



12 Security Experts

on Changing Endpoint Security

Moving to a Cloud-Based,
Next-Generation Platform for
Endpoint Security

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 12 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 make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

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

FOREWORD: ENDPOINT SECURITY

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

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

As endpoints become smarter, new challenges emerge: emerging ransomware and 0-day exploits infect all kinds of systems with ease, while many attackers use no malware at all to accomplish their malicious goals. With all this change, we spoke to 12 leading security experts to identify what's working and how they've influenced their organization to make the necessary changes before becoming the next victim.



Regards,

Mike Viscuso

CTO and Cofounder of Carbon Black

Carbon Black.

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

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



Chris Thompson

Adopting Endpoint Security Involves Both Business and Technical Considerations.....5



Richard Davis

Make Sure the Solution Fits the Environment and the Need.....9



Brian Timmeny

Endpoints Must Be Protected at Several Levels.....12



Dan Bowden

Automated Forensics Boost a Security Team's Effectiveness.....16



David Merrill

Implementation Should Be Gradual and Collaborative.....19



John Meakin

Effective Deployment Depends on Understanding Your Threat Scenarios.....23



Daniel Schatz

Keys to Maximizing the Value of Endpoint Security.....26



Isabel Maria Gómez González

Effective Implementation Depends on Effective Communication.....30



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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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.



Download the full e-book: [Security Experts on Changing Endpoint Security](#)



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.





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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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.



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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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 parry 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.



Download the full e-book: [Security Experts on Changing Endpoint Security](#)



**CHRISTOPHER
LAJINESS**

Sr. Systems Engineer,
Symantec



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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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.



AUTOMATED FORENSICS BOOST A SECURITY TEAM'S EFFECTIVENESS

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."

AUTOMATED FORENSICS BOOST A SECURITY TEAM'S EFFECTIVENESS

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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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.



Download the full e-book: [Security Experts on Changing Endpoint Security](#)



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.





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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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."

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.

KEYS TO MAXIMIZING THE VALUE OF ENDPOINT SECURITY



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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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.



KEYS TO MAXIMIZING THE VALUE OF ENDPOINT SECURITY

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.



Download the full e-book: [Security Experts on Changing Endpoint Security](#)



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.





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



Download the full e-book: [Security Experts on Changing Endpoint Security](#)

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."

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.