

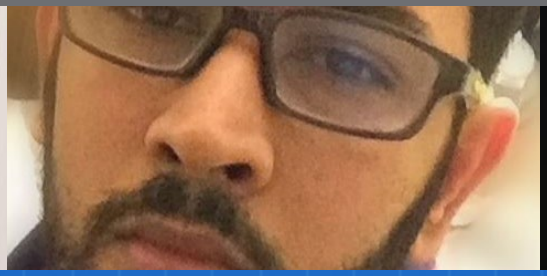


Mighty Guides

4 Security Experts

on Changing Endpoint Security

Justifying the Value of Endpoint Security

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 4 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. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I 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 4 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.

JUSTIFYING THE VALUE OF ENDPOINT SECURITY

CATHARINA "DD" BUDIHARTO

Director, Information Security, CB&I

During her 20-plus years in the security field, Catharina "Dd" Budiharto has upgraded information security practices to next-generation programs and developed information security systems from the ground up. She is a co-chair, speaker, and moderator for Evanta CISO Executive, CIO magazine, and various IT security conferences. She is a former chair of the American Petroleum Institute IT Security committee, and actively participates in the information-security community's intelligence-sharing network.

LinkedIn

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

"In talking about securing endpoints, you must recognize that threat vectors come from many different angles," says Catharina Budiharto, IT security director at CB&I, a global logistics company. "My general rule is that prevention is the first line of defense, whether at the network layer, at the perimeter, or at the endpoint. Prevention is better than having to do the detection and response later."

Having said that, Budiharto recognizes there are many reasons why prevention alone is not enough. There may be budget or organizational challenges that limit a preventive strategy, and just as in cases where precautionary measures do not always stop the spread of disease, a security practice must also have the means to detect and respond to cyber incidents that get past its defenses. "Then you must have people trained to respond to incidents, and you need tools to monitor and detect. Those capabilities can be used to strengthen prevention. Implementing these things varies depending on different states of maturity of a company," she says.

> *We now have a metric that proves my team spends less time chasing those incidents. It's become such a low-maintenance thing that now we can focus on maturing the other areas.*

Finding the right balance in any organization depends on assessing risk and then convincing executive management to fund what's needed. Budiharto has been in situations ranging from organizations where she had to transform a security practice that paid scant attention to endpoints, to a new organization where she had an almost unlimited budget to build the practice from the ground up. More recently she has faced the necessity of adjusting a security practice to operate with a significant budget reduction. Regardless of the circumstances, you need to justify the security expense and use the resources at your disposal to deliver the best level of cyber risk-management possible.

Budiharto says in some organizations it is difficult to make the case in terms that management understands. Real examples are useful to a point, but after a while it's not so effective. "You can use examples like ransomware that encrypts all the data in a health-care business, and how they lost their data and it disrupted their business, etc. But you can only use that scenario so much," she says.

Budiharto believes a better approach is to use actual metrics that show the effectiveness of something that's been deployed. "I implemented a next-generation tool, and we've not had any ransomware or outbreak of malware. We now have a metric that proves my team spends less time chasing those incidents. It's become such a low-maintenance thing that now we can focus on maturing the other areas."

"By presenting it in terms of service level you can deliver, when funds become available, you have already shown how you can build up the practice to meet the cyber risks you face."

Facing a budget reduction, which can come as an across-the-board fiscal-management policy, can be trickier. "In that case we need to reset expectations," Budiharto says. "I tell them our service-level agreement, for example, our response time is not going to be immediate as before. There are certain services we won't have the resources for. It might change our level of risk." Management can accept these trade-offs, or not, in which case they must find the resources to support the level of security they need. Budiharto points out the positive side of this situation. "By presenting it in in terms of service level you can deliver, when more funds become available, you have already shown how you can build the practice up to meet the cyber risks you face," she says. ■

KEY POINTS

1. **Finding the right balance in any organization depends on assessing risk and then convincing executive management to fund what's needed.**
2. **To sell the need for a security solution, use actual metrics that show the effectiveness of something that's been deployed.**

HARSHIL PARIKH

Director of Security,
Medallia, Inc

Harshil Parikh is versatile security professional with experience in building enterprise-wide security function at global organizations. Currently, Parikh leads the Trust and Assurance Group at Medallia, Inc. His responsibilities include strategy, execution, and operations of various security functions including application security, infrastructure security, security operations, and response. Parikh spent a number of years leading and advising security teams at large organizations in high-tech, finance, and insurance verticals.

LinkedIn

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

As Harshil Parikh knows, it can be challenging to secure adequate resources for an endpoint-security solution. When making the case, he says, it's important to demonstrate the risk that the business faces in terms that the CIO or CFO can understand so they can make a fully informed decision. "Demonstrating an actual exploit that shows that your company's laptops are really vulnerable, and what could actually happen as a result," is a good way to achieve this, he says.

Parikh and his colleagues typically perform such demonstrations for executive leadership using a team exercise in which an extremely skilled penetration tester compromises a laptop and extracts company data in front of a CIO or CFO. "It brings the reality to them that, 'Hey, my data is really exposed, this can happen any day,'" he explains. Sharing a few real-life examples of how such vulnerabilities have actually led to incidents—whether in a high-profile case such as the Target breach or another company whose security has been jeopardized through laptop incidents—also tends to bring home the seriousness of the threat as well as its potential consequences.

Parikh's firm, Medallia, where he is the director of security and compliance, is a software-as-a-service company catering to Fortune 500 organizations. Considering that his organization operates in a DevOps model, a developer or an engineer could potentially have access to critical parts of the company infrastructure, which is an industry-specific concern he and his colleagues must factor in when advocating for resources devoted to endpoint security.

> *"A lot of the work that starts on one of our developers' laptops impacts our platform because we operate in a DevOps lifecycle."*

MAKING THE CASE FOR AN ENDPOINT SECURITY SOLUTION

Medallia works with enterprises that have incredibly strong restrictions surrounding the handling and management of their data. "Our customers are very sensitive to requirements, all the way from how we secure software to how we manage our endpoints," Parikh says. "So just for us to be able to be in business, we need to implement a lot of the controls that our customers require—especially those in the financial and telecommunications sectors." Accordingly, he often directly ties a specific endpoint-security request to a contractual requirement, which provides a solid justification to decision-makers at the company.

When making the case for an endpoint-security solution, it's important to remember that collaboration between the security team and IT is essential for ensuring successful implementation. "Typically, most security teams are not responsible when endpoint-security software runs amok and ends up impacting the performance of the laptop significantly," Parikh notes. "So the IT teams are usually on the hook for making sure that endpoint-security software is doing its job within proper bounds and controls, and that it's not affecting the user experience." For this reason, he recommends closely aligning any proposal for an endpoint-security solution with IT's expectations so that the deployment and operationalization is as effective for the company as possible.

"Our customers are very sensitive to requirements, all the way from how we secure software to how we manage our endpoints."

KEY POINTS

1. **A real-world demonstration can be helpful in making the case for why an endpoint-security solution is necessary from a risk-management perspective.**
2. **Highlighting risk factors that are specific to the business is another effective way of making the argument for an endpoint-security solution.**

AHMER BHATTY

Field Solutions Engineer - Networking and Security, SHI International Corp.

LinkedIn

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

I can't begin to stress how important early detection and response is when it comes to mitigating threats and minimizing damage. Being proactive to prevent damage in the first place is always better than fixing it after the damage has already taken place. By implementing early detection and response (EDR) solutions in a corporate environment, companies can proactively detect a threat and take the appropriate actions needed to resolve it. Pair the EDR solution with endpoint protection platform (EPP) solutions, and you have got yourself a very robust endpoint security!

TO SECURE SECURITY FUNDING, GET QUANTITATIVE

MIKE SANTOS

Director of Security & Information Governance, Cooley LLP

Mike Santos is the director of security and information governance at Cooley LLP. He works with firm leadership and information services to establish and maintain policies, frameworks, systems, and controls to govern and secure Cooley's information assets. Santos has over 20 years of experience in leadership, team building, information technology operations, risk and security governance, and management. At Cooley, Santos built and is responsible for maintaining an ISO 27001:2013-certified information security management system.

Website | LinkedIn

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

Mike Santos, director of security and information governance at Cooley LLP, believes that when making the case for an investment in endpoint security, it's best to share actionable information with leadership about the state of your company's security and its readiness relative to industry standards rather than using a fear-based argument to secure funding. "It's especially helpful to present security information in the form of metrics and useful data points—after all, when having a conversation with business leaders, numbers provide an effective common language" says Santos.

Security professionals can and should continue to communicate the value of endpoint security with decision-makers even after the security budget has been approved. "You've got to show your colleagues that once you put these tools in, they're really working. That's what sells things," says Santos. Reviewing statistics like how many links are clicked every month provides a useful starting point for a conversation about how best to halt and reverse that trend: is it a question of process, does the security team have to increase employee awareness, or should they tweak the tool? By engaging in such dialogue, the business can decide what goals to set and how best to go about achieving them. This is far more effective than simply referring to a study or a recent news article about attacks originating from a nation-state such as China, which may or may not be relevant to your own business and the unique threat environment it faces.

> *"It's especially helpful to present security information in the form of metrics and useful data points—after all, when having a conversation with business leaders, numbers provide an effective common language."*

TO SECURE SECURITY FUNDING, GET QUANTITATIVE

During annual security awareness training, Santos showed his colleagues exactly the types of threats their business encountered in an information sheet called A Day In The Life at Cooley, which presented a wide range of daily security metrics broken down on a daily basis. "I asked, 'Do you know how much malware we stop a day? Do you know how many malicious links get blocked? And do you know how much legitimate email we receive in one day?'" he says. Upon seeing the big-picture view of the company's security environment at the firm for the first time, his colleagues were incredibly surprised. They had no idea of the complexity and vastness of the threats already being faced and prevented every day.

Using quantitative analysis and gap analysis, Santos and his team are able to provide recommendations on how to improve certain metrics, allowing leadership to make more informed decisions. He thinks this approach could be beneficial for other organizations. "I think it would be great if the industry did that as a whole by performing gap analyses against standards like NIST, ISO, and PCI. The business should be able to ask, 'How do I stand up against these standards and where are my gaps? That's what the business likes to talk about,'" Santos explains.

"You've got to show your colleagues that once you put these tools in, they're really working. That's what sells things."

TO SECURE SECURITY FUNDING, GET QUANTITATIVE

This is how security professionals can engage the business in a higher-level strategic conversation about how best to manage risk. Rather than using fear-based arguments or describing security threats in confusing qualitative terms such as "Very high" or "High," which business leaders understandably may not know how to interpret, it's more effective to provide quantitative data and actionable recommendations for improving metrics that the business deems important. In doing so, the security team can make a more persuasive case for funding by ensuring decision-makers fully understand both the nature of the risks and how to address them.

KEY POINTS

1 **When making the case for security funding, it's often effective to share quantitative information about specific risks that the business faces.**

2 **Business conversations about how best to manage security risks should be ongoing, continuing after the tools have been implemented.**