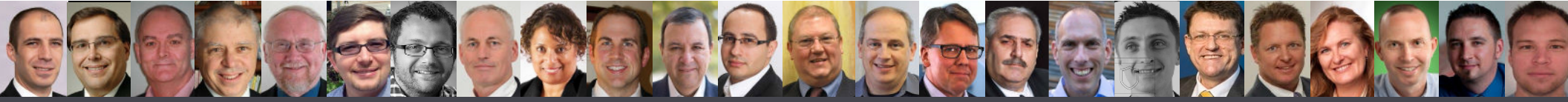

Mighty Guides

Securing Your Network and Application Infrastructure

Part 2: Protecting the Core of Your Network

5 Experts Share Their Secrets

SPONSORED BY:

FORTINET®

FOREWORD

Network security challenges are evolving faster than ever as a result of new technologies and application complexity. In addition, many old issues continue to plague organizations, from simple password security to keeping software up-to-date.

This collection of 24 essays covers a broad array of topics grouped into five major areas, ranging from the necessity of planning your network security up front to the new challenges that social engineering and other advanced, persistent threats bring. A major theme throughout many of them is the loss of the perimeter and the effectiveness of traditional defenses. Bring Your Own Device (BYOD) and cloud-based services open many holes in an organization's network that require a rethinking of security to protect the data, not just the methods of access.

Fortinet's Cyber Security platform can address most of the problems outlined in the essays in this e-book. Our ASIC-powered FortiGate firewalls deliver the industry's fastest Next Generation Firewall (NGFW) performance and are the foundation of an end-to-end security solution that spans your users, network, data centers, and the cloud. For the problems we can't solve directly, we offer tools such as enforcing business policies on password changes and vulnerability scanners for your applications to help you catch weaknesses.

We hope you find these essays as interesting and thought provoking as we do and that they can help you improve your network and application security defenses.

INTRODUCTION

For all the attention data security has received in recent years and all the technical advances in risk detection now available to protect network infrastructures, you might imagine that data are safer than ever before. Unfortunately, the number of recent, frighteningly large data breaches contradicts that notion. In the past 18 months alone, we have seen breaches at Adobe, eBay, JPMorgan Chase, Target, Home Depot, Community Health Services, and the US Government that together compromised more than 500 million records. Will the world ever be a safe place for the data so vital to businesses and individuals?

With the generous support of Fortinet, we have created this e-book to help you better understand the security challenges that business—and midsized businesses in particular—face today. This e-book is a compilation of responses to the following question:

What are the greatest challenges you face in securing your network and application infrastructure?

A range of industry analysts, consultants, and hands-on security experts provided responses to this question. They offered fascinating insights into the security challenges we face today—security issues made even more challenging because of the changing character of infrastructure and its loss of network perimeter, rapidly evolving application environment, lack of security awareness among users, and the increasing complexity of security solutions. Attacks and data theft have also become a big business underwritten by sophisticated, well-funded entities.

Security and vigilance are a never-ending battle, but I trust you will find the many perspectives provided by those who are on the front lines useful as you work to secure your own business infrastructures.

All the best,
David Rogelberg
Publisher

Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Protecting the Core of Your Network

In cybersecurity, there's A LOT OF HYPE...

...and then there are facts.

Flashy marketing has a way of clouding the truth: slow is broken. You don't have to choose between having a strong security posture and having optimal network performance to power your business.

You can have both—but only from us.

97.3% effective breach detection

5X NGFW performance

#1 unit share worldwide in network security

Over 200 zero-day attacks discovered

Get a Cyber Threat Assessment today and get the facts about your security posture.
www.fortinet.com/ctap

FORTINET®

Security Without Compromise

MANAGING VENDOR SECURITY IS CRITICAL TO OUR BUSINESS

ALEX PAPADOPULOS

Head of Operations,
Striata Inc.

Alex Papadopulos is the head of operations for Striata America and currently heads up all technical operations for North, Central, and South America. He is responsible for all areas of technical and project operations, including project management, support, development, and project implementation. Alex has more than 12 years of experience in the IT field, primarily focused on electronic billing presentment, billing, and supply chain management.

Twitter | Website | Blog

Download the full eBook:
Securing Your Network and Application Infrastructure

In providing electronic billing services to clients as well as sending and receiving emails associated with billing and payments, we deal with our clients' customer data. Ensuring the security of that data is an essential aspect of our businesses. Our two greatest security concerns are managing hosting vendors whose services we use and managing inadvertent or accidental breaches by staff.

As far as vendor management goes, this is important because we don't physically manage our own data and application servers. Instead, we rely on third-party hosting providers for our hardware and network infrastructure. Every business is a potential target, and the more data it processes, the bigger a target it is. We do not handle actual payments, so we don't have credit card data or information that would enable funds transfer, but there is always the possibility that somebody could use our data in a fraudulent billing scheme, so we must be vigilant. At the end of the day, however, the responsibility for any losses that affect our clients is ours.

> *"Our two greatest security concerns are managing hosting vendors whose services we use and managing inadvertent or accidental breaches by staff."*

KEY LESSONS

1. LOOK FOR VENDORS THAT ARE TOTALLY OPEN WITH YOU ABOUT EVERYTHING AND WHO ARE FLEXIBLE IN ADDRESSING ACTION ITEMS THAT NEED TO BE ADDRESSED.

2. ONE BIG CONCERN IS PEOPLE TAKING INADVERTENT OR ACCIDENTAL ACTIONS THAT INTRODUCE RISKS TO THE OPERATION.

MANAGING VENDOR SECURITY IS CRITICAL TO OUR BUSINESS

To manage expectations and foster confidence in our ability to deliver on security promises, we perform a full security evaluation of our vendors, determining whether they follow best security practices, how they secure their data, and how they secure their facilities.
We have detailed security policies that specify everything from how we manage our internal systems to security requirements and expectations of our vendors. We build these expectations into our SLAs, and we visit the physical locations of vendor data centers to see for ourselves how well the vendors protect their facilities. We often bring clients on these visits to demonstrate to them that the data they are entrusting to us are secure. We look for vendors that use an approach similar to ours. We define what we want and need from a vendor, and then perform annual reviews of the controls and policies.

Our other big concern is people taking inadvertent actions that introduce risks to the operation. We track every action taken. Then, red flags alert us if employees or customers take an action without understanding its potential consequences, such as clicking a phishing email or providing a credential that can then be used to gain unauthorized entry to a system or process.

Protecting against such accidental situations requires continuous education. For example, we send fake phishing emails to staff; anyone who clicks them is not reprimanded, but the episode becomes an opportunity to educate them on the risk and the proper way to handle suspicious communications. Continuous training and education are incredibly important.

To secure against human error, policies must be well defined, in place, and updated regularly. New staff must be trained on security policies before being given access to any systems. Staff must be regularly updated if a policy changes and re-trained at least annually. Finally, always test staff as a way to identify weaknesses, strengthen training, and improve policies.

> *“We have detailed security policies that specify everything from how we manage our internal systems to security requirements and expectations of our vendors.”*

SECURING VITAL DATA IS THE GREATEST CHALLENGE

JOHN MADDISON

Vice President, Marketing,
Fortinet, Inc.

John Maddison has more than 20 years experience in the telecommunication, IT Infrastructure and security industries. Previously he held positions as General Manager Data Center division and Senior Vice President Core Technology at Trend Micro. Before that John was Senior Director of Product Management at Lucent Technologies. He has lived and worked in Europe, Asia and the United States. John graduated with a Bachelor of Telecommunications Engineering degree from Plymouth University, United Kingdom.

Website | Blog

Download the full eBook:
Securing Your Network and Application Infrastructure

KEY LESSONS

1. THE REAL PROBLEM FOR SMALL AND LARGE BUSINESSES ALIKE IS NOT HAVING THE RESOURCES THEY NEED TO IMPLEMENT SECURITY THEY SHOULD HAVE FOR THE LEVEL OF PROTECTION THEY REQUIRE.

2. YOU MUST PROTECT THE NETWORK, WHICH ALSO INCLUDES PEOPLE WHO USE THE NETWORK AND ALL THE DEVICES CONNECTED TO IT.

The greatest vulnerability for many businesses, especially midsized companies, is data vital to daily operations. We worked with a machine shop that used computer-controlled machines to create parts. Periodically, the shop would connect to the Internet to update its machines; somewhere along the way, the company picked up malware that remained dormant in its system. After a time, when the shop went onto the Internet again, the malware received an instruction and immediately encrypted all the data the shop's very expensive machinery needed to operate. Soon after, the company received a ransom email asking for $50,000 in exchange for decrypting the data. The business had little choice. A week with idle machines would have bankrupted it, so it paid the ransom, the data was decrypted, and it was up and running again.

Most businesses today depend on data, whether it is unique intellectual property or simply data that enable them to operate. Losing that data would literally put them out of business. So, how do you protect that vital asset? You must protect the network, which also includes people who use the network and all the devices connected to it. This is becoming an increasingly difficult task.

> *"Most businesses today depend on data, whether it is unique intellectual property or simply data that enable them to operate."*

SECURING VITAL DATA IS THE GREATEST CHALLENGE

As businesses build infrastructures, they are extending beyond their core systems to data centers, cloud services, and mobile devices; managing connectivity to the Internet; and making sure their core network provides all the services their users need. Performance is a key factor. Users expect high performance from their dispersed network infrastructure. With all this going on, the network boundary becomes larger and more porous, which makes it more vulnerable.

One approach is for companies to think about their infrastructure as being made up of an internal network and an external network. They can apply their own security solutions to their internal network. Securing the external network involves applying policies and procedures and relying on SLAs with service providers, but there are limits to what they can do with that, which means that a certain level of risk will always be associated with their external network. It comes down to levels of trust in different parts of the network.

One strategy we are seeing is companies securing their internal network from within. They do this by segmenting their core network, breaking it down based on users or applications or traffic or other criteria. Then, they apply trust levels to each segment. They can implement different levels of protection between different segments based on the trust level between those two segments. Anything passing from one segment to another must pass that segment's trust-level security protections. In this way, if a threat breaches one segment, the chances of it spreading across the internal network are much less.

The real problem for small and large businesses alike is not having the resources they need to implement security they should have for the level of protection they require. They often do not discover this until after they have experienced a breach. Finding the right balance among cost, levels of security, and data protection is not easy. Businesses need a trusted partner that has qualified and certified staff. The business should build a personal relationship with that trusted partner.

> *"One strategy we are seeing is companies securing their internal network from within."*

ROBERT SHULLICH

Enterprise Security Architect,
AmTrust Financial Services

Robert Shullich is an enterprise security architect at AmTrust Financial Services. He has worked in the financial services sector for more than 30 years, having held senior-level roles in information risk and information security. In his current role, he assesses information risk for IT projects and proposes additional controls or design changes that will reduce the risk to the project. He has also taught cyber-risk management at the graduate level.

Twitter | Website

Download the full eBook:
Securing Your Network and Application Infrastructure

KEY LESSONS

1. MANY ORGANIZATIONS LACK INVENTORIES OF ASSETS. THE REALITY IS, YOU CAN'T PROTECT WHAT YOU DON'T KNOW YOU HAVE.
2. THIS LACK OF COMPLETE SITUATIONAL AWARENESS IS A RESULT OF THE EVAPORATION OF THE LEGACY CONCEPT OF THE PERIMETER.

Enterprise computing today is made up of a mixture of in-house systems; cloud-based services; a diverse collection of mobile devices that employees use to access data from anywhere; and even consumer-grade cloud-based services, such as file sharing, that the enterprise may not know its employees are using. It is difficult in this environment to have an accurate idea of what your assets are and who is using or should be allowed to use them. Many organizations lack inventories of assets, including employees, software, hardware, and data centers. The reality is, you can't protect what you don't know you have.

This lack of complete situational awareness is a result of the evaporation of the legacy concept of the *perimeter*. We have punched holes in that perimeter to allow employees access to internal networks for work-at-home scenarios, to provide mobile salespeople the ability to more effectively service new and current customers while traveling, and to outsource operations of our networks to third parties. The data all these people access with their smartphones and tablets must be protected, but in this environment, it is often difficult to know where that data is.

> *"It is difficult in this environment to have an accurate idea of what your assets are and who is using or should be allowed to use them."*

Consider, for example, a typical third-party cloud service provider that is delivering a Software as a Service business application that depends on your critical business data. As part of your SLA, you may require the third-party vendor to ensure certain levels of risk abatement and threat protection. However, it is likely that the vendor is relying on a fourth-party cloud service provider to store your data. So, where is your data *really*, and how do you assess the risks to your data if it is difficult to know exactly where it is physically located.

Another problematic area for some companies is employees' use of low-cost file-sharing services without the knowledge of security people. This is typically not a malicious act: it is simply a case of employees trying to do their jobs as efficiently as possible. Nevertheless, it exposes proprietary data to risk, and if the practice is unknown to those who manage corporate security, it represents a risk they cannot see or defend against.

> *"The security person needs to get it right every hour of every day; the data thieves need to get it right only once."*

To address these security challenges, organizations need to start with accurate asset inventories. Whether an asset is purchased, leased, or acquired as a service, it must be tracked for its entire life cycle. An entire life cycle begins with acquisition or creation, carries through maintenance, and ends with destruction. Assets include hardware, software, data, and even people. Assets should be classified so that the organization knows what they are and how much protection each asset requires. Organizations need to integrate all business processes with asset acquisition so that expenses and purchases can be tracked. Loopholes in expense tracking allow employees to purchase cloud instances on a credit card and build applications that bypass IT governance processes. Above all, organizations need clear written policies and procedures on the handling of assets and an effective communications and training program (security awareness) to reinforce adherence to those policies.

The reality here is that most businesses are not in the business of fighting malicious hackers. They are in the business of doing their business. They have a security department or person who does the best job possible to address the highest-risk issues so the business can minimize risk to its revenue-generating operations. But they are up against professional data thieves who operate 24x7 to figure out how to steal that data. The security person needs to get it right every hour of every day; the data thieves need to get it right only once.

In cybersecurity, there's the slick SALES PITCH...

...and then there are facts.

Our focus on innovation over the last 15 years means you can simplify your security strategy and stay ahead of the threat today—not in an upcoming version that only exists in a pitch over golf.

We deliver a consolidated approach from datacenter to endpoint, plus global visibility and control on one OS with one management console.

It's because we like our labs more than the golf course.

97.3% effective breach detection

5X NGFW performance

#1 unit share worldwide in network security

Over 200 zero-day attacks discovered

Get a Cyber Threat Assessment today and get the facts about your security posture.
www.fortinet.com/ctap

FORTINET®

Security Without Compromise

DAVE WATERSON
CEO,
SentryBay

Founder and chief executive of SentryBay Limited, Dave Waterson is an information security technologist and inventor of patented technology in the anti–key logging and anti-phishing areas. Based in London, United Kingdom, Dave has guided the company from startup to become a recognized leader in its sector of information security software development, with security solutions for PC, mobile, the cloud, and the Internet of Things. He has a master's degree in economics and is a registered CISSP.

Twitter | Website | Blog

Download the full eBook:
Securing Your Network and Application Infrastructure

Organizations used to focus security on the enterprise network perimeter. Organizations built virtual walls—firewalls and demilitarized zones—at the periphery to stop people from getting inside. Unfortunately, the network was breached anyway.

Then, the industry shifted focus to endpoints - PC equipment and mobile devices. Antivirus applications became our shields of choice. Sadly, we now know that antivirus software grows less effective daily.

My view is that we need to shift the defenses closer to the enterprise core—down to the granular level of data, where several big challenges await:

- **Personal information.** Personally identifiable information (PII) is an enormous enterprise problem—the Sony Pictures Entertainment and Target Store hacks demonstrate just how enormous. Many enterprises hold the PII data of millions of people within their IT core.

"I recently wrote a blog post in which a fictitious IoT-enabled garage door becomes part of an attack botnet."

KEY LESSONS

1. THE FOCUS OF ENTERPRISE NETWORK SECURITY NEEDS TO SHIFT CLOSER TO THE ENTERPRISE CORE—TO DATA.

2. BEYOND TECHNICAL SOLUTIONS, PROCEDURES AND RAPID RESPONSE TEAMS NEED TO BE PUT IN PLACE.

- **Cloud computing.** There are actually two challenges here. First, the cloud technically extends the enterprise network beyond direct enterprise control. Second is the sheer volume of data. Cloud computing offers far greater storage and process volume than companies have ever had. Security issues arise from both.
- **The Internet of Things (IoT).** The IoT is not a big factor yet, but every company is examining it. In factories and retail, data-producing sensors will be attached to almost everything. The IoT will control office energy settings and meeting room management. Attack surfaces will multiply exponentially. I recently wrote a blog post in which a fictitious IoT-enabled garage door becomes part of an attack botnet. That might give you some idea of the scale of this impending danger.

So, how do we meet these challenges?

First, we keep protecting the perimeter. Web application firewalls, intrusion-detection and prevention services, honeypots, and all the rest remain crucial. These are the sentries at the gate that can radio into headquarters when something is amiss.

> *"I think companies today realize that it is not a matter of whether they will get breached but when."*

Next, figure out what data you have. A surprisingly large number of enterprises do not know this. After that, track data flows throughout the organization. Where and how are data coming in? Where do they sit around unencrypted? What are the attack vectors at each phase of data flow?

Finally, carefully assess what types of data need to be secured. Some data, frankly, needs little security—they just are not that sensitive. Knowing which data types are where will allow you to target security investment where it has the greatest payoff.

If it sounds as if a big data solution is where this is heading, you are right. Big data technologies (Apache Hadoop, in-memory computing [IMC], Scala, Spark, etc.) offer the measurements, machine learning, and early warnings that can show you if and where security breaches exist. Securing data at entry is also important. Beyond the purely technical solutions, you need to establish procedures and assemble a well-trained, rehearsed, and practiced response team that can spring into action immediately.

I think companies today realize that it is not a matter of *whether* they will get breached but *when*. The secret in securing the enterprise network is to focus at the level of data.

LINDA CURETON

Former CIO,
NASA

Linda Cureton is CEO of Muse Technologies and former CIO of NASA, with more than 34 years of service in IT management and at the U.S. federal cabinet level. She holds a B.S. degree in mathematics from Howard University and an M.S. degree and a post-master's advanced certificate in applied mathematics from Johns Hopkins University. A strategic innovator, thought leader, prolific blogger, and pathfinder for federal CIOs using social media, Linda has received many awards and is a bestselling author.

Twitter | Website | Blog

Download the full eBook:
Securing Your Network and Application Infrastructure

Protecting data and understanding the risks data faces are two of our greatest weaknesses. We have focused on protecting the perimeter and put so many resources into doing so that we have, perhaps, neglected the data itself, especially when you look at insider and advanced persistence threats. Protecting the perimeter doesn't necessarily afford you the protection you need: I think that our strategy needs to focus on protecting data.

KEY LESSONS

1. UNDERSTAND THE THREATS THAT ARE SPECIFIC TO YOUR ORGANIZATION, AND DON'T FORGET TO LOOK AT THE THREATS THAT MAY COME FROM WITHIN.
2. DESIGN YOUR SECURITY PROGRAM BASED ON THE UNIQUE NEEDS OF YOUR ORGANIZATION RATHER THAN TRYING TO FIND A ONE-SIZE-FITS-ALL SOLUTION.

This is not to say that you shouldn't protect the network, but I don't think that our defense matches our risks very well. One way to protect against insider threats is two-factor authentication (2FA), which uses what you know and what you have. The issue preventing adoption of 2FA might be the cost associated with it and the fact that legacy applications aren't always able to use such methods.

Another way is the protected data approach—basically taking the stance of "trusting no one." Trust is verified: if you are who you say you are, prove it. When this approach has been applied and users have been verified, they can go anywhere and access anything on the network.

One example of how inside threats can compromise an organization is the breach that happened at the Office of Public Information several years ago.

> *"I don't think that our defense matches our risks very well."*

A person who was not authorized to access certain documents not only did but managed to take many off premises. In that example, we relied too much on passwords to secure things. We often think the solution is to change or strengthen passwords, but this issue is much larger than a password problem. Organizations need to understand that these threats go much deeper.

Understanding the threat and the risk factors help guide you to better defense approaches. A good way to better understand those risks is for organizations to think about them from the beginning. We spend a lot of time and resources on checking the box next to risk analysis, but we don't really dig in to figure out what the true risks are. We need to do a good, old-fashioned "What are our risks?" assessment. Those risks vary from organization to organization.

We also spend a lot of time and resources understanding compliance, and doing so can get in the way of finding the right kind of protection. We are pressured to comply with a laundry list of things that may or may not apply to our situation or organization. It would be better if we spent that time on risk assessment. If we understood our risks, we could then prioritize the laundry list, pick the most critical risks, and find the right solutions to mitigate them.

As it is, we have a tendency to look for a single solution that fits everyone, but the scenario just doesn't apply. There are a lot of security solutions out there, so many that it's becoming a problem. How do you choose the right solution? Some think all you have to do is have a firewall, but really, you've got to have a firewall, intrusion protection, good authentication mechanisms, good network topology—the list goes on—so that when a breach occurs you're able to recover better.

There is no magic bullet that addresses every security risk. True security requires a layered defense of several solutions, put together to give you the right kind of protection for your specific organization. No single tool will keep your network and data safe.

"True security requires a layered defense of several solutions, put together to give you the right kind of protection for your specific organization."