RESEARCH
Influence and insight through social media

February 2018

HOW TO ENABLE DIGITAL TRANSFORMATION AND IMPROVE ROI

with Fortinet Security Fabric

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

EXECUTIVE SUMMARY

Companies are rushing to digitize their operations to increase productivity, gain competitive advantage and improve customer service. Mobility, cloud and the Internet of Things (IoT) have combined to enable previously unimagined connections between items in a supply chain and important corporate assets in an enterprise.

With all of this progress comes security risks. Previously well-defined corporate perimeters have eroded, and the number of entry points (for both the good guys and the bad guys) continues to grow. Businesses need a flexible security foundation to ensure they can deploy any service anywhere, when required.

Most enterprises have turned to point products looking for the best possible vendor for each location or application. In fact, ZK Research found the average number of security vendors in businesses today is 32. This approach means staff must be trained on 32 different systems, and IT departments must run several distinct and disconnected management consoles. Isolating issues to a single vendor can be a challenge, and maintaining relationships with dozens of vendors is time consuming. In the end, the point-product approach is highly inefficient.

Businesses that deploy a security fabric will realize a number of benefits, including the following:

Simplified management

Improved organizational effectiveness

Greater visibility through a single dashboard

Faster threat detection to minimize the impact of a breach

Better automation of security functions

Consolidation of talent and ability to reskill security operations

Ability of security operations to focus on strategic initiatives instead of managing multiple, disparate platforms

In addition to its qualitative benefits, the security fabric also delivers a significant quantitative advantage. Initially, the point-product approach may appear to offer superior pricing because companies can make purchase price one of the important selection criteria. In fact, in the first year, point products may actually be cheaper than making the investment in a security fabric. However, the initial price benefit of point products dwindles quickly.

ZK Research's six-year total cost of ownership (TCO) model compared the cost of maintaining an environment composed of 20 vendors for 20 individual products to the cost of replacing the vendors with a single Fortinet Security Fabric. The replacement cycle was mapped out for a five-year period, with a sixth year added after everything is in place. Every company is different and will need to do its own calculations.

This model shows that the point-product approach costs significantly more over the six-year period. The costs include only the subscription, labor and maintenance costs; we have assumed that these costs are fixed over the six-year period and have not included the initial purchase in the calculations, as it is assumed that security is currently in place.

It's important to note that the impact of some of the qualitative benefits, such as faster breach detection and greater visibility, could dwarf the cost of the technology; however, this is almost impossible to quantify. Consider many of the high-profile breaches that have happened over the past few years. These companies suffered damage to the brand and customer loyalty and—in the case of publicly traded companies—saw their stock price fall precipitously.

The results will vary from business to business, but this model shows that the Fortinet Security Fabric provides an 11.5% savings over the six-year period. ZK Research took an approach that was most favorable to the point-product approach. Also, because the refresh was conducted over five years, the savings were lower than a more aggressive timeline. ZK Research believes that every organization will see a savings of at least 10% but estimates the savings could easily be 20% or more.

This white paper explores the advantages of a security fabric over the point-product approach. We look closely at the benefits of the Fortinet Security Fabric and outline the gaps it fills in a world that increasingly relies on mobile, cloud and IoT.

INTRODUCTION: DIGITAL TRANSFORMATION IS DRIVING THE NEED FOR PERVASIVE SECURITY

Even though the average enterprise has 32 individual security vendors, it still takes an average of four months to find a breach.

The increasingly digitized world is a boon to consumers. It's easier now than ever to do things that were once impossibly complex. Companies, too, are digitizing at breakneck pace with the goal of increasing productivity, gaining competitive advantages and improving customer service. With the introduction of mobility, cloud and IoT, the progress has been astounding. Just about anything that can be connected is connected. These previously unimagined connections—such as garage door openers and refrigerators in the home, individual items in a supply chain and important corporate assets in an enterprise—are enabling companies and individuals to abandon archaic analog processes and enter the digital age.

But all this progress does have a downside. The increasing quantities of digital assets come with security risks. For example, the previously well-defined corporate perimeter has eroded. There are no walled-garden IT operations anymore. People, devices and assets live everywhere. Consequently, the number of entry points (for both the good guys and the bad guys) continues to grow exponentially. In addition, unsanctioned "shadow IT" operations, cloud services and IT have combined to create new blind spots that can elude the tracking of traditional IT methods.

As a result of this increased complexity, security is the top IT challenge for most businesses today—and it's not just because of the challenges they face. The number of vendors is a challenge in itself. According to the ZK Research 2017 Security Survey, on average, an enterprise has 32 security vendors providing a dizzying array of services—some related and some unrelated. Interestingly, 90% of point-product security spending happens at the perimeter of an enterprise, even though the perimeter is becoming less relevant from a security perspective, and only 27% of breaches occur at the perimeter.

The traditional perimeter remains important, but attacks are happening in so many more places. Security at the perimeter is mature and state of the art, so the bad guys are focused on finding other ways of penetrating companies. Therefore, the attack surface and risk grow exponentially with each passing year.

It seems like the advice enterprises are getting from vendors and consultants is misguided. After all, the vendors that provide perimeter security have a product to sell, and their marketing can be compelling—and sometimes even scary. But all that's happening is security teams are falling further behind as they invest in products that don't solve the complete problem.

Purchasing additional point products doesn't make organizations more secure. In fact, even though the average enterprise has 32 individual security vendors, it still takes an average of four months to find a breach. The impact on a business from a threat such as ransomware, advanced malware and targeted attacks can far exceed the hard costs that show up on a spreadsheet (e.g., time, manpower and plain old dollars). The damage to a brand can be incalculable.

The security fabric is gaining traction because it delivers required visibility and detection to any location, from the endpoint to the cloud, in real time.

As if those challenges weren't enough, companies trying to secure their operations are hampered by a lack of security expertise. Because they're in such high demand, finding and retaining highly skilled security team members is a significant challenge.

The cobbled-together strategy of using dozens of vendors simply doesn't work, especially in a crisis, so it's time for security teams to change their thinking. It's also time for organizations to reevaluate their security strategies and move to a model that deploys security components that work together throughout the entire organization.

In this white paper, ZK Research explores the reasons why an enterprise should deploy a security fabric as well as its advantages over a security platform and point products. We also look at the benefits of this approach and outline the gaps a security fabric fills in a world that increasingly relies on mobile, cloud and IoT.

SECTION II: SECURITY FABRIC VS. POINT PRODUCTS

The number of entry points to an enterprise network continues to grow, and businesses need a flexible security foundation to ensure they can deploy any service anywhere, when required. The point-product approach entails finding the best possible vendor for each location or application. The benefit of this is the fact that the organization has access to the best security technology from every vendor. However, this drives up the costs that arise from having to train staff on different systems, run separate management consoles, isolate issues to a single vendor and maintain relationships with numerous vendors.

A new approach, known as the security fabric, is gaining traction because it delivers required visibility and detection to any location, from the endpoint to the cloud, in real time. In the process, it greatly reduces the gaps typically seen in a point-product approach. It also creates uniformity of security features, increases visibility and should shorten the time to detection and remediation—because a security team can see more and take action faster.

Both approaches can be used to secure the following areas (see Exhibit 1 for definitions of the various terms used in this white paper):

Campus/edge: Including firewall, IPS, web proxy, SSL

Branch offices: Including UTM, router, wireless controller

Data center: Including firewall, IPS, cloud firewall

Not location specific: Sandbox, secure email gateway, WAF, ADC, EPP, CASB, identity management, NAC, SIEM

Exhibit 1: Defining the Terms

ADC (Application Delivery Controller)
A data-center device used to perform tasks to optimize websites and other applications (e.g., load balancing, SSL compression, security)

CASB (Cloud Access Security Broker)
Software or services that act as an intermediary between on-premises and cloud resources

Cloud Firewall
Similar to a firewall, protects assets and services in a cloud infrastructure

EPP (Endpoint Protection Platform)
Software that secures the devices that connect to computer networks

Firewall
A device that sits at the network edge and blocks unauthorized access while allowing traffic to exit the company

Identity Management
Identifies individuals in a system and controls access to resources based on user rights and restrictions

IPS (Intrusion Prevention System)
Monitors the network for security threats or policy violations

NAC (Network Access Control)
Unifies endpoint security technology, authentication and network security enforcement

Router
Manages the movement of data packets between networks

Sandbox
A virtual space used to securely run new or untested applications

SD-WAN (Software-Defined WAN)
An application of software-defined networking (SDN) technology that is applied to the WAN

Secure Email Gateway
A gateway-focused approach to blocking ransomware, phishing and other cyber threats seeking entry via incoming email, while ensuring that outgoing messages don't leak sensitive data

SIEM (Security Information and Event Management)
Provides real-time analysis of security alerts from hardware and applications on a network

SSL (Secure Sockets Layer)
A standard security technology used to encrypt links between applications and servers

UTM (Unified Threat Management)
A compact appliance that consolidates network and security functions to protect small and medium-sized businesses

WAF (Web Application Firewall)
Similar to a firewall, but secures traffic coming in from and going out to the web

Web Proxy
Acts as an intermediary between endpoints and servers that handle service requests

Wireless Controller
A device that provides centralized control and intelligence for WiFi networks to simplify management of large-scale wireless networks

WOC (WAN Optimization Controller)
A network device that optimizes the performance of applications over the WAN

ZK Research, 2017

The security fabric approach means that all services are available to all points in the environment—not just isolated areas like in the point-product approach.

A security fabric relies on components that can work together seamlessly, often from one vendor and its technology partners, for the required functionality at every location. The deployment can start with a single function, and then other features can be turned on with additional license keys.

Both approaches could eventually lead to a business having the right security in the right places, but the point-product approach is more complex and costly. A security fabric isn't just about cost; it's about putting the right features at different points in the network. The result is there's no trade-off between a security fabric and risk.

For example, in the campus/edge environment, a company will need to find providers to provide a firewall, IPS and web proxy. Each branch office will require a next-generation firewall, router and wireless controller. In the data center, a company will need to find a firewall, IPS and cloud vendor. Then there are the items that are not location specific, including sandbox, email security, WAF, ADC, EPP, CASB, identity management, NAC, SSL and SIEM. The effort to find one product—say, a firewall—can be time consuming, involving IT resources, procurement and management signoff. Multiply that by about 20—depending on how many branch offices or campuses are involved—and that quickly becomes unmanageable.

Forgetting for the moment about the ordeal that procuring all this technology would produce, the most notable challenge with a point-product approach is a lack of scale. We live in a world that is increasingly vibrant and distributed, and security technology needs to scale dynamically. The point-product approach scales by either replacing the existing products with newer, higher-performing ones or by adding more devices. Both methods are inadequate for today's digital world.

In addition, the way the point-product approach puts several technologies together under a single umbrella may actually decrease visibility due to the need to use multiple management tools as well as having logs spread out among different systems, decentralized IT functions and geographically dispersed locations.

Some operations might try to aggregate the information manually and normalize the data, but that requires significant work and won't present data in real time—which is critical for a vigilant security operation. Perhaps more alarming for a company that chooses point products is the fact that each separate product has its own APIs and interfaces, making integration and training a challenge. Several standards exist—such as Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX) and the Cyber Threat Alliance—but they do not guarantee interoperability.

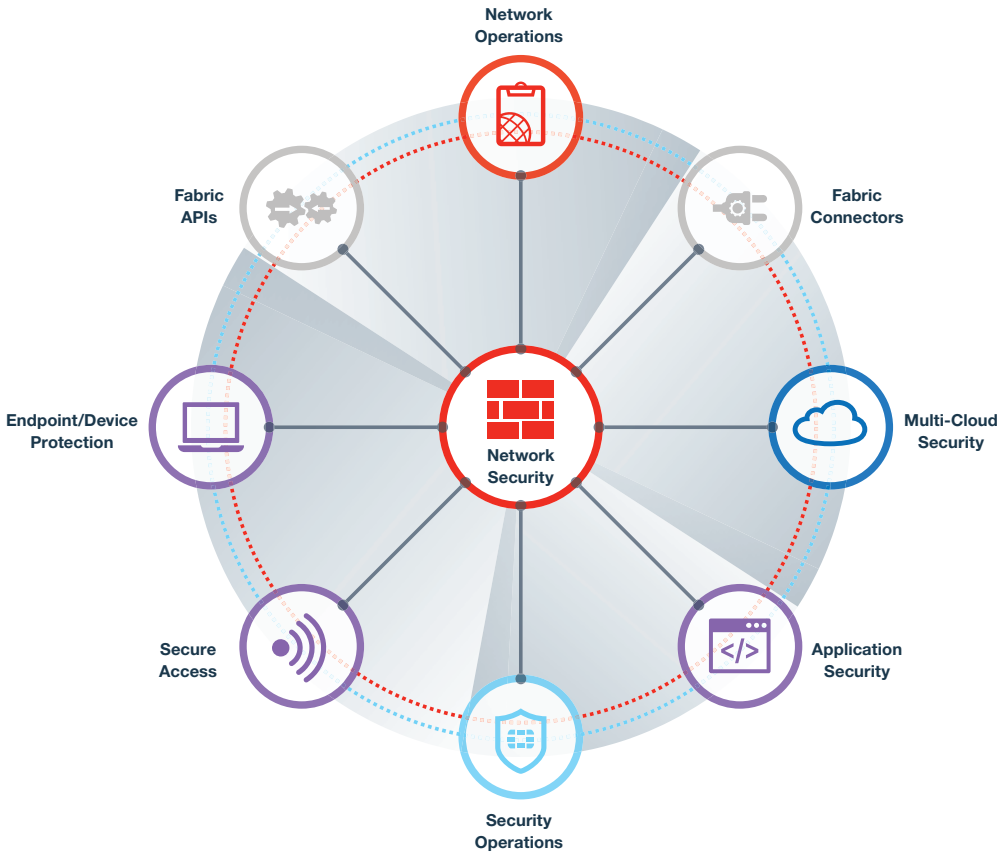
The security fabric approach means that all services are available to all points in the environment—not just isolated areas like in the point-product approach.

Other areas of the technology industry have used fabrics. Perhaps the most prominent is the storage-area network (SAN). With a data storage network, all services must be available to all points at wire speed or it will fail. To accomplish this, the storage fabric is so fast and so tightly knit that the servers think the storage is directly connected. This is the only way distributed storage will work, so the industry solved that problem.

Similarly, the security fabric delivers the required security features to any location, from the endpoint to the cloud, in real time. Two main factors have enabled this development.

First, Fortinet, the company that pioneered the development of a security fabric (Exhibit 2), builds most of its products itself—from the ground up—with the fabric concept in mind. The company has quickly incorporated new technologies, through in-house innovations and acquisitions, while enabling centralized management that reduces the complexity that organizations grapple with when faced with multiple point-product consoles. In addition, Fortinet natively integrated these technologies and provided open APIs that allow other technologies to all work tightly within the security fabric.

Exhibit 2: Understanding the Fortinet Security Fabric



Fortinet, 2018

With a security fabric, a company can achieve the hardware price/performance it wants and still get the latest technology within its renewal budget.

The second factor gives Fortinet its performance differentiation: it understands the need to scale from the smallest location to the largest cloud, and it builds its own security processors (SPUs) along with optimized software architectures. The world seems to be enamored with doing everything in software, but not everything is best done in software. Some functions work best in hardware and some in silicon. Fortinet's SPUs provide robust security to be applied to speeds into the Tbps and can extend into virtual and cloud environments.

In addition, the company's services include access to the work of the 200 expert researchers at FortiGuard Labs, which operates 24/7 to discover and study breaking threats. The team produces world-class, in-house–developed tools and technology using data collected from more than three million sensors around the globe to protect more than 300,000 customers every day.

SECTION III: QUALITATIVE BENEFITS OF A SECURITY FABRIC

With a security fabric, a company can achieve the hardware price/performance it wants and still get the latest technology within its renewal budget. The investment a customer makes at the outset enables the addition of functions to the security fabric as point products come up for renewal. Instead of upgrading to the next version of the point product, the customer can simply implement that component of the fabric. Organizations that choose a security fabric will realize many benefits, including the following:

Simplified management: Because the security fabric components are built on the same codebase, administrators can learn one operating system to manage all of them. Juxtapose this with the difficulty in having to dedicate a team of people to learn dozens of configuration interfaces and management tools, and it's easy to see why a security fabric is so much easier to deploy and maintain than a set of point products.

Improved organizational effectiveness: A security strategy built on point products requires having many more people doing numerous tasks, often independent of one another. This can cause organizational chaos, as security administrators often must react quickly to other changes that occurred, leading to human errors. The simplified management of a security fabric means more tasks can be done with fewer people involved, enabling more resources to be dedicated to strategic initiatives.

Consolidation of talent and ability to reskill security operations: The world of security is always changing, and security professionals constantly need to update their skills. The improved organizational effectiveness facilitated by a security fabric has the benefit of using people more efficiently so time can be dedicated to keeping skills up to date.

With a security fabric, everything happens in one environment, which makes it simpler to manage and monitor.

Greater visibility via a single dashboard: Security teams often use something colloquially referred to as "swivel chair management," where an individual or several people sit in the middle of several management consoles and watch all the information across all the screens. The only way to make sense of the data is through manual correlation. A single dashboard gives security professionals significantly greater end-to-end visibility, simplifying the process of correlating information.

Faster threat detection and response to minimize the impact of a breach: Another benefit of the single dashboard is being able to understand a baseline state and then look for anomalies that could indicate a breach anywhere in the network. With point products, breaches can occur and go unnoticed for months as the data is spread across several systems.

Better automation of security functions: Scaling security operations is dependent on automation. Having a common codebase and operating system greatly simplifies the process of updating software, using orchestration tools or using scripts to automate management tasks.

The simplicity of using a security fabric can't be overstated. Not having to worry about how to blend disparate technologies is a significant advantage. With a security fabric, everything happens in one environment, which makes it simpler to manage and monitor.

As if managing multiple vendors weren't enough of a chore, managing and negotiating multiple contracts means multiple headaches. Working with a security fabric, like the one Fortinet has built, means a company has to worry about only one vendor—there's only "one throat to choke," as the saying goes.

Perhaps more importantly, the Fortinet Security Fabric makes advanced security features such as segmentation, rapid threat sharing and single-pane-of-glass management all available on day one, without the worry of scaling or adding individual licenses.

SECTION IV: QUANTIFYING THE BENEFITS OF A SECURITY FABRIC

As the previous section outlined, a security fabric provides many qualitative benefits. However, it also offers a lower overall TCO. The point-product approach may seem like it offers superior pricing, as companies can make purchase price one of their important selection criteria. In fact, in the first year, point products will likely be cheaper than investing in a security fabric. However, ironically, there is a price to be paid for the initial price benefit—a long-term TCO premium as the products are renewed. Once the pricing has been set, the costs are linear and inflexible short of a major renegotiation, which can add significant complexity to a relationship.

To demonstrate this, ZK Research created a six-year TCO model that compares the cost of maintaining individual point products versus purchasing and deploying a security fabric. A very conservative approach was taken to ensure that the model doesn't overstate the benefits. For example, it is

unlikely that an entire point-product infrastructure will be in place for six years without a need for additional capital expenditures or replacement costs. Nonetheless, we believe this approach illustrates the challenge that organizations face and outlines the difference between point products and the Fortinet Security Fabric.

The Methodology

The model compares the cost of maintaining an environment composed of 20 vendors for 20 individual products to the cost of replacing the vendors with a single Fortinet Security Fabric. The replacement cycle was done over five years, with a sixth year added as everything is in place.

In building the model, it was assumed that the company has 10,000 employees, one main campus, 200 branch offices and 100,000 devices. Another assumption was that the customer had all of the point-product infrastructure in place, so only subscription, support and staffing costs were included in the calculation of these devices. Security fabric costs included the initial purchase of the equipment as well as staff, support and subscription.

For detailed calculations that cover every aspect of the model, see Appendix 1.

The model includes the following security products, which are required to secure an enterprise with the assumed number of employees and locations:

- 4 edge firewalls
- 4 IPSs
- 10,000 web proxies
- 10 data-center firewalls
- 4 data-center IPSs
- 1,000 private cloud instances
- 1,000 public cloud instances
- 200 branch-office routers, branch-office WAN optimization controllers
- 400 switches and WiFi installations
- 4 sandbox environments
- 10,000 endpoints
- 100,000 SIEMs
- 10,000 CASBs
- 8 ADCs

The point-product calculation added up the cost of the individual components. The Fortinet Security Fabric includes the cost of the fabric components plus the cost of the point-product infrastructure that has not been migrated to the security fabric. For example, the Year 1 number for the security fabric includes the cost of the Fortinet Next-Generation Firewall, Next-Generation IPS and Web Proxy, and it adds in the cost of maintaining the 17 other point products. This methodology was applied over five years to replace all 20 components with the security fabric.

One important note: For the model, we started with the data center, which is a logical starting point. However, different organizations might have other needs, so they can start wherever it makes the most sense.

Details of the models can be found in Appendix 1. Aggregated numbers are provided later in the report for ease of reading. Exhibit A and Exhibit B present the detailed costs for the point-product approach and the Fortinet Security Fabric approach, respectively. Exhibit C and Exhibit D show the particulars of the annual costs, while Exhibit E details the total costs for both approaches over six years.

The Results

The overall numbers presented in Exhibit 3 and Exhibit 4 show a stark difference between the point-product and security fabric approaches. It's not a big bang; rather, over a six-year time frame, with a gradual shift of components from point products to a security fabric in the first couple of years, companies will start to reap significant rewards in the third, fourth, fifth and sixth years. At the end of the six-year period, the savings are substantial, even without any point products reaching a natural refresh cycle requiring replacement.

If you compare point products with the security fabric approach—and even if you omit the qualitative benefits—the cost benefit of a security fabric makes the argument for itself.

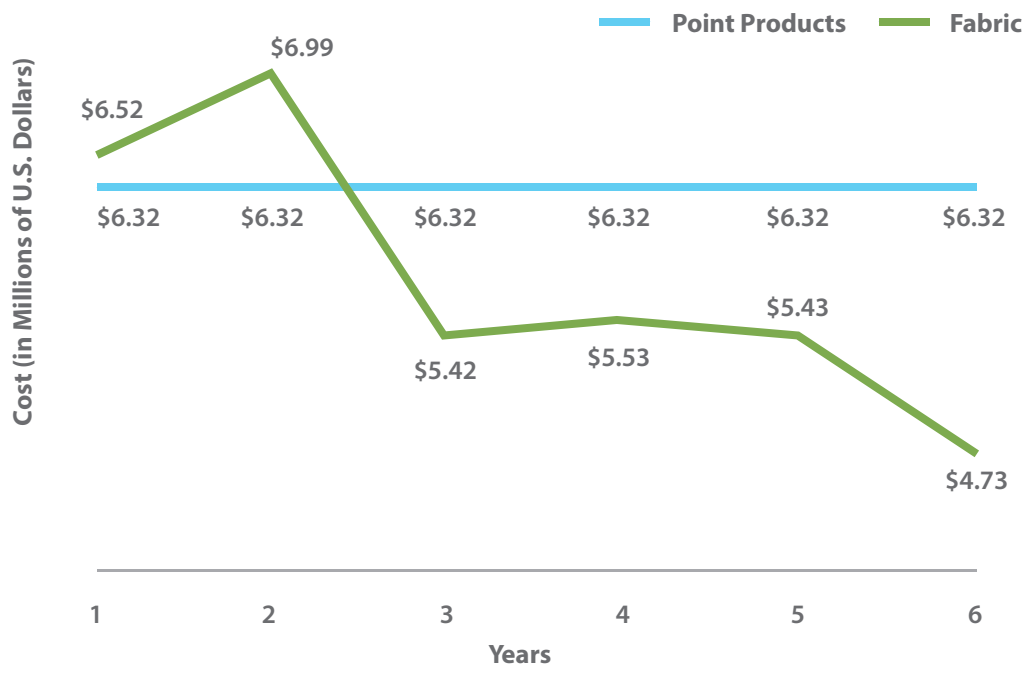
The model shows that the point-product approach costs a consistent $6.32 million per year, for a total six-year cost of $37.92 million. The costs are linear, as only the subscription, labor and

Exhibit 3: Overall Security Fabric vs. Point Products

Year	Point Products	Fortinet Security Fabric	Cumulative Savings
1	$6.32 million	$6.52 million	($0.20 million)
2	$6.32 million	$6.99 million	($0.87 million)
3	$6.32 million	$5.42 million	$0.03 million
4	$6.32 million	$5.53 million	$0.82 million
5	$6.32 million	$5.43 million	$1.70 million
6	$6.32 million	$4.73 million	$3.31 million
Total	**$37.92 million**	**$34.62 million**	**$3.31 million**

ZK Research, 2017

Exhibit 4: Year-over-Year Security Fabric vs. Point Products



ZK Research, 2017

maintenance costs are included. There is an assumption that these costs are fixed over the six-year period. In actuality, the costs could rise as the cost of talent and subscription costs rise.

By contrast, the security fabric starts out a bit more expensive ($6.52 million) and increases slightly through the first-year renewal ($6.99 million), but then it steadily decreases, well below the Year 3 to 5 costs of the point-product approach. At the end of the six years, the Fortinet Security Fabric in our model costs $34.62 million—a savings of $3.31 million over the six-year period. As was mentioned before, a very conservative model was used, and in many cases the financial benefits will accelerate at a faster pace.

The advantage of adopting a security fabric approach is even more clear with a couple of the components. For example, a campus rollout of the point-product approach—including firewall, IPS and web proxy—would cost $1.14 million per year. With a security fabric, the first-year cost would be $1.34 million, slightly more than the cost of point products. But then the costs for Years 2 through 6 would drop significantly, to $644,000. This is a six-year savings of $2.27 million on just the campus costs alone.

Today, IT departments are pushed to save every penny and ensure their ROIs are industry leading—and they're being asked to do that all while taking on unprecedented challenges. The idea that the security fabric approach, while improving a company's security posture, could save significant money over a six-year period bears emphasizing. Not only can an organization save

money and devote fewer resources to its security, but it can vastly improve its security in the process. This simple result should get the attention of every IT leader around the world.

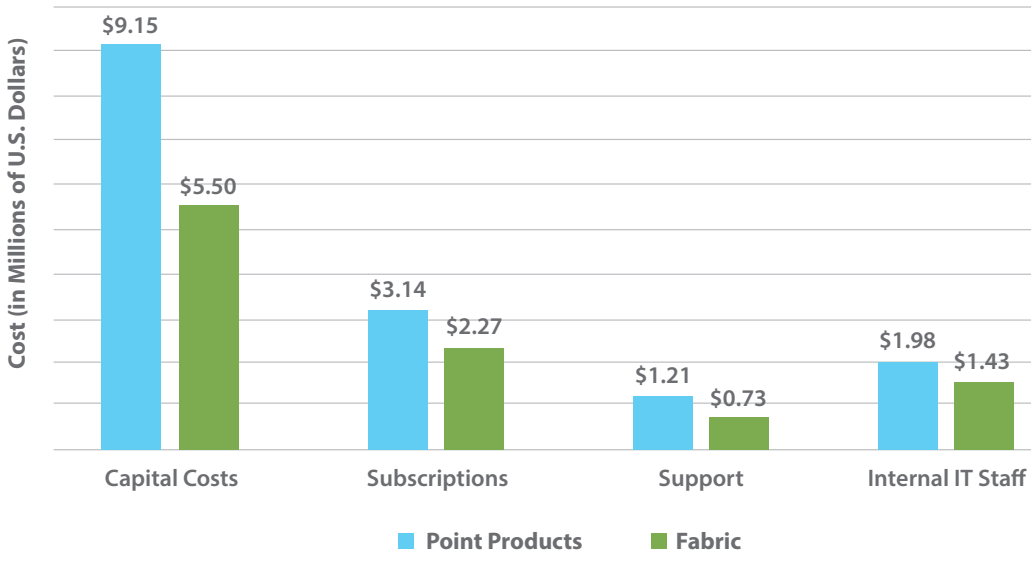
Exhibit 5 illustrates that the security fabric has cost benefits with respect to capital costs and subscription costs (due to consolidation of infrastructure), support costs (as a single vendor is used) and internal IT staff (since training is simplified).

SECTION V: CONCLUSION AND RECOMMENDATIONS

The digital era has arrived, causing the business landscape to change faster than ever. Organizations are adopting new processes and a wide range of new technologies such as IoT, cloud computing and mobility. This adoption has enabled organizations to achieve unprecedented levels of productivity and create new business models. However, securing the organization has never been more difficult. The tightly controlled IT environment with a well-defined perimeter has given way to a highly chaotic system with new entry points and an order-of-magnitude increase in the number of attack surfaces.

The security industry has evolved rapidly to help organizations better protect themselves. It seems new security startups pop up on a weekly basis, and now there are point products to protect the traditional perimeter, client devices, applications, cloud services and anything else that touches the company network. However, the addition of so many point products has come with a hefty price tag that is often hard to see and can cost companies millions over a five-plus-year period.

Exhibit 5: Point Products vs. Security Fabric Components over Six Years



ZK Research, 2017

The goal should be to minimize the number of security vendors in order to simplify the environment as much as possible.

To help maximize the company's investment in security technology, ZK Research makes the following recommendations:

Consider the security implications at every step of digital transformation. Security is often an afterthought for many companies. Generally, technology gets deployed and moved into production before security is even considered. Given that every company is becoming increasingly digital, security must be at the forefront of digital transformation.

Simplify the environment. When it comes to security, complexity is the enemy. Having more point products can make the environment more complex, as each requires its own training, management tools and vendor contracts. The goal should be to minimize the number of security vendors in order to simplify the environment as much as possible. It may not be possible to use just a single vendor, but the ZK Research–calculated number of 32 is far too high.

Take a step back and develop a security strategy. Security is too often done in an ad hoc manner. Breaches happen, and companies respond by implementing yet another point product. Security leaders should consider taking a step back and evaluating a security fabric, such as the one offered by Fortinet. Even done over multiple years, the migration to a security fabric can decrease risk and lower costs.

APPENDIX 1

Exhibit A: Detailed Calculations for Point Products

	Point Products	Vendor	Quantity	Original Purchase Price	Extended Amount	Subscription Services	Support Costs	IT Staff Costs	Total Cost
YEAR 1	**1. Campus Security**					10%	15%	25%	
	1. Edge Firewall	Vendor A	4	$150,000	$600,000	$60,000	$90,000	$150,000	$300,000
						40%	15%	25%	
	2. Next-Generation IPS	Vendor B	4	$200,000	$800,000	$320,000	$120,000	$200,000	$640,000
						40%	15%	25%	
	3. Web Proxy	Vendor C	10,000	$25	$250,000	$100,000	$37,500	$62,500	$200,000
	Subtotal				**$1,650,000**	**$480,000**	**$247,500**	**$412,500**	**$1,140,000**
YEAR 2	**2. Data Center and Cloud**					0%	15%	25%	
	4. Data-Center Firewall	Vendor D	6	$200,000	$1,200,000	$0	$180,000	$300,000	$480,000
						30%	15%	25%	
	5. Data-Center IPS	Vendor E	4	$300,000	$1,200,000	$360,000	$180,000	$300,000	$840,000
						30%	15%	25%	
	6. Private Cloud Virtual Machine	Vendor F	100	$1,000	$100,000	$30,000	$15,000	$25,000	$70,000
						30%	30%	15%	
	7. Public Cloud Virtual Machine	Vendor G	100	$1,000	$100,000	$30,000	$30,000	$15,000	$75,000
	Subtotal				**$2,600,000**	**$420,000**	**$405,000**	**$640,000**	**$1,465,000**
YEAR 3	**3. Branch Office**					40%	15%	25%	
	8. Router/UTM	Vendor H	200	$1,500	$300,000	$120,000	$45,000	$75,000	$240,000
						30%	15%	25%	
	9. WOC	Vendor I	200	$750	$150,000	$45,000	$22,500	$37,500	$105,000
						100%	0%	0%	
	10. WAN Transport	Vendor J	200	$6,000	$1,200,000	$1,200,000	$0	$0	$1,200,000
						0%	15%	25%	
	11. Switch	Vendor K	400	$500	$200,000	$0	$30,000	$50,000	$80,000
						0%	15%	25%	
	12. WiFi	Vendor L	400	$500	$200,000	$0	$30,000	$50,000	$80,000
	Subtotal				**$2,050,000**	**$1,365,000**	**$127,500**	**$212,500**	**$1,705,000**
YEAR 4	**4. Sandboxing and Email**					40%	15%	25%	
	13. Sandbox	Vendor M	4	$150,000	$600,000	$240,000	$90,000	$150,000	$480,000
						40%	15%	25%	
	14. Endpoint	Vendor N	10,000	$15	$150,000	$60,000	$22,500	$37,500	$120,000
						40%	15%	25%	
	15. WAF	Vendor O	4	$75,000	$300,000	$120,000	$45,000	$75,000	$240,000
						40%	15%	25%	
	16. Email	Vendor P	10,000	$25	$250,000	$100,000	$37,500	$62,500	$200,000
	Subtotal				**$1,300,000**	**$520,000**	**$195,000**	**$325,000**	**$1,040,000**
YEAR 5	**5. CASB**					20%	15%	25%	
	17. SIEM	Vendor Q	100,000	$6	$600,000	$120,000	$90,000	$150,000	$360,000
						100%	15%	25%	
	18. CASB	Vendor R	10,000	$15	$150,000	$150,000	$22,500	$37,500	$210,000
						10%	15%	25%	
	19. ADC	Vendor S	8	$100,000	$800,000	$80,000	$120,000	$200,000	$400,000
	Subtotal				**$1,550,000**	**$350,000**	**$232,500**	**$387,500**	**$970,000**
	Grand Total				**$9,150,000**	**$3,135,000**	**$1,207,500**	**$1,977,500**	**$6,320,000**

Note: Pricing information for point-product security infrastructure is an estimate based on an average of available information. Subscription, support and IT support costs vary depending on the product.

ZK Research, 2017

Exhibit B: Detailed Calculations for the Fortinet Security Fabric

		Fabric	Vendor	Quantity	Original Purchase Price	Extended Amount	Subscription Services	Support Costs	IT Staff Costs	Total Cost Year 1	Total Cost Years 2–5
YEAR 1	1. Campus Security						20%	12%	20%		
		Next-Generation Firewall	Fortinet	4	$175,000	$700,000	$140,000	$84,000	$140,000	$1,064,000	$364,000
							20%	0%	0%		
		Next-Generation IPS	Fortinet	0	$0	$0	$140,000	$0	$0	$140,000	$140,000
							20%	0%	0%		
		Web Proxy	Fortinet	0	$25	$0	$140,000		$0	$140,000	$140,000
	Subtotal	Total				**$700,000**	**$420,000**	**$84,000**	**$140,000**	**$1,344,000**	**$644,000**
YEAR 2	2. Data Center and Cloud						0%	10%	20%		
		Data-Center Firewall	Fortinet	6	$200,000	$1,200,000	$0	$120,000	$240,000	$1,560,000	$360,000
							20%	12%	20%		
		Data-Center IPS	Fortinet	0	$0	$0	$240,000	$144,000	$240,000	$624,000	$624,000
							30%	12%	20%		
		Private Cloud Virtual Machine	Fortinet	100	$750	$75,000	$22,500	$9,000	$15,000	$121,500	$46,500
							30%	30%	20%		
		Public Cloud Virtual Machine	Fortinet	100	$750	$75,000	$22,500	$22,500	$210,000	$330,000	$255,000
	Subtotal					**$1,350,000**	**$285,000**	**$295,500**	**$705,000**	**$2,635,500**	**$1,285,500**
YEAR 3	3. Branch Office						40%	12%	20%		
		SD-WAN/UTM	Fortinet	200	$1,250	$250,000	$100,000	$30,000	$50,000	$330,000	$80,000
							20%	12%	20%		
		WOC	Fortinet	0	$2,000	$0	$50,000	$30,000	$50,000	$130,000	$130,000
							100%	0%	0%		
		WAN Transport	Fortinet	200	$4,000	$800,000	$800,000	$0	$0	$600,000	$800,000
							0%	12%	20%		
		Switch	Fortinet	400	$400	$160,000	$0	$19,200	$32,000	$211,200	$51,200
							0%	12%	20%		
		WiFi	Fortinet	400	$400	$160,000	$0	$19,200	$32,000	$211,200	$51,200
	Subtotal					**$1,370,000**	**$950,000**	**$98,400**	**$164,000**	**$1,482,400**	**$1,112,400**
YEAR 4	4. Sandboxing and Email						40%	12%	20%		
		Sandbox	Fortinet	4	$100,000	$400,000	$160,000	$48,000	$80,000	$688,000	$200,000
							40%	12%	20%		
		Endpoint	Fortinet	10,000	$8	$80,000	$32,000	$9,600	$16,000	$137,600	$57,600
							40%	12%	20%		
		WAF	Fortinet	4	$50,000	$200,000	$80,000	$24,000	$40,000	$344,000	$144,000
							40%	12%	20%		
		Email	Fortinet	10,000	$20	$200,000	$80,000	$24,000	$40,000	$344,000	$144,000
	Subtotal					**$880,000**	**$352,000**	**$105,600**	**$176,000**	**$1,513,600**	**$545,600**
YEAR 5	5. CASB						20%	12%	20%		
		SIEM	Fortinet	100,000	$5	$500,000	$100,000	$60,000	$100,000	$760,000	$260,000
							100%	12%	20%		
		CASB	Fortinet	10,000	$10	$100,000	$100,000	$12,000	$20,000	$132,000	$132,000
							10%	12%	20%		
		ADC	Fortinet	8	$75,000	$600,000	$60,000	$72,000	$120,000	$852,000	$252,000
	Subtotal					**$1,200,000**	**$260,000**	**$144,000**	**$240,000**	**$1,744,000**	**$644,000**
	Grand Total					**$5,500,000**	**$2,267,000**	**$727,500**	**$1,425,000**	**$8,719,500**	**$4,231,500**

Note: Pricing information for the Fortinet Security Fabric is based on interviews with the company. Subscription, support and IT support costs vary depending on the product.

ZK Research, 2017

Exhibit C: The Model—Six-Year Cost of Point Products

Point Products		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Campus	Firewall	$300,000	$300,000	$300,000	$300,000	$300,000	$300,000
	Next-Generation IPS	$640,000	$640,000	$640,000	$640,000	$640,000	$640,000
	Web Proxy	$200,000	$200,000	$200,000	$200,000	$200,000	$200,000
Subtotal		**$1,140,000**	**$1,140,000**	**$1,140,000**	**$1,140,000**	**$1,140,000**	**$1,140,000**
Data Center and Cloud	Data-Center Firewall	$480,000	$480,000	$480,000	$480,000	$480,000	$480,000
	Data-Center IPS	$840,000	$840,000	$840,000	$840,000	$840,000	$840,000
	Private Cloud Virtual Machine	$70,000	$70,000	$70,000	$70,000	$70,000	$70,000
	Public Cloud Virtual Machine	$75,000	$75,000	$75,000	$75,000	$75,000	$75,000
Subtotal		**$1,465,000**	**$1,465,000**	**$1,465,000**	**$1,465,000**	**$1,465,000**	**$1,465,000**
Branch Office	Router	$240,000	$240,000	$240,000	$240,000	$240,000	$240,000
	WOC	$105,000	$105,000	$105,000	$105,000	$105,000	$105,000
	Transport	$1,200,000	$1,200,000	$1,200,000	$1,200,000	$1,200,000	$1,200,000
	Switch	$80,000	$80,000	$80,000	$80,000	$80,000	$80,000
	WiFi	$80,000	$80,000	$80,000	$80,000	$80,000	$80,000
Subtotal		**$1,705,000**	**$1,705,000**	**$1,705,000**	**$1,705,000**	**$1,705,000**	**$1,705,000**
ATP	Sandbox	$480,000	$480,000	$480,000	$480,000	$480,000	$480,000
	Endpoint	$120,000	$120,000	$120,000	$120,000	$120,000	$120,000
	WAF	$240,000	$240,000	$240,000	$240,000	$240,000	$240,000
	Email	$200,000	$200,000	$200,000	$200,000	$200,000	$200,000
Subtotal		**$1,040,000**	**$1,040,000**	**$1,040,000**	**$1,040,000**	**$1,040,000**	**$1,040,000**
Campus	SIEM	$360,000	$360,000	$360,000	$360,000	$360,000	$360,000
	CASB	$210,000	$210,000	$210,000	$210,000	$210,000	$210,000
	ADC	$400,000	$400,000	$400,000	$400,000	$400,000	$400,000
Subtotal		**$970,000**	**$970,000**	**$970,000**	**$970,000**	**$970,000**	**$970,000**
Grand Total		**$6,320,000**	**$6,320,000**	**$6,320,000**	**$6,320,000**	**$6,320,000**	**$6,320,000**

ZK Research, 2017

Exhibit D: The Model—Six-Year Cost of Security Fabric

Fabric		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
Campus	Firewall	$1,064,000	$364,000	$364,000	$364,000	$364,000	$364,000
	Next-Generation IPS	$140,000	$140,000	$140,000	$140,000	$140,000	$140,000
	Web Proxy	$140,000	$140,000	$140,000	$140,000	$140,000	$140,000
Subtotal		**$1,344,000**	**$644,000**	**$644,000**	**$644,000**	**$644,000**	**$644,000**
Data Center and Cloud	Data-Center Firewall	$480,000	$1,560,000	$360,000	$360,000	$360,000	$360,000
	Data-Center IPS	$840,000	$624,000	$624,000	$624,000	$624,000	$624,000
	Private Cloud Virtual Machine	$70,000	$121,500	$46,500	$46,500	$46,500	$46,500
	Public Cloud Virtual Machine	$75,000	$330,000	$255,000	$255,000	$255,000	$255,000
Subtotal		**$1,465,000**	**$2,635,500**	**$1,285,500**	**$1,285,500**	**$1,285,500**	**$1,285,500**
Branch Office	Router	$240,000	$240,000	$330,000	$80,000	$80,000	$80,000
	WOC	$105,000	$105,000	$130,000	$130,000	$130,000	$130,000
	Transport	$1,200,000	$1,200,000	$600,000	$800,000	$800,000	$800,000
	Switch	$80,000	$80,000	$211,200	$51,200	$51,200	$51,200
	WiFi	$80,000	$80,000	$211,200	$51,200	$51,200	$51,200
Subtotal		**$1,705,000**	**$1,705,000**	**$1,482,400**	**$1,112,400**	**$1,112,400**	**$1,112,400**
ATP	Sandbox	$480,000	$480,000	$480,000	$688,000	$200,000	$480,000
	Endpoint	$120,000	$120,000	$120,000	$137,600	$57,600	$120,000
	WAF	$240,000	$240,000	$240,000	$344,000	$240,000	$240,000
	Email	$200,000	$200,000	$200,000	$344,000	$144,000	$200,000
Subtotal		**$1,040,000**	**$1,040,000**	**$1,040,000**	**$1,513,600**	**$641,600**	**$1,040,000**
Campus	SIEM	$360,000	$360,000	$360,000	$360,000	$760,000	$260,000
	CASB	$210,000	$210,000	$210,000	$210,000	$132,000	$132,000
	ADC	$400,000	$400,000	$400,000	$400,000	$852,000	$252,000
Subtotal		**$970,000**	**$970,000**	**$970,000**	**$970,000**	**$1,744,000**	**$644,000**
Grand Total		**$6,524,000**	**$6,994,500**	**$5,421,900**	**$5,525,500**	**$5,427,500**	**$4,725,900**

ZK Research, 2017

Exhibit E: The Model—Side-by-Side Point Products vs. Fabric Six-Year Costs

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Total	Difference
Point Products	$6,320,000	$6,320,000	$6,320,000	$6,320,000	$6,320,000	$6,320,000	$37,920,000	
Fabric	$6,524,000	$6,994,500	$5,421,900	$5,525,500	$5,427,500	$4,725,900	$34,619,300	$3,300,700

ZK Research, 2017

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447

Office: 978-252-5314