

The Total Economic Impact™ Of Fortinet NGFW For Data Center And AI-Powered FortiGuard Security Services Solution

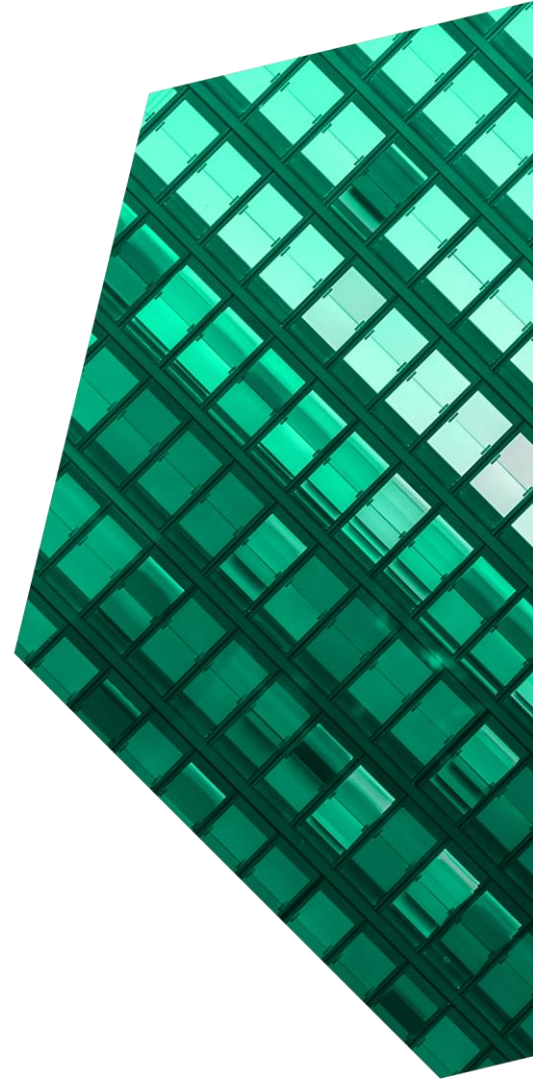
Cost Savings And Business Benefits
Enabled By NGFW For Data Center and AI-Powered
FortiGuard Security Services Solution

JULY 2023

Table Of Contents

Consulting Team: *Nikoletta Stergiou*
Adam Birnberg

- Executive Summary 1**
- Fortinet NGFW For Data Center And AI-Powered FortiGuard Security Services Solution Customer Journey 6**
 - Key Challenges 6
 - Solution Requirements/Investment Objectives 7
 - Composite Organization 7
- Analysis Of Benefits 8**
 - Improved Networking And Security Performance .. 8
 - Networking Team Efficiencies 10
 - End-User Productivity Improvement 13
 - Security Operations Team Efficiencies 14
 - Previous Solution Cost Savings 16
 - Unquantified Benefits 17
 - Flexibility 19
- Analysis Of Costs 20**
 - Hardware And Licensing Costs 20
 - Installation And Deployment Costs 21
 - Ongoing Management Costs 22
- Financial Summary 24**
- Appendix A: Total Economic Impact 25**
- Appendix B: Endnotes 26**



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester’s seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com.

Executive Summary

According to Forrester research, security decision-makers are implementing and expanding next-gen firewalls more than any other on-prem security service.¹ Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution is a comprehensive cybersecurity solution for the data center that converges an organization's security and networking to protect its mission-critical data across the hybrid IT infrastructure. The solution delivers a standardized framework that provides coordinated, automated, and consistent threat protection through a single operating system with performance optimized by a purpose-built ASIC architecture.

[Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution](#) offers secure connectivity through a consolidated framework through a single operating system (OS) that provides coordinated and automated threat protection while maintaining a user-friendly experience. The solution combines network and security to reduce complexity and increase performance while enabling sustainability goals through green cybersecurity design and cost-effective appliance and licensing. Threat protection and real-world threat intelligence is automated through Fortinet FortiGuard services.

Fortinet commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution.² The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Fortinet NGFW for Data

Reduction in network outages

50%



KEY STATISTICS



Return on investment (ROI)
318%



Net present value (NPV)
\$8.03M

Center and AI-Powered FortiGuard Security Services Solution on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives of organizations with experience using Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single [composite organization](#) that is industry agnostic, generates annual revenue of \$2.5 billion, has more than 15,000 employees, and uses three data centers.

Interviewees noted that prior to using Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution, their organizations used multiple other NGFW [next-generation firewall] solutions in their environments. This yielded limited success and left the organizations exposed to an expanding attack surface and inefficient processes. These limitations

led to difficulties in maintaining and upgrading firewalls, disruptions to daily business operations, and limitations in networking and security talent to manage firewalls.

After the investment in Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution, the interviewees' organizations consolidated multiple firewalls with Fortinet's complete cybersecurity solution, augmented talent gaps, and gained clearer visibility across their network infrastructures. Key results from the investment include improved networking and security performance, increased networking and security team efficiencies, end-user productivity gains, and solution cost savings.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:


- **Improved networking and security performance resulting in 50% reduction in outages.** Fortinet provides the composite organization with features to identify threats and attacks that would disrupt business continuity. As a result, the composite improved networking and security performance worth \$5.4 million over three years.
- **Networking team efficiencies that result in a 90% reduction in full-time equivalents (FTEs), a 50% reduction in device reimaging, and a 95% reduction in ancillary device connections.** The composite finds Fortinet to be easy to use, and this impacts the employee experience for networking teams by automating areas that previously required manual or time-consuming processes (e.g., maintaining and upgrading hundreds of firewalls). Over three years, networking team efficiencies are worth \$1.3 million to the composite organization.

- **End-user savings of 2,535 hours.** The composite's end-user productivity increases due to automation and more secure measures that lead to less device reimaging and IT ticket submissions for ancillary device connections. Over three years, this is worth \$147,000 to the composite organization.
- **More than \$1.2 million in efficiency gains resulting in three avoided security operations FTEs.** The composite's security operations team is augmented by Fortinet features that assist in mitigating threats and attacks, and this gives time back to employees and improves the overall employee experience. Over three years, security operations efficiencies are worth more than \$1.2 million to the composite organization.
- **40% savings to previous other NGFW solution costs.** Fortinet is 40% more cost effective than the composite's other NGFW appliance and services solutions, which leads to significant cost savings. Over the course of three years, other NGFW solution cost savings are worth more than \$2.6 million to the composite organization.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Improved security posture.** Interviewees said their organizations' security postures improved as a result of Fortinet's FortiGuard real-time protection against known and unknown threats across data centers, clear visibility into the threat landscape, and protection against and mitigation of potential attacks that would lead to significant financial and reputational impact.
- **Improved visibility and network reliability.** Interviewees said Fortinet offers simplified, centralized management for network infrastructure and that this improved visibility for IT teams and reduced network-related management, maintenance, and monitoring

costs. They also said firmware updates take less time and are more reliable and that configurations, testing, and training require fewer resources and present fewer challenges. Additionally, the permissions required for roll-back configurations and similar tasks minimize the possibility of human error, which provides consistency and assurance for network teams.

 **Improved sustainability.** Fortinet firewalls are powered by purpose-built security processing units (SPUs) that are designed to deliver high performance. Interviewees said this improves and maintains sustainability efforts and ultimately reduces the overall power consumption in data centers.

- **Fortinet customer support.** Interviewees said the vendor's support team is notably responsive and supports customers with technical support 24x7, high-touch support, and professional services.
- **Mergers and acquisitions (M&A) efficiencies.** Interviewees said Fortinet is quick to implement and deploy, which enables organizations that deal with M&A activity to easily consolidate and standardize solutions across data centers.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Hardware and licensing costs of \$1.9 million.** Fortinet offers hardware and licensing options in bundles or a la carte, and the composite organization opts for the advanced threat protection (ATP) bundle in Year 1 at a cost of \$350,000 in threat protection per data center. Its licensing costs in Year 2 and Year 3 are a percent of the hardware costs, and the cost of hardware and licensing is the unit cost of each data center.
- **Installation and deployment costs of \$15,000.** The composite deploys the solution across its

data centers and the primary cost is the salary of a network engineer FTE who works on this.

- **Ongoing management costs of \$640,000.** The composite requires two FTEs to upgrade and maintain the solution.

The representative interviews and financial analysis found that a composite organization experiences benefits of \$10.55M over three years versus costs of \$2.53M, adding up to a net present value (NPV) of \$8.03M and an ROI of 318%.



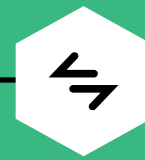
ROI
318%



BENEFITS PV
\$10.55M

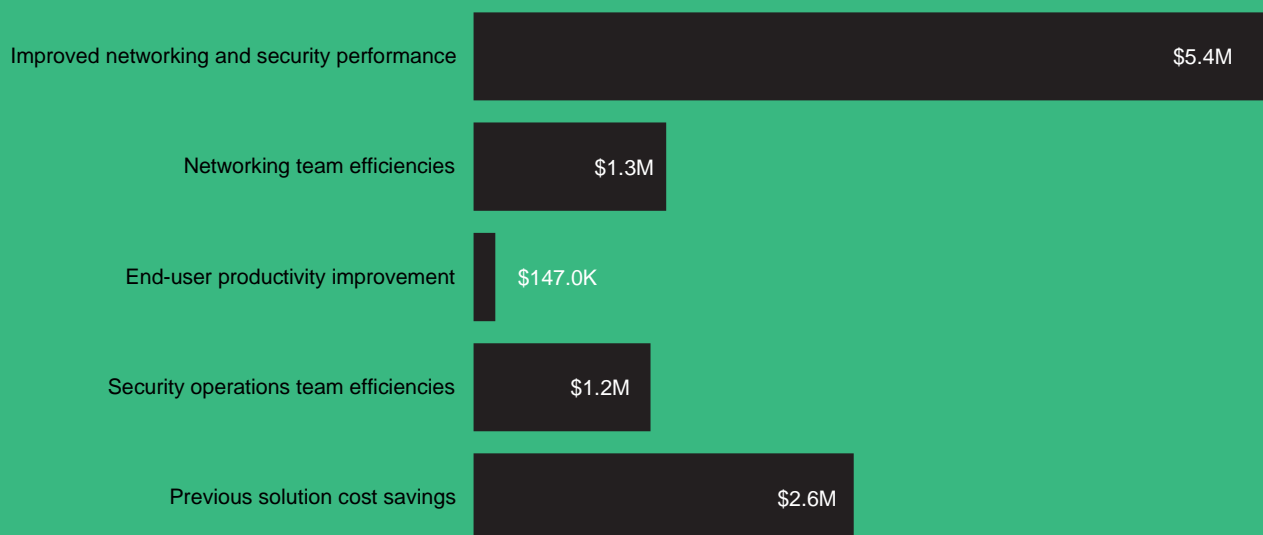


NPV
\$8.03M



PAYBACK
<6 months

Benefits (Three-Year)



“Fortinet is more than just a firewall. They converged several network and security components for improved network and security performance. The selling point for Fortinet is that it does more than just a firewall.”

— Network and technical security manager, natural resources

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Fortinet and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution.

Fortinet reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Fortinet provided the customer names for the interviews but did not participate in the interviews.



DUE DILIGENCE

Interviewed Fortinet stakeholders and Forrester analysts to gather data relative to Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution.



INTERVIEWS

Interviewed five representatives at organizations using Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution to obtain data with respect to costs, benefits, and risks.



COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.



FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.



CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Fortinet NGFW For Data Center And AI-Powered FortiGuard Security Services Solution Customer Journey

■ Drivers leading to Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution

Interviews					
Role	Industry	Region	Annual revenue and employees	Data centers	Endpoints
Senior network engineer	Insurance	Headquarters: US Operations: Local	Revenue: \$2.5 billion Employees: 10,000	2	10,000 to 15,000
Chief security officer (CSO)	Education	Headquarters: US Operations: Local	Revenue: \$90 million Employees: 700	1	15,000
Chief information security officer (CISO)	Healthcare	Headquarters: US Operations: Local	Revenue: \$2.7 billion Employees: 15,000	3	15,000 to 16,000
Network and technical security manager	Natural resources	Headquarters: Switzerland Operations: Global	Revenue: N/A Employees: 135,000	4	40,000
Deputy CISO	Real estate	Headquarters: US Operations: Global	Revenue: \$4.7 billion Employees: 3,500	360+	35,000 to 38,000

KEY CHALLENGES

Prior to investing in Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution, interviewees' organizations used multiple other NGFW solutions across their environments. Interviewees described the difficulty in meeting all their business objectives and security requirements with previous solutions because processes to upgrade and maintain other NGFW in data centers were complex and time-consuming. Furthermore, the organizations faced disruptions due to other NGFW solutions crashing and impacting daily business operations.

Interviewees' organizations also faced limited networking and security talent to manage firewalls, which led to overworked employees and a difficult work/life balance. In some cases, the organization did not have a firewall in place, which left it vulnerable to threats and attacks.

The interviewees noted how their organizations struggled with common challenges, including:

- **Previous NGFW were difficult to upgrade and maintain.** Interviewees cited the challenge of managing multiple firewalls in their data centers. In some cases, there were hundreds of firewalls to upgrade and maintain, and this resulted in lengthy and inefficient processes. The CISO at a healthcare organization described: "The challenge was [having] firewalls all over the

“The biggest challenge or pain point was the management of the devices. That was a pivotal point for us to make the switch to Fortinet.”

Senior network engineer, insurance

place. [We] had to do separate updates for all of them. It was a management nightmare.”

- **Previous NGFW would crash and impact daily operations.** Interviewees noted that their previous environments often crashed, which led to outages and ultimately impacted the organizations’ daily business operations. The CSO at an education organization said: “[Our previous solution] was crashing three times a day. That firewall would take down our entire finance office and hinder ... processing payroll [and] paying bills. [Supporting] daily operations was extremely hamstrung at that point.”
- **There was limited talent to manage multiple firewalls.** Interviewees described the limited manpower on their teams to manage firewalls in their organizations. Their organizations’ networking and security teams ranged from two to five experts in the field, on average. The senior network engineer at an insurance organization said: “We are only a team of three network engineers. If we needed to upgrade the WAN [wide area network] [in our firewalls], we had no way to do it in one fell swoop. This was certainly the biggest challenge we faced with [our prior environment].”

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that would:

- Be cost-effective and come from a brand leader.
- Consolidate multiple firewalls with a complete cybersecurity solution.
- Provide services beyond a firewall to augment talent gaps.
- Provide clear network visibility across endpoints and easily scale as devices grow.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global organization is industry agnostic, generates annual revenue of \$2.5 billion, and has more than 15,000 employees. It seeks to consolidate technologies across its three data centers that reach more than 20,000 endpoints with one firewall solution to augment a small team of networking engineers and security analysts. The solution should easily scale with the growing organization and be easy to implement for future data centers.

Deployment characteristics. The composite organization consolidates and retires its other NGFW solutions to deploy Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution.

Key Assumptions

- **\$2.5 billion annual revenue**
- **15,000+ employees**
- **20,000+ endpoints**
- **3 data centers**

Analysis Of Benefits

■ Quantified benefit data as applied to the composite

Total Benefits						
Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Improved networking and security performance	\$2,160,000	\$2,160,000	\$2,160,000	\$6,480,000	\$5,371,600
Btr	Networking team efficiencies	\$520,223	\$520,223	\$520,223	\$1,560,668	\$1,293,716
Ctr	End-user productivity improvement	\$59,130	\$59,130	\$59,130	\$177,390	\$147,048
Dtr	Security operations team efficiencies	\$477,900	\$477,900	\$477,900	\$1,433,700	\$1,188,467
Etr	Previous solution cost savings	\$1,575,000	\$708,750	\$708,750	\$2,992,500	\$2,550,056
	Total benefits (risk-adjusted)	\$4,792,253	\$3,926,003	\$3,926,003	\$12,644,258	\$10,550,887

IMPROVED NETWORKING AND SECURITY PERFORMANCE

Evidence and data. Prior to using Fortinet, interviewees' organizations faced challenges with networking and security performance. Complex firewall upgrades and time-consuming maintenance processes across multiple firewalls led to susceptibilities in performance, and this disrupted daily operations.

With Fortinet, the organizations experienced improvement as a result of different services and features deployed with the solution.

- The network and technical security manager at a natural resources company described several use cases in which Fortinet provided their organization's data centers with solutions beyond a firewall. The interviewee highlighted: "[We've deployed the Fortinet] UTM feature set with things like IPS and IDS malware. We leverage things like FortiSandbox, FortiMail, and DHCP. Those are important to me [because] they reduce the need to have the specific service run somewhere else, and I can control it from the same point."

"I ran a report for a 12-month period prior to switching to Fortinet [regarding the] number of outages. I ran the same report after the migration to Fortinet to show an apples-to-apples comparison, and the number of outages was 50% less over a 12-month [period]."

Senior network engineer, insurance

- The deputy CISO at a real estate organization described several Fortinet features that added value to their organization's networking and security performance. The interviewee said: "[With Fortinet,] we are adopting IP bandwidth, some of the software-defined networking stuff, [and] the SDN [software-defined networking]"

approach versus staying [with] some of the old-school IPsec [internet protocol security] tunnel routes that we did statically. We are doing more of the SD-WAN [software-defined wide area network] technologies. For IPS and threat, we are able to turn on more of those types of signatures than what we've had in the past to do more granular visibility on the specific traffic that's happening in the networks.”

- Interviewees noted that FortiNAC — a network access control solution that enables organizations to easily manage their network access policies and ensure compliance with security policies — improved network and security performance. The senior network engineer at an insurance organization described: “FortiNAC consists of two virtual machines spread across two datacenters. Not only is [FortiNAC] easier to maintain, cheaper, [and] a whole lot less complex [than other solutions], but ... it is the security liaison for our edge ports at any branch site.”
- Networking and security performance are critical for business continuity and ensuring minimal downtime for end users. Interviewees noted the impact that Fortinet had on reducing outages and downtime at their organizations. The senior network engineer at an insurance company said their organization saw a 50% reduction in outages as a result of improved networking and security performance with Fortinet.

Modeling and assumptions. For the composite organization, Forrester assumes:

- An outage affects 20% of the composite's 15,000 business end users.
- In its prior environment, the composite had an average of 40 outages per year. The average downtime per outage is 2 hours.
- With Fortinet, there is a 50% reduction in outages.

- The average fully burdened hourly rate of an employee is \$40.
- There is a 50% productivity recapture to account for recovered time spent on non-work activities (e.g., improving work/life balance, socializing with coworkers).

“A laptop flags [if] an indicator is compromised. Fortinet goes through and automatically quarantines it, and it does that on two levels where we have FortiSwitch and FortiAP set up. We’ll get a notification that it has been quarantined, [which] reduces the attack surface from the threat. That’s a bonus that the [previous] system did not do.”

CSO, education

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The cause and severity of outages may vary depending on the organization's industry.
- The average number of hours may vary depending on the cause of an outage.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of \$5.4 million.

Improved Networking And Security Performance					
Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Total business end users	Composite	15,000	15,000	15,000
A2	Percent of business end users impacted by an outage	Composite	20%	20%	20%
A3	Average number of outages that result in downtime in the prior environment	Composite	40	40	40
A4	Average downtime per outage (hours)	Composite	2	2	2
A5	Percent reduction in outages with Fortinet	Interviews	50%	50%	50%
A6	Average fully burdened hourly rate of a business end user	TEI standard	\$40	\$40	\$40
A7	Productivity recapture	TEI standard	50%	50%	50%
At	Improved networking and security performance	A3*A1*A2*A4*A5* A6*A7	\$2,400,000	\$2,400,000	\$2,400,000
	Risk adjustment	↓10%			
Atr	Improved networking and security performance (risk-adjusted)		\$2,160,000	\$2,160,000	\$2,160,000
Three-year total: \$6,480,000			Three-year present value: \$5,371,600		

NETWORKING TEAM EFFICIENCIES

Evidence and data. Interviewees said that prior to using Fortinet, there was an imbalance between the number of networking professionals on their teams and the number of workloads. Networking team members were overworked with maintaining and upgrading multiple firewalls across the organizations, reimaging devices that were exposed and affected by exposures, and resolving IT tickets related to connecting ancillary devices (e.g., contractor laptops) to the organizations’ networks.

With Fortinet, the organizations were able to increase efficiencies on their networking teams, which allowed them to reallocate FTEs to other value-add activities and improve their overall employee experiences.

- The network and technical manager at a natural resources company commented: “We’re continually trying to tweak [processes] so that we spend less time doing operational work and more

time dealing more with architectural-type things. I’ve had good feedback from the guys around the group as we’ve moved through and introduced new ways of doing things. There’s definitely been marked improvement.”

- Interviewees said maintaining protocol changes and upgrading firewalls efficiencies improved by 90% with Fortinet. The CISO at a healthcare organization described: “[Prior to using Fortinet, protocol changes took] 30 minutes per firewall, and we average 40 major protocol changes a year [across 280 firewalls]. [With Fortinet,] it takes us an hour total [per protocol change]. [And it’s the] same thing for our system upgrades. Those upgrades would take probably 4 or 5 hours per firewall when we had to do them [before using Fortinet]. [With Fortinet,] it’s probably 8 hours total of testing and completion of a push for our firewall.”

- Fortinet contributed to reducing the number of devices that need reimaging across interviewees' organizations. On average, interviewees described scenarios in which 15% of devices needed reimaging in their prior environments. With Fortinet, their organizations reduced the number of devices that need reimaging by 50%. The CSO at an education organization highlighted: "[Fortinet] FortiEDR is definitely effective. The number of systems we have to reimage due to picking up viruses or malware got cut by half."
- Interviewees also attributed improved efficiencies within their networking teams to Fortinet FortiNAC as it relates to reducing the number of tickets to connect ancillary devices to the network. The senior network engineer at an insurance company noted: "We can be completely hands off because we know that FortiNAC is going to protect these ports all by itself just from the policies that we created and deployed."

Modeling and assumptions. For the composite organization, Forrester assumes:

- Prior to using Fortinet, the composite needed three networking engineer FTEs to maintain and upgrade firewalls across the organization. With Fortinet, the time spent maintaining and upgrading firewalls across three networking engineer FTEs is reduced by 90%.
- Prior to using Fortinet, an average of 15% of the composite's 20,000 endpoint devices were compromised and required reimaging. With FortiEDR, devices that require reimaging is reduced by 50%. On average, device reimaging takes 2 hours. With Fortinet, the organization avoids 2,250 hours annually on device reimaging.
- Prior to using Fortinet, the composite's networking team received 600 tickets annually that were related to connecting ancillary devices

“[With Fortinet,] the visibility that we have on the traffic is kind of the single pane of glass that allows us to make changes portfolio-wide. It allows us to change our footprint from reactionary break-fix to more proactive measures.”

Deputy CISO, real estate

to the networking. With Fortinet FortiNAC, the composite avoids 95% of network connection tickets. On average, these tickets take 30 minutes to complete. With Fortinet, the organization avoids 285 hours annually on ancillary device connections.

- The average fully burdened annual salary of a networking engineer is \$135,000. The average hourly rate of a networking FTE is \$65.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The time associated with upgrading and maintaining firewalls may vary depending on the number of firewall solutions and complexity of processes.
- The number of reimaged devices may vary depending on industry and end-user security training.
- The number of IT tickets to connect ancillary devices may vary depending on an organization's services.
- Salary and hourly rates may vary depending on location and industry.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$1.3 million.

Networking Team Efficiencies					
Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Networking engineer FTEs required to maintain and upgrade firewalls in the prior environment	Composite	3	3	3
B2	Percent reduction in networking engineer FTEs required to maintain and upgrade firewalls with Fortinet	Interviews	90%	90%	90%
B3	Average networking engineer fully burdened annual salary	TEI Standard	\$135,000	\$135,000	\$135,000
B4	Subtotal: Firewall maintenance savings	B1*B2*B3	\$364,500	\$364,500	\$364,500
B5	Endpoint devices	Composite	20,000	20,000	20,000
B6	Percent of devices that required reimaging in the prior environment	Composite	15%	15%	15%
B7	Percent reduction in devices that require reimaging with Fortinet	Interviews	50%	50%	50%
B8	Average hours spent per device on reimaging	Composite	2	2	2
B9	Hours avoided on device reimaging with Fortinet	B5*B6*B7*B8	3,000	3,000	3,000
B10	Average networking engineer fully burdened hourly rate	TEI Standard	\$65	\$65	\$65
B11	Subtotal: Device reimaging savings	B9*B10	\$195,000	\$195,000	\$195,000
B12	Average number of IT tickets to connect to ancillary devices to network per year	Composite	600	600	600
B13	Average time spent completing IT ticket in the prior environment (hours)	Composite	0.5	0.5	0.5
B14	Network connection tickets avoided with Fortinet	Interviews	95%	95%	95%
B15	Time avoided on IT tickets to connect to ancillary devices to network per year (hours)	B12*B13*B14	285	285	285
B16	Subtotal: IT ticket cost avoidance	B10*B15	\$18,525	\$18,525	\$18,525
Bt	Networking team efficiencies	B4+B11+B16	\$578,025	\$578,025	\$578,025
	Risk adjustment	↓10%			
Btr	Networking team efficiencies (risk-adjusted)		\$520,223	\$520,223	\$520,223
Three-year total: \$1,560,668			Three-year present value: \$1,293,716		

END-USER PRODUCTIVITY IMPROVEMENT

Evidence and data. As a result of improved networking team efficiencies, including reimaging and reduced IT tickets in connecting ancillary devices to the network, interviewees said there was an impact on productivity for end users who no longer have to wait for these issues to be resolved. With Fortinet, the improvement in end-user productivity impacts overall business continuity.

- Interviewees noted the recurrence of compromised devices that needed reimaging from some end users, which resulted in these end users being impacted by more downtime than others. The CSO at an education organization commented that with Fortinet, they no longer have to rely on end users to notify the networking team about potential compromises. The interviewee stated: “You’re talking days in our prior systems [to know if there was a compromised device]. We wouldn’t know that something was infected. Now, the minute [the end user] loses network connectivity, that’s the first thing I look for. I receive alerts through [Fortinet] FortiExplorer on my phone when something gets quarantined. It’s more proactive than reactive.”
- The reduction in submitting IT tickets due to the ease of use in device connectivity with Fortinet also reduced the downtime end users spent waiting to be connected to the organizations’ networks. The senior network engineer at an insurance organization stated: “The local contact has to reach out to IT operations, then IT operations will have to open a ticket. Then they need to send that ticket to [the networking team] because they don’t have access to our [systems]. You’re looking at least an hour [to resolve the ticket].”

Modeling and assumptions. For the composite organization, Forrester assumes:

“There were [many] web browsers getting through with [our previous solution] that shouldn’t have been. That’s no longer happening, and that was probably more like once to twice a week. And it always seemed to be the same users.”

CSO, education

- The composite organization’s end users avoid 2,250 hours of waiting for their devices to be reimaged annually.
- End users avoid 285 hours of waiting for their IT tickets to connect to the network annually.
- The average fully burdened hourly rate of a business end user is \$40.
- There is a 50% productivity recapture to account for recovered time spent on nonwork activities (e.g., improving work/life balance, socializing with coworkers.)

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The number of reimaged devices may vary depending on the industry and end-user security training.
- The number of IT tickets to connect ancillary devices may vary depending on the organization’s services.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$147,000.

End-User Productivity Improvement					
Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Avoided end user time spent waiting for reimaging devices with Fortinet (hours)	B9	3,000	3,000	3,000
C2	Avoided time spent on IT tickets to connect ancillary devices to network with Fortinet	B12*B13*B14	285	285	285
C3	Average fully burdened hourly rate of a business end user	TEI Standard	\$40	\$40	\$40
C4	Productivity recapture	TEI Standard	50%	50%	50%
Ct	End-user productivity improvement	(C1+C2)*C3*C4	\$65,700	\$65,700	\$65,700
	Risk adjustment	↓10%			
Ctr	End-user productivity improvement (risk-adjusted)		\$59,130	\$59,130	\$59,130
Three-year total: \$177,390			Three-year present value: \$147,048		

SECURITY OPERATIONS TEAM EFFICIENCIES

Evidence and data. Interviewees said that prior to using Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution, there were inefficiencies among their organizations’ security operations teams. Most of the organizations had small security operations teams ranging from three to five individuals and these workers were often burdened with tasks beyond their job descriptions (e.g., firewall maintenance). This impacted their ability to focus on security-related activities that demanded greater manpower such as investigating, mitigating, and remediating incidents. According to Forrester research, enterprises that lack adequate incident and crisis response preparation take a median of 35 days to find and eradicate an attack.³

Interviewees said that with Fortinet, their organizations’ security operations teams gained efficiencies that ultimately led to overall improvements to their employee experiences.

- Interviewees highlighted that the Fortinet Security Fabric automated certain processes and

“[Fortinet] certainly gives us the ability to reduce the amount of pure network security staff and firewall management staff and allows us to focus other area on other areas [of security] that we have concerns with.”

CISO, healthcare

ultimately saved time for security operations teams. The CSO at an education organization cited: “To do what I have been doing automatically using [the Fortinet solution], I’d need a full SOC [security operations center] team. The system is almost completely automated. [When] we get hit with [a] DDoS [distributed denial-of-service] [attack], the system

automatically remediates it and quarantines the IPs, [and] malware gets detected. [Fortinet] goes through and kills the device access at the layer 2 level on the switches or the wireless [network].”

- Interviewees described Fortinet as an extra layer of protection that allowed security operations professionals to gain back time needed to fully remediate security risks. The deputy CISO at a real estate organization stated: “[Fortinet] allows me to implement a solution faster and get more fidelity and visibility on risks that I have and can mitigate until I’m able to do a full remediation of any zero day that sits in the network. It buys me more time and layers of protection than what we used to have.”
- Security operations teams at the organizations improved their analyses because they refocused employee time solely on security-related activities rather than tasks beyond their formal job descriptions. The deputy CISO at a real estate organization described: “[Fortinet] allows me to reallocate and focus staffing [efforts]. My security engineers can focus more on security [activities] instead of maintenance. They’re able to do a lot

more analysis [and] are able to look at about 20% to 30% more things than what we normally have been in the other environments.”

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite avoids three security operations FTEs.
- The average fully burdened annual salary of a security analyst is \$177,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- Security event remediation may vary depending on the severity of the incident.
- Salary may vary depending on location and industry.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$1.2 million.

Security Operations Team Efficiencies					
Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Avoided security analyst FTEs	Composite	3	3	3
D2	Average fully burdened annual salary of a security analyst	TEI Standard	\$177,000	\$177,000	\$177,000
Dt	Security operations team efficiencies	D1*D2	\$531,000	\$531,000	\$531,000
	Risk adjustment	↓10%			
Dtr	Security operations team efficiencies (risk-adjusted)		\$477,900	\$477,900	\$477,900
Three-year total: \$1,433,700			Three-year present value: \$1,188,467		

PREVIOUS SOLUTION COST SAVINGS

Evidence and data. Prior to using Fortinet, interviewees' organizations utilized multiple vendors and solutions in their environments. The costs of the previous solutions were often high and, in some cases, the organizations incurred additional fees for services needed to meet the organization's networking and security requirements.

Interviewees noted the impact of cost savings after consolidating their environments with Fortinet and retiring their previous solutions.

- The organizations experienced an overall reduction in costs that they attributed to consolidating firewalls with Fortinet. The senior network engineer at an insurance organization commented: "The complexity goes down because you're not managing as many products. You don't have to register or re-register subscriptions for licensing on all those platforms. Naturally, the overall cost goes down with the Fortinet solution because of its simplicity."
- Some organizations further expanded their consolidation savings because they were able to consolidate other aspects of their data centers (e.g., cable modems, applications) with Fortinet. The senior network engineer at an insurance organization noted: "When we introduced Fortinet, we were able to put two cable modems in a site as opposed to an expensive MPLS [multiprotocol label-switching] connection as well as a cable modem. We didn't have that ability with the old solution. [Additionally], I can think of four applications that went away with the [previous solution]."

- Interviewees said hardware and licensing costs were notably less when compared to their organizations' prior environments. Multiple

"[There is] about a 30% to 40% reduction in costs on licensing and deployments [with the Fortinet solution]."

Deputy CISO, real estate

interviewees cited cost savings within a range of 30% to 50% with the Fortinet solution.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Hardware and licensing costs are bundled in Year 1 and result in \$1,750,000.
- Licensing costs in Year 2 and Year 3 are 45% of Year 1 costs.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the costs of previous solutions, which may vary depending on the size and security needs of the organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of \$2.6 million.

Previous Solution Cost Savings					
Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Previous solution costs	Composite	\$1,750,000	\$787,500	\$787,500
Et	Previous solution cost savings	E1	\$1,750,000	\$787,500	\$787,500
	Risk adjustment	↓10%			
Etr	Previous solution cost savings (risk-adjusted)		\$1,575,000	\$708,750	\$708,750
Three-year total: \$2,992,500			Three-year present value: \$2,550,056		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Improved security posture.** With Fortinet, interviewees said their organizations improved their security postures as a result of the solution’s quick implementation, clear visibility into threats, and stronger barriers against potential attacks.
 - **Quick implementation.** Interviewees said the quick Fortinet implementations ensured that data centers at their

organizations were not left exposed to [exposures] for long. The deputy CISO at a real estate organization noted: “[Many] times when you implement a solution in [the data center], you have to peel back a lot of controls just to get the solution working, which means you’re not actually implementing the technology as smoothly or as securely as possible. We’re noticing the ease of entry with faster Fortinet implementations.”

- **Clearer visibility.** Fortinet provided interviewees’ organizations with clearer visibility into threats and vulnerabilities. The senior network engineer at an insurance organization noted: “[With Fortinet,] you can see [the] top threat, [and] you can see outbreak prevention statistics centralized inside of [the Fortinet] FortiAnalyzer reports. You can look at historical and live data. You can see it all. It’s expanded our security posture more than I can tell you.”
- **Mitigating potential attacks.** Interviewees described testing Fortinet’s security against different ransomware attacks and compromises that could potentially impact their organizations. The CISO at a healthcare organization noted:

“We’re able to phase in [Fortinet] quicker and faster [than other solutions], which allows us to go back and tune things. In terms of risk, I’m able to put more protections in place and [do it] faster, which inherently lowers my [organization’s] overall risk posture in scenarios that [it’s] being faced with.”

Deputy CISO, real estate

“When we test the Fortinet products we have our purple team exercises, we’ve never had a successful attack through purple teams against any of our Fortinet appliances.”

- **Improved visibility and network reliability.**

Interviewees said Fortinet offers simplified, centralized management for network infrastructure, which improved visibility for IT teams and reduced network-related management, maintenance, and monitoring costs.

- **Reduced management, maintenance, and monitoring.** Firmware updates take less time and are more reliable, and configurations, testing, and training require fewer resources and present fewer challenges. The senior network engineer at an insurance organization noted: “With the type of network visibility that is available with [Fortinet] FortiOS and the Security Fabric, there [doesn’t seem] to be any competition. [Fortinet] was involved in one of the first ISACs [information sharing and analysis centers] in the industry. They have an open API as opposed to something closed, which provides flexibility depending on which products you want to go through in their ecosystem.”



Improved sustainability. Fortinet also enabled interviewees’ organizations to improve their sustainability efforts within their data centers, and this led to reduced power usage and potential cost savings.

- **Designed for sustainability.** Interviewees highlighted that Fortinet SPU-based solutions created a notable impact on their organizations’ data centers. The deputy CISO at a real estate organization described: “That’s one of the

advantages of going with Fortinet: how they’re doing ASIC [application-specific integrated circuit]-based technology that’s very designed and optimized to their solution set. We are looking at these in terms of efficiency and power generation because that allows me to have better rack density versus having racks where I’m half full because I am fully consumed non-power.”

- **Reduced power usage.** Interviewees also highlighted that reduced power usage across their data centers, which can lead to cost savings in the long run. The CISO at a healthcare organization commented: “We’ve seen an overall reduction in power usage as we still have some [previous solutions] in our environment. As we take out each one of those [previous] firewalls, we see an overall reduction in power consumption.”

- **Fortinet customer support.** Interviewees notably mentioned Fortinet’s customer service as a benefit.

- **Access to technical account managers (TAMs).** Some interviewees’ organizations opted to include a TAM in their enterprise agreement, which added to the success of the Fortinet deployment at the organization. The senior network engineer at an insurance organization highlighted: “We have a weekly cadence call with our TAM. He provides us [with insight about] anything that may impact [our] environment.”

- **Highly responsive customer service.** Interviewees also commented about Fortinet’s responsiveness when it comes to communicating with its customers. The CSO at an education organization described: “You get introduced to

everybody. I've personally talked on the phone to [Fortinet's] VP of east coast sales, [which] I've never had with another vendor. We're a relatively small customer of theirs, but that type of care, thought, and following up [makes a difference]."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Fortinet NGFW for Data Center and AI-Powered FortiGuard Security Services Solution and later realize additional uses and business opportunities, including:

- **M&A efficiencies.** Interviewees from organizations with heavy M&A activity said Fortinet enabled them to efficiently standardize technology across new data centers. The network and technical security manager at a natural resources organization stated: "I do appreciate that we can spin up things very, very quickly in the Fortinet world. I was just in a meeting today where we're going to spin up another connectivity hub in the US, and it'll be done by tomorrow. This has really benefited me specifically because I drive all of our merger acquisitions and divestments."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in [Appendix A](#)).

Analysis Of Costs

■ Quantified cost data as applied to the composite

Total Costs							
Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ftr	Hardware and licensing costs	\$0	\$1,155,000	\$519,750	\$519,750	\$2,194,500	\$1,870,041
Gtr	Installation and deployment costs	\$14,850	\$0	\$0	\$0	\$14,850	\$14,850
Htr	Ongoing management costs	\$0	\$257,400	\$257,400	\$257,400	\$772,200	\$640,116
	Total costs (risk-adjusted)	\$14,850	\$1,412,400	\$777,150	\$777,150	\$2,981,550	\$2,525,007

HARDWARE AND LICENSING COSTS

Evidence and data. Fortinet offers different hardware and licensing bundles to accommodate the different needs of data center customers.

Interviewees said most customer use cases utilized the Advanced Threat Protection (ATP) bundle and the Unified Threat Protection (UTP) bundle that provide coverage for device, content, and web-based attacks through the deployment of security services.

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite deploys the ATP bundle for hardware and licensing at a cost of \$350,000 per data center in Year 1.
- Licensing costs in Year 2 and Year 3 are 45% of the total costs in Year 1.
- There are three data centers in the organization.
- Pricing may vary. Contact Fortinet for additional details.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on hardware and licensing costs, which may also vary depending on the bundle type.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of \$1.9 million.

Hardware And Licensing Costs						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Hardware and licensing per data center	Composite	\$0	\$350,000	\$157,500	\$157,500
F2	Data centers	Composite	0	3	3	3
Ft	Hardware and licensing costs	F1*F2	\$0	\$1,050,000	\$472,500	\$472,500
	Risk adjustment	↑10%				
Ftr	Hardware and licensing costs (risk-adjusted)		\$0	\$1,155,000	\$519,750	\$519,750
Three-year total: \$2,194,500			Three-year present value: \$1,870,041			

INSTALLATION AND DEPLOYMENT COSTS

Evidence and data. The adoption journey for interviewees’ organizations varied, but there was consensus that the installation and deployment of the Fortinet solution was simple when evaluated against different firewall vendors.

Interviewees described proof-of-concept scenarios in which their team compared different firewalls to determine which would best fit their needs. The senior network engineer at an insurance organization noted: “It’s our job to vet out the technologies and determine if they’re going to be a good fit or not. Our CTO was kind enough to fund five firewalls, which we [used to build] a demo environment. We put one [firewall] in each data center, and then we took the last three and we assigned them to myself and my two colleagues.”

Modeling and assumptions. For the composite organization, Forrester assumes:

- One networking engineer is assigned to vet, install, and deploy the Fortinet solution in the organization’s data centers. This engineer dedicates 10% of their time to completing these activities.

- The average fully burdened annual salary of a networking engineer is \$135,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The size of the organization and its number of data centers will vary.
- Salary may vary depending on location and industry.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of \$15,000.

Installation And Deployment Costs						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Networking engineer FTEs	Composite	1	0	0	0
G2	Percent of time spent on Fortinet upgrade	Composite	10%	0%	0%	0%
G3	Fully burdened annual salary of a networking engineer	TEI Standard	\$135,000	\$0	\$0	\$0
Gt	Installation and deployment costs	G1*G2*G3	\$13,500	\$0	\$0	\$0
	Risk adjustment	↑10%				
Gtr	Installation and deployment costs (risk-adjusted)		\$14,850	\$0	\$0	\$0
Three-year total: \$14,850			Three-year present value: \$14,850			

ONGOING MANAGEMENT COSTS

Evidence and data. Interviewees said training was notably simple, and they highlighted the free training resources available to new users. Furthermore, interviewees described the ease of ongoing management efforts to upgrade and maintain the Fortinet solution when compared to other NGFW solutions. From a networking and security perspective, FTEs involved in ongoing management included those from both networking teams and security operations teams.

- Free training and ease of use was critical to a successful deployment of Fortinet at the interviewees’ organizations. The deputy CISO at a real estate organization stated: “For training, the nice thing is Fortinet has a lot of [free] trainings, but their ease of use is so much easier than [that of our previous solution]. [For our previous solution, we would] have to send people away to do training and understand devices. [The previous solution is] not easy to use and the ease of adoption is much lower.”
- Ongoing management labor efforts were also reduced with Fortinet across interviewees’

organizations. The CSO at an education company noted: “[Ongoing management] is like an hour a day just going through and checking what happened last night ... as I drink my morning coffee.”

Modeling and assumptions. For the composite organization, Forrester assumes:

- One full-time security analyst spends 75% of their time maintaining Fortinet.
- One full-time network engineer spends 75% of their time maintaining Fortinet.
- The average fully burdened annual salary of a security analyst is \$177,000.
- The average fully burdened annual salary of a networking engineer is \$135,000.

Risks. Forrester recognizes that these results may not be representative of all experiences and results will vary depending on the following factors:

- The size of the organization will vary.
- Salary and hourly rates may vary depending on location and industry.

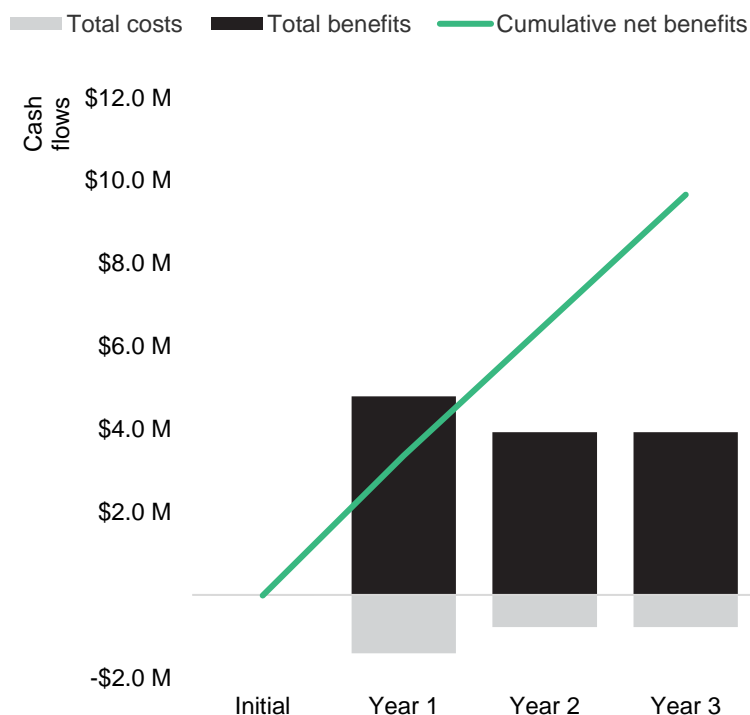
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of \$640,000.

Ongoing Management Costs						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Security analyst FTEs	Composite	0	0.75	0.75	0.75
H2	Fully burdened annual salary of a security analyst	TEI Standard	\$0	\$177,000	\$177,000	\$177,000
H3	Subtotal: Security analyst ongoing management costs	H1*H2	\$0	\$132,750	\$132,750	\$132,750
H4	Network engineer FTEs	Composite	0	0.75	0.75	0.75
H5	Fully burdened annual salary of a network engineer	TEI Standard	\$0	\$135,000	\$135,000	\$135,000
H6	Subtotal: Network engineer ongoing management costs	H4*H5	\$0	\$101,250	\$101,250	\$101,250
Ht	Ongoing management costs	H3+H6	\$0	\$234,000	\$234,000	\$234,000
	Risk adjustment	↑10%				
Htr	Ongoing management costs (risk-adjusted)		\$0	\$257,400	\$257,400	\$257,400
Three-year total: \$772,200			Three-year present value: \$640,116			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	(\$14,850)	(\$1,412,400)	(\$777,150)	(\$777,150)	(\$2,981,550)	(\$2,525,007)
Total benefits	\$0	\$4,792,253	\$3,926,003	\$3,926,003	\$12,644,258	\$10,550,887
Net benefits	(\$14,850)	\$3,379,853	\$3,148,853	\$3,148,853	\$9,662,708	\$8,025,880
ROI						318%
Payback						<6 months

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.



PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.



NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.



RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.



DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.



PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

¹ Source: Forrester's Security Survey, 2022.

² Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

³ Source: "[The 2021 State Of Enterprise Breaches](#)," Forrester Research, Inc., April 8, 2022.

FORRESTER®