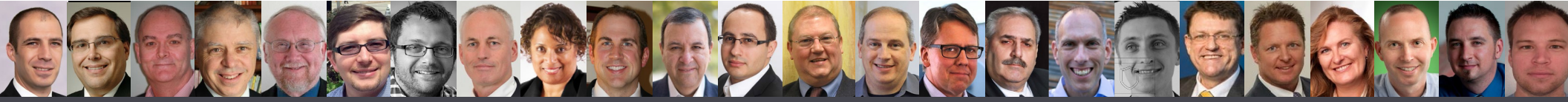

Mighty Guides

# Securing Your Network and Application Infrastructure

## Part 3: Staying Ahead of Hackers

3 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.

# Staying Ahead of Hackers

# 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

**TOM ESTON**

**Manager, Penetration Testing,**
Veracode

Tom Eston is the manager of Penetration Testing at Veracode. His work over the years has focused on security research, leading projects in the security community, improving testing methodologies, and team management. He is also a security blogger; co-host of the Shared Security Podcast; and a frequent speaker at security user groups and international conferences, including Black Hat, DEFCON, DerbyCon, Notacon, SANS, InfoSec World, OWASP AppSec, and ShmooCon.

Twitter | Website | Blog


**Download the full eBook:**
***Securing Your Network and Application Infrastructure***

## KEY LESSONS

1. MOST CORPORATE BREACHES START WITH SOCIAL ENGINEERING TACTICS.
2. APPLICATIONS VULNERABILITIES AND SYSTEM MISCONFIGURATIONS ARE TOO OFTEN OVERLOOKED.

Once I was part of a no-holds-barred red team assessment of a famous actor. He had put a lot of digital safeguards in place and was confident his digital life was hack-proof. It wasn't.

As a first step, I had one of my team members place a phone call to Amazon tech support. He told the worker that he wanted to add a credit card to the actor's Amazon account. The staffer asked a security question: What is one of your most recent purchases? My staff member knew that our guy was a *Game of Thrones* nut, so our caller winged it. "*Game of Thrones*, DVD Box, Season 1," he said. "Right," the support worker replied. "We'll reset your password."

That single move gave my team access to a lot of the actor's personal details. It allowed us to hack into his Twitter account, then his email. We reset passwords to practically every account he had. Within days, we had infiltrated his entire digital life. Needless to say, the actor was shocked.

There is a lesson here for organizations: many respond to their vulnerabilities only after a breach. That's not good enough. My take is that the defensive corporate mindset needs to become proactive.

> *"That single move gave my team access to a lot of the actor's personal details."*

Here are three of the biggest electronic security challenges I see for companies that operate in the digital realm:

- **Social engineering.** Most corporate breaches start with phishing emails or phone calls or with an attacker physically walking into a building and claiming to work there. It's called *social engineering* because attackers take advantage of the natural human desire to trust. From a computer security perspective, this is a dangerous attack vector—the same one my team used to hack our actor friend. It shocks me how easy the human factor is to exploit.
- **Application vulnerability.** Web applications are the front end of most organizations and the way most of them make money. In recent years, immense new layers of complexity have been introduced behind the scenes to allow apps to work in the cloud. With complexity comes human error. I often find that companies don't take the time to build security into their application infrastructure or to perform proper security testing from the beginning. This remains true even today, when security is top of mind with most executives.
- **System misconfigurations.** These, too, are often overlooked. Web management consoles, even production systems, often remain in their default configurations, accessible through default passwords. When hardening application coding and infrastructure that applications live on, spend some time focused on this piece. As an attacker, if I can access your web management console by using a default password, I no longer care about the application. I can access everything on your server.

The moral is simple: be vigilant. Continually educate your employees. Have third-party consultants conduct penetration tests, and be prepared to hear things you wish you hadn't—like you've already been hacked. Stage your own social engineering tests so that employees know what these attacks look like and what to do when they happen.

A lot of what we call *network security* is really just a question of human awareness.

> *"Stage your own social engineering tests so that employees know what these attacks look like and what to do when they happen."*

**STEVEN WEISKIRCHER**

**Chief Information Officer,**
ThinkGeek, Inc.

Steve Weiskircher has more than 19 years of direct leadership experience in the e-commerce industry, having served as the chief information officer of multiple top "e-tailers," including Crutchfield, Fanatics, and most recently ThinkGeek, where he is responsible for the technology and user experience teams. Steve holds a B.S. degree in mechanical engineering from Virginia Tech and an M.S. degree in management information systems from the University of Virginia.

Twitter | Website


**Download the full eBook:**
***Securing Your Network and Application Infrastructure***

Once, I tried to sell an executive management team on investing in an intrusion-prevention system (IPS) and web application firewall (WAF). They were not impressed. Who would attack us, they asked?

To answer that question, I set up a dummy server—with up-to-date patches—just outside the corporate firewall. Within three minutes, it was being robotically mapped and scanned. Within 12 minutes, it was under direct assault. That convinced them.

That was long ago, but people still see security investment as an insurance policy they will never collect on. That's partly why these three challenges keep me up at night:

- **External predators.** These are the attackers and nefarious bots that beat on the door, day and night, pounding away at my perimeter defenses trying to break in. As an e-commerce retailer, we deal with these a lot. I also see the tertiary effects of other breaches—somebody's account or credit card is compromised during another retailer's breach.

> *"Within three minutes, it was being robotically mapped and scanned. Within 12 minutes, it was under direct assault."*

## KEY LESSONS

1. EXTERNAL PREDATORS, INTERNAL THREATS, AND CRUMBLING NETWORK BOUNDARIES ARE BIG WORRIES.
2. THOROUGH RISK ANALYSIS SHOULD BE PART OF ANY NEW TECHNOLOGY IMPLEMENTATION, PARTICULARLY WHEN YOU WORK WITH EXTERNAL PARTIES.

The nefarious individuals then use that account data on another site. More recently, I have seen a shift in this fraud where account data that was compromised during one of the mass breaches is sold or traded to another individual. That person attempts to buy product and return it for cash. They do not even have to go through the effort of hacking someone's account, as there is ample supply of previously compromised accounts in the wild.

- **Crumbling boundaries.** Familiar network and application boundaries are falling at an incredible rate. Cloud services, coupled with a next-generation Bring Your Own Device workforce, are blowing away the borders. We used to have nice, hardened perimeters, and extensive device management. That era has ended. We now have to protect our data in an always on, always connected world where there are no longer clear perimeter boundaries. Quite simply, we don't have the same measure of control anymore.
- **Internal threats.** These threats can come from disgruntled employees or contractors looking to profit off of your critical data. It is difficult to protect against every possible threat vector involving an internal employee that has access to sensitive data and the Internet. It has become too easy to shift large volumes of data relatively undetected. While this does occur, the more probable scenario is the unintentional hole that an employee or contractor creates. Outsourced third-party contractors can be a particular risk; they often have direct and/or privileged access into the interior of your network. The challenge is you do not manage their devices or the networks they connect into. Such unintentional exposures can create holes through all your defenses.

> *"The days of simply instituting IP restrictions or even stateful firewalls are over."*

There are mitigation steps you can take, of course. Providers like Fortinet and others offer advanced IPS, WAF, and centralized login tools. These technologies are requirements for any public-facing web servers or exposed application programming interfaces. Regular threat assessments are also key. Internal and external vulnerability scans should be regular events. The days of simply instituting IP restrictions or even stateful firewalls are over.

For cloud-based risks, in conjunction with the threat-assessment piece, I recommend thorough risk analysis. That should also be part of any new technology implementation, particularly when you work with external parties. A full-on penetration test or vulnerability assessment starts with automated scanning, but you should also have your people performing careful risk-management assessments. What data does that server hold? What networks or systems can access it? Should you restrict access, or cordon it off all together?

It would be great if there were such a thing as a straight, universal security checklist. Unfortunately information security is not a recipe that we can follow. We live in a world of gray, not black and white. Therefore, security will always be a combination of advanced technology and smart people. It is only by carefully sorting through the risk factors that you can come up with the right strategies to mitigate the danger.

*“Security will always be a combination of advanced technology and smart people.”*

# 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

**WILL LEFEVERS**

**Lead Information Security Architect,**
Constant Contact

Will Lefevers is an information security architect who has 15 years of experience, including military tours in satellite operations, counterintelligence, cyber operations, and vulnerability research. Prior to joining Constant Contact, he was the application security engineer for a multimillion-dollar next-generation cloud platform. His foci include insider threat detection, behavioral analysis, malware reverse-engineering, and hunting threat actors in live networks. He's also an avid homebrewer and writes exceptionally mediocre code.

Twitter


**Download the full eBook:**
***Securing Your Network and Application Infrastructure***

My greatest challenge is finding talent. The market is awash with people who claim they can do InfoSec. Bolstered by a master's degree in IT management, a freshly minted Certified Information Systems Security Professional certification, or a few years of managing firewalls, plenty of folks are willing to sign up to try network security. Most of them fall far short of the mark. I need hunters.

The industry sells all manner of fascinating tools to find the bad guys on your network. Intrusion-prevention systems, next-generation firewalls, big data security analytics—they all offer you the grail. They're each going to save you. Each claims to have built something that knows your network well enough to pinpoint aberrant behaviors in the vast oceans of noise. They all purport to find the needle in the haystack. I have yet to find one that does.

To be clear, I'm hunting hunters—people who think like the bad guys. People who study offense and keep up to speed on the latest developments in hacker subculture. People who can write exploits and malware and know exactly why that new vulnerability is going to spread like wildfire in the Russian underground.

*"My greatest challenge is finding talent . . . . I need hunters."*

## KEY LESSONS

1. NOTHING BUT EXPERIENCE CAN TEACH YOU HOW TO RESPOND IN THE MOMENT WHEN YOU HAVE BEEN BREACHED. YOU NEED PEOPLE WHO WILL RUN TOWARD THE FIRE.

2. FINDING TALENTED PEOPLE WHO STUDY OFFENSE AND KEEP UP TO SPEED ON THE LATEST DEVELOPMENTS IN HACKER SUBCULTURE IS KEY.

# HUNTING THE HUNTERS

People who can quote off the top of their head the black market price of someone's full medical file. People who blend in with both the suits and the punks. People who make it their lifestyle to stay on the cutting edge of security. People who live it instead of just working it.

The reality is that each of us will be breached. We'll all get to experience that dazzling rush of panic and excitement. We'll all live under the pressure of unsteady upper management, certain that intense scrutiny will meet our every decision for the next few weeks. Maximum pressure will be applied with near-zero tolerance for common mistakes. Nothing but experience can teach you how to respond in that moment. In situations like that, I've seen two kinds of personalities: those who run from the fire and those who run toward it. I revel in those moments. I need people who run toward the fire. I need people who look forward to the next chance to prove their skills.

The hacker world evolves in response to every new defense. The cat-and-mouse game between attacker and defender plays out continuously. At the end of the day, shiny toys and fancy degrees won't save you. I need the hackers who hunt hackers.

*“The reality is that each of us will be breached. We'll all get to experience that dazzling rush of panic and excitement.”*