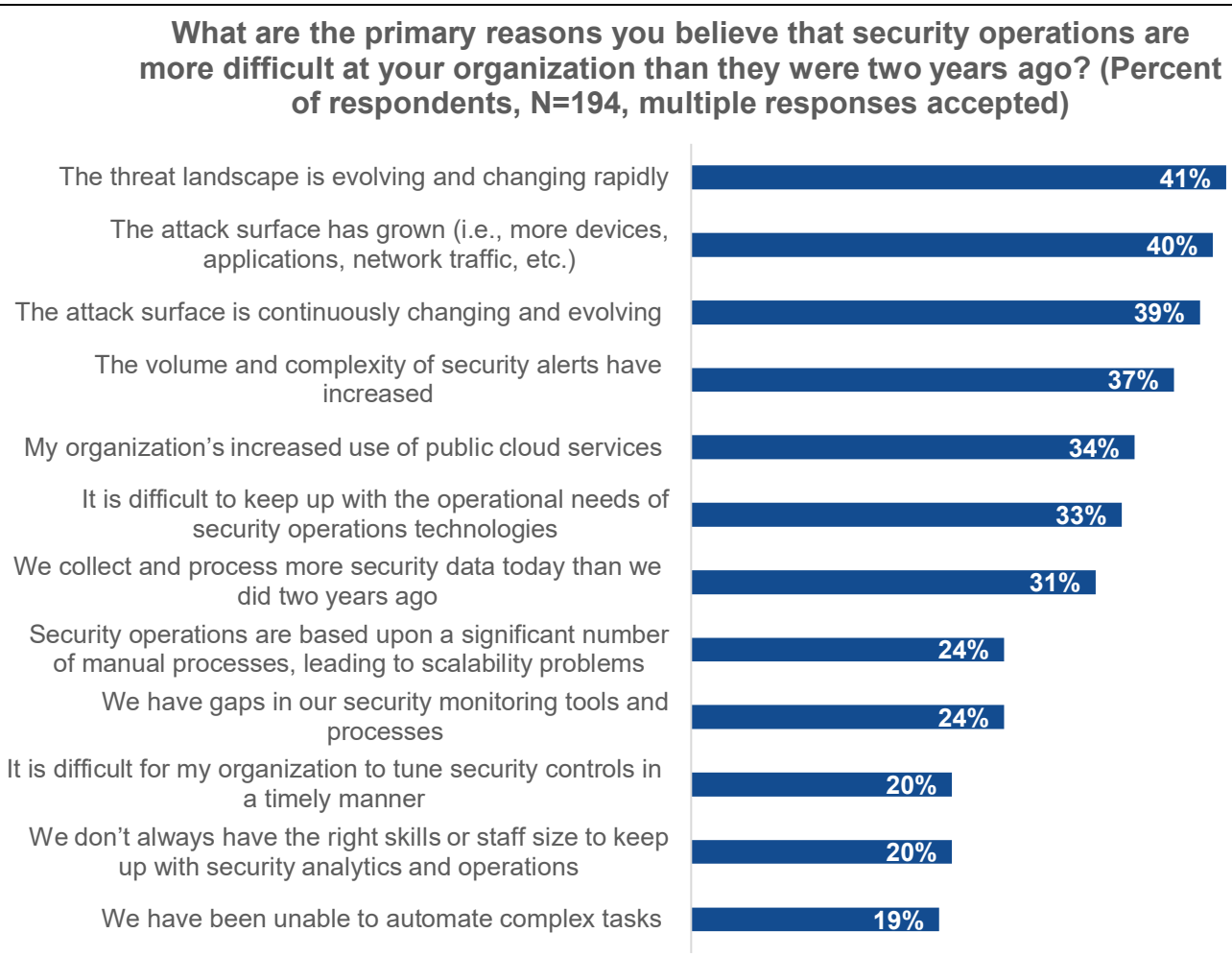
Introduction

This Economic Validation from TechTarget's Enterprise Strategy Group focused on the quantitative and qualitative benefits organizations can expect by using Fortinet Security Operations solutions rather than continuing to use several alternative point security products.

Challenges

Building a modern and effective SOC is costly and increasingly complex. It is difficult and expensive to hire and train security expertise and even more difficult to retain that talent, as resources are always in demand. There is no shortage of tools to choose from, leading many organizations to have to learn multiple interfaces, combat alert fatigue, and manage tool sprawl and overlapping functionality. In fact, despite growing functionality in choice of effective tools, Enterprise Strategy Group research found that 52% of organizations felt that security operations are more difficult today than they were two years ago.[1] The leading drivers of that increased difficulty are shown in Figure 1.

Figure 1. Top 12 Reasons Security Operations Are More Difficult Than They Were 2 Years Ago



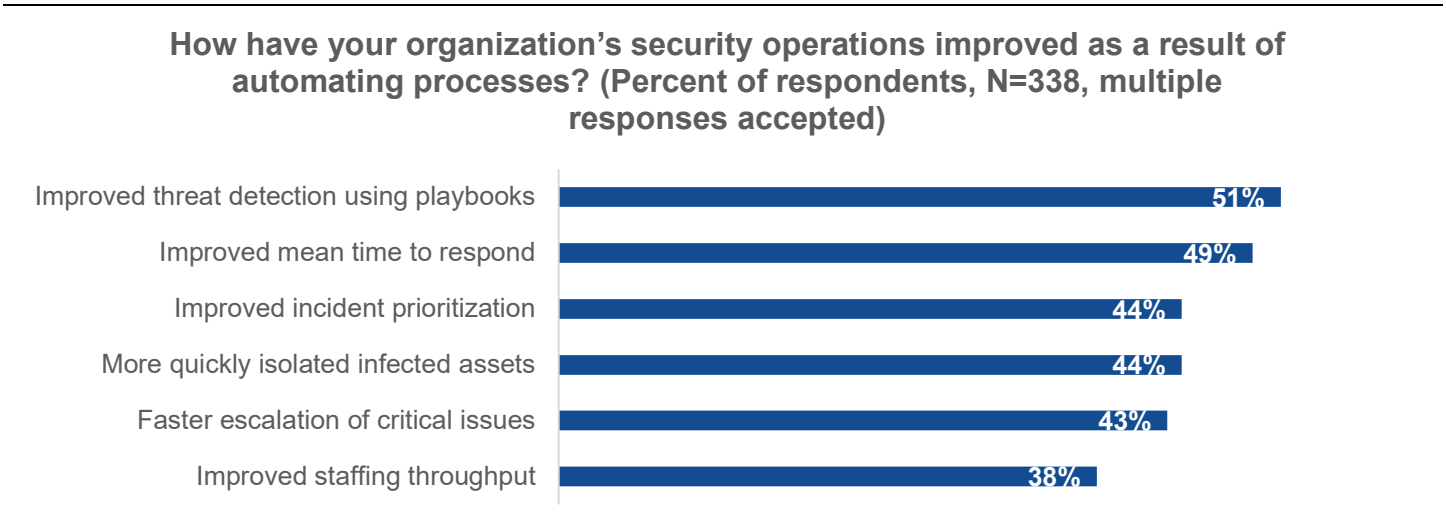
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022. All Enterprise Strategy Group research references and charts in this economic validation have been taken from this report.

As organizations grow and new technologies emerge, the result is a rapidly expanding attack surface, with more threats being created from more sources and across more devices than ever before. Employees are working from more places and using more devices, while companies are integrating IT services with customers and suppliers and shifting toward using more cloud technologies. This places even more pressure on security teams to keep up, and attackers are constantly evolving and trying to stay one step in front of existing security methods and tools. Attackers have access to their own supply chain of shared information and products and are made more effective by using services provided by more experienced cybercriminals such as malware-as-a-service (MaaS) and ransomware-as-a-service (RaaS). They also have access to distributed attacks (such as distributed denial of services or DDoS attacks) and are able to coordinate attacks with other individuals into campaigns that are much harder to detect and prevent against (it is not enough to simply block an IP or particular geography). This can lead to a steep learning curve for SOC teams and makes it difficult to stay ahead of the latest threats. The result is that organizations without colossal budgets required to build and operate an effective SOC are slow to identify and remediate potential attacks.

To become more effective, a SOC may need to integrate with various other tools and systems within an organization to collect more information, such as identity and access management systems, network and application performance monitoring tools, and early detection and prevention (EDP) capabilities focused on specific attack vectors. Ensuring that all these new detection-oriented tools work seamlessly together can be a significant challenge but is necessary to avoid adding to SecOps complexity. Effective automation and orchestration of functions between people, processes, and tools is a critical requirement for the modern SOC. Enterprise Strategy Group research found that, by deploying more early detection and central response tools that integrate to enable automation, organizations have improved their security posture and operational excellence. Specifically, they have improved mean time to detect possible incidents, sped the investigation and validation of these incidents, responded faster to minimize impact, improved incident prioritization, more quickly isolated infected assets, realized faster escalation of critical issues, and improved staffing efficiency. The top factors driving improvement in security operations due to automation are shown in Figure 2.

Figure 2. Automation Has Improved Security Operations



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

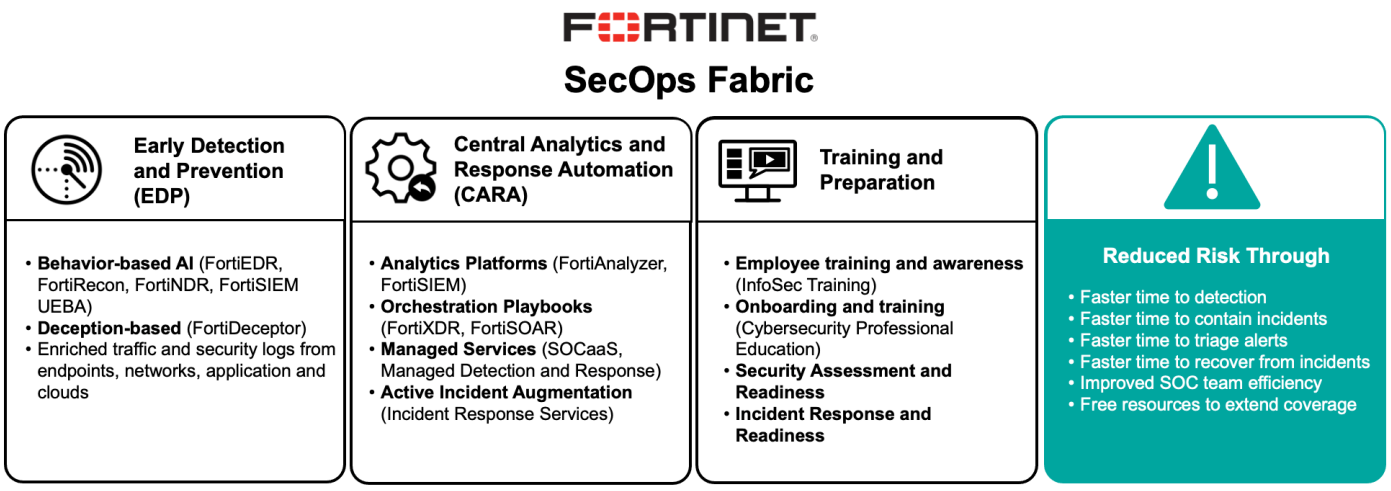
A modern SOC requires a skilled and dedicated team, with the right tools and processes in place, to stay ahead of the evolving threat landscape and protect an organization's digital assets effectively. Proactive training and preparation, effective automation, and synergistic orchestration of security tools is critical to enabling early detection and prevention and reducing risk across the organization.

Fortinet Security Operations Solutions

Fortinet Security Operations solutions provide real-time threat detection and response capabilities to protect organizations against cyberattacks. They are delivered by an integrated SecOps Fabric made up of components that combine threat intelligence, advanced analytics, and automation to help security teams quickly identify and respond to threats. The SecOps Fabric uses machine learning and artificial intelligence (AI) algorithms to analyze massive amounts of data from multiple sources, including network traffic, endpoints, applications, and more. It also leverages threat intelligence from the global network of Fortinet sensors and security operations centers to stay up to date on the latest threats, as well as active threats, and provides security teams with a single pane of glass for visibility and management of security incidents. It uses a closed-loop approach to automate the incident response process, from detection to containment and remediation. This enables security teams to respond quickly and efficiently to threats, reducing the time it takes to detect and mitigate attacks.

Fortinet offers expert security services to support in-house security resources and integrates with the broader Fortinet security portfolio, including firewalls, intrusion prevention systems, and additional endpoint protection solutions. This enables organizations to provide effective and comprehensive protection across the entire attack surface and helps them stay ahead of today's advanced threats and protect their sensitive data and digital assets.

Figure 3. Fortinet Security Operations Solutions



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The SecOps Fabric provides the people, technology, and proven processes to reduce cyber-risk for organizations across three pillars:

- **EDP** – Fortinet provides effective detection and prevention by deploying technologies such as endpoint detection and response (EDR), network detection and response (NDR), user and entity behavior analytics, digital risk protection service, Sandbox, and deception networks. These technologies monitor real-time behaviors and activity, detect anomalies (often using AI), and alert on automated/human attacks as well as external threats, creating an active defense layer. They also integrate with other security tools to automate an effective response, helping to minimize mean time to detection (MTTD) and mean time to response (MTTR).
- **Central analytics and response automation (CARA)** – FortiSIEM provides a comprehensive multivendor visibility, analytics, and incident management solution, while FortiAnalyzer provides a visibility, analytics, and incident response component dedicated to the Fortinet Security Fabric. FortiXDR provides a number of security tools that help small and growing security teams detect and automate response to threats, and

FortiSOAR provides flexible and powerful orchestration and automation for established SOC teams. In addition, Fortinet Managed Detection and Response (MDR) and SOCaaS can offload security team functions, helping midsize organizations with limited resources deliver higher levels of security and offload resources from established SOC teams to focus on other tasks.

- **Training and preparation** – Providing assessments, training, and visibility helps make organizations' employees and business units more aware of potential cyberthreats, with actionable readiness plans that help guarantee immediate and effective responses to contain or prevent potential damage when needed. Technical training helps accelerate onboarding and ramping up of expertise for all security resources.

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group (ESG) completed a quantitative analysis of Fortinet Security Operations solutions. ESG's process is a proven method for understanding, validating, quantifying, and modeling the value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical/economic validation.

ESG conducted in-depth interviews with end users to better understand and quantify how the use of Fortinet products has impacted their organizations, particularly in comparison with previously deployed and/or experienced security operations and solutions. ESG spoke with were organizations that had deployed one or more Fortinet security products. ESG also reviewed vendor-created technical documentation, existing case studies, and third-party analyses and leveraged our own expert analyst opinions and knowledge of the industry, markets, and alternative technologies. The qualitative and quantitative findings around time and effort savings were then used as the basis for a simple economic analysis predicting the potential operational cost savings and reduced risk for an organization.

Fortinet Security Operations Solutions Validation Overview

Enterprise Strategy Group's analysis revealed that Fortinet Security Operations solutions have provided customers with significant savings and benefits across the following three categories:

- **EDP** – Fortinet EDP technologies helped to provide earlier detection and protection against known/unknown threats for customers, employees, and partners (supply chain vendors).
- **CARA** – Fortinet CARA products provided the insight and automation to better identify and take action against threats and reduce the burden on existing security resources.
- **Improved training and preparation** – Fortinet-provided training helped cybersecurity professionals and employees quickly gain the security-related skills they require and offered services to help customers better assess and plan for efficient incident response.

Benefits of EDP

Fortinet EDP products include behavior-based AI products like FortiEDR, FortiNDR, and tools like FortiRecon digital risk protection (DRP) service, FortiSandbox, and FortiDeceptor for zero-false positive detection and detonation. These tools provides enriched traffic and security logs from endpoints, network, applications, and clouds. Customers were able to deploy these products to help identify, triage, and contain incidents in seconds or minutes, as well as provide information that helps accelerate time for investigation and remediation. Fortinet Early Detection and Prevention technologies provide the ability to detect many threats in seconds, which previously would have remained undetected for weeks, with triage and containment in minutes rather than hours. Enterprise Strategy Group validated the following benefits:

- **Improved and expanded coverage of the attack surface:** Customers were able to use the tailored alert data FortiRecon DRP service provides to extend threat intelligence coverage outside of their network control, keep an eye on advisories, and better monitor their brand. In addition, External Attack Surface Management (EASM) can help to identify attacker-exposed assets, leaked credentials, code vulnerabilities, misconfigurations, and more. Customers felt that they were able to cover more of the potential attack using the FortiRecon DRP service to monitor for brand and executive impersonations, as well as data breaches and ransomware attacks relevant to them and their supply chain vendors. Companies reported that they were able to identify and protect assets that they did not even know existed, helping to reduce the number of exposed assets.

> **"FortiRecon allows us to find potentially stolen credentials and monitor websites to identify sites that we did not know about and reduce risk by finding sites that are typo squatting or potentially harmful to our customers."**

- **Increased number of threats detected:** Customers reported that by using Fortinet early detection and prevention products, they were able to identify up to 94% more threats than they had before deploying these products. Without these tools, customers reported that most of the threats would not even be known until they had caused damage. Fortinet tools provided them with better coverage of the attack surface, AI-based analysis, and deception-based defenses (FortiDeceptor) to do a better job of detecting sophisticated known and unknown attacks that otherwise may have gone unnoticed or been successful.

> **"Without our Fortinet security tools, we were completely blind. We would often have to wait for something to cause damage before we even knew to act on it. We knew we needed to be more proactive."**

- **Faster time to detection:** Customers reported that, on average, Fortinet EDP technologies like FortiEDR, FortiNDR, and FortiDeceptor helped them to reduce MTTD by 99% or more. While it is difficult to quantify because, before Fortinet, many threats would have gone undetected until after they had done damage, customers reported that the threats that were now found in minutes would have taken days to weeks to find before, if at all, giving the organization earlier warning and enabling quicker intervention.

> **"FortiEDR monitors our processes, identifies anomalies, and quarantines the threat almost instantly—even if it is a zero-day threat."**

- **Faster time to contain threats:** In addition to earlier detection of threats, Fortinet customers also reported that FortiEDR provided the ability to automate the containment of known threats by taking actions directly in the next-generation firewall, unified threat management systems, or endpoint protection platforms. FortiDeceptor and FortiSandbox were used to proactively identify and contain potentially harmful access or operation (part of human/automated attacks) and quickly quarantine the attack and investigate files. Customers reported that they were able to reduce the time to contain incidents from 4-9 hours to only a few minutes, or even seconds, which was up to 88% faster where human interaction was required and up to 100% faster for automated containment. Customers also reported that, with FortiEDR, when threats were quarantined, the user was able to continue working without impact to productivity until a responder was able to remediate the issue. **"Before FortiEDR, it was 100% dependent on someone happening to see something and then taking about 1 hour to manually contain; now it is instantaneous, and we catch almost everything."**
- **Improved SOC productivity –** In addition to threat detection and containment, Fortinet early detection and prevention tools provided zero false positive detection with tools, such as FortiDeceptor and FortiRecon, in addition to timely and prioritized insight to security teams that helped to reduce the number of hours required to fully investigate and remediate threats. On average, this insight made security teams up to 86% more

operationally efficient and freed them to investigate complex cases deeper, invest in training, and collaborate with other areas of the organization.

These improvements are summarized in Table 1.

Table 1. Enterprise Strategy Group Validated Benefits of Fortinet EDP

Security Task	Baseline (Manual Operations)	Fortinet EDP Technologies	Technology Description
Time to identify threats	168 Hours or more (many threats never detected)	Under 1 Hour (in seconds for most)	Behavior-based protection and detection
Time to triage threats	8 Hours	10 Minutes	Threat insight and automated validation
Time to contain threats	4.2 Hours	1 Minute	Automated containment

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Benefits of CARA

With early detection and prevention tools, Fortinet customers were able to dramatically speed time to detection and containment, with modest improvement to investigation and response. By adding tools that provide CARA (FortiSIEM, FortiSOAR, FortiAnalyzer), customers are able to fundamentally improve security team productivity through automation and orchestration and augment their security teams with experienced Fortinet managed services (FortiMDR and SOCaaS). After adding CARA, customers reported a reduction of time to investigate and time to remediate each incident from hours to minutes, a major time savings given alert and incident volumes. In fact, one customer estimated they would have to hire 12-15 additional resources to accomplish what's currently handled by their team of 3 with the help of Fortinet technologies and services. CARA provided customers the following benefits:

- **Automated and intelligent detection:** Fortinet combines improved visibility, automated response, and threat intelligence into easy-to-use products like FortiAnalyzer, FortiSIEM, FortiXDR, and FortiSOAR, which help organizations further improve advanced detection and accelerate triage. Teams reported that they were able to leverage the AI-powered intelligence built into these products to identify and detect more critical threats. By combining the insights from different tools and analyzing interactions with AI, organizations were in a better position to be able to detect and identify complex and coordinated attacks across multiple vectors.

> **"When we tell people that we don't even have a security engineer, people's jaws drop because Fortinet gives us the technologies we need to secure our environment and be totally hands off."**

- **Reduction in the number of false positives:** Fortinet customers leveraging the automated intelligence built into these products were able to reduce the number of false positives by 85%, enabling their security teams to focus their attention where it was most needed.

- **Automated response triage:** Teams reported that by automating the triage of alerts and orchestrating the required actions of evaluating, assessing, confirming, and prioritizing incidents for response, triage went even faster. Because these tasks were nearly fully automated, customers were able to triage alerts in only a few minutes, rather than the 10 minutes with the Fortinet early detection products or the 4-9 hours it took their teams previously without them.
- **Improved time to contain, remediate, and recover from incidents:** Leveraging analytics and intelligence, automating response and playbooks, and orchestrating events across people and technologies help to create a more automated SOC, which improves productivity and minimizes the time to contain, remediate, and recover from incidents faster. Since deploying FortiSOAR and/or FortiXDR, teams reported that they were able to contain incidents on the device immediately and then follow up with automated east-west containment in under five minutes and with little to no manual steps. This was nearly 100% faster than the 4 hours, on average, it took to contain incidents manually and without the use of Fortinet early detection products. In addition, teams were able to fully remediate and recover from incidents in about 8 minutes, on average, compared to the 6 to 12.5 hours it took to remediate manually.
- **Improved security team scalability and capabilities:** Fortinet managed services such as SOCaaS and Managed Detection and Response were used by customers to augment and reduce the burden on resource constrained security teams and/or improve the scale of their security operations without having to hire and train new full time security engineers. Teams reported that the MDR service enabled their limited resources to focus on the easier tasks and that the more experienced Fortinet MDR service could handle the more complex cases. Teams also reported that their resources were able to learn from the MDR teams and build their own capabilities to better handle similar issues in the future. Customers estimated that they would need to hire 4 full-time experienced security analysts to do the work that they used the MDR service to accomplish.

> **"Adding SOAR and Analytics reduced the number of false positives by 85%, and this continues to improve over time as we learn more."**

- **Improved operational efficiency of existing security resources:** Leveraging Fortinet CARA offerings helped security teams spend less time and operate more effectively at nearly every task they performed. Fortinet products enabled them to spend up to 99% less time responding to incidents, freeing them to focus on deeper investigations of complex cases and growing their capabilities. One customer was able to run its security operations with a team of only 3 full-time network and security resources and estimated that they would need to hire an additional 12-15 resources to accomplish the work that they were able to automate with Fortinet.

> **"We can go to any one of our three tools (EDR, Analyzer, SIEM) and run a report over a custom time period to give us the information that we need to triage in minutes versus a meeting with the whole team logging into our devices and trying to figure out what we were seeing—this could even take days."**

The productivity savings provided by using Fortinet CARA platforms are summarized in Table 2.

Table 2. Enterprise Strategy Group Validated Benefits of Fortinet CARA

Security Task	Baseline (Manual Operations)	Fortinet CARA Technologies	Technology Description
Time to investigate threats	6 Hours	1 Minute	AI-powered intelligence, automation, and orchestration
Time to remediate threats	12.5 Hours	5-10 Minutes	Fully or partially automated response with playbooks

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Benefits of Improved Training and Preparation

The customers that we spoke with generally reported that they felt they didn't have sufficient security team resources to protect the organization using manual security processes. Fortinet offered these customers a number of services to help improve the overall effectiveness of their security teams and internal processes. This included training that helps to onboard and increase the capabilities of security professionals and reduce risk by educating employees about security risks. Security assessments and readiness programs also help to better prepare organizations and employees for potential scenarios. The potential benefits of Fortinet Training and Preparation services include:

"I think education is key—the more that you expose your end user base to the dangers of emails and what to do and what not to do around phishing campaigns, the better off the company is."

- **Improved employee awareness and training:** Infosec training can result in employees who are more aware and can better identify and avoid risk around file, password and email risks, website phishing campaigns, etc.

  By educating more employees, organizations can reduce the number of potential harmful links and emails that their employees click on, helping to reduce risk for the organization. One customer estimated that this type of training helped to reduce the number of people that clicked on harmful links by 84%. This ultimately results in fewer cases that have to be responded to by security teams, freeing them up to focus on other tasks.

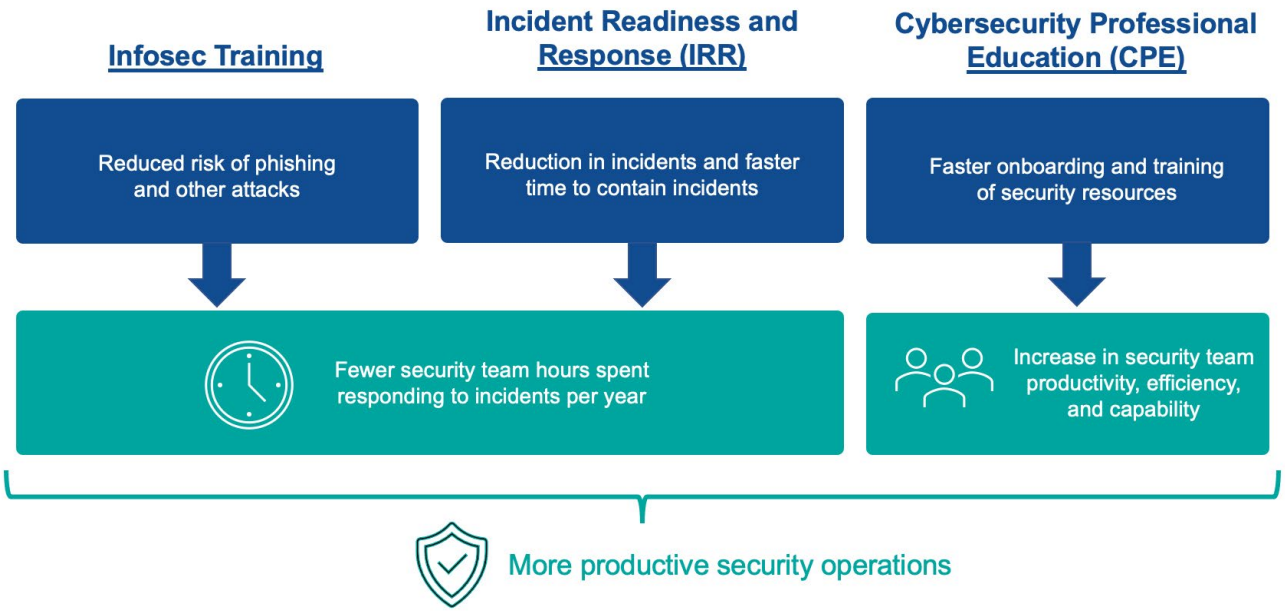
- **Faster onboarding and training of security team resources:** Customers that leverage Fortinet Cybersecurity Professional Education benefit from quicker training and reduce the average time to onboard newly hired cybersecurity employees. Advanced training for existing cybersecurity resources can quickly make them more effective at performing the security-related tasks that they need to perform. By onboarding new employees faster and providing advanced training for existing resources, companies reduce the time to grow their security capabilities, resulting in a more effective team and reducing risk to the organization.

Why This Matters

Predicting the benefits provided by security products comes down to how much more efficient you can make existing resources and how much you can reduce risk to the organization through faster, more intelligent, and more comprehensive detection through remediation.

- **Improved security processes and workflows:** Incident response and readiness (IRR) security assessments and readiness planning help security organizations improve their existing processes, extend their coverage, and speed the time it takes their organization to detect, contain, investigate, and remediate issues. Customers felt that IRR programs could help them to improve their operational efficiency while reducing the number of incidents and reducing the time required to contain incidents.

Figure 4. Benefits of Fortinet Training and Preparation Services



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Analysis

Enterprise Strategy Group (ESG) leveraged direct customer interviews as well as the information collected through vendor-provided material and public and industry knowledge of economics and technologies to report and model the expected savings and benefits that customers could expect by deploying Fortinet solutions. ESG's interviews with customers who have deployed the technologies, combined with experience and expertise in economic modeling and technical validation of security products helped to form the basis for our modeled analysis.

Specifically, ESG utilized the average times to identify, triage, contain, investigate, and remediate threats reported by customers in a series of interviews covering each of three cases:

- **Baseline Case** – The time, prior to selecting Fortinet SecOps Fabric components, estimated to manually identify and deal with threats.
- **Fortinet EDP Case** – This case reflects the estimated time (and time savings) to automate the identification, triage, and containment of threats when using early detection technologies like FortiEDR, FortNDR, FortiRecon, FortiSandbox, and FortiDeceptor. It also reflects the time (and time savings) expected to investigate and remediate issues based on the information provided by early detection tools.
- **Fortinet EDP with CARA Case** – This case adds the CARA technologies of FortiAnalyzer, FortiSIEM, FortiXDR, FortiSOAR and FortiGuard MDR service for improvement in the time to conduct broader incident investigation and coordinated remediation.

Table 3 summarizes the validated combined improvements of using both Fortinet EDP and CARA technologies:

Table 3. Enterprise Strategy Group Validated Benefits of Fortinet EDP with CARA

Security Task	Baseline (Manual Operations)	Fortinet EDP + CARA Technologies	Technology Description
Time to identify threats	168 Hours or more (many threats are never detected)	Under 1 Hour (in seconds for most)	Behavior-based protection and detection
Time to triage threats	8 Hours	5 Minutes	Threat insight and automated validation
Time to contain threats	4.2 Hours	1 Minute	Automated containment
Time to investigate threats	6 Hours	1 Minute	AI-powered intelligence, automation, and orchestration
Time to remediate threats	12.5 Hours	5-10 Minutes	Fully or partially automated response with playbooks

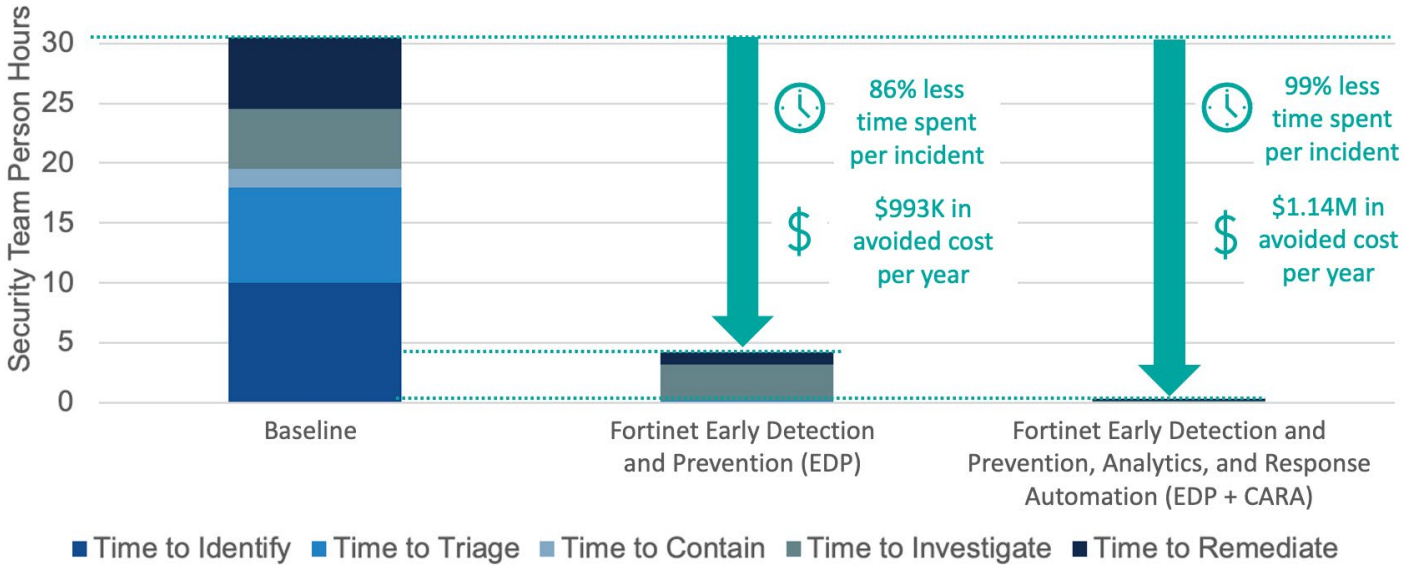
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Operational Savings

The expected average calendar times reported to identify, triage, contain, investigate, and remediate threats are summarized in Table 1 and Table 2 of this report. Enterprise Strategy Group then estimated the expected person-time spent (comprising effort made by a range of titles/functions within an organization) for each of these tasks based on which functions could be automated versus manually performed (this time can vary widely for an organization based on technologies, people, and processes in place). Most of these times were very similar to those reported in the tables, except for the baseline case, in which much more idle time would be expected between tasks, especially for identification of threats.

Using these expected times, Enterprise Strategy Group was able to model the expected operational savings provided by Fortinet technologies against the baseline case. We found that using Fortinet EDP technologies could reduce the average time spent per incident by 86%, and adding Fortinet CARA technologies could provide a 99% time savings over the baseline case. Our modeled analysis, based on a 6-person security team (in house or managed service) with an average hourly rate of $100/hour, concluded that the expected time savings would enable the 6 resources to perform the work of a much larger team, avoiding between $993K to $1.14M in annual operational cost. The results of our analysis are shown in Figure 5.

Figure 5. Operational Savings



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

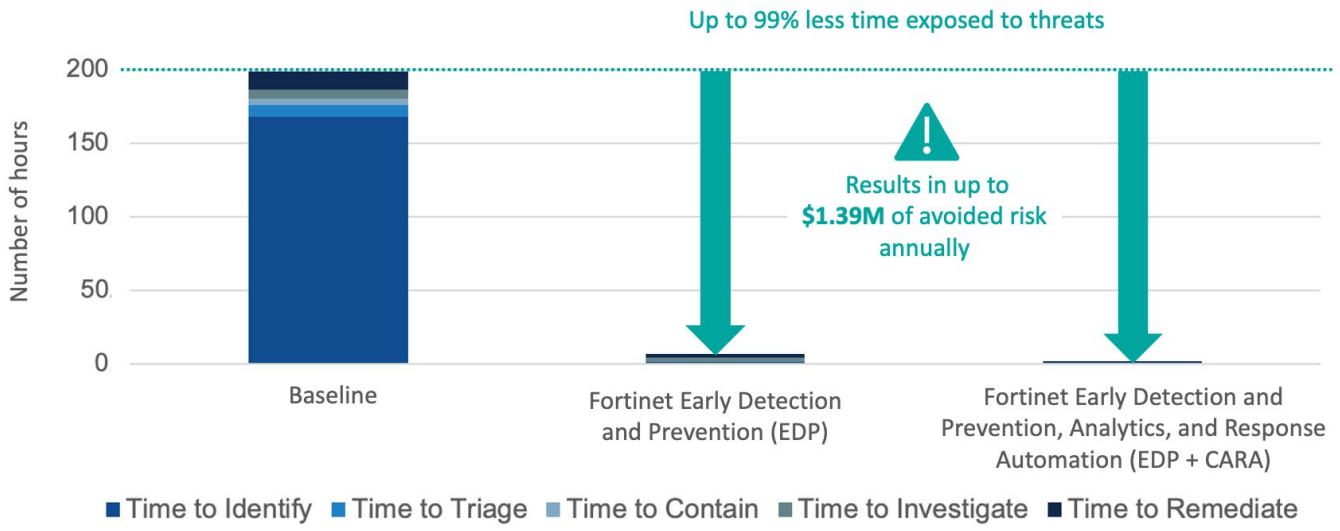
The savings predicted by our conservative analysis predicts that an organization could avoid roughly doubling the size of their security team from 6 to 12 (based on dividing the annual savings by the fully burdened cost of an analyst). It should be noted that the organizations we spoke with estimated that they would require maybe 3 times the number of analysts to handle incidents without Fortinet products, and even then, they would not benefit from the same level of protection. By adding the Fortinet Managed Detection and Response service, organizations felt that they avoided the need to hire another 4 experienced full-time analysts, increasing the expected operational savings by an additional $768K to as high as **$1.91M/year**. This results in a productivity savings-only ROI of up to 587% and a payback period of only 1.7 months.

Avoided Risk

The Ponemon Institute estimates that the average cost of a successful data breach caused by insufficient response to a security event in the United States is $9.4M (this varies from $4.3M to $10.1M worldwide).[2] Further, the probability of a data breach occurring over a two-year period has been reported at 29.6%.[3] Annualizing this results in an expected risk of data breach of $1.397M per year. Assuming this is the baseline case and leveraging the times reported in Table 1 and Table 2 of this report, Enterprise Strategy Group predicts that Fortinet products can reduce the average time exposed to risk by 97% (with EDP) to 99% (with EDP and CARA). This would mean that Fortinet could help organizations avoid $1.351M to $1.388M in cyberattack costs per year. While these two savings profiles seem very close (based on both providing a substantial increase to the security posture from a time perspective), it should be noted that by adding CARA, organizations will potentially be able to consider more information to better identify complex and coordinated threats that may not be detected with early detection technologies alone. The results of our avoided risk analysis are shown in Figure 6.

[2] Source: IBM, *Cost of a data breach 2022.*
[3] Source: UpGuard, *What is the Cost of a Data Breach in 2022?*

Figure 6. Risk Reduction



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Total Expected Savings

Enterprise Strategy Group took the results of the analysis and projected the 1-, 3-, and 5-year savings for an organization based on expected benefits of improved security team operational efficiency and avoided risk. The results are summarized in Table 4.

Table 4. Summary of Benefits Modeled by Enterprise Strategy Group

	Fortinet EDP	Fortinet EDP + CARA
Improved Security Team Productivity and Avoided Cost of Security Operations	$993K/year	$1.91M/year
Risk Avoidance	$1.35M/year	$1.39M/year
1-Year Total Savings:	**$2.35M**	**$3.30M**
3-Year Total Savings:	**$7.04M**	**$9.90M**
5-Year Total Savings:	**$11.73M**	**$16.50M**
Return on Investment (ROI): (With and Without Risk Avoidance)	**387% to 1048%**	**591% to 1093%**
Payback Period	**1 to 2.5 months**	**1 to 1.7 months**

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Considerations

Enterprise Strategy Group's models are built in good faith upon conservative, credible, and validated assumptions; however, no single modeled scenario will ever represent every potential environment. Each organization has a unique set of considerations that will determine how much of an impact Fortinet products will have on their organization. The benefits realized by an organization depend on the size of the organization; the nature of the business; the specific Fortinet and alternative technologies in use; and the current processes, capabilities, and characteristics of the security organization, along with many more variables. Enterprise Strategy Group recommends that you perform an analysis of your situation and goals and then consult with your Fortinet representative to understand and discuss the potential benefits that may be achievable for your organization.

Conclusion

Security is a paramount concern for any organization. With an increasing number and variety of threats and a rapidly expanding attack surface, security teams are finding it more difficult than ever to do their job. It is hard to grow and retain security talent, especially with limited budgets. Organizations need to invest in tools and services that help to minimize risk and enable security teams to operate more efficiently with the resources that they have.

Enterprise Strategy Group validated with Fortinet customers that the technologies that make up Fortinet solutions have delivered on this requirement. Fortinet training and preparation services, early detection and prevention technologies, and CARA tools and services have reduced the total time required to detect and respond to incidents from several weeks or longer to as few as 6 minutes, an improvement of 97% to 99%, while reducing false positives and improving their ability to detect complex threats. Our models predict that this can help organizations avoid up to $1.39M of risk per year.

But more importantly, these technologies help existing security resources operate significantly more efficiently. The customers we spoke with were generally smaller teams responsible for protecting quite large organizations. The Fortinet solutions helped them to operate as much larger and more capable teams. We found that these teams were able to spend 86% to 99% less time dealing with security incidents, freeing up 191 to 220 person-hours of security operations per week and enabling them to provide far more coverage, while spending more time investigating complex threats deeper and growing their teams' skills and, most importantly, avoiding the need to grow their security team by 12 to 15 additional people.

Customers leverage a variety of Fortinet technologies, and Enterprise Strategy Group found that customers can benefit significantly by using EDP or CARA products individually, integrating them with alternative technologies, or simplifying and optimizing even further by combining Fortinet technologies. If you are looking to better protect your organization while significantly reducing complexity and improving the operational efficiency of your existing security resources, Enterprise Strategy Group suggests that you contact Fortinet to learn more about Fortinet Security Operations solutions.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com