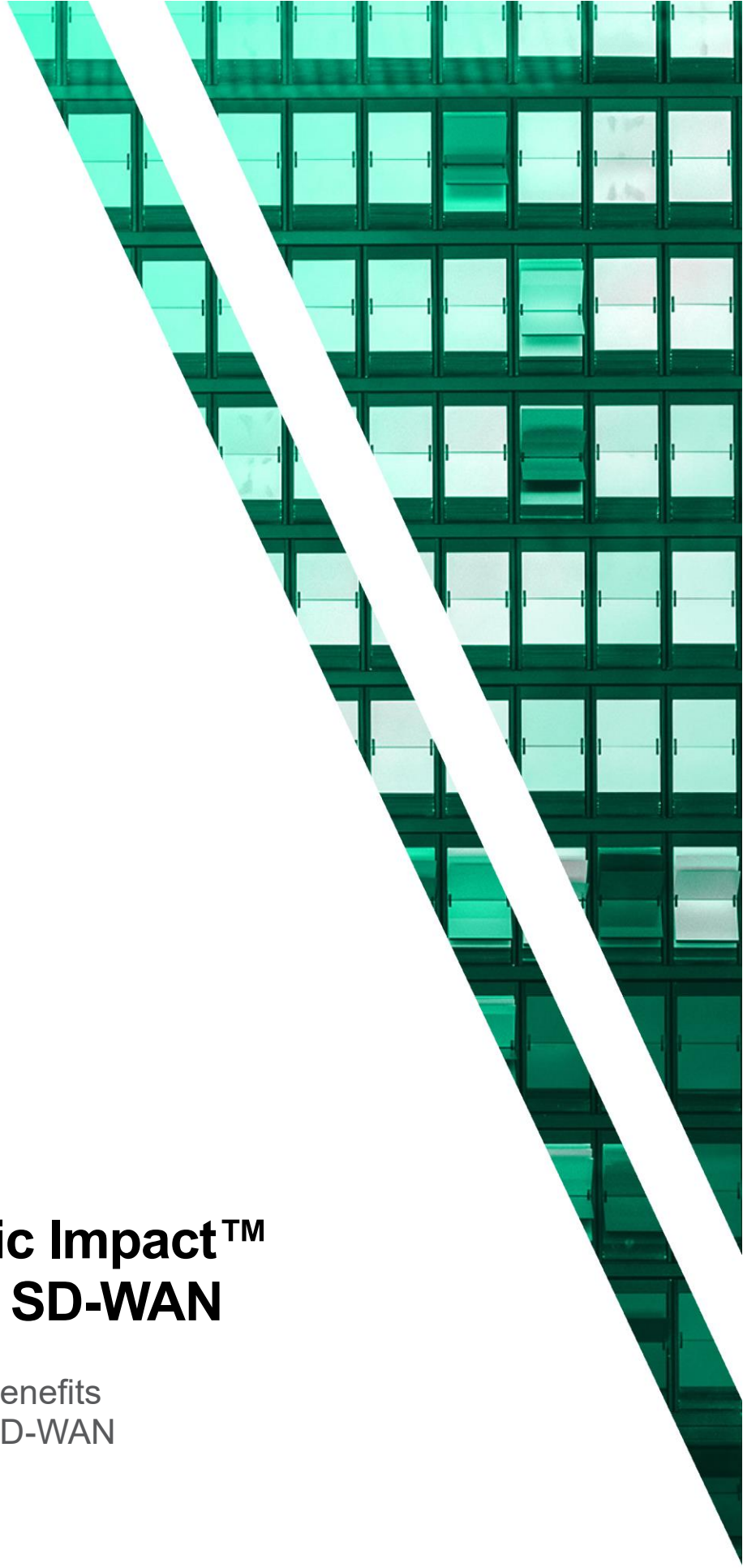
FORRESTER®



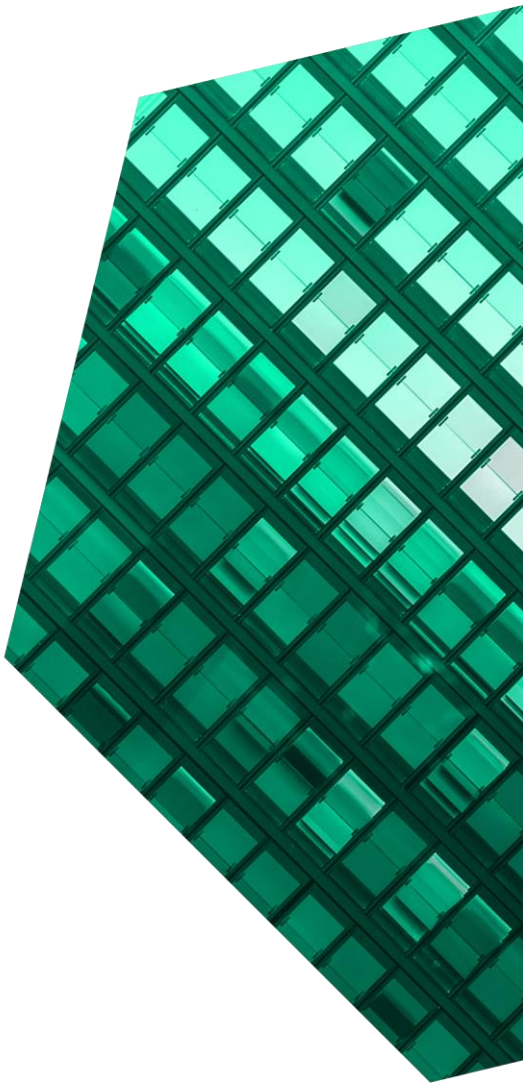
The Total Economic Impact™ Of Fortinet Secure SD-WAN

Cost Savings And Business Benefits Enabled By Fortinet Secure SD-WAN

DECEMBER 2022

Table Of Contents

Consulting Team: Joan Rosania
Rachel Ballard
Kris Peterson



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.

Executive Summary

Fortinet offers a consolidated, lightweight SD-WAN solution designed to improve connectivity and protect enterprises from costly security events resulting in network outages, performance degradation, and ultimately, lost revenue. Providing enhanced network visibility, the platform allows engineers to address security events more quickly, reducing network downtime and increasing operational productivity.

Fortinet provides enterprises with a full suite of security solutions that protect networks, data, and endpoints from potential security threats and attacks. Its converged network and security solution, Secure SD-WAN, replaces disparate network security solutions, eliminates stack friction, offers increased efficiencies, and reduces legacy costs. The built-in agility of Fortinet Secure SD-WAN, illustrated by its self-healing capability driven by machine learning (ML) technology and AI-powered security services, helps organizations address ever-changing security risk and allows users to benefit from a cost-effective, cutting-edge solution that combines enhanced coverage with improved network performance.

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 the Fortinet Secure SD-WAN solution.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Fortinet on their organizations.

Reduction in network disruption:

65%

KEY STATISTICS

Return on investment (ROI)
300%

Payback period
8 months

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives from the retail, financial services, manufacturing, and healthcare industries with revenue ranging from $2 billion to $18 billion and experience using Fortinet Secure SD-WAN solution. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global organization with 27,000 employees, 1,000 sites, and revenue of $1 billion per year.

Prior to using Fortinet, these interviewees noted how their organizations managed private networks with a combination of multiprotocol label switching (MPLS) and internet. Maintaining and monitoring MPLS was time-consuming, upgrading was expensive, and the infrastructure was not scalable. The legacy networks lacked reliable link performance between sites, and internet use exposed the organizations to security risks, leaving them vulnerable to breaches and

attacks. Legacy networks also presented operational limitations as well as inefficiencies in site management:

- The router architecture/approach wasn't designed to support new traffic patterns to reach distributed applications.
- IT had no visibility into traffic to help them troubleshoot potential issues.
- Legacy security architecture required traffic to be directed to the data center for inspection before being directed to its final destination.

After the investment in Fortinet Secure SD-WAN, the interviewees significantly reduced network costs associated with MPLS and improved site connectivity and communication, enhanced security and risk mitigation, and improved user experience. With enhanced network visibility, teams could react more quickly to security events, thereby reducing the number of outages and performance degradation, which lead to unproductive downtime and, depending on the severity of the event, a loss of revenue and reputation.

KEY FINDINGS

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

- **Reduced communication costs.** Deploying Fortinet Secure SD-WAN and its natively integrated firewall considerably reduce the cost of communications per site and increase network flexibility and scalability, without compromising network performance and security. The composite organization is able to limit its reliance on MPLS by more than 80%, as well as avoid other costly network management and monitoring solutions. The total risk-adjusted communications cost savings totals $6.6 million over three years.
- **Increased productivity of security and network team.** A centralized, cloud-based system, Fortinet offers increased visibility and effective, broad protection, allowing the security and network team to more quickly identify and remediate network issues**.** Improving time to issue resolution by as much as 50% enables the composite organization to reassign security and network team resources to higher-value activities, resulting in a three-year, risk-adjusted productivity benefit of $1.4 million.
- **Improved network and security performance.** With enhanced network performance enabled by Fortinet Secure SD-WAN, business users experience a 65% reduction in the number of network disruptions. For the disruptions and outages that still occur, resolution time improves by 50%, creating productivity gains for all end users and a healthier security posture for the composite organization. The three-year, risk-adjusted network and security performance benefit is valued at $1.4 million.
- **Increased productivity of deployment team.** Fortinet Secure SD-WAN enables the composite organization to save 6 hours (75%) per new deployment, resulting in significant efficiencies for the deployment team. The three-year, risk-adjusted present value (PV) savings due to deployment efficiencies totals $321,000.

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

- **Improved visibility and network reliability.** Fortinet offers simplified, centralized management for network infrastructure, improving visibility for IT teams and reducing network-related management, maintenance, and monitoring costs. Firmware updates take less time and are more reliable, and 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, providing consistency and assurances for the network team.

- **Enhanced security and risk mitigation.** In addition to more effectively addressing performance and associated security issues, the Fortinet solution offers users access to timely reports and vulnerability testing information necessary for regulatory agencies and internal management. Fortinet also provides a security feature that scans network data to ensure compliance with Payment Card Industry (PCI) data security standards, the Health Insurance Portability and Accountability Act (HIPAA), and other regulatory mandates.
- **Improved user experience.** The Fortinet Secure SD-WAN enables fast and secure access to applications with fewer issues, directly correlating to fewer support tickets. The reduction in systems outages allows employees to maintain uninterrupted network access, avoiding end user frustration and productivity loss.
- **Ability to scale.** Fortinet Secure SD-WAN offers the ability to scale globally and integrate with other solutions as sites and applications are deployed. The agility of the Fortinet solution allows the organization to grow and adapt to changes while minimizing interruptions in connectivity and exposure to security risk.

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

- **Fortinet hardware, warranty, and subscription costs.** Initial costs to implement the Fortinet network solution include hardware purchases as well as services. The total risk-adjusted, three-year PV of these costs for the composite company is $1.8 million.
- **Implementation design and ongoing management.** Implementation requires network engineering hours, while ongoing maintenance of the system requires dedicated time of network administrators. The risk-adjusted, three-year PV of initial implementation design and ongoing management totals $596,000.

The representative interviews and financial analysis found that the composite organization experiences benefits of $9.7 million over three years versus costs of $2.4 million, adding up to a net present value (NPV) of $7.3 million and an ROI of 300%.

“Mean time to resolution has been reduced because we are now able to know where the problem comes from. On average, the time to resolution has been cut by 50%.”

Global connectivity services director, manufacturing

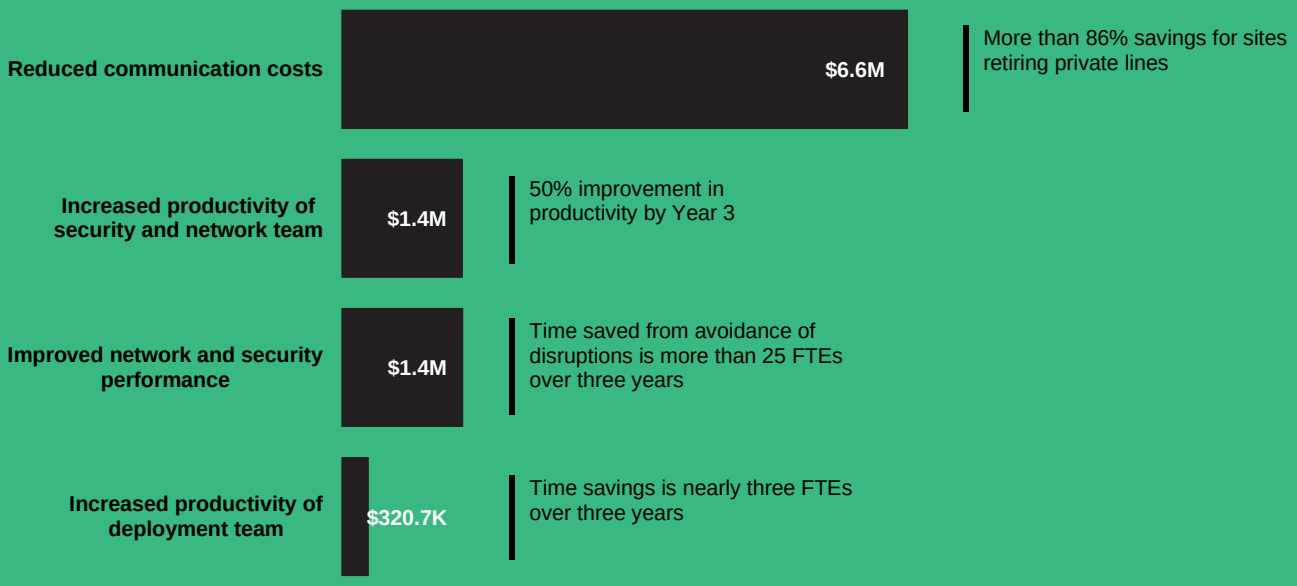
ROI
300%

BENEFITS PV
$9.74M

NPV
$7.3M

PAYBACK
8 months

Benefits (Three-Year)



“Fortinet Secure SD-WAN is very simple. With its single pane of glass, you can see everything about any device and any traffic that’s going through. It is one of the best products I have ever used.”

— Senior network engineer, healthcare services

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 Secure SD-WAN.

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 Secure SD-WAN can have on an organization.

DUE DILIGENCE

Interviewed Fortinet stakeholders and Forrester analysts to gather data relative to Fortinet Secure SD-WAN.

INTERVIEWS

Interviewed four representatives at organizations using Fortinet security solutions 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.

The Fortinet Secure SD-WAN Customer Journey

Drivers leading to the Fortinet investment

Interviews

Role	Industry	Region	Revenue	Employees	Sites
CTO solution services	Retail	Asia HQ, global	$13 billion	16,000	8,500
Global connectivity services director	Manufacturing	North America HQ, global	$17 billion	133,000	1,000
Global lead network architect	Financial services	Europe	$18 billion	86,000	2,500
Senior network engineer	Healthcare services	North America	$1.7 billion	3,500	750

KEY CHALLENGES

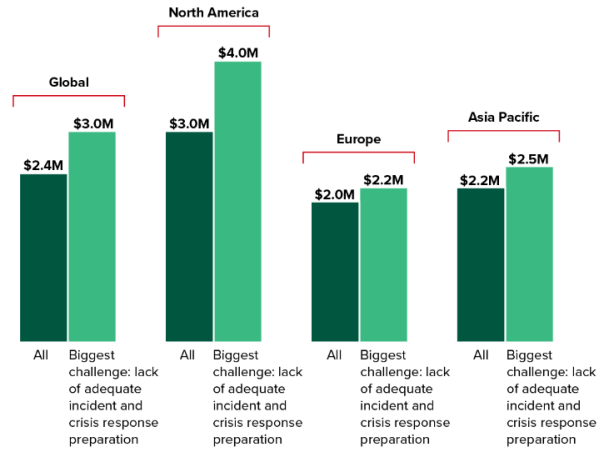
Prior to implementing Fortinet Secure SD-WAN, the organizations used a combination of technologies and vendors to manage, maintain, and monitor their networks. These hybrid solutions — relying on MPLS, internet, and assorted hardware — lacked visibility and adequate security coverage, forcing network engineers and administrators to spend excessive time identifying and resolving unanticipated problems on an ad hoc basis. Additionally, scaling and modifying existing solutions increasingly became cost-prohibitive and time-consuming.

Forrester research shows that 63% of surveyed organizations experienced at least one breach in 2021, up from 59% in 2020. On average, these breaches took 37 days to find and eradicate and cost $2.4 million.[2]

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

- **Insufficient security coverage.** With the expanding hybrid network infrastructure and growing use of the cloud, organizations found they were increasingly vulnerable to the threat of a security event. When faced with a security issue, IT teams were often unable to isolate the degraded link, allowing further network degradation and security risk until resolution. The organizations lacked a reliable, standardized system across all sites and endpoints.
- **Lack of network management and monitoring capabilities.** Without a centralized command center, network managers lacked visibility and the ability to effectively monitor networks. They spent much of their time reacting to unanticipated events, leaving little time to proactively identify minor issues before requiring escalated intervention.

"Using your best estimate, how much did the latest breach experienced by your organization cost the company in total?"
(US$ millions)



Note: Sample varies by region.
Base: 40 to 778 security decision-makers who have experienced a breach in the past 12 months
Source: Forrester Analytics Business Technographics Security Survey, 2021

- **Unsustainable cost increases.** As the organizations continued to grow, systems modifications became necessary to accommodate the increase in network traffic. These additions and changes became cost-prohibitive, requiring both financial and engineering resources. The organizations sought a streamlined, scalable solution that could adapt according to their dynamic connectivity and security needs without impacting their bottom line.

"When assessing Fortinet, we were looking for the ability to see what traffic was going through the links. We wanted to improve uptime in a more cost-effective, secure way."

Global connectivity services director, manufacturing

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could reduce the costs of managing and maintaining their enterprise networks while improving security and performance. Their criteria included:

- A standardized and centralized SD-WAN solution.
- Enhanced user security throughout globally distributed networks.
- Fast issue resolution through better network visibility and more actionable alerts.
- Effective blocking of cyberattacks, both at the endpoint and in the firewall.
- Segregation and control of traffic flow to improve security performance and minimize downtime.
- Easy scalability across thousands of sites.

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 four 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 company with 27,000 employees reports $1 billion in annual revenue. The organization seeks to retire its legacy network infrastructure and replace it with a consolidated, more secure SD-WAN solution that offers the ability to quickly resolve network issues, avoiding costly outages and security risk.

Deployment characteristics. The composite organization has operations across 1,000 sites, with 27 business users per site, and it deploys 300 sites in Year 1, 350 in Year 2, and 350 in Year 3. The organization transitions from an MPLS network to an internet network solution with Fortinet Secure SD-WAN.

Key Assumptions

- **Global company**
- **$1 billion annual revenue**
- **27,000 employees**
- **1,000 sites**
- **27 business users per site**

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	Reduced communication costs	$2,395,725	$2,795,013	$2,795,013	$7,985,750	$6,587,794
Btr	Increased productivity of security and network team	$460,800	$576,000	$691,200	$1,728,000	$1,414,251
Ctr	Improved network and security performance	$272,952	$590,682	$908,820	$1,772,454	$1,419,115
Dtr	Increased productivity of deployment team	$116,640	$136,080	$136,080	$388,800	$320,738
	Total benefits (risk-adjusted)	$3,246,117	$4,097,775	$4,531,113	$11,875,004	$9,741,898

REDUCED COMMUNICATION COSTS

Evidence and data. The interviewees reported that Fortinet Secure SD-WAN allowed their organizations to retire legacy equipment and improve network communication flow between sites at a significantly lower cost.

- The CTO from a retail organization commented: "The cost savings came with the technology transfer. Now, we're not using MPLS at every site. We have more efficient communication between our data centers. At the same time, we have reduced bandwidth in the internet access. Our uptime has increased, and there is less impact on operation."
- Regarding an improved security posture, a global lead network architect in a financial services firm mentioned: "We have user security abilities without additional costs. The Fortinet Secure SD-WAN is a firewall with the SD-WAN capability built in, as compared to other solutions that are pure SD-WAN on top of the firewall." A senior network engineer in healthcare services added: "We reduced the footprint dramatically at one site, which led to a significant reduction in cost. And with all Fortinet devices, we've seen a huge cost reduction, while also seeing an improvement in speed and functionality."

> **"By replacing MPLS over broadband links, we are saving significant money. We can maintain traffic flow if something goes wrong and resolve it quickly. There's no longer a performance or security concern. That's a huge benefit."**
>
> *Senior network engineer, healthcare services*

Modeling and assumptions. For the financial model, Forrester assumes that:

- The composite organization saves $11,400 annually per site from improved communications.
- The organization retires 80% of private lines.

- The organization eliminates the need for optimizer appliance at 25% of sites with Fortinet Secure SD-WAN built-in application optimization.
- The cost of a WAN optimizer is $1,100.

Risks. The reduction in communication costs will vary with:

- The size of the organization and the number of sites impacted.
- Legacy solutions and their associated costs.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $6.6 million.

Reduced Communication Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Annual cost of communications per site prior to Fortinet deployment	Interviews	$13,200	$13,200	$13,200
A2	Annual cost of communications per site after Fortinet deployment	Interviews	$1,800	$1,800	$1,800
A3	Subtotal: communications cost savings per site	A1-A2	$11,400	$11,400	$11,400
A4	Number of sites	Composite	300	350	350
A5	Number of sites with retired private lines	A4*80%	240	280	280
A6	Cost of WAN optimizer	Composite	$1,100	$1,100	$1,100
A7	Percentage of sites with WAN optimizer cost savings	Composite	25%	25%	25%
A8	Subtotal: WAN optimizer cost savings with Fortinet	A4*A6*A7	$82,500	$96,250	$96,250
At	Reduced communication costs	(A3*A5)+A8	$2,818,500	$3,288,250	$3,288,250
	Risk adjustment	↓15%			
Atr	Reduced communication costs (risk-adjusted)		$2,395,725	$2,795,013	$2,795,013
	Three-year total: $7,985,750			**Three-year present value: $6,587,794**	

INCREASED PRODUCTIVITY OF SECURITY AND NETWORK TEAM

Evidence and data. For some organizations, a breach can take more than one month to identify and recover from.[3] According to the interviewees, Fortinet provided a centralized, streamlined, secure SD-WAN solution that required fewer resources to manage than their legacy network solutions, increasing the productivity of their security and network teams.

- The CTO reported: “Without the centralized solutions and visibility of Fortinet, I could not get by with the number of employees on my team. I would not have enough. Fortinet allows us to manage all devices, all the way down to the smallest branch we have, from one location. That makes it possible for my team.”
- With Fortinet Secure SD-WAN’s enhanced security, engineering teams spent less time on issue remediation. The senior network engineer said: “Before Fortinet, it was just a constant fire show. Every day they were fighting a fire for something. Now our team is half the size, and we do some firefighting still, but most is not related to

the SD-WAN. The sites run smoothly. Instead of replacing employees due to attrition, we automated what they were doing. This would not have been possible before."

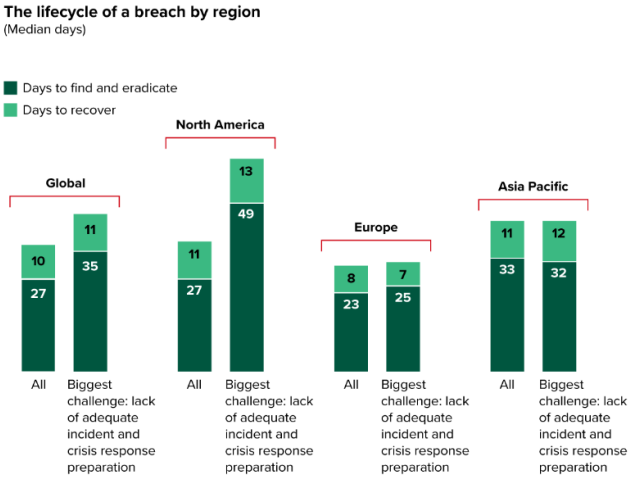
Modeling and assumptions. For the financial model, Forrester assumes:

- Four engineers are reassigned within the organization to higher-value tasks in Year 1, increasing to six engineers reassigned in Year 3.
- The fully burdened annual salary of an engineer is $144,000.

Risks. The cost savings due to the reassignment of engineers will vary with:

- The size and sophistication of the engineering team in the legacy environment.
- Salary levels, depending on geography and experience.
- Previous solutions and their effectiveness.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.4 million.



Note: Sample varies by region.
Base: 65 to 1,243 security decision-makers
Source: Forrester Analytics Business Technographics Security Survey, 2021

Increased Productivity Of Security And Network Team

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of engineers reallocated to other value-added work	Interview	4	5	6
B2	Fully burdened annual salary — operations team	TEI standard	$144,000	$144,000	$144,000
Bt	Increased productivity of security and network team	B1*B2	$576,000	$720,000	$864,000
	Risk adjustment	↓20%			
Btr	Increased productivity of security and network team (risk-adjusted)		$460,800	$576,000	$691,200
	Three-year total: $1,728,000			**Three-year present value: $1,414,251**	

IMPROVED NETWORK AND SECURITY PERFORMANCE

Evidence and data. Forrester research reveals that, according to survey respondents, most will suffer from at least one breach.[4] Fortinet Secure SD-WAN allowed the interviewees' organizations to quickly detect issues while providing the necessary tools for effective resolution.

- The senior network engineer at a healthcare services organization noted: "Prior to implementing Fortinet, we had a phishing incident that took about 22 people and three days to track down. With Fortinet in place, we had something similar the other day, and it took us 15 minutes to find out exactly where it was, 20 minutes to get the user to disconnect from the network, and 15

“I can definitely say that day in and day out, the self-healing aspect is a huge, huge savings. It equates to money saved.”

Senior network engineer, healthcare services

minutes to remediate it by blocking those source IPs.”

- The Fortinet integrated solution employed machine learning that continuously reviewed data, identified potential threats, and offered self-healing capabilities when possible. The senior network engineer said: “All of our tunnels are dynamically handled and will self-heal if there’s a problem, which I believe is a major advantage in the network. The self-healing aspect of the SD-WAN solution is hands-down the top benefit. It allows your team to not have to be immediately reactive all the time. They can be proactive because the SD-WAN literally fixes itself when things start going down.”

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization manages 300 sites in Year 1 with 27 users per site, 650 sites in Year 2, and 1,000 sites in Year 3.
- Network disruption impacts 10% of users in the legacy environment.
- The organization experiences a 65% reduction in network disruption.
- Remaining disruptions take 50% less time to resolve.
- The fully burdened hourly rate of a business user is $40.

Organizations Breached At Least Once In The Past 12 Months

Note: Sample varies by year and region.
Base: 306 to 1,243 security decision-makers
Source: Forrester Analytics Business Technographics Security Surveys, 2020 and 2021

Risks. An improvement in network and security performance will vary with:

- The size of the organization and number of sites and users.
- The degree of disruption in the legacy environment.
- Hourly compensation rates, depending on geography and skill set.

“The performance in Teams has improved. As a user you can tell. There were a lot of blinks and black screens that would come back frequently, and outages. Now, both voice and video, everything just runs smoothly.”

Global connectivity services director, manufacturing

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of more than $1.4 million.

Improved Network And Security Performance

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of sites	Composite	300	650	1,000
C2	Number of business users	C1*27	8,100	17,550	27,000
C3	Percentage of business users effected by disruption in prior state	Composite	10%	10%	10%
C4	Reduction in disruption with Fortinet	Interviews	65%	65%	65%
C5	Business users avoiding disruption with Fortinet	C2*C3*C4	527	1,141	1,755
C6	Annual disruption in prior state (hours)	Composite	12	12	12
C7	Business users' time saved from avoided disruption events (hours)	C5*C6	6,324	13,689	21,060
C8	Business users still experiencing disruption events with Fortinet (rounded)	(C2*C3)*(1-C4)	284	614	945
C9	Reduction in length of disruption with Fortinet	Interviews	50%	50%	50%
C10	Average disruption avoided per affected user with Fortinet (hours)	C6*C9	6	6	6
C11	Business user time saved from avoided disruption events (hours)	C8*C10	1,704	3,684	5,670
C12	Average fully burdened hourly salary of business user	TEI standard	$40	$40	$40
Ct	Improved network and security performance	(C7+C11)*C12	$321,120	$694,920	$1,069,200
	Risk adjustment	↓15%			
Ctr	Improved network and security performance (risk-adjusted)		$272,952	$590,682	$908,820
	Three-year total: $1,772,454		**Three-year present value: $1,419,115**		

INCREASED PRODUCTIVITY OF DEPLOYMENT TEAM

Evidence and data. The interviewees reported that Fortinet Secure SD-WAN allowed their organizations to automate, standardize, and simplify the deployment process, saving significant time for their deployment teams.

- The CTO commented: "Before managing with Fortinet, deploying was more of a manual process, rather than automated." Another mentioned: "The major value is with the

"Previously, our operations team took one week to deploy a new site. Now, with Fortinet, it is copy and paste. We can get it up and running in one day, test the other day, and we are done."

Global connectivity director, manufacturing

architects, the ops teams, and the engineers, who are spending less time configuring sites."

- Automation not only saved time for the deployment teams, but it also provided added security as well. Less burdensome than they had been in the previous environments, configuration and deployment management required fewer internal IT resources. The CTO relayed: "Fortinet offers a VPN connection to the system that allows me to do what I have to, wherever I am, in a very secured manner. The Security Fabric platform monitors all connections and sends alerts if something is happening."

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The composite organization deploys Secure SD-WAN solutions at 300 sites in Year 1 and 350 sites each in Years 2 and 3.
- The network engineering team realizes a 6-hour time savings per deployment.
- The fully burdened hourly rate of a network engineer is $72.

Risks. The increased productivity of the development team will vary with:

- The number of solution deployments per year.
- The hourly rate of a network engineer, depending on geography and skill set.
- Deployment time required in the legacy environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of nearly $321,000.

Increased Productivity Of Deployment Team

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	New deployments per year	Composite	300	350	350
D2	Network engineer time savings to deploy solutions (hours)	Interviews	6	6	6
D3	Network engineer fully burdened hourly compensation	TEI standard	$72	$72	$72
Dt	Increased productivity of deployment team	D1*D2*D3	$129,600	$151,200	$151,200
	Risk adjustment	↓10%			
Dtr	Increased productivity of deployment team (risk-adjusted)		$116,640	$136,080	$136,080
	Three-year total: $388,800			**Three-year present value: $320,738**	

UNQUANTIFIED BENEFITS

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

- **Improved visibility and network reliability.** Fortinet allows organizations to replace multiple legacy network management tools with a single standardized, automated, centralized solution, offering visibility, consistency, and reliability across an organization's entire network. The senior network engineer commented: "In our previous environment, something as common as firmware updates took time, and they required

certain procedures, and the vast majority of them failed. Now I can upgrade our entire environment reliably in under an hour. The Fortinet solution forces us to adopt good, consistent practices. We now have the ability to see what's going on, and the automation takes care of most things for you."

"Since implementing Fortinet, our vision for hiring has changed. We now look for more senior, experienced hires. We want people who can work a strategy, not just configure and fix anything that goes down."

Global connectivity services director, manufacturing

- **Enhanced security and risk mitigation.** The security protection inherent in the Fortinet solution fulfills most regulatory requirements and enforces consistent security rules across all departments and sites. With timely access to reports, fulfilling proof of compliance to internal management and outside regulatory agencies is less time-consuming, and the information is more accurate. This is particularly beneficial given the increasing prevalence of organizations experiencing breaches and average costs exceeding $2 million.[5] The CTO reported: "It's necessary that each device that connects to a switch is protected because we have to report unusual network activity to our IT steering committee and to the board of directors in order to comply with industry regulations." A senior network engineer in healthcare services mentioned: "Fortinet has a security feature that scans data based upon PCI DSS and HIPAA compliance, providing a security rating service score. That is what our CIO and CSO actually use to see what our security posture is. It has absolutely improved our ability to comply with the internal regulatory compliance standards."
- **Improved user experience.** Fortinet provides fast, reliable connections for end users, reducing delays and enhancing the user experience. The senior network engineer reported: "There are definitely fewer tickets since implementing Fortinet. There have been major improvements to the overall user experience." The interviewee added: "When the network goes down, it's a problem. With Fortinet, we have redundancy in place, and the SD-WAN automatically handles most problems. Outages rarely happen anymore, so users are happier."
- **Increased ability to scale.** Fortinet is designed with built-in agility that offers organizations consistent performance amid changes due to growth, downsizing, or direction.

"The Fortinet Secure SD-WAN backbone is 100% capable of scaling to huge size, and it's all very easy. We have processes templated, so what used to take months is now done in days. It's a hugely scalable product."

Senior network engineer, healthcare services

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Fortinet Secure SD-WAN and later realize additional uses and business opportunities, including:

- **Increased innovation.** Engineers spend significantly less time on issue resolution and can focus on more proactive work. A senior network engineer reinforced this point, stating: "With Fortinet running smoothly, we are now able to innovate. We don't have to be reactive. We can be proactive. That was not the case before — it was purely reactive for the engineering team, which is a horrible job. Reactive is not fun."
- **Improved network agility.** The network architecture of Fortinet Secure SD-WAN can be easily modified according to an organization's requirements. Endpoints can be configured using various transports, and they can be quickly connected or disconnected as needed. A global lead network architect in financial services commented, "With the structure and automation of the Fortinet system, we can easily manage internet breakout and activate the Wi-Fi controller."

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

"Prior to Fortinet, we were defaced. Now, at the endpoint and in the firewall, we are able to block or actually eliminate malware and ransomware. We've never had an incident in terms of a virus breakout."

— CTO solution services, retail

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**
Etr	Fortinet hardware, warranty, and subscription costs	$1,842,390	$0	$0	$0	$1,842,390	$1,842,390
Ftr	Cost of implementation design and ongoing administration	$17,424	$158,400	$237,600	$316,800	$730,224	$595,804
	Total costs (risk-adjusted)	$1,859,814	$158,400	$237,600	$316,800	$2,572,614	$2,438,194

FORTINET HARDWARE, WARRANTY, AND SUBSCRIPTION COSTS

Evidence and data. The composite organization, according to its size and needs, purchased hardware, warranty, and subscription services, for a three-year period.

Modeling and assumptions. For pricing details specific to your organization, please contact Fortinet.

Risks. The hardware, warranty, and subscription costs will vary with:

- The size of the organization and related scope of network equipment and service needs.

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 $1.8 million.

Fortinet Hardware, Warranty, And Subscription Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Fortinet solution including hardware and services costs (three years)	Composite	$1,674,900	$0	$0	$0
Et	Fortinet hardware, warranty, and subscription costs	E1	$1,674,900	$0	$0	$0
	Risk adjustment	↑10%	□			
Etr	Fortinet hardware, warranty, and subscription costs (risk-adjusted)		$1,842,390	$0	$0	$0
	Three-year total: $1,842,390			**Three-year present value: $1,842,390**		

COST OF IMPLEMENTATION DESIGN AND ONGOING ADMINISTRATION

Evidence and data. According to the interviewees, initial implementation design required network engineering resources, and ongoing administration and maintenance required dedicated network administrators beginning in Year 1.

Modeling and assumptions. For the financial analysis, Forrester assumes that:

- The network engineering hours required for implementation design total 220 at a fully burdened hourly rate of $72.
- Ongoing administration requires one dedicated network administrator in Year 1, one and a half in Year 2, and two in Year 3, at a fully burdened annual salary of $144,000.

Risks. The cost of implementation design and ongoing administration will vary with:

- Size of the organization, its network needs, and the complexity of the transition from its legacy environment.
- Salary levels and hourly rates, depending on geography and skill set.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $596,000.

> **"Fortinet provides user security capabilities without additional cost. We achieved our target total cost of ownership (TCO) and saved millions on cost avoidance."**
>
> *Network architect, financial services*

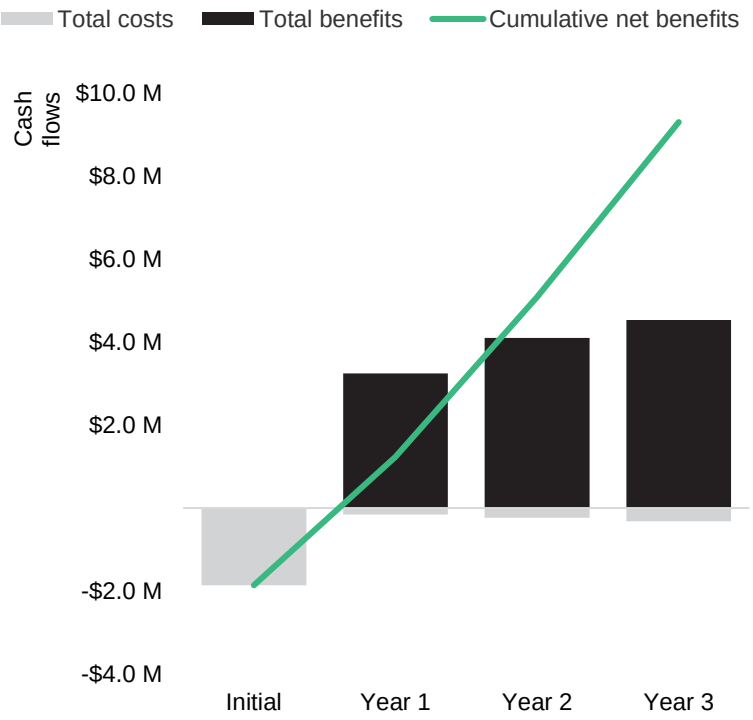
Cost Of Implementation Design And Ongoing Administration

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Network engineer hours for design and implementation	Interviews	220	0	0	0
F2	Fully burdened hourly salary for network engineer	TEI standard	$72	$72	$72	$72
F3	Subtotal: cost of network and security design and implementation	F1*F2	$15,840	$0	$0	
F4	Network admin FTEs for ongoing administration	Interviews	0	1.0	1.5	2.0
F5	Fully burdened annual salary for network admin	TEI standard	$144,000	$144,000	$144,000	$144,000
F6	Subtotal: cost of ongoing administration	F4*F5	$0	$144,000	$216,000	$288,000
Ft	Cost of implementation design and ongoing administration	F3+F6	$15,840	$144,000	$216,000	$288,000
	Risk adjustment	↑10%				
Ftr	Cost of implementation design and ongoing administration (risk-adjusted)		$17,424	$158,400	$237,600	$316,800
	Three-year total: $730,224			**Three-year present value: $595,804**		

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	($1,859,814)	($158,400)	($237,600)	($316,800)	($2,572,614)	($2,438,194)
Total benefits	$0	$3,246,117	$4,097,775	$4,531,113	$11,875,004	$9,741,898
Net benefits	($1,859,814)	$3,087,717	$3,860,175	$4,214,313	$9,302,390	$7,303,704
ROI						300%
Payback period (months)						8

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] 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.

[2] Source: "The 2021 State Of Enterprise Breaches," Forrester Research, Inc., April 8, 2022.

[3] Ibid.

[4] Ibid.

[5] Ibid.


FORRESTER®