Mighty Guides

8 Security Experts

on Changing Endpoint Security

Keys to Shutting Down Attacks

Sponsored by Carbon Black.

INTRODUCTION: ENDPOINT SECURITY

Without a doubt, endpoint security has become an urgent priority for many organizations, and it's not hard to see why. Industry research by IDC is showing that 70 percent of successful breaches enter through an endpoint. Other research shows that more than half of companies have been hit with successful attacks, and more than three-quarters of those attacks were fileless.

For many companies, the modern business environment has become a mobile workplace in which employees work from wherever they happen to be. The fact that people continue to be the weakest security link has made mobile PCs and extended networks a sweet spot for attackers. So how are companies responding?

To find out, we drilled into the question of endpoint security with the generous support of Carbon Black. We approached 8 security experts to discuss these aspects of endpoint security:

- **Keys to shutting down attacks**
- **Rethinking your network strategy**
- **Justifying the value of endpoint security**
- **Moving to a cloud-based next-generation platform for endpoint security**

In speaking to security experts from a number of different industries, two things are clear. Endpoint security has become a critical piece of a broader security strategy, and securing the traditional network perimeter alone will not save you. One contributor observed that endpoints are in fact the new perimeter.

These essays contain useful and practical insights into evaluating endpoint security needs and implementing endpoint strategies. Regardless of how you think about the role of endpoint security in your overall strategy, I highly recommend that you read what these experts have to say.

All the best,
David Rogelberg
Publisher,
Mighty Guides, Inc.

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.

© 2017 Mighty Guides, Inc. | 62 Nassau Drive | Great Neck, NY 11021 | 516-360-2622 | www.mightyguides.com

FOREWORD: ENDPOINT SECURITY

Everyday companies put more of their assets in digital form. Healthcare records, retail purchases and personnel files are just some of the many examples of how our entire lives have moved online. While this makes our interconnected lives more convenient, it also makes them more vulnerable to attack. The monetary benefits of exploiting these vulnerabilities have created an extremely profitable underground economy; one that mimics the same one we all participate in and has led to an increase in the sophistication and frequency of attacks.

At the same time, mobility and cloud are changing the security landscape. We've moved from a centralized to a decentralized model as end users increasingly work on-the-go and access critical business applications and resources from anywhere. As such there is more emphasis on the endpoint and individual identities - from both the defender and the attacker - than ever before.

As endpoints become smarter, new challenges emerge: emerging ransomware and 0-day exploits infect all kinds of systems with ease, while many attackers use no malware at all to accomplish their malicious goals. With all this change, we spoke to 8 leading security experts to identify what's working and how they've influenced their organization to make the necessary changes before becoming the next victim.

Regards,
Mike Viscuso
CTO and Cofounder of Carbon Black

Carbon Black.

Carbon Black (NASDAQ:CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 3,700 customers globally, including 33 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise, or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus. To learn more about Carbon Black visit www.carbonblack.com.

KEYS TO SHUTTING DOWN ATTACKS

ROBERT HOOD

Security Solutions Architect,
BJ's Wholesale
Warehouse Club

An atypical thinker ("I typically don't think outside the box, I'm not in the same building as the box," he says), Robert Hood has most recently worked on internet and intranet security, penetration testing, social engineering, and the applied attack vector discovery and defense of the company network assets. The self-described hacker and red teamer's main focus is social engineering. He has experience as a senior security engineer, network engineer, network manager, and project manager in multiple industries, including, retail, biotech, healthcare, government, education, and electronics manufacturing.

Twitter | LinkedIn

Download the full e-book: Security Experts on Changing Endpoint Security

"In retail, when you think about endpoint, you're typically thinking about the corporate laptop," says Robert Hood, information security solutions architect at BJ's Wholesale Club. "Most of the computers given to corporate employees are laptops. And a lot of employees now have the ability to work from home, so mobility is a very big issue. Being mobile, they're connecting to foreign networks with corporate equipment. The security tools you have on the system have to be active all the time."

Hood points out that securing endpoints involves protecting the endpoints themselves, having analysts who can look at endpoint data and use tools that make it easier to find legitimate incidents, and also having ongoing social-engineering training to reduce the risk of insider threats. "It's really all about balance," he says. "On the technology side, you have to have protection. PCI mandates the some protections. You must have antivirus. You must have anti-malware. But you also need to log data for back-end analysis. And you have to remember it's not just the endpoint you have to protect. It's the person *typing* on the endpoint." »

> *Solutions now are almost doing real-time forensics at the endpoint.*

Hood believes the biggest challenge in securing the endpoint continues to be the person behind the keyboard, who is susceptible to social-engineering attacks like phishing. Although endpoint-protection technology may be able to block someone from going to a known unsafe website, for the most part there is no technical defense against these endpoint threats. “These kinds of attacks have been around for thousands of years—it’s called being a con artist, or one of the other hundreds of names given to them throughout history. Only now, the con artists are using more up-to-date methods, and really the only defense is education and training,” says Hood.

Although technology can’t always protect the user, the newest generation of endpoint-security technologies goes way beyond simple antivirus protection. Hood says this is necessary because of the role mobile PCs play in modern business workflow, especially in retail. “PCs effectively extend the perimeter,” he explains. “Your corporate network is not just your network, it’s the network for all the corporate people who take work home. Their machines are an extension of your network. Whatever network they’re connecting to is actually an extension of your network. You can’t prevent anything on that network from happening, but you need to prevent it from happening on that laptop before and after it reconnects to your internal network.” »

> **“The idea is to remove as much of the human factor as possible on the back end and have it self-correlate so it takes 10,000 hits and reduces that to one incident.”**

Protecting these mobile endpoints that are processing valuable business information and providing potential access to hackers requires more sophisticated tools. “Solutions now are almost doing real-time forensics at the endpoint,” says Hood. They log activity, generate alerts, and they also correlate and validate alerts. Of course this generates a lot of new data that an already-stressed security-operations team needs to analyze. “Security-operations engineers have too many separate things they have to look at,” he adds. “If they see an alert in one thing, often they then have to manually correlate these to alerts from other applications and hope all the timestamps are correct. All of this takes a lot of time.”

But that is changing. Endpoint-security solutions with back-end analytics engines can analyze and validate all the different alerts before the SOC engineer even sees a report. “They’re no longer getting tons of alerts each day for each person,” says Hood. “The idea is to remove as much of the human factor as possible on the back end and have it self-correlate so it takes 10,000 hits and reduces that to one incident.” This not only enables a single analyst to process more alerts, it speeds response to validated incidents.

Of course, these are the personal opinions of Hood himself, and do not reflect the policies, processes or strategy of his current employer. ■

KEY POINTS

1 **Securing endpoints involves protecting them, having analytical tools that make it easier to find legitimate endpoint incidents, and educating against social-engineering attacks.**

2 **Endpoint-security solutions with back-end analytics engines generally based in the cloud can analyze and validate all the different alerts before the SOC engineer even sees a report.**

WAYNE PETERSON

Chief Information Security Officer, Kroll Associates, Inc

Wayne Peterson is chief information security officer (CISO) for Kroll. Peterson is a globally recognized enterprise security risk executive, having bridged the government and private sectors in a distinguished career that included two decades with the US Secret Service. As a veteran security professional, he has led numerous international risk management, cybercrime investigations, remediation, and security initiatives in highly complex, dynamic environments.

Website | LinkedIn

Download the full e-book: Security Experts on Changing Endpoint Security

Wayne Peterson considers it a top priority to identify and shut down attacks before they threaten the business. The first thing he did, both as CISO at Kroll and in his prior role at the US Secret Service, was to beef up and build out a robust incident-response team. When some of his colleagues asked why he was starting there, he responded that it takes time to make changes in an organization. “While you’re changing things and beefing up your security, you want to know that if something happens, it’s going to be early detection that keeps incidents small,” he says. “In today’s world every company has some type of incident, so you’re not really judged on whether or not you have an incident anymore. You’re judged on how you respond to an incident. Early detection and quick response are key to that.”

This wasn’t always the case. “Back in the old days, the first order of business was to build a robust firewall. And you built up your wall around your castle so nobody could get in. Today your most critical vulnerability footprint, in my opinion, is your endpoints,” Peterson explains. For example, remote workers may already have escalated privileges—and if their systems get compromised, it’s very easy for attackers to gain access. Accordingly, businesses must evolve their approach to security with an emphasis on depth and endpoint security beyond standard anti-virus.

> “ *You're judged on how you respond to an incident. Early detection and quick response are key to that.* ”

Adapting to this new reality may require executives to update their conceptions about what a good security strategy looks like. “When I was at the Secret Service, we did all the major breach investigations. And their CEO or their CISO would ask, ‘What tool can I go to buy to prevent this from happening again?’ I would often tell them, ‘Look, you can’t buy your way into security. You have to go back to the basics of blocking and tackling,’” he says. Once you have a solid endpoint strategy in place you can buy tools to help automate certain processes, but it’s essential to start at the endpoint first.

Endpoint security solutions can often shed greater light on the true nature of threats that a business faces, providing more visibility into the threat environment. Peterson once discussed this point with a CEO who wanted to reduce the number of vulnerabilities he had, often getting worried if a weekly number would go up. “I said, ‘Look, that’s a good thing,’” Peterson says. “‘How can that be a good thing? The number is high,’” the CEO countered. “I said, ‘It means we’re detecting them better. They were always there.’” Armed with better information, the business can make smarter decisions about how to counter the threat. This may involve updating security awareness training to address end-user behaviors that weren’t visible before, for example.

> **“Today your most critical vulnerability footprint, in my opinion, is your endpoints.”**

TO PREVENT ATTACKS, START WITH THE ENDPOINTS

While it is true that adopting greater endpoint security requires you to extend the perimeter of what you must protect, Peterson feels that many of the solutions available today make that process fairly seamless. This way, a business can fully take advantage of moving to the cloud and supporting its remote workers without having every device or every user connect to the office network in order to be secured. Most importantly, it can better detect and thwart attacks at the place they most often begin—the endpoint—before they threaten the business.

KEY POINTS

1 **Businesses today must first secure their endpoints in order to have the greatest chance of fending off attacks.**

2 **Once you have an endpoint-security strategy in place, you can optimize it with automated processes and smart data insights.**

32 Security Experts

Download the full e-book: Security Experts on Changing Endpoint Security

CHAD STORM

Cloud Network Security Engineer at IBM – Global Team Lead,
IBM

Twitter

LinkedIn

As security measures are generally established in layers, compromising each layer generally takes time. Early detection and response often minimizes the damage as it reduces the time an attacker has to infiltrate the next security measure.

EARLY DETECTION IS KEY TO SHUTTING DOWN ATTACKS

SCOTT SAUNDERS

Cyber Security Consultant,
Exelon

Scott Saunders provides cybersecurity consulting for Exelon. He has more than 20 years of information-security experience, previously working for the Sacramento Municipal Utility District and for the federal Medicaid program for the state of California. Saunders is a Certified Information Security Manager (CISM) and a Certified Information Security Systems Professional (CISSP). He holds a BS in Information Technology-Security and an MS in Information Security Assurance, both from Western Governors University.

Twitter | LinkedIn

Download the full e-book: Security Experts on Changing Endpoint Security

For cybersecurity consultant Scott Saunders, early detection is critical for shutting down an attack. “It’s important to be on the lookout for any abnormal behavior before an attack can escalate or expand across the organization,” he says. This is why it’s important to monitor your endpoints so that you can identify unusual behavior. It provides an early warning if, for example, a well-intentioned employee makes a change to your prevention program that generates a risk that you don’t know about, says Saunders. Detection and monitoring help your business verify that your prevention program is working as intended.

After all, if you’re not monitoring, then your business is effectively in the dark as to the threats it faces. “If you’re trusting only in prevention, an attacker could get embedded in your system and stay there for a really long time,” he explains. From there, the attacker could use a compromised endpoint as an entry point to more important assets in your organization. You therefore need to have as much of a heads-up as you can. »

> *“It's important to be on the lookout for any abnormal behavior before an attack can escalate or expand across the organization.”*

EARLY DETECTION IS KEY TO SHUTTING DOWN ATTACKS

Given this state of affairs, Saunders thinks that businesses may be shifting their focus slightly from prevention toward early detection and response. “I don’t want to diminish the need for prevention,” he cautions. “I think we need those tools as a layer of defense because security is all about layered defenses. But I do think that incident response has become much more prevalent today because we’ve seen our defenses get violated.” In light of so many high-profile breaches, businesses understand that prevention is a crucial layer of defense, but it’s not the only one—and so they must have sufficient monitoring in place in the event that an attacker breaches their network.

When setting security priorities at his own organization, Saunders aims for a roughly equal investment in both technology and process. “My approach is to have a little bit of both at the same time,” he says. “I’m going to train and educate my workforce about why I’m adopting certain strategies. That way, as we develop requirements for the tools and evaluate them, my colleagues are better educated, better able to evaluate and adopt those tools, and able to use them as intended.” He finds it most effective to bring people along for the entire process in this way. ❯❯

“If you’re trusting only in prevention, an attacker could get embedded in your system and stay there for a really long time.”

EARLY DETECTION IS KEY TO SHUTTING DOWN ATTACKS

Saunders and his team find artificial intelligence capabilities especially useful for their endpoint security efforts. "A lot of our monitoring tools have correlation searches to go after things like privileged account use, learning about how user accounts are used and authenticated," This functionality can help the business spot anomalous behavior. For example, if typically no one logs in with administrative rights on a specific holiday like Christmas Day, yet all of a sudden the system shows 50 log ons on that day, these monitoring tools can immediately alert an operator that something unusual has happened and should be reviewed.

Ultimately, any business needs to have early detection and monitoring as well as prevention in place in order to secure its digital assets. That being said, Saunders believes that there is an advantage to putting a special emphasis on detection since that can help stop an attack in its tracks and prevent it from causing greater damage. With the benefit of smart tools that monitor endpoints for anomalous behavior and flag unusual events in a timely manner, a business can more effectively and efficiently protect its network. ■

KEY POINTS

1 **Early detection and monitoring are important because they help a business shut down a potential attack before it worsens.**

2 **Monitoring tools that incorporate artificial intelligence features can speed up the process of identifying and flagging unusual behavior.**

BETTER SECURITY THROUGH EARLY DETECTION AND RESPONSE

SCOTT HARRIS

Vice President – Chief Information Security Officer, Lockton Companies

Scott Harris, vice president and chief information security officer (CISO) at Lockton Companies, has more than 30 years of combined IT and information-security experience. He is a Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), and Certified in Risk and Information Systems Control (CRISC). He volunteers as a mentor at CyberPatriot, a national youth cyber education program to inspire high school students toward careers in cybersecurity or other STEM disciplines. Harris holds a bachelor's degree in Information Systems and a master of information systems management (MISM) in Information Security.

Twitter | Website | LinkedIn

Download the full e-book: Security Experts on Changing Endpoint Security

Scott Harris believes that early detection and response are essential for thwarting attacks originating at the endpoint and minimizing damage to the business. “It’s very important. Whether it’s an attack or a phishing email, the earlier you detect and respond, the less of an impact it’s going to have,” he explains. Reducing the mean time it takes your team to detect a potential threat can save your organization considerable costs in the long run. “The average time that someone is in a network undetected is more than 200 days,” Harris says. “That’s a long time to sit there unaccounted for and exfiltrating data.”

When considering the relative priority he would assign detection and response versus prevention, Harris says that 100 percent prevention is simply not achievable at this point. “Everyone has heard, it’s not a matter of if, but when an attack is going to happen,” he says. Businesses absolutely should still bolster their defenses by adopting security frameworks as well as using the basics, such as firewalls, antivirus software, and even secure coding techniques. But when asked if there is a transition underway from the traditional perimeter-based security approach toward a greater focus on the endpoint, he says, “Well, the perimeter is slowly fading. Businesses are moving to cloud-based applications and all this integration, so you really do need to be able to detect.”

> *Whether it's an attack or a phishing email, the earlier you detect and respond the less of an impact it's going to have.*

Facing the daunting task of finding patterns on large data sets, security professionals may be hesitant to add yet another layer of analytics to their existing security systems. With this in mind, Harris recommends factoring in staff training when evaluating an endpoint-security solution. “When we propose a new solution, I always request resources, because the solution is not just going to sit there and operate itself,” he stresses. Harris also advises businesses to let their risk assessment guide the decisions they make about allocating resources, both technical and human, toward an endeavor such as endpoint security. That way, the business can be assured that its security investments are designed to mitigate the greatest risks it faces.

That being said, Harris does feel that businesses can maximize the benefits of their endpoint-security solution by making a concerted and intentional investment in staff training. “That’s where you’re going to get the most ROI on anything. Obviously, we have a security-awareness program. But we’re also trying to change that culture to make it more of a security-centered culture,” he explains. Having previously worked in the utility space, Harris saw how his employer gradually achieved this goal by constantly emphasizing safety as a priority with the employees. “It took years to get to the point where everybody consistently, daily thought about safety,” he says. “If we apply that same type of logic to security, it’s going to be a slow change, but it certainly is a goal to get everybody moved over to a security mindset.”

“Obviously, we have a security-awareness program. But we’re also focused on changing that culture to make it more of a security-centered culture.”

BETTER SECURITY THROUGH EARLY DETECTION AND RESPONSE

In this rapidly changing security environment, businesses that want to secure their systems against a potential attack should prioritize early detection and response, as doing so gives them the best opportunity to halt an exploit before it takes hold, minimizing potential damage. But they should also train their staff so that the organization as a whole ultimately operates with a security-first mindset. With those two measures in place, the company can make the most of its endpoint-security solutions, better protecting itself in the short and long term. ■

KEY POINTS

1 **With the rise in cloud-based applications and third-party integration, early detection and response has become more important.**

2 **To achieve the greatest ROI possible from their endpoint-security investment, businesses should also prioritize staff training and culture change.**

Download the full e-book: Security Experts on Changing Endpoint Security

OMAR TODD

Technical Director (CTO/CIO),
Sea Shepherd Conservation

Twitter

Website

Security and prevention are a very difficult sell. I have found using media reports of hacking that has destroyed companies and their top management in one fell swoop to be quite effective.

BE AGGRESSIVE IN PROTECTING YOUR ENDPOINTS

KEVIN FIELDER

CISO,
Just Eat

Kevin Fielder is an innovative and driven security professional who strives to enable businesses to meet their goals and objectives securely. He recognizes the need to balance technical capabilities with business understanding to achieve and align both security and business goals. He has a proven track record building and delivering security teams and programs across many industry sectors. His experience encompasses startups to multinational companies.

Twitter I Blog | LinkedIn

Download the full e-book: Security Experts on Changing Endpoint Security

"In many ways, especially with working from home, in multiple offices, and working from third-party locations, the endpoint is kind of the perimeter for a lot of offices now," says Kevin Fielder, who as CISO of Just Eat, is tasked with securing a highly mobile workforce in a company that operates in 13 countries. The entire business model is geared toward mobile workers and customers. "We've got 20 million customers and 75,000-plus restaurants or partners that we work with."

This makes for a complex endpoint environment. "We've got people with Apple and Android phones, we've got Mac and Windows, and Linux endpoints floating around in the environment. But we also have third parties that have access to our systems, and they've got a bunch of endpoints that we don't technically manage, but we allow to access our systems," Fielder explains. He also points out the importance to the businesses of balancing endpoint security and usability.

> *In many ways, especially with working from home, multiple offices, and working from third-party locations, the endpoint is kind of the perimeter for a lot of offices now.*

In this kind of disparate environment spread across multiple countries, early detection of unusual endpoint behavior and quick response are an integral part of the security strategy. But this doesn't mean giving up on traditional prevention strategies; a balance is necessary, Fielder says. "You might spend proportionate amounts in each area," he explains. "Maybe you divide it into thirds and spend a third on prevention, and that's everything from anti-malware, host detection, permissions, and whatever else. Then you spend a proportionate amount on detection, whether that's a monitoring tool on the local host, or whether it's cloud monitoring so you don't have to have hugely super advanced stuff on the endpoint. You need to have something in place that detects misbehavior as early as possible, and that can also be looking at the behavior of other systems."

The final third can be spent on response strategies, because if you're not in a position to respond quickly, early detection does you no good. When you detect something unusual in an endpoint, how quickly do you isolate the machine? Are you prepared to do the necessary investigation to determine exactly what you've found? "This is why I've got the correct tooling in place. As soon as I think something's up, bang—it's off the network, that person has access to nothing. We try to lock them out as quickly as possible, and then we contact them another way," says Fielder. "You can be aggressive with your response to endpoint incidents, because you're only affecting one user at that point. It's unlikely that one person losing use of their machine for a short time is going to bring down the whole business." »

> **"This is why I've got the correct tooling in place. As soon as I think something's up, bang—it's off the network, that person has access to nothing."**

Making all this work means investing in tools and people. “Obviously you can’t protect the endpoints without technical solutions, especially on anything more than very few machines,” says Fielder. “I think tooling and automation are critical, especially for lean companies. The more you can automate and the more you can get people to do things for you, the better. But to back that up, you need the right people with the right understanding.”

For Fielder, protecting the endpoints is essential. “People take work home, or they log into a dodgy wireless point, or whatever else, because they’re trying to do the right thing, which is get their work done. Sometimes in trying to do the right thing, they do the wrong thing. Whether it’s malicious or accidental, there are a lot of ways for things to come in via the endpoint environment.”

KEY POINTS

1 **You need to have something in place that detects misbehavior as early as possible, and that can also be looking at the behavior of other systems.**

2 **You can be aggressive with your endpoint response. It’s unlikely one person losing use of their machine for a short time is going to bring down the whole business.**

32 Security Experts

Download the full e-book: Security Experts on Changing Endpoint Security

AARON LENNON

Security Architect,
Critical Start

LinkedIn

In my opinion a good mix of prevention and detection is optimal. There is no silver bullet so you are never going to prevent everything, but you can minimize the attack surface and prevent a lot of commodity threats through prevention. This reduces the time spent dealing with such threats so you can focus time and energy on detecting advanced attacks as well as proactive threat hunting.