Mighty Guides

32 Security Experts

on Changing Endpoint Security

CISOs and Information Security Experts Share Their Stories Around Changing the Endpoint Security Mindset

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 32 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 32 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 is the leading provider of next-generation endpoint security. Customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including advanced ransomware and non-malware attacks. Our pioneering approach to application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) has been rigorously tested and proven. Carbon Black has more than 3,000 customers with more than 14 million endpoints under management, including 30 of the Fortune 100. With an eye on empowering every security team and protecting every endpoint, we stand true to our founding vision: **To create a world safe from cyberattacks.**

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

KEYS TO SHUTTING DOWN ATTACKS

In this Section...

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

"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.**

TO PREVENT ATTACKS, START WITH THE ENDPOINTS

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

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."*

TO PREVENT ATTACKS, START WITH THE ENDPOINTS

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.**

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

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.**

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

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.**

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 | Blog | LinkedIn

"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."

BE AGGRESSIVE IN PROTECTING YOUR ENDPOINTS

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.**

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.

RETHINKING YOUR NETWORK STRATEGY

In this Section...

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

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

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

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

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

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.

BE ABLE TO UTILIZE THE DATA GENERATED BY ENDPOINT SECURITY TOOLS

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

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

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

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.**

JUSTIFYING THE VALUE OF ENDPOINT SECURITY

In this Section...

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

"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

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."*

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

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

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.**

MOVING TO A CLOUD-BASED, NEXT-GENERATION PLATFORM FOR ENDPOINT SECURITY

In this Section...

CHRIS THOMPSON

Global Director, IT Security and Controls, Bentley Systems

Chris Thompson is a global director of information security who works with commercial organizations to establish risk-based information-security programs. Thompson understands the challenges of designing and maintaining a cost-effective program that can adapt to the rapidly evolving threat landscape. He has implemented strategies for multinational firms designed to meet the business requirements of securing information, while ensuring compliance with regulatory obligations. He is a CISSP, CISM, and GLEG with an MS in Security Management.

LinkedIn

After deciding to strengthen your endpoint security, there are things to consider that go beyond just the technology itself, says Chris Thompson, global director of IT security and controls at Bentley Systems. If you are looking at a cloud-based solution, you need to have a service-level agreement. You also need to consider the privacy implications of collecting more data at your endpoints, and, of course, you will have to make a business case that supports this added layer of security.

All of these points relate to the original reasons for enhancing endpoint security. "It comes back to what's causing your incidents," Thompson says. "If you see that your other controls are performing as expected, but you're still finding uncomfortably high incident rates at the endpoints, that's a clear indicator your endpoints need more protection."

Before adopting a solution, you'll need to evaluate providers. Thompson believes a cloud-based solution is a natural fit for mobile endpoints such as laptops or notebook PCs. "The endpoint is where all the action is, so having visibility into endpoint activity is important. I like the idea of cloud-based endpoint security. You've got to get those logs off the endpoint in near real time so you don't lose visibility to hackers cleaning up after themselves. I also like that I have visibility into and can effectively quarantine systems that may be outside of the corporate network for extended periods of time," he says.

> *"I like cloud-based endpoint security. You've got to get those logs off the endpoint in near real time so you don't lose visibility to hackers cleaning up after themselves."*

It's also important to make vendors prove themselves. "My approach is to get a good deal on basic endpoint protection, and then layer that with a leading-edge endpoint detection and response [EDR] product," Thompson says. "I'll look to see if it really gives me the visibility and advanced detection and response and quarantine capability that the traditional products don't have." He also says that you need to test products to make sure they play well together. "Test them on machines with varying configurations, and if you get good results and a better, more resilient endpoint, you're in a good place."

But Thompson also points out that there's lots to think about besides the technology. "There will be a lot of conversation around support and technical considerations," he explains. "But you have to look at business issues too." For instance, endpoint monitoring may add a new dimension to privacy and compliance, especially if you're a global company operating in different regulatory environments. Another key consideration is how you work with a service provider to create an incident-response program that meets your needs, and how you maintain visibility into what the service provider does with the information they collect.

"There will be a lot of conversation around support and technical considerations, but you have to look at business issues too."

You may even spend more time on working on these process-management issues than actually assessing technical issues such as management consoles, performance, agent footprints, and other tactical considerations, says Thompson. "My advice would be not to look just at technical questions, but also to spend a good amount of time working on things like compliance and incident response."

At the end of the day, you have to sell the idea of endpoint security within the organization and to executives who control budget and resource allocations. "This is where it comes back to understanding your incidents and being able to show the risk," Thompson stresses. " I like to position it that we're not just changing products, but we're enhancing our capabilities, and yes, we are adding cost, but we also add insight and response capability to the traditional endpoint protection tools that are insufficient by themselves." On the business operations side, one of the greatest concerns is performance. "If a human can detect a degradation in performance, it's probably not going to work. If you can add technology without adversely impacting system performance, and the business case makes sense, you'll get a ton of support," he says.

KEY POINTS

1 **It's important that vendors prove themselves, to show their solution delivers the visibility and advanced detection and response you need, and it plays well on your endpoints.**

2 **Do not look just at technical questions, but also spend time working on things like compliance related to increased endpoint monitoring, and the vendor service-level agreement.**

RANDY MARCHANY

Chief Information Security Officer,
Virginia Tech

Twitter

Website

Blog

LinkedIn

Never waste a breach. Use the cost of recovering from a previous breach to emphasize the ROI of doing things ahead of time.

MAKE SURE THE SOLUTION FITS THE ENVIRONMENT AND THE NEED

RICHARD DAVIS

Executive Director of IT Security, Embry-Riddle Aeronautical University

Richard Davis has more than 22 years of IT experience, including more than 10 specifically in information security. He has a BS in Cybersecurity from the University of Maryland University College, and holds 22 industry certifications, including CISSP, CCNP Security, CCNP Routing and Switching, GCFA, GCFE, and GPEN. Davis also creates YouTube videos on a variety of security topics, including digital forensics and incident response; writes software for macOS and iOS; and is very involved in the information-security community.

Twitter | Website | LinkedIn

For Richard Davis, executive director of IT security at Embry-Riddle Aeronautical University, endpoint security is a critically important piece of the institution's overall security strategy. Embry-Riddle has global and online campuses. "Any time you're dealing with an organization that has global reach and endpoints connected all over the place, you have a large attack surface that presents a special security challenge," he says. Educational environments are particularly challenging because of the culture of idea sharing and the free flow of information.

Davis believes that when modifying any security practice, whether it's changing the emphasis on something or adopting new or stronger endpoint-security tools, it's important to maintain a holistic perspective. "You don't put all of your eggs in one basket or in one particular defense mechanism," he says. "Make sure you've got all the bases covered and you maintain a defense in-depth strategy."

Sometimes this involves convincing management that there needs to be greater focus on strengthening endpoint security. Davis believes one of the best ways to do this is with a simple demonstration. "Honestly, it is extremely trivial in many cases to bypass antivirus," he says. "You can demonstrate to management a piece of malware. 'Oh, look the AV caught it. Let me modify this.' You make a simple change, maybe use a Hex editor and change a couple of bytes. Then you run it and it completely bypasses AV. 'Oh, look, no alarms.' That's pretty effective."

> *Honestly, it is extremely trivial in many cases to bypass antivirus.*

MAKE SURE THE SOLUTION FITS THE ENVIRONMENT AND THE NEED

Even with high-level buy-in, you still need to find the right solution. Davis stresses the importance of doing your homework before deciding on any endpoint-security solution. "You don't want to pick a solution that seems like a good fit based on ads and recommendations and then just bring them in," he says. "You need to know your environment extremely well. You need to know what kinds of data you have on your endpoints, and how people use it. You need to understand your risks, and what is the worst-case scenario for an endpoint in your environment. Only after you've done this can you determine what kind of endpoint protection is right for your situation." This may include next-gen antivirus, cloud implementation for easy access and scalability, application whitelisting, the ability to monitor and log attempts to download non-whitelisted code, and other tools for monitoring and controlling endpoint activity. "Doing your homework and choosing a reputable vendor are important to making it work for you," says Davis.

Another consideration in rolling out a solution is gaining end-user acceptance. "There's often pushback at first. People question why they need security-awareness training, or complain about alarms that keep popping up on their computer when they try to download something," says Davis. This resistance may be more prevalent in higher-ed than a more traditional corporate environment, because of a culture that is less concerned about security. "You need to build a culture of security, which can be difficult in an education environment that thrives on academic freedom," he adds.

"Any time you're dealing with an organization that has global reach and endpoints connected all over the place, you have a large attack surface that presents a special security challenge."

MAKE SURE THE SOLUTION FITS THE ENVIRONMENT AND THE NEED

Beyond awareness training and reminders, one approach that helps is encouraging people to use your security practices in their own personal environments. "If you can help people apply the security principles you're trying to preach in your organization to their own home or personal computing use, that's something that can help them and help your organization," Davis explains. "It helps build a culture of security by essentially telling users the behavior you're asking of them is no different than what they should be doing at home."

KEY POINTS

1. **When modifying any security practice, whether it's changing emphasis or adopting new or stronger endpoint security tools, it's important to maintain a holistic perspective.**

2. **You need to know what kinds of data you have on your endpoints, how people use it, understand your risks, and know the worst-case scenario for an endpoint in your environment.**

ENDPOINTS MUST BE PROTECTED AT SEVERAL LEVELS

BRIAN TIMMENY

Global Head of Advanced Engineering, DevOps, Engineering Processes, BBVA

Brian Timmeny serves as the head of advanced engineering, DevOps and engineering processes, at BBVA, a global financial services company. He currently drives the agile and devops transformation of the global engineering group toward next-generation devops and advanced engineering delivery, driving continuous integration and deployment into the application suites within the global-engineering portfolio.

LinkedIn

Brian Timmeny believes that endpoint security is mission-critical, particularly in a DevOps environment. "We protect our endpoints at several levels," he says. "All of our tool suites are built via endpoints or on a microservice model available via a common endpoint with common contractual services and common testing." To ensure that these common endpoints are secure, Timmeny's team develops and implements the exposure of those applications according to the services and security policies that govern them.

There's another side of the endpoint security coin in a DevOps context, of course: ops. "When we think about the ops side implementation, we're making sure that everything is also accessible via an endpoint that we create with respect to monitoring as a service. Everything is through a service contract that must be discovered through an endpoint," he explains. "There are two major security considerations to address. The first, naturally, is that you have to know where that endpoint is. The second is that you have to have a dual-authenticated access in place to obtain access to that endpoint."

> *"Whenever someone tries to access an endpoint, those security policies kick in to say, 'Where did you come from? Who are you? Do I know you?'"*

ENDPOINTS MUST BE PROTECTED AT SEVERAL LEVELS

Once this level of security has been accomplished, Timmeny, the head of advanced engineering at the financial services company BBVA, aims to ensure that the endpoints have self-correcting policies. "We have a protection store that houses all of the policies, rules, and regulations," he says. If someone has doubly authenticated and accessed one of their endpoints, Timmeny's application suite must confirm that person's identity. If they cannot obtain that information, they shut down the endpoint to prevent a potential man in the middle scenario in which an unauthorized party is able to determine and pardy traffic in both directions.

A DevSecOps approach protects not just the endpoints, but also the environment that protects them. Timmeny achieves this with back-running policies (for example, Lambda policies when within an Amazon context) that are constantly running. "Whenever someone tries to access an endpoint, those security policies kick in to say, 'Where did you come from? Who are you? Do I know you?'" he says. "We're not only ensuring that upon deployment we have that security, but in runtime operation, every time an event fires, we have those same policies that are constantly enforcing security."

"We're able to log event information to prove compliance, and we can also analyze how effective our controls actually are."

ENDPOINTS MUST BE PROTECTED AT SEVERAL LEVELS

Since BBVA sits inside the financial industry, the company must also evidence its secure policies. "We have the ability to log whether there was a breach, when we averted a breach, and so on at a very detailed level," he says. Endpoints are of course included in this log. As a result, "we're able to log event information to prove compliance, and we can also analyze how effective our controls actually are," he notes. In the future, Timmeny would like to be able to leverage AI to better understand potential breaches that are happening and then create policies arising from those events. It's very important to be able to apply machine learning to these problems because, as he points out, "attacks and attack methods are increasing exponentially and it's critical to outthink hackers."

Ultimately, Timmeny believes that endpoints are never static points unto themselves. "Endpoints are points within an ecosystem that must be protected, and you can protect an individual endpoint," he says. "But if you're not protecting the ecosystem, you remain vulnerable to a hack. You're vulnerable to new and exciting ways of hacking, which are coming out daily." This is why it is imperative to simultaneously protect endpoints at several levels using a comprehensive approach.

KEY POINTS

1. **It's important to protect not just an endpoint but also the surrounding environment that protects that endpoint.**
2. **Effectively using AI and machine learning will be key to keeping up with the increasing volume and complexity of attacks.**

CHRISTOPHER LAJINESS

Sr. Systems Engineer, Symantec

LinkedIn

Prevention is great, but detection is an absolute must. While prevention will protect your network from many attacks, it is inevitable that someone WILL get into your network if there isn't someone there already. Patches and updates aren't always applied regularly and leave security holes for a malicious actor to get in. The ability for a security team to detect a breach and remediate quickly is paramount.

AUTOMATED FORENSICS BOOST A SECURITY TEAM'S EFFECTIVENESS

DAN BOWDEN

VP & CISO,
Sentara Healthcare

Dan Bowden, VP and CISO at Sentara Healthcare, has had a career spanning 25 years in cybersecurity and technology. His experience encompasses the military, retail, banking, higher education, and healthcare sectors. Now a two-time CISO, he has successfully built two organizational cybersecurity programs from the ground up. Bowden is active in cyber workforce development, blockchain technology research, and healthcare technology innovation. His success as a leader and CISO has been founded on winning board and executive leadership support for cybersecurity.

Twitter | LinkedIn

Dan Bowden believes that cloud-based endpoint-security solutions have greatly enhanced his organization's security capabilities. "Many of these technologies can help us answer a lot of questions more easily now than we could in the past," says Bowden, who is VP and CISO at Sentara Healthcare. "We have the ability to automate incident response, forensic work, and things like that." With that in mind, he advises security professionals to take advantage of this next-generation automation technology, which augments security professionals' ability to analyze incidents and address vulnerabilities at the endpoint.

Businesses that are operating with lean resources while facing increasingly stringent compliance requirements will find these capabilities especially helpful, since they allow the security organization to operate with greater agility, speed, and thoroughness. "In healthcare, just explaining how many malware incidents we've experienced isn't enough anymore," Bowden says. "We've got to show that we're categorizing them and that we've taken appropriate follow-up measures to do a risk analysis and determine what happened." He can now report not just how many malware events his organization has encountered, for example, but also how many of them were remote access Trojans and how many command and control events his team was able to block.

> *"Many of these technologies can help us answer a lot of questions more easily now than we could in the past."*

From there, Bowden can use these automated forensics tools to gain a greater understanding of the endpoint-security threats his organization must address, such as the likelihood of command and control events occurring on laptops outside the company network. He can drill down further to understand what type of data was on a specific device, what level of access permissions the user had, and when the malware arrived. "With the next-gen endpoint solutions, I'm now able to answer tougher questions using a single automated interface," he says.

When adopting advanced solutions such as these, Bowden advises that organizations pay careful attention to change management. "A lot of the time, you're trying to unseat an incumbent tool," he explains. The legacy tool may be perfectly serviceable, but it likely doesn't offer the full range of features that the newer tool does. Accordingly, it's a good idea to walk your colleagues through the differences and explain how the organization will benefit from next-generation technology.

"With the next-gen endpoint solutions, I'm now able to answer tougher questions using a single automated interface."

Bowden finds that his colleagues are more comfortable getting on board with technology change than they were in the past. "They know that money's tight so if we decided to spend money on this, we should make sure we do what we need to make it work," he says. He recently noticed this during a 2FA rollout, in which his boss checked in with a woman working in the administrative division to see how she was adapting to the new 2FA tool on her phone. When he asked, "Oh, what do you think of it?" she said, "You know, when I get that little challenge authentication and I confirm it, it makes me feel like I'm doing more to protect our data."

Having worked with legacy tools and users who were once resistant to technology change, Bowden feels that security professionals have a promising opportunity to enhance their effectiveness using the next generation of cloud-based endpoint security tools. Businesses that invest in advanced capabilities will find not only that they are able to defend the organization with greater speed and agility, but that their colleagues are more likely to appreciate the value of security and want to do their part, thereby improving the company's ability to defend itself against the threats it faces.

KEY POINTS

1. **Security professionals can answer tougher, more complex security questions in less time using next-generation endpoint security tools based in the cloud.**
2. **When colleagues understand the need for security, they are more likely to want to do their part to protect the organization.**

IMPLEMENTATION SHOULD BE GRADUAL AND COLLABORATIVE

DAVID MERRILL

Senior Director,
Travelers Insurance

David Merrill is the senior director of data security at Travelers. Previously, he was the strategist for endpoint security and malware protection in IBM's Chief Information Security Office while also advising dozens of IBM's Fortune 500 clients. He also served as IBM's global security operations manager where he directed the daily running of the company's worldwide internal IT security. A multiple patent holder, he is also the inventor and architect of the IBM Threat Mitigation Service.

Twitter | Website | LinkedIn

David Merrill, senior director of data security for Travelers Insurance, is an advocate for endpoint security, but suggests the technologies and implementation should be well considered and companies should know exactly what they want to achieve before rolling out a new strategy. "There are signal flares that you need to worry about more advanced attacks," he explains. "But you should also understand just how penetrated, how poked at, is your system. And from where?"

Understanding how vulnerable your organization is to advanced or specifically targeted attacks helps illuminate the type of endpoint strategy that's best suited to your needs. For example, Merrill says, companies should consider the architecture of their infrastructure. "Business is transforming to a point where most user endpoints aren't inside the infrastructure. They're physically and logically outside to the point where they represent their own data center." The result of this shift is that existing security isn't sufficient or progressive enough to protect the endpoints.

Once you understand the breadth of risk your organization faces, Merrill suggests you can then begin looking for the right tools. "Where you need to apply the controls has now changed completely, so looking at that leads you to really solid requirements," he notes. The other key part of a selection process involves determining how usable and operationally supportive those tools are. "That's fundamentally important," Merrill says. "We need to help the business manage risk, but never get in the way of the business. To me, that's the hardest part."

> *"Business is transforming to a point where most user endpoints aren't inside the infrastructure."*

IMPLEMENTATION SHOULD BE GRADUAL AND COLLABORATIVE

It's because balancing security and risk mitigation with the company's best interests is so difficult that Merrill suggests considering cloud-based services as an effective solution. "Often in cloud-based solutions, you're not the one who has to stand up all the back ends. That's going to be done for you as part of an SaaS. It lets you focus on control, usability, and communication," he points out. That means you have more time to prepare users for changes that are part of implementing the product.

However, Merrill says there are two possible mistakes that organizations make when they're implementing endpoint strategies that include cloud-based and next-gen technologies. "I think one is overselling it. It helps if the change is coming from a place of, 'I'm helping you transform the business,'" he says.

Merrill says another mistake organizations make is trying to roll out a solution at scale. "You should have a staged method for bringing this into the environment without breaking the business," he advises. "Advanced products fail when they're brought in too fast and they break business. They disrupt users. You will be asked to remove it and never bring it back, and now you've lost." A more gradual, collaborative approach of implementing an endpoint strategy is more effective, he says. "How we do it is just as critical as what we're doing, because there will be problems. Doing this gradually—crawl, walk, run—is a good approach to implementing this kind of solution."

"We need to help the business manage risk, but never get in the way of the business. To me, that's the hardest part."

KEY POINTS

1. **To know the type of endpoint strategy that's best suited to your needs, you must understand how vulnerable your organization is to advanced or specifically targeted attacks.**
2. **Cloud-based services may offer an effective solution to the difficult task of balancing security and risk mitigation with the company's best interests.**

IMPLEMENTATION SHOULD BE GRADUAL AND COLLABORATIVE

Beyond awareness training and reminders, one approach that helps is encouraging people to use your security practices in their own personal environments. "If you can help people apply the security principles you're trying to preach in your organization to their own home or personal computing use, that's something that can help them and help your organization," Davis explains. "It helps build a culture of security by essentially telling users the behavior you're asking of them is no different than what they should be doing at home."

KEY POINTS

1. **When modifying any security practice, whether it's changing emphasis or adopting new or stronger endpoint security tools, it's important to maintain a holistic perspective.**

2. **You need to know what kinds of data you have on your endpoints, how people use it, understand your risks, and know the worst-case scenario for an endpoint in your environment.**

CHARLES LI

CTO, Integration and Innovation Lead,
IBM GBS Cyber Security and Biometrics

Twitter

LinkedIn

Effectively identifying the most severe cybersecurity threat and mitigating the most impactful attacks are imperative for cyber defense. In my view, we should deploy cognitive technologies and apply intelligent event-suppression techniques to the endpoints, and maximize both computer and human resources for cybersecurity event and incident response.

EFFECTIVE DEPLOYMENT DEPENDS ON UNDERSTANDING YOUR THREAT SCENARIOS

JOHN MEAKIN

CISO,
Formerly Burberry

Dr. John I. Meakin has recently retired as chief security and risk officer at Burberry, and now advises a number of businesses on cyber risk. He is a specialist in information and systems security with more than 25 years of experience. Most recently he was chief security officer for the luxury-goods conglomerate Richemont International SA. Previously, he built and led security functions in a range of banks, BP, and Reuters. He has a PhD in experimental solid state physics.

LinkedIn

For John Meakin, former chief risk and security officer at Burberry, today's retail environment is rich in endpoint computing that encompasses core office activities, connections to manufacturing facilities, and sales assistants working within the retail network. Beyond this, there is a very active online customer engagement and sales process that often involves multiple channels. "We see the endpoint being right there on the perimeter," Meakin says, emphasizing the importance of endpoints to his overall security strategy.

This is a view shared in the organization. "Interestingly, it's never been easier in my experience as a security leader to make the risk-based cost-benefit equation, because there is so much evidence out there of what happens when things go wrong," Meakin says. But just because it's easier to enlist support and funding, that does not mean the task of securing endpoints is any easier. "The difficulty in achieving effective deployment of these technologies is still very high. It's complicated. So my life's a little bit easier, but it's not a breeze," he notes. These challenges relate to finding the right technologies to fit your endpoint activities, and being able to support them.

> *"You need to think about how you are going to manage whatever you deploy."*

Meakin offers this advice:

- **Don't think about it as finding a single perfect solution for the endpoint.** Meakin says you have to think carefully through the most likely threats that apply at the endpoint. For example, in Burberry's case it has the core office environment, the manufacturing environment, and the retail network environment. Each presents its own usage patterns and threat scenarios, and they are complicated by frontline activities with customers inside and outside the store. "I have not yet found one product with the richness of functionality that gives me enough to address the variety of endpoint-threat scenarios," he says. "Also, you need to recognize that the endpoint is one very important part in a bigger context of the other things you deploy across your network, because the endpoint-security solution is never going to be 100% effective."
- **Look for the smallest number of solutions needed to address your threat scenarios.** This is because implementing endpoint-security tools presents a management challenge. "You need to think about how you are going to manage whatever you deploy," Meakin explains. "One thing that distinguishes the endpoint from other places in your IT estate is that the endpoint is multiple. Whatever you deploy to the network, you need to multiply by 1,000, or 10,000, or 100,000. Scale makes it more challenging to get every security technology deployed to every endpoint, operating fully effectively in line with the standard configuration, with every endpoint patched to the relevant level."

"The only way you can practically get new data in a timely and rich enough manner, is if you've got the endpoint agent taking action based on analysis happening in the cloud."

EFFECTIVE DEPLOYMENT DEPENDS ON UNDERSTANDING YOUR THREAT SCENARIOS

Meakin believes the best approaches for securing the endpoint broadly fit into architecture where there's an agent on the endpoint that it is fed actionable machine intelligence from a cloud service that comes along with that endpoint technology. Behavior analysis is a good example. "The only way you get behavioral analysis is if you keep feeding the analysis algorithms with new data," he comments. "The only way you can practically get new data in a timely and rich enough manner, is if you've got the endpoint agent taking action based on analysis happening in the cloud."

KEY POINTS

1. **Rather than searching for the perfect endpoint solution, begin by carefully thinking through the most likely threat scenarios that apply to your endpoint estate.**
2. **The best approaches for securing the endpoint broadly fit into architecture where there's an agent on the endpoint that it is fed actionable machine intelligence from a cloud service.**

DANIEL SCHATZ

CISO,
Perform Group

Daniel Schatz is currently the chief information security officer (CISO) at Perform Group's London office. Prior to this he led the global Threat and Vulnerability Management program for Thomson Reuters. He is a Chartered Security Professional (CSyP) and a member of the International Systems Security Association (ISSA-UK), and he holds several qualifications including CISSP, CISM, CCSK, CVSE, MCITP-EA, ISO27001 LA/LI, and MS Information Security & Computer Forensics.

Twitter | LinkedIn

At the UK-based digital sports content and media group Perform, Daniel Schatz is responsible for a dynamic environment in which most employees are mobile, working from outside the office in various locations including the sports games that Perform Group covers. Most of Schatz's endpoints are Windows-based (about 60 percent Windows and 40 percent MacOS), with a few Linux devices mixed in. To secure these diverse endpoints, he has been evaluating new endpoint-security strategies, including cloud-based solutions that offer real-time threat monitoring and detection at the endpoint.

Schatz advises businesses considering cloud-based and next-gen endpoint-security solutions to make sure they focus first and foremost on what is actually needed in their environment. "Typically, the business doesn't really know what it needs," he explains. "It really falls upon the security professional to understand the business, and then understand the front landscape around it. Where am I, in terms of the threat actors that have a potential impact on what I'm doing? Who's after me, simply said, and what is their capability?" he adds.

Facing increasingly complex threats, a security professional might be tempted to seek the greatest amount of visibility into all the potential threats the business could conceivably encounter. But, Schatz says, "If you don't have the skilled staff to dive into it and actually find what's going on, and then try to remediate it, or at least raise it to the right level, it's not really helping you." It's therefore important to make sure you're thinking about how your team can make practical daily use of any endpoint-security solution you might choose.

> *"It really falls upon the security professional to understand the business, and then understand the front landscape around it."*

Once you understand your business needs and have taken your staff's resources into account, it's time to figure out which vendors provide the solutions that fit your environment's unique requirements. From there, Schatz recommends partnering with a vendor to take a promising product for a test drive. This will give you an opportunity to ascertain what kinds of security insights the solution provides your business, and how well your team might be able to use them.

Along the way, you might find that today's next-gen solutions require less administrative resources from your security team than they would have in the past. "Nowadays, most of the newcomers in the markets provide cloud-based services, where the heavy lifting is done in the background. That means you don't have to go and provision a server farm just to support your antivirus or your endpoint detection and response [EDR] correlation engine," Schatz explains. "This is now sitting away from your on-premises. It's not costing you capex. It's not costing you anyone to manage it. You have that benefit nowadays."

"Nowadays, most of the newcomers in the markets provide cloud-based services, where the heavy lifting is done in the background."

KEYS TO MAXIMIZING THE VALUE OF ENDPOINT SECURITY

Businesses that are considering moving to a cloud-based next-generation platform for endpoint security will derive maximum value from any investment they make by first ensuring they know what risks the business faces before seeking a solution. Once they have identified a tool that might be a fit, they can test it out with the vendor to determine how the staff can glean actionable insights from the reporting it provides. In this way, businesses will have the best chance of ensuring that any endpoint-security solution they select will be a worthwhile asset to their overall cybersecurity strategy.

KEY POINTS

1. **A business considering moving to a cloud-based next-generation platform for endpoint security must first clearly understand the security risks it faces.**
2. **Security professionals must also consider how their staff will use the insights provided by any endpoint-security solution they select.**

BRIAN HUSSEY

VP of Cyber Threat Detection & Response, Trustwave

Website

LinkedIn

There will be a continued industry-wide shift from prevention only security strategies in favor of detection and response as attacks become increasingly sophisticated and adaptive. Early detection is paramount for preventing cybercriminals from moving laterally, escalating privileges and concealing other nefarious activities once inside a network. If an organization has been breached, early detection can be the difference between a minor inconvenience lasting minutes or crippling incident costing millions of dollars and irreparable damage to public brand perception.

EFFECTIVE IMPLEMENTATION DEPENDS ON EFFECTIVE COMMUNICATION

ISABEL MARIA GÓMEZ GONZÁLEZ

Group Information Security Manager, Bankia

Isabel M. Gomez is a certified executive manager with cross-functional expertise in risk management specialized in information security, cybersecurity, data protection, compliance, and digital transformation. During her more than 18-year career, she has managed and led projects that involve different legal, normative, technical, and financial areas. She is an expert-cited contributor and participant in forums, articles, and discussions on issues related to new technologies and regulations.

Twitter | Website | Blog | LinkedIn

When implementing an endpoint-security strategy, one of the keys to success is recognizing that what you implement affects everyone. "If you are not a great negotiator and communicator, you will have a problem within your company," says Isabel M. Gomez, group information security manager at the Spanish banking group Bankia. "You need to find a compromise between all the business interests, and all of them need to be happy with your decision."

Gomez comes to endpoint security from the perspective of the overall threat environment the bank and the financial-services industry face. Endpoint security plays an important role in an incident-response strategy that is built on big-data analytics and fraud prevention. This requires developing a security strategy that finds a balance between securing the perimeter, endpoints, apps, regulatory compliance, and other things as well.

How you choose and implement an endpoint solution depends a lot on your business sector. "It's very different, for example, for a bank and an electric company," says Gomez. "It's absolutely not the same. In our case as a bank, my recommendation is to find a solution that can tell you what is happening in the world in close to real time. We need information close to real time, and we need to verify this information all around the world. Our business is digital."

> *"You have to be able to trust the results. You want a company that demonstrates it can obtain information and control everything all around the world."*

It's not good enough for vendors merely to say they can deliver on your needs, or their product has great capabilities—they have to prove it as well. "There are a lot of technologies. You have to be able to trust the results. You want a company that demonstrates they can obtain information and control everything all around the world," Gomez points out. You also need a solution that works for your analytical team. "My security team is the key to selecting a tool," she says. "They work hard, and they work a lot of hours, and they need to obtain the response that they expect to obtain. If I have a solution that sends me a lot of amazing information, but I can't handle this information, I can't do anything with it." The solution provider needs to understand that they are working closely with the security team, and the security team is going to develop rules for selecting the information that's needed. The solution provider has to prove they can deliver on these needs.

However one of the biggest challenges is getting alignment within the organization on the kind of solution that best serves everyone's needs. That means working with business-unit managers to understand what they need. "In my case," says Gomez, "I have established a strong network with all the reach areas—legal, brand, compliance, and so on. Your strength is that you can help them. They don't really understand security. You become the bridge between the different areas, and you can translate from legal to IT security, or from compliance to business, or from reach to business. You can explain to all of them what is happening."

"I have established a strong network with all the reach areas—legal, brand, compliance, and so on. Your strength is that you can help them."

EFFECTIVE IMPLEMENTATION DEPENDS ON EFFECTIVE COMMUNICATION

Gomez believes that presentations need to be brief and focus on key security issues. "When you explain it, be simple, transparent, and focus on the four big pillars of governance, protection, monitoring, and response." She also advises keeping in mind what interests your audience most, which is achieving their business plan and avoiding anything that will disrupt this goal. "They want to obtain their results or meet their goals. If you are speaking to a business unit, they are most interested in improving their results. If you are speaking to a compliance officer, they don't want to compromise privacy or lose data."

KEY POINTS

1 **One of the biggest challenges is getting alignment within the organization on the kind of solution that best serves everyone's needs.**

2 **The solution provider needs to understand that the security team is going to develop rules for selecting the data that's needed, and then prove it can deliver on these needs.**