Sponsored by: **Forcepoint**

Authors:
Robert Ayoub
Matthew Marden

May 2017

Quantifying the Operational and Security Results of Switching to Forcepoint NGFW

Business Value Highlights

70%
Faster development

53%
Less IT staff time

70%
Less maintenance

38%
Fewer outages

86%
Fewer cyberattacks

69%
Fewer security breaches

73%
Faster incident response

7-month
Payback

$43,845
In benefits per year per Forcepoint NGFW

EXECUTIVE SUMMARY

Connecting and protecting organizations as their people disperse to more locations and need access to resources inside and outside the enterprise are driving a renewed focus on operational efficiency and security efficacy. While the fundamental concerns of confidentiality, integrity, and accessibility are unchanged, the cost and potential losses to organizations continue to increase, making the role of C-level infrastructure and security executives more complex than ever before. A recent IDC survey of CISOs ranked the following as the top 5 scenarios keeping them up at night:

- Breach disclosure on the front page of WSJ and so forth
- Leak of 50% of employee HR records
- IT systems to be a source of major attack against partner
- Target-style breach
- Leak of 10% of PHI/PII customer records

Networking teams are looking for new ways to increase and sustain connectivity throughout the enterprise while modern CISOs are focusing on lowering the risk to these increasingly distributed networks as attacks become more complex and more targeted. The resurgence of ransomware over the past couple of years has also awakened boards to the real damage that can be caused by a cyberattack. Historically, CISOs looked at security as layers, and the focus was on protecting each layer with the very best solution on the market. Today, it is more effective to implement a security platform that protects against multiple vectors of attack, allowing organizations to focus on maintaining a single solution to address the rapidly changing threat landscape.

To understand the impact of protecting networks against threats using Forcepoint Next Generation Firewall (Forcepoint NGFW) solutions, IDC interviewed organizations that have deployed the solutions across their distributed network environments. Study participants reported that Forcepoint NGFW made their network security efforts more robust, agile, and efficient. With Forcepoint, they have lowered operational risk associated with network-related security events by reducing their frequency, duration, and impact. Combined with other efficiencies and cost savings Forcepoint brings, IDC projects that study participants will realize value worth an average of $43,845 per Forcepoint firewall per year over five years, which would result in a five-year ROI of 510%, by:

- Ensuring higher network availability by reducing the frequency of disruptions and outages associated with breaches, cyberattacks, and other security events
- Reducing the frequency and impact of network security–related events on employees and the business
- Requiring less staff time to manage network security and respond to incidents
- Supporting more agile and robust network security operations through ease of deployment and performance

SITUATION OVERVIEW

IDC has seen customer demand for NGFW solutions grow much faster than any other network security technology. This growth can be attributed to interest in solutions designed to detect targeted attacks, adoption of newly offered subscription-based services, and ongoing initiatives among organizations to modernize their network security infrastructure. The following are several significant trends driving customers to evaluate modern NGFW solutions:

- **High-profile breaches and ransomware:** High-profile breaches again took a toll on the industry. The long line of retail breaches showed that well-organized cybercriminals can carry out multistaged, targeted attack-style campaigns. Other breaches also led to many organizations reassessing their security posture and the state of their security infrastructure. Criminals also proved that ransomware attacks can be extremely successful as most organizations are willing to pay a ransom rather than have their businesses disrupted by an attack that forces a complete rebuild of the system.

- **Specialized threat analysis and protection (STAP):** Interest in and adoption of specialized threat analysis and protection solutions stem from the need to spot zero-day threats, malware, and hacker tactics that are increasingly successful in evading signature-based network security solutions. Organizations are embracing sandboxing technology for suspicious file analysis, and interest is growing around offerings for advanced endpoint threat detection products. IDC estimated that the market generated over $1 billion in revenue in 2015.

- **SaaS and subscription-based services adoption:** Most network security vendors are attaching subscription-based security services to the sales of NGFW appliances and other networking security gear. These services were traditionally updates to antivirus and intrusion prevention system (IPS) signatures, but many vendors have started to build entire products — most sandboxing, threat intelligence, and even endpoint products fall into this subscription category. Hybrid solutions consisting of on-premise and SaaS services are a growth engine while organizations gain comfort with the benefits of a SaaS delivery model and increase their investments over time.

- **Skills shortage:** The first and foremost challenge to the deployment of new cybersecurity solutions is the severe lack of cybersecurity talent. The availability and the skill level of cybersecurity talent has a direct impact on markets as diverse as network security and outsourcing. Managed and security services continue to play a key role in addressing this talent shortage. Organizations are also seeking ways to increase automation around both networking and security gear to free up overburdened IT staff.

Market Challenges

Despite significant growth in the NGFW space in recent years, there are still challenges that could disrupt the NGFW market. While IDC believes that the market for NGFW products will continue to experience strong growth for the foreseeable future, organizations should understand upcoming trends that could have an impact on their buying behavior.

First, the movement of data and applications to the cloud could reduce the appetite of organizations to invest in perimeter security such as NGFWs. We continue to witness extraordinary adoption of cloud-based products. Security is still a critical component of cloud deployments, but a variety of vendors are targeting security in the cloud. Coupled with a growing number of companies that are born in the cloud, this means that there are buyers that have a very limited physical footprint and therefore aren't as interested in investing in perimeter security as they once were.

Another challenge for the NGFW market is that many organizations have already upgraded to newer NGFW devices and are happy with their existing vendors. Since they have already made these investments, many enterprises are more interested in evaluating additional security technologies such as advanced endpoint, forensics, and advanced analytics. This puts the onus on NGFW vendors to offer these advanced capabilities to customers.

FORCEPOINT NEXT GENERATION FIREWALL SOLUTIONS

Forcepoint is a joint venture of Raytheon Company and Vista Equity Partners that emerged as the new brand consisting of security products from Websense, Raytheon Cyber Products, Stonesoft, and Skyfence in a move designed to allow cybersecurity research from Raytheon to be more effectively brought to commercial markets in Forcepoint products.

The combined company has over 2,500 employees and more than 22,000 customers and provides a variety of security functions including web security, data loss prevention, cloud application security brokering, network security, and protection against insider threats. Forcepoint executives see the combined company as a win for customers by enabling the customers to eliminate the complexity of managing a patchwork of point products. The company is building security platform that ultimately will help organizations understand people's behaviors and motivations as they interact with data and intellectual property everywhere. Forcepoint NGFW is a key part of this vision, providing visibility into people's actions and enabling enforcement of enterprise policies.

Forcepoint NGFW is built on software and appliances from Stonesoft, which was acquired from Intel Security in a deal that also included the Sidewinder legacy firewall assets. Intel Security acquired Stonesoft in 2013 in a nearly $400 million deal. Stonesoft had been headquartered in Helsinki, Finland, and gained a reputation for its unique antimalware engine designed to detect threats that use evasion techniques. Stonesoft appliances have built-in IPsec and SSL VPN capabilities as well as application control and intrusion prevention capabilities. Forcepoint moved rapidly to add further security capabilities to its NGFW, integrating both the company's global threat intelligence and its Sidewinder proxy technology for protecting mission-critical applications to create a unified software core that powers its physical, virtual, and cloud network security appliances. The company will be further integrating the NGFW with other Forcepoint technology as part of its vision to protect the point where people and data interact, which the company calls "The Human Point."

THE BUSINESS VALUE OF FORCEPOINT NEXT GENERATION FIREWALL SOLUTIONS

Study Demographics

IDC interviewed eight organizations about their use of Forcepoint NGFW solutions to protect against network threats. These interviews were designed to cover both qualitative and quantitative topics related to securing their network infrastructures. The interviewed organizations were large, ranging in size from under 1,000 employees to over 100,000 employees). The average number of employees is 54,000. Interviews reflected the experiences of organizations based in EMEA (five in total) and North America (three in total) and in different industry verticals (see Table 1). Study participants have deployed an average of 36 Forcepoint firewalls across 75 sites, reflecting their distributed use.

TABLE 1 Firmographics of Interviewed Organizations Using Forcepoint NGFW

	Average	Median
Number of employees	54,000	40,000
Number of IT staff	1,644	375
Number of IT users	50,900	29,500
Number of Forcepoint firewalls	36	35
Number of offices/sites supported by Forcepoint NGFW	75	37
Countries	United States, France, Germany, and United Kingdom	
Industries	Financial services, government, higher education (2), logistics, managed technology services, manufacturing, and software	

n=8 Source: IDC, 2017

The Need for Improved Network Security

Study participants articulated similar challenges and reasons for choosing Forcepoint NGFW. They mostly deployed Forcepoint to replace a legacy firewall solution or as a net-add to their existing network security architectures. They stressed that they needed a cost-effective, efficient, and high-performing firewall solution and cited the following attributes of Forcepoint as driving its selection:

- **Cost-to-feature ratio.** Several organizations perceived strong value in Forcepoint from a feature-to-price perspective. One interviewed organization noted: "With Forcepoint, you get all of the features, whereas we would have had to pay for each feature with other vendors."
- **Operational efficiency**. Given the challenges of providing robust security with limited resources, study participants needed an efficient solution. One Forcepoint customer said: "Our main reason for choosing Forcepoint was the ability to get the centrally managed infrastructure so we can manage all the firewalls from a single point."
- **Performance.** Interviewed organizations consistently cited the need for a high-performing firewall solution to ensure network security and availability. As one organization noted: "If our internet goes down for more than three minutes, our phone rings."

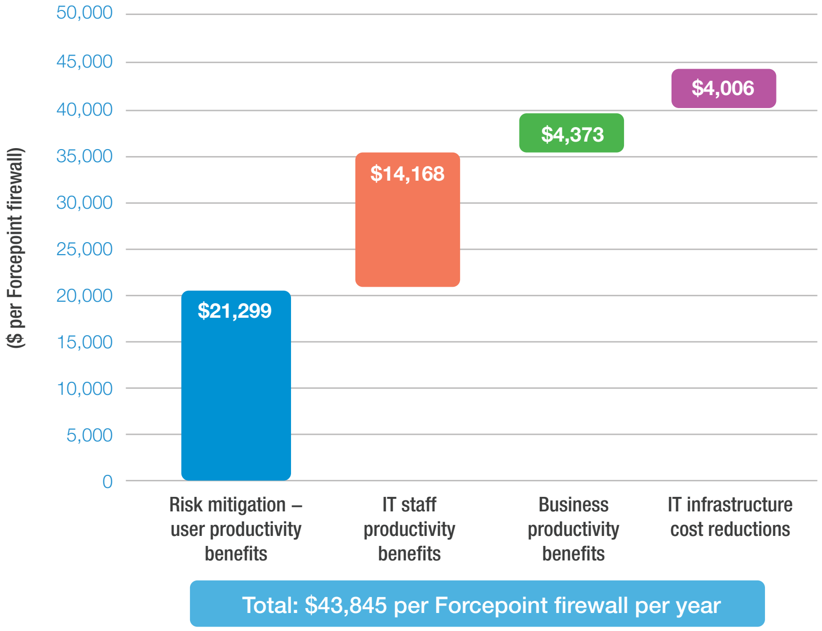
Business Value Analysis

Study participants are achieving strong value with Forcepoint NGFW by limiting the operational risk and cost of network-related security events in an efficient manner. By reducing the frequency, duration, and impact of security incidents, the cost of such events in terms of lost employee productivity and even business outcomes is also reduced. Meanwhile, Forcepoint enables network security teams to operate more efficiently. In total, IDC projects that these organizations will realize benefits with an average annual value of $43,845 per Forcepoint firewall over five years ($1.59 million per organization), in the following areas (see Figure 1):

- **Risk mitigation — user productivity benefits.** Study participants have indicated that with Forcepoint, they have reduced the impact of network-related security incidents such as breaches, cyberattacks, policy violations, and unplanned outages. This means lower cost in terms of disruptions to employees' work, and organizations benefit from reduced risk in terms of reputation, customer relations, and business results. IDC projects that study participants will realize benefits from higher user productivity worth $21,299 per firewall per year over five years ($774,800 per organization).

- **IT staff productivity benefits.** Study participants have increased the efficiency of their network security operations. With Forcepoint, these teams require 53% less time to manage network security and respond to network security events, thus ensuring that these skilled IT staff members are spending as much of their time as possible on business enablement activities rather than day-to-day operational activities. IDC puts the value of IT network security staff time efficiencies at $14,168 per firewall per year over five years ($515,400 per organization).
- **Business productivity benefits.** Study participants are better supporting their evolving businesses. With Forcepoint, they lose less revenue due to network security events and can deploy more firewalls to protect new applications and sites in less time. IDC puts the value of resultant higher revenue and employee productivity at an annual average of $4,373 per firewall over five years ($159,100 per organization).
- **IT infrastructure cost reductions.** Study participants have lowered costs associated with previous network security solutions, including legacy firewalls, and are reducing or avoiding bandwidth-related costs. IDC calculates that these organizations will save an average of $4,006 per firewall per year over five years ($145,700 per organization).

FIGURE 1 Average Annual Benefits per Forcepoint Firewall



n=8 Source: IDC, 2017

Minimizing Risk Related to Network Security: Combating Theft and Breaches

Interviewed organizations reported that they have substantially reduced risk associated with network-related security events with Forcepoint. By better identifying threats, cutting incident response time, and taking the necessary remedial steps to prevent threats from impacting operations or even damaging their competitive positions, these organizations have minimized the operational cost of network security events and increased business confidence.

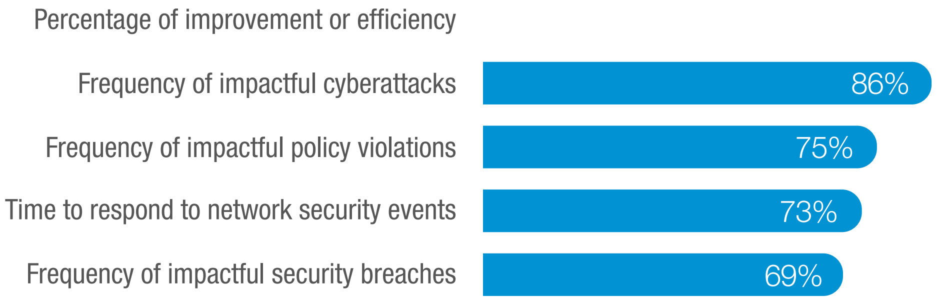
Reducing the Frequency and Duration of Impactful Events

Study participants' network security priority is to prevent threats from becoming impactful events and then limiting the duration and breadth of impact of events that do occur. Events that can negatively affect operational performance and potentially create business risk include cyberattacks, employee and other user violations of organizational IT security policies, and other types of security breaches. Study participants reported that Forcepoint is enabling them to achieve both objectives. Interviewed Forcepoint customers attributed significant reductions in the frequency of impactful events (86% fewer cyberattacks, 75% fewer policy violations, and 69% fewer security breaches) to better identification of threats, improved firewall performance and resiliency, and increased visibility across their network environments. Further, Forcepoint enables their IT security teams to respond faster (73% on average) when threats arise, thereby reducing the scope for damage associated with each event (see Figure 2).

Interviewed organizations provided numerous examples of these types of efficiencies with Forcepoint:

- **Fewer impactful security events.** "If we didn't have Forcepoint, then the number of security events we would face would at least double — I can't even say what it would be without Forcepoint."
- **Faster resolution of security events.** "To get to resolution for a network security event with Forcepoint takes a few hours on average. In those areas where we don't have Forcepoint, it takes more like a day."
- **Improved visibility.** "We're blocking a ton of cyberattacks with Forcepoint. Many of these were probably being blocked before, but we weren't even seeing them before, and didn't even know what was happening."

FIGURE 2 Network Security Benefits with Forcepoint NGFW



n=8 Source: IDC, 2017 (% improvement or efficiency)

Reducing the Operational Impact of Security Events

Network security incidents have the potential to exert a significant cost in terms of lost employee productivity and lost revenue. Employees are highly dependent on unimpeded access to IT systems and business applications. Thus they can be negatively affected by performance degradation, let alone outages or not having access to their devices. As a result, interruptions in access to systems and applications means that employees are not providing maximum value to their organizations.

IDC's interviews with Forcepoint customers demonstrate the strong value they are achieving by minimizing the frequency and duration of network security events. As Table 2 shows, they are reducing the cost of lost employee productivity by an average of $14,160 per Forcepoint firewall per year.

TABLE 2 Impact of Network Security-Related Incidents with Forcepoint NGFW

	Before Forcepoint NGFW	With Forcepoint NGFW	Difference	Benefit (%)
Number of events per week	6.9	2.2	4.7	69
MTTR (hours)	9.1	3.0	6.1	67
Lost hours of productive time per Forcepoint firewall per year	657	261	396	60
Value of productivity loss per Forcepoint firewall per year ($)	23,493	9,333	14,160	95

n=8 Source: IDC, 2017

Reducing Operational and Business Risk

In addition to minimizing the productivity cost of network-related security events, study participants noted that they have lowered business-level risk with Forcepoint, which can carry significant potential costs in terms of business outcomes, fines, or reputation. These costs can be more challenging than productivity-related impacts to quantify, but can be substantial and long-lasting. By reducing the frequency and duration of security events, and providing improved visibility that can be leveraged to take steps to reduce operational risk, Forcepoint is helping study participants avoid these types of "worst case" scenarios. One organization noted the major impact that Forcepoint has had on ensuring business continuity and minimizing revenue losses associated with network security events: "With Forcepoint, we've gone from multiple impactful security events that entail lost revenue — probably $20,000 per hour — per month to a couple per year, and resolve them in four hours compared with eight hours previously, and they impact far fewer employees."

Network Availability: Minimizing Downtime

Interviewed organizations are also benefiting from improving network availability with Forcepoint, resulting in fewer disruptions to systems and applications. With Forcepoint, they are suffering fewer unplanned network-related outages (38%) and carrying out less frequent user-impacting maintenance windows (70%). As shown in Table 3, this means that IT users face less frequent interruptions due to network and/or security solution outages, thereby further minimizing the cost of network outages.

TABLE 3 Impact of Network Security-Related Incidents with Forcepoint NGFW

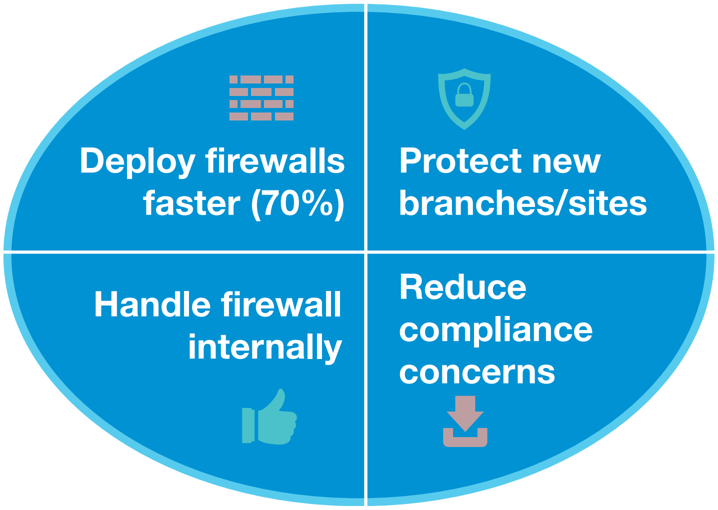
	Before Forcepoint NGFW	With Forcepoint NGFW	Difference	Benefit (%)
Unplanned downtime				
Number of outages per year	10.4	6.5	3.9	38
MTTR (hours)	2.0	1.6	0.4	20
Lost hours of productive time per Forcepoint firewall per year	274	221	53	19
Value of productivity loss per Forcepoint firewall per year ($)	9,808	7,916	1,892	19
Planned maintenance				
Number of maintenance events per year	3.2	1.0	2.2	70
MTTR (hours)	0.7	0.3	0.4	52
Lost hours of productive time per Forcepoint firewall per year	105	66	39	37
Value of productivity loss per Forcepoint firewall per year ($)	3,747	2,350	1,397	37

n=8 Source: IDC, 2017

Network Security Agility and Performance

Forcepoint is also helping study participants support their evolving business strategies with agility and performance. These organizations prioritize network security for the previously discussed reasons, but still must achieve it in a way that is as transparent for users and business operations as possible. Study participants reported that Forcepoint helps them minimize potential friction in ensuring network security in ways such as faster deployment of new firewalls (70% faster on average), protecting new business operations sooner, allowing for internal staff to deploy and manage firewalls, and ensuring efficient and effective regulatory compliance (see Figure 3). By increasing confidence in security measures and enabling improved security in a way that does not impede business operations, utilization of applications and services can grow, creating further operational efficiencies.

FIGURE 3 Network Security Agility and Performance with Forcepoint NGFW


Deploy firewalls faster (70%)
Protect new branches/sites
Handle firewall internally
Reduce compliance concerns

n=8 Source: IDC, 2017

Agility and performance gained with Forcepoint can translate into operational efficiencies as well as more revenue. Users benefit from the speed with which Forcepoint firewalls can be deployed, encouraging their adoption of productivity-enhancing applications (see Table 4). Meanwhile, teams such as application development and compliance teams take advantage of more secure network environments and higher network security agility. One interviewed organization commented: "We need less time today with Forcepoint to ensure compliance, and reporting is easier. For us, compliance goes all the way down to log reviews and reporting. Thousands of people are impacted in their work, and all of them are positively impacted by Forcepoint." Meanwhile, Forcepoint also supports business operations by instilling confidence in the ability to adapt to and address security challenges. One study participant explained: "Forcepoint supports our business strategy because costs are easy to predict and new features are included with the solution. We're more secure and customers are happier."

TABLE 4 User Productivity and Business Impact with Forcepoint NGFW

	Per Organization	Per Forcepoint Firewall
User productivity benefits		
Number of users impacted	50	
Equivalent productivity gain	1.0 FTEs	54 hours/year
Value of productivity gain per year	$70,100	$1,927
Application development productivity benefits		
Equivalent productivity gain	1.4 FTEs	74 hours/year
Value of productivity gain per year	$142,800	$3,926
Regulatory compliance		
Equivalent productivity gain	1.4 FTEs	72 hours/year
Value of productivity gain per year	$140,000	$3,850
Business impact: Increased revenue		
Higher revenue per year	1.4 FTEs	72 hours/year
Revenue recognized for model (operating margin)	$89,000	$2,446

n=8 Source: IDC, 2017

Note: Recognized revenue is calculated by applying an assumed 15% operating margin.

Operational and Cost Efficiencies in Network Security

Study participants also reported that Forcepoint has made their IT network security teams more efficient (see Table 5). These teams are often called upon to secure increasingly complex and disparate operations, so ensuring efficient support is imperative for many organizations. With Forcepoint, these teams are spending less time on day-to-day activities, and study participants have needed to make fewer hires to support expanding operations. One interviewed organization commented: "Our network security team is not that large compared to the size of our network, so we needed a solution that is efficient because we don't have the time nor manpower to work every day on the firewalls."

On average, study participants' IT network security teams are 53% more efficient with Forcepoint, as the result of:

- **Ease of management.** Features of Forcepoint such as centralized management mean that day-to-day management of network security requires less time. One interviewed organization reported that Forcepoint supports the same security environment with one-half of the staff resources.
- **Alleviate pressures from IT skills shortage.** Many organizations find it challenging to staff for IT network security positions that require specific skills and competencies. Thus Forcepoint NGFW solutions help customers manage this skills shortage by minimizing the staff time required to manage network security. One organization referenced its lean staffing model in describing the benefit of Forcepoint: "There are just two of us to manage everything related to network security, so we need central management and to do administrative tasks easily. Forcepoint is one of the best solutions for doing this."
- **Automated updating and patching.** Less staff time is required for essential processes such as patching and updates with Forcepoint. One organization reported that it has stopped paying a third-party $2,000 per quarter to carry out updates, and now needs only one hour of staff time.
- **Alert and event response.** Staff can respond faster and more effectively to potential threats, which reduces the time spent on threat identification and remediation. One organization has gone from requiring 100 hours per month of staff time to 15 hours per month of staff time.

In addition, several interviewed organizations reported that they viewed Forcepoint as being a cost-effective next-generation firewall solution from a feature-to-price perspective. They also reported that they were able to retire legacy firewall solutions and leverage Forcepoint's capabilities to reduce their need for increased bandwidth. As a result, IDC projects that they will save an average of $4,006 per firewall per year over five years ($145,700 per organization).

TABLE 5 Network Security IT Staff Efficiencies with Forcepoint NGFW

	Before Forcepoint NGFW	With Forcepoint NGFW	Difference	Benefit (%)
Network security management (hours per firewall per year)	172	115	57	33
Network security hires avoided (hours per firewall per year)			44	
Network event response (hours per firewall per year)	43	8	35	82
Total network security team (hours per firewall per year)	260	123	137	53
Value of staff time cost per Forcepoint firewall per year ($)	13,281	6,285	6,995	53

n=8 Source: IDC, 2017

ROI Analysis

IDC's ROI analysis is based on data collected during interviews with organizations using Forcepoint NGFW solutions to secure their network environments. To complete its analysis, IDC:

1. Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Forcepoint NGFW solutions. In this study, the benefits included staff time savings and productivity benefits, higher revenue, and IT-related cost reductions.

2. Created a complete investment (five-year total cost analysis) profile based on the interviews. Investments go beyond the initial and annual costs of deploying Forcepoint NGFW solutions and can include additional costs related to migrations, planning, consulting, configuration or maintenance, and staff or user training.

3. Calculated the ROI and payback period. IDC conducted a depreciated cash flow analysis of the benefits and investments for study participants' use of Forcepoint NGFW solutions over a five-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

TABLE 6 Five-Year ROI Analysis

	Per Organization	Per Forcepoint Firewall
Benefit (discounted)	$5.69 million	$156,528
Investment (discounted)	$0.93 million	$25,669
Net present value (NPV)	$4.76 million	$130,859
Return on investment (ROI)	510%	510%
Payback	7 months	7 months
Discount rate	12%	12%

n=8 Source: IDC, 2017

CHALLENGES/OPPORTUNITIES

Despite having a compelling platform built on proven technology, Forcepoint still has several challenges ahead as it expands in this fiercely competitive space. Forcepoint must address the following challenges:

- **Creating a unified platform:** Creating a cohesive platform requires more than optimism. Engineers will need to bridge Websense TRITON, Stonesoft, and the SureView Analytics (all acquired by Forcepoint) offering with a complete NGFW console and reporting capabilities that span the capabilities of all three product lines.

- **Balancing defense history with commercial education:** Forcepoint already has interest at the federal level, leveraging Raytheon's strong defense contractor standing. Forcepoint executives must balance federal sales opportunities while growing the new company beyond Raytheon's defense contractor roots to expand its commercial customer base.

- **Entering an already crowded space with a new brand:** The NGFW space is already well established with new players like Palo Alto Networks and Fortinet and legacy firewall vendors such as Check Point and Cisco — all offering compelling products. Stonesoft was a strong brand in the NGFW space, but Forcepoint must educate customers about the new brand. In addition, many customers have made initial investments in NGFW products, therefore requiring Forcepoint to show greater functionality and management capabilities than its competitors.

These challenges facing Forcepoint are not impossible to overcome, and the company has already shown a commitment in each of the aforementioned areas. There are still plenty of opportunities in the NGFW market for Forcepoint to take advantage of.

Interest is growing around modern endpoint security solutions and, in turn, could also fuel growth in insider threats, a strong component of the Forcepoint offering. The Forcepoint analytics platform appeals to incident responders proactively hunting for security threats.

The struggle to attract and retain talented IT professionals is fueling significant growth in managed and professional services providers. This is a key area where unified management across the Forcepoint product lines could be a key differentiator.

All organizations have gaps. Many vendors in the NGFW space have focused primarily on adding application control and copying components from stand-alone vendors. Forcepoint has the ability to draw on both best of breed technologies and innovative new technologies for both connectivity and security. This combination should allow it to both differentiate against other vendors and provide interesting and innovative capabilities for the foreseeable future.

SUMMARY AND CONCLUSION

The increasingly distributed nature of many organizations and the changing nature and scale of threats are creating new pressures related to network security operations. Traditional approaches and tools are more often neither sufficiently effective nor efficient. Meanwhile, increasing levels of virtualization and use of cloud-based delivery models exacerbate these pressures, pushing organizations to look for solutions such as next-generation firewall solutions that deliver with consistency and efficiency across these environments.

This IDC study shows how Forcepoint Next Generation Firewall solutions can serve as a core component of organizations' efforts to address the aforementioned challenges. Study participants indicated using Forcepoint greatly reduced the frequency and duration of impactful network-related security events, enabling them to minimize the operational cost and disruption associated with such incidents. Further, Forcepoint has made their network security efforts more effective even as they realize staff and cost efficiencies. Thus Forcepoint is helping these organizations achieve the levels of network security and availability their changing businesses require, but without creating additional burdens for their IT networking security teams. This means these organizations are realizing significant value relative to their investment in Forcepoint NGFW solutions in the form of efficiencies for users and IT staff teams while instilling greater business confidence through improved and more agile network security.

APPENDIX

Methodology

IDC's standard ROI methodology was used for this project. This methodology is based on gathering data from current users of Forcepoint NGFW solutions as the foundation for the model. Based on interviews with eight organizations protecting their network environments with Forcepoint NGFW, IDC performed a three-step process to calculate the ROI and payback period:

- Measure the savings from reduced operational cost of network-related security events in terms of employee productivity and revenue, efficiencies in ensuring network security, and network security-related cost reductions over the term of the deployment compared with their previous infrastructure environments.
- Ascertain the investment made in deploying Forcepoint NGFW solutions and the associated migration, training, and support costs.
- Project the costs and savings over a five-year period and calculate the ROI and payback for the deployed solution.

IDC bases the payback period and ROI calculations on several assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. IDC assumes a fully burdened salary of $100,000 per year for IT and regulatory-related staff and $70,000 for other employees, with an assumption of 1,880 hours worked per year.
- Downtime and network security event values are a product of the number of hours of downtime multiplied by the number of users affected.
- The impact of unplanned downtime and other network security events is quantified in terms of impaired end-user productivity and lost revenue.

- Lost productivity is a product of downtime multiplied by burdened salary.
- The net present value of the five-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.

Because every hour of downtime does not equate to a lost hour of productivity or revenue generation, IDC attributes only a fraction of the result to savings. As part of our assessment, we asked each company what fraction of downtime hours to use in calculating productivity savings and the reduction in lost revenue. IDC then taxes the revenue at that rate.

Further, because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

IDC Analyze the Future