Mighty Guides

8 Security Experts

on Changing Endpoint Security

Rethinking Your Network Strategy

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.

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.

RETHINKING YOUR NETWORK STRATEGY

A GOOD ENDPOINT SECURITY STRATEGY FOCUSES ON DATA USAGE

ELLIOTT BREUKELMAN

Senior Information Security Engineer,
Land O'Lakes, Inc.

Elliott Breukelman is an information security engineer with several years of experience in the field under various organizations. Currently, he is responsible for engineering endpoint security at Land O'Lakes, Inc. in Arden Hills, MN. With 10,000 employees across 50 states and more than 50 countries, the company has a unique security footprint in an ever-changing technology landscape. Breukelman holds a BA and MA in Information Systems with specializations in infrastructure analysis, change management, and networking.

Website | LinkedIn

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

Although Land O'Lakes, Inc. already had an endpoint-security strategy in place when Elliott Breukelman joined the company as a senior information security engineer, one of his roles has been to help mature that strategy. Land O'Lakes operates a farm-to-fork business model, which means it manages a complex supply chain that includes farmers, feed suppliers, processors and distributors, transport logistics, and retailers. Its IT infrastructure plays a key role in tying these pieces together, and securing that infrastructure is critical to sustaining business operations.

"We have a cloud-first strategy," says Breukelman. "As more of our IT resources shift to the cloud, and more workers become mobile, the importance of endpoint security increases." He points out that endpoint security is one of the hottest topics in today's security discussions, largely because security challenges are rapidly evolving even if the basics of network technology, such as routers and switches and the way networks work, have not changed as much. With many business activities moving into the cloud and onto mobile devices, that's where you find the new security challenges.

Deciding when it's time to focus more resources on securing endpoints varies from one business to another, and it depends on what kind of data the business handles and where that data is located. "We are not a highly regulated industry like banking or healthcare, so we don't have those kinds of compliance requirements," Breukelman notes. With business operations in all 50 states and overseas too, Land O'Lakes employees are highly mobile. "Everybody has a laptop they can take home or use to work wherever they need to," he adds.

> *"As more of our IT resources shift to the cloud, and more workers become mobile, the importance of endpoint security increases."*

A GOOD ENDPOINT SECURITY STRATEGY FOCUSES ON DATA USAGE

According to Breukelman, designing an endpoint-security strategy involves assessing risk associated with the value of your business data and where it is located, and balancing that against the amount of mobile access to that data. You also need to look at past incident data. "We monitor how data flows,the number of attacks mitigated every month, and how many require manual intervention," he says. These metrics not only provide insights into the need for stronger endpoint security, they also tell you if your endpoint strategy is working. "If we can see we got hit by a form of ransomware and our endpoint solution successfully mitigated that attack without us having to do anything, that's a good sign," he says.

Deciding when it's time to focus more resources on securing endpoints varies from one business to another, and it depends on what kind of data the business handles and where that data is located. "We are not a highly regulated industry like banking or healthcare, so we don't have those kinds of compliance requirements," Breukelman notes. With business operations in all 50 states and overseas too, Land O'Lakes employees are highly mobile. "Everybody has a laptop they can take home or use to work wherever they need to," he adds.

"The prevention piece is still very important, but now we're adding a layer that allows you to correct an issue once it's there."

KEY POINTS

1. **Deciding on endpoint security involves assessing risk based on the value of your business data, where it is located, and the amount of mobile access to that data.**
2. **Endpoint security adds a new layer of protection that does not require a wholesale change in an existing security practice.**

CLINT MENZIES

Senior Cyber Threat Engineer, Cyber Threat Detection & Response, Trustwave Managed Security Services

LinkedIn

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

Early detection and response is as important as having locks on your doors and windows. It is always easier to catch a crook in the act rather than after the fact.

ALINA SARVEY

Endpoint Security Engineer, Managed Security Services Provider

Alina Sarvey is a highly effective and enthusiastic professional, able to tackle issues head on without delay. She has acquired a rich background involving cybersecurity technologies for endpoint protection. Sarvey is a conscientious planner, which enables her to facilitate and support her team's efforts smoothly. She holds multiple certifications from (ISC)2, CompTIA, and Committee on National Security Systems (CNSS), in addition to master's degrees in Cybersecurity and in Business and Management.

LinkedIn

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

According to Alina Sarvey, a range of indicators might point a security organization to the need for increased endpoint security. How a business responds to them will depend on the company's unique profile, business requirements, and even business culture. "I strongly believe in the human factor, and I think that personal preferences from the management or the owners can play a role at times. Some owners are more interested in being top notch in security and sleep better at night knowing that their business is well protected, whereas others don't really perceive a huge benefit," she says.

With this in mind, as an endpoint security engineer, Sarvey has found it helpful to provide her clients with reports that illustrate the need for increased endpoint security. "The majority of the tools I work with provide data that I can use for reporting. My usual approach is to define a baseline security posture for the system. I can create reports based on that baseline for pretty much any point of time on a daily basis, hourly, weekly, by location or by type of system," she says. If the reports indicate that the business is experiencing greater threats than its security posture can tolerate, Sarvey may issue specific recommendations for enhancing endpoint security to defend the business against the threats it faces.

If a business is charged with meeting certain compliance requirements, of course, the task of reporting on security threats can be very straightforward. "I introduce this monitoring on a daily basis with quite a few of my customers. The monitoring allows me to track the data and pinpoint when we dropped out of compliance versus when we were in compliance," she explains. However, as a managed-services provider, Sarvey is a step removed from the inner workings of the business and so she must rely on her clients to provide her with the appropriate level of access and information in order to generate accurate reports. "The quality of the information depends on the quality of collaboration and the comprehensiveness of the information provided," she notes.

> *"My usual approach is to define a baseline security posture for the system."*

DATA SHOWS THE NEED FOR BETTER ENDPOINT SECURITY

At the end of the day, such collaboration depends on whether the business and its leaders consider security a priority. Endpoint security can shed light where this is concerned as well, pointing to the need for better C-level compliance training to ward off phishing attacks and other exploits that may gain access via devices such as USB drives. In such cases, it's important for CISOs to engage effectively with their C-level counterparts. "The CISO must encourage C-level management to be more vigilant and savvy," Sarvey explains, which is important "because C-level executives are not usually subject to compliance training."

So, as Sarvey suggests, there are a variety of indicators that may show security professionals that increased endpoint security is necessary for their organization. Very often, they take the form of metrics and other security statistics that correspond to the company's baseline security posture, allowing the CISO and the business to understand where their vulnerabilities lie and how they must be rectified. Once implemented, endpoint-security solutions can then provide the business with even deeper insight on how it can optimize its policies and practices in order to prevent attacks more effectively.

"The monitoring allows me to track the data and pinpoint when we dropped out of compliance versus when we were in compliance."

KEY POINTS

1. **How a business views security's importance can often play a role in the decisions made about improving endpoint security.**
2. **Baseline security reports can help security professionals and the business decide whether there is a need for increased endpoint security.**

PAUL HEFFERNAN

CISO,
Unipart Group

Paul Heffernan is the group CISO for Unipart Group. With experience in the cybersecurity world, consulting to some of the world's biggest brands, he engages with the business at board level to enable trusted secure commerce. Heffernan is a regular international speaker at conferences such as the e-Crime Congress, GBI CISO Summit, and CISO360 Barcelona. He is proud to have been recognized at the Cyber Security Awards in London as "Highly Commended" CISO of the Year 2017.

Twitter I LinkedIn

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

According to Paul Heffernan, when trying to determine whether there is a need for increased focus on endpoint security, a security organization should first make sure it has a solid understanding of its environment . "Do you have a good handle on how your users use data inside the organization?" he asks. "Are you predominantly field based? Are you using company-provided devices? Are they all in one location?" The answers to all of these questions will determine what kind of endpoint-security solution is needed for the company. They will also influence how the endpoints must be protected.

After that step is complete, Heffernan, who is CISO at Unipart Group, recommends threat modeling. "When you know where your systems are and how they are being used, what typical attack vectors could be used in those contexts to gain access to the data or the systems?" he asks. For example, a field-based employer with traveling employees might face the risk of lost or stolen devices. "So it may be in that case I need to focus on device encryption because I know there is a probability the device could be lost or stolen. If I'm operating on a fixed terminal instead, I may need to look at what I'm going to do to make sure the device can't be tampered with," he says. After that, the security team can conduct some threat actor simulations in which it hypothesizes how attackers would gain access to the company's endpoints based on the context that it has just defined.

> *"There are certainly metrics that one can use to detect whether the endpoint is the root cause or is involved in some way."*

Metrics may also shed light on whether the business requires increased endpoint security. "There are certainly metrics that one can use to detect whether the endpoint is the root cause or is involved in some way," Heffernan says. "Clearly, we can look at useful lag indicators, like the number of antivirus alerts, or the number of bad websites visited. But we should also pay attention to potential lead indicators like executables that were run on those workstations. Were they company sanctioned applications? Were they gray or shadow IT applications or were they illegal or immoral or against our policy?" he questions.

Some organizations may not yet have the technical capabilities to identify an emerging threat. "We're trying to understand this activity that we saw when correlated with this other activity and when correlated with this context, whether that's time, location, user, or some other piece of metadata. Does that indicate the beginning signs of an attack, of starting reconnaissance or having run an exploit?" Heffernan explains. Answering these questions requires a certain level of technical knowledge, so it's worth looking for tools that automate or take away some of that pain. "Some tools can triage correlation and analytics so that you don't need to rely so much on human capacity to do that," he adds.

"Some tools can triage correlation and analytics so that you don't need to rely so much on human capacity to do that."

UNDERSTANDING YOUR COMPANY'S ENDPOINT SECURITY REQUIREMENTS

Businesses can determine whether they need increased endpoint security by fully ascertaining their environment's unique characteristics, performing threat models and threat actor simulations, and analyzing relevant metrics. If the security team is encountering challenges identifying endpoint threats, that might be another sign that endpoint security tools could be of benefit. After considering these factors, the company can make an informed decision on whether to enhance its existing endpoint-security strategy.

KEY POINTS

1 **To determine your endpoint-security requirements, you must first understand your environment's unique characteristics.**

2 **Threat modeling, threat actor simulations, and metrics may also indicate whether there is a need for increased endpoint security.**

CARY DAHL

SHI,
Principal Architect – Cloud & Security Solutions

Twitter

LinkedIn

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

Evaluate the current state of the endpoint-security posture: What are the gaps and where can it be improved? Does it make sense to look at augmenting the current signature-based antivirus software with a next-generation endpoint detection and response product, which can leverage machine learning and artificial intelligence to get zero-day malware? Weigh the pros and cons of doing a full replacement or augmentation—leveraging next-generation technologies should be one of the organization's highest priorities.

KALIN KINGSLAND

Sr. Security Architect, Global Financial Services Organization

Kalin Kingsland, CISM, has over 10 years of security experience, primarily in the financial sector. His background spans firewalls, load balancers, endpoint security, cloud security, incident response, and infrastructure architecture. He has expertise in PCI and HIPAA, where he is primarily focused on risk mitigation. Kingsland currently provides guidance and strategic vision for a global financial-services organization and works with executive leadership to increase the posture and response of the organization.

LinkedIn

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

Kalin Kingsland, information security leader at a global financial services organization, believes the best indicator there is a need for stronger endpoint security is in the data coming out of the security operations center. "If you're starting to see a lot more noise, either false flags or even true flags pointing toward endpoints, that's when you should start looking. Look for a movement toward the endpoints. You have to listen to your metrics and analytics about what you're seeing in your organization," Kingsland says. This is exactly what is happening now in his organization. "We're actually seeing a lot of our issues coming from endpoints, with credentials that have been compromised. So we're getting more focused on mobile devices and laptops, shifting more towards behavior mapping, securing the human, if you will."

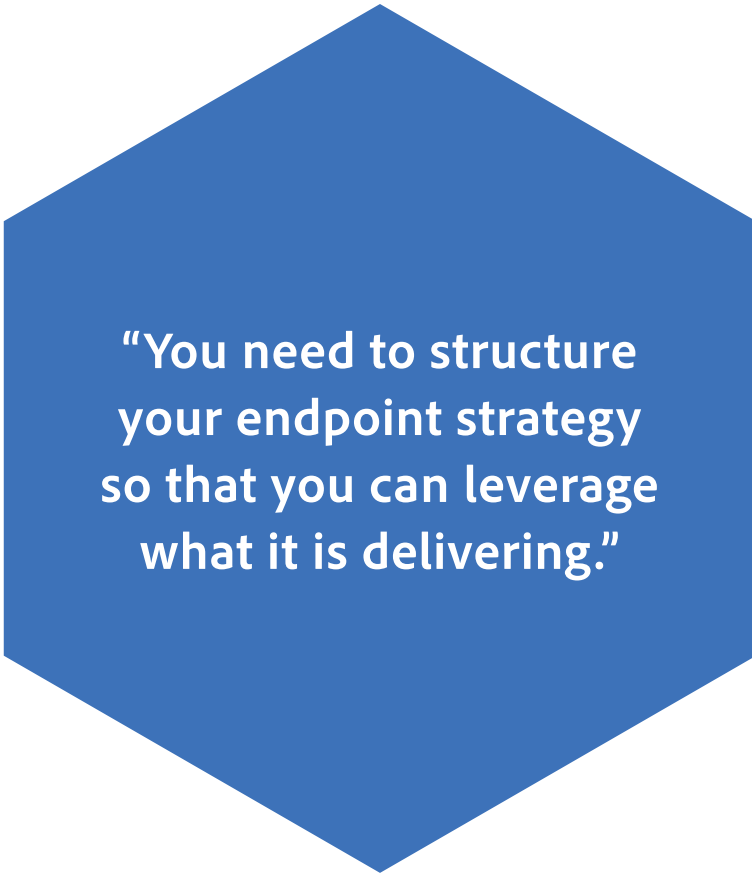
Applying more protection at the endpoints requires considering a few key factors, including how the endpoint-security tools impact system performance. "Everything is an agent now," Kingsland explains. "You can quickly go from having just one AV agent to having 15 different agents that are all trying to do something, and this bogs down endpoint processors and increases disk utilization. I watch out for the user environment. If you make it so the environment is becoming a hassle, people will try to circumvent it, which defeats the purpose of having the tools."

I watch out for the user environment. If you make it so the environment is becoming a hassle, people will try to circumvent it, which defeats the purpose of having the tools.

BE ABLE TO UTILIZE THE DATA GENERATED BY ENDPOINT SECURITY TOOLS

Another important consideration is that more advanced security tools at the endpoint generate more data, which must be analyzed if the tools are going to be effective. "In my view, you can never have too much data coming in from a system. But the backend may not be happy with all that data," Kingsland says. The big risk is generating so much data that your back-end process cost goes way up, which impacts the budget for everything else. And if you're not utilizing the data, you are spending money that is not giving you anything in return. "You need to structure your endpoint strategy so that you can leverage what it is delivering," he comments. "For instance, you may not need to have the same tool set running on every endpoint." Whatever data you are capturing, it is important to have the means to process it and leverage it into meaningful risk mitigation.

Striking the right balance between functionality, total operational cost, and actual risk mitigation can provide value to other parts of the business that goes beyond strengthening the security posture. For example, strong endpoint security provides greater freedom and flexibility for the workforce. "Many companies limit remote working capabilities because they can't control what's going on outside their internal network," says Kingsland. "The stronger the endpoint gets, the more comfortable the organization can be in its remote operations. This gives workers a more satisfying work environment, and it enables the business to be more flexible in the way it operates." It's important to factor these kinds of benefits into the return you expect from an investment in stronger endpoint.



BE ABLE TO UTILIZE THE DATA GENERATED BY ENDPOINT SECURITY

It's also important to assess whether the endpoint strategy is working for you. Once again, Kingsland says to listen to the data, but also listen to the people. "If everything is quiet, you're probably doing OK," he says. "You know you have issues if your SOC is quiet, but your users are grumbling. Then you're impacting the user base. And if the user base is quiet but the SOC is lighting up, you're not protecting the endpoint well enough." The goal is to find that balance where everything is calm and the analysts are quickly identifying and blocking threats.

KEY POINTS

1. **Whatever data you are capturing, it is important to have the means to process it and leverage it into meaningful risk mitigation.**

2. **Striking the right balance between functionality, operational cost, and risk mitigation provides value to other parts of the business, which goes beyond strengthening the security posture.**

CRAIG WILLIAMS

Security Design Architect, AOS

LinkedIn

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

When it comes to security, a layered approach is the best way to protect. Endpoints are just one part that is imperative to protect as one of the threat vectors. As the threats become more prominent we need to become more vigilant in our protection efforts.

ENDPOINT SECURITY DECISIONS REQUIRE A STRATEGIC APPROACH

BRENT MAHER

CISO,
Johnson Financial Group

Brent Maher was appointed senior vice president – chief information security officer in 2015. In this role, he is responsible for reducing enterprise risk of threats against the confidentiality, integrity, and availability of Johnson Financial Group's information assets. This includes program management, risk management, awareness and training, architecture, engineering, and security operations.

LinkedIn

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

In Brent Maher's experience, there are two key indicators that may tell you there's a real need for an increased focus on endpoint security in your organization. "If you're fielding a volume of security incidents on your endpoints that are beyond what you would expect in terms of your user population, you know it's time to have a look at your endpoint controls," he says. That's something reactive companies would typically do. But mature organizations that are proactively managing their endpoint security also allow their security frameworks to inform their decision-making on a more strategic level.

This is how Maher and his colleagues approach decisions at Johnson Financial Group. Referring to their security framework, they review their total environment and make sure they are not over-investing in one area at the expense of another. "The NIST framework helps dive through that discipline, and you really get to think through the identify, protect, detect, respond, and recover elements. That covers the life cycle of a threat, and that helps you prioritize," he says. A maturity model also helps the organization identify where it is currently weak and what areas urgently need resources, allowing the security team to address vulnerabilities in a holistic way.

> *"With a strategic approach, you could solve an important problem that you really have, not just a threat you have identified in your program."*

Maher feels that this approach is valuable for all aspects of security strategy, including but not limited to endpoint security. Rather than being driven by momentary fears or industry buzz about specific tools, companies should base their decisions on a framework or maturity scale to make sure that the step they're taking really is the right one. "With a strategic approach, you could solve an important problem that you really have, not just a threat you have identified in your program. I think that takes discipline," he says.

It's also important to assess whether or not you've fully maximized the value of the tools that you already have before investing in a new solution. "If you have some controls that you haven't realized meaningful value out of, you have to be honest with yourself and make sure that you're not just buying the next flashy tool, and that you're really leveraging what you have now. Or you come to a disciplined realization that it's a dead end for whatever reason," he explains. Security organizations should also be certain that the solution they are considering solves the problem that they face. "Before you buy it, to the extent possible, can you actually demonstrate that the product can solve the problem in your specific environment?" Maher asks.

"Before you buy it, to the extent possible, can you actually demonstrate that the product can solve the problem in your specific environment?"

Finally, Maher advises that organizations carefully consider the human element of the endpoint-security investment they're contemplating. This includes factoring in their capability, whether via staff or managed services, to the tool, operationalize it, and extract maximum value from it. By making sure this critical factor is accounted for, businesses can be sure not only that they have made the right decision and secured the right product but that they can make the most of it, thereby achieving their security goals and defending the firm from the threats it faces.

KEY POINTS

1. **Mature security organizations refer to a security framework or maturity model when deciding whether to adjust their endpoint-security strategy.**
2. **It's important to be certain that the endpoint-security solution you purchase can actually solve the problems you have identified for your specific environment.**