Mighty Guides

Sponsored by:
GoSecure

# 10 Experts on Active Threat Management

Expert Advice to Better Detect, Predict and Prevent Today's Attacks

# INTRODUCTION

In today's world of cybersecurity, it often feels like the good guys are losing. New research by the Ponemon Institute shows that the average enterprise only has resources to investigate 4% of the security alerts it receives every week. The same research finds that more than one third of cyber exploits go undetected, successfully evading antivirus and intrusion-prevention systems.

The reality is that security practices can no longer wait for their endpoint-security tools to tell them something is wrong. Many are adopting a more aggressive approach to threat management, but this requires new tools and skills that challenge security teams already stretched thin. How are they doing? With the generous support of GoSecure, we asked 10 security experts the following question:

**What advice, best practices, and cautions can you offer SOC leaders who want to upgrade their security capabilities to become more proactive?**

We spoke to security experts in different cyber environments and at different stages in their use of active endpoint-security techniques. They talked about the inadequacy of traditional defenses and their experiences with new approaches—including predictive analytics and machine learning—and they discussed skills needed to apply these new technologies successfully.

What I see in these essays, in addition to a lot of practical advice, is the emergence of a rich new generation of security tools and practices that may give security practitioners an upper hand.

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.

© 2019 Mighty Guides Inc. I 9920 Moorings Drive I Jacksonville, Florida 32257 I 516 840 0244 I www.mightyguides.com

# FOREWORD

In the past year, cybercriminal introduced over 357,000,000 new malware variants to evade traditional endpoint protection solutions.  High profile attacks like WannaCry and NotPetya demonstrate how fast these new variants move through a network.  One victim of NotPetya had over 49,000 endpoints flatline before they could mount a response.

In addition, hackers continue to devise new attack vectors to bypass today's defenses. According to latest Verizon DBIR, 49% of the all threats are fileless and 25% are insider.  As a result, many organizations are under-protected, exposing sensitive data and business operations.

No organization is safe.  Ransomware represents a change in the cybercriminal business model.  Hackers now cast a wider net to go after large volume of small to medium enterprises, for smaller but faster payoffs.  With the advent of Ransomware as a Service, it's a business that even less skilled hackers can enter.

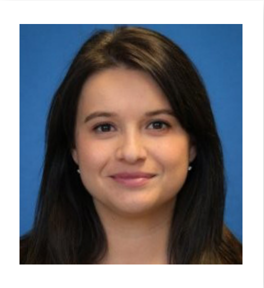
Successful Security Teams recognize the need to adopt new security strategies and technologies.  They incorporate Active Threat Management into their security strategies. They implement endpoint solutions that deliver the predictive intelligence needed to enable proactive threat mitigation.  To survive in today's dynamic threat landscape Security Teams need to detect potential threats, predict what they can do and respond before they evolve into full scale attacks.

Regards,
Neal Creighton
Chief Technology Officer, GoSecure

GoSecure

**GoSecure** is an innovator and pioneer in endpoint security.  They are leading the market in the consolidation of next generation Endpoint Protection Platform with Endpoint Detection and Response solutions.  GoSecure delivers full spectrum threat detection on-disk and in the OS.  It is the only solution to also detect threats in-memory, with their patented Digital DNA.  Its predictive analytics provides security teams with a view of the past, present and future of potential threats.  In this way, GoSecure enables Active Threat Management needed to survive in the new threat landscape.  GoSecure – Detect, Predict and Prevent.

# TABLE OF CONTENTS



# QUICK RESPONSE IS THE KEY

**HEMANTA SWAIN**
Sr. Director & Information Security Officer
TiVo

During his 15 years at TiVo, Hemanta Swain, currently a senior director and information security officer, has held many roles, including IT security architect and team leader for IT systems and security. He has managed a team of security professionals to drive security initiatives, compliance, and budget management. Swain's certifications include CISM, CISSP, and CCNA (Cisco Certified Network Associate).

in
Linkedin

In recognizing the failure of signature-based security to protect against many modern attacks, Hemanta Swain, senior director and information security officer at TiVO, focuses on two key elements in his security strategy:

- **Protecting data**—This involves managing access to data and protecting it wherever it resides. An important part of this is protecting any data that is located on an endpoint. "Encryption is key," Swain says. "You have to encrypt data where you store it, when you access it, and when you are moving it. You have to encrypt communications, and you have to keep encryption on your endpoint for any data that may be stored locally."

> *"At first you will have more false positives, but as you teach the tool through guided learning, the tools get better."*

- **Active security at the endpoint**—This includes protecting endpoints with new EDR tools that monitor activity, monitor memory, and have whitelisting and blacklisting capabilities. This is especially important in hybrid environments where some critical resources are stored in the cloud. "In the cloud computing world, some key resources are moving to the cloud, and SaaS vendors become responsible for the security posture of that service. But when users access that data on their endpoint devices, those devices must be protected." >

When protecting endpoints with EDR tools, the technology continuously monitors, analyzes, and correlates activities to spot potential issues quickly. Although this makes it possible to identify unusual activates more rapidly, it also involves analyzing far more data than could be done manually. “These tools consume log data and process that for abnormal behaviors,” Swain explains. “They process the data and apply behavior analytics to score it. The tools use machine learning and AI to automate this correlation and analysis.” If the score exceeds a threshold, the tool sends an alert or triggers an action, and then security people can look more closely at the event to determine its true nature.

Swain points out that to be most effective and minimize false positives, the tools must be trained. “At first you will have more false positives, but as you teach the tool through guided learning, the tools get better,” he says. He also believes that using machine learning and AI-based tools is critical to reducing the response time to abnormal events.

Another advantage of these tools is that the smarter they become, the more effective less trained analysts become. This is an important consideration at a time when demand for security analysts outstrips supply. Security people need to be trained in using the tools, but the technology rapidly correlates and analyzes data, and visualizes alerts, making it useful to a broader base of security personnel. “The tools are becoming so intelligent and user friendly, everybody is diving in,” Swain says. >

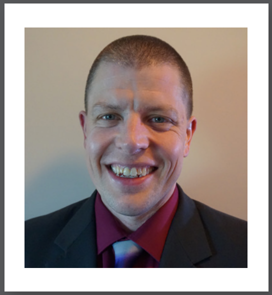
> “If you’re not able to detect threats, you can’t take the next steps to minimize the impact.”

For Swain, everything comes back to response time. “Speed matters,” he says. “In my office, if you know something, tell it quickly and think later. It’s the same with the tools. If the tool is saying something, we have to act on it. If you’re not able to detect threats, you can’t take the next steps to minimize the impact. Speed matters. That is the key.” ■

## KEY POINTS

1 **Although active endpoint security makes it possible to identify unusual activities more quickly, it involves analyzing far more data than could be done manually.**

2 **The technology’s ability to rapidly correlate and analyze data, and visualize alerts, makes it useful to a broader base of security personnel.**



### JASON KINDER

Director of Corporate Security
Leonardo DRS

Jason A. Kinder is the director of corporate security for Leonardo DRS. Over the past 13 years, he has held multiple roles managing core network, infrastructure, and security groups at the company. Kinder has been in his current position for four-plus years. He manages a small cybersecurity team that designs the security infrastructure, is responsible for cybersecurity operations, and leads incident-response activities.

Linkedin I Twitter

One of the most compelling reasons for adopting a more active approach to threat management is that attacks have become far too sophisticated for traditional "set and forget" perimeter and endpoint defense strategies. "Traditional antivirus, and to some degree firewalls, work using known parameters or signatures. They are not as effective against attacks that have never been seen before. Traditional antivirus solutions can't react quickly enough against new variants or threats," says Jason Kinder, director of corporate security at Leonardo DRS.

This does not mean it's time to throw away the traditional antivirus solutions. "I wouldn't tell anybody to dump their traditional antivirus software," says Kinder. "It still plays an important role in the overall security architecture." But threats that use multiple attack vectors and newly generated variants are specifically designed to bypass traditional defenses, which is why organizations need to engage in more aggressive threat-hunting strategies.

> “*Having the proper tools is important, because without the tools, you're not going to have the visibility.*”

Doing this successfully requires adopting new tools and developing new skills within the security team. Tools need to be able to monitor and analyze what is happening on endpoints, including what applications are doing and how memory is being accessed. "Having the proper tools is important, because without the tools, you're not going to have the visibility," says Kinder, noting that visibility and analytical capability are key to earlier detection. >

“Behavior-analysis and machine-learning techniques can look at how malware is working and what its are on the  system, and then stop it before it can carry out its intended action,” explains Kinder. Sometimes a tool may not be a new product, but a custom script or existing tool used in a new way that can be used to query systems for key information previously not used.  In addition to new tools, key skills for active threat management include memory analysis, forensics, and knowledge about active threat-hunting techniques.

Having the right tools and threat-hunting skills is critical, but you also need to begin by establishing a baseline of network, user, and application behaviors. This baseline comes from a combination of documented normal application and system behaviors as well as monitoring, logging, and analyzing activity on the network. “It will take time to gather all that information and create a baseline of how that system should be operating,” says Kinder. “But once you have that baseline, you can use that to start hunting on your own.” At first this involves actively engaging in defining anomalies, but as the system matures, automated threat scoring becomes more accurate, the number of false positives declines, and the dwell time of threats in your environment shrinks. “Once you start getting detections, you’ll quickly be able to see this was valid, this was not, and figure out the parameters that will make that more accurate,” Kinder says. >

> “It will take time to create a baseline of how that system should operate, but once you have that, you can start hunting on your own.”

By triaging alerts in this way, the tools used can become more predictive in identifying threats by more accurately assigning threat scores indicating the likelihood of malicious activity. "To improve scoring and get closer to zero false-positives, a tool needs to allow you to customize rules for the installed environment and modify built-in rules as it monitors the environment," notes Kinder. "Over time this allows you to get closer to the goal of zero false-positives."

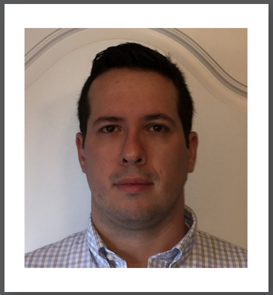
He points out that active threat management must be a continuous activity. This is because network environments are constantly changing with new applications, data, and usage patterns, and also because the threat landscape changes constantly. "If you don't make it a continuous activity, you will fall behind the curve very quickly and miss potential threats," Kinder says. ■

## KEY POINTS

1 **Modern multi-vector threats are specifically designed to bypass traditional defenses, necessitating more aggressive threat-hunting strategies.**

2 **Active threat management must be a continuous activity because of ever-changing network environments and the constantly shifting threat landscape.**

# ENDPOINTS ARE PART OF ONE GIANT, INTEGRATED SYSTEM



## JOSEPH SMITH

Interim Director of IT
University of Maryland
Eastern Shore

Over his 20-year IT career, Joseph Smith's experience has ranged from the trenches of help-desk tickets to running an enterprise IT department with a multimillion-dollar budget. As the acting director of IT for UMES, he has focused priorities and budget with a mindset of simplicity, functionality, and security, adopting the KISS methodology to IT project management.

in Linkedin | Website

To secure the collaborative IT environment that's needed in a university setting, Joseph Smith, interim director of IT at the University of Maryland Eastern Shore, oversees a defense in-depth strategy that includes traditional perimeter-type defenses, limits functionality at user endpoints, and performs behavior analytics across the system. "The objective is to observe, catch unusual behaviors as fast as possible, and perform threat analysis based on the possible that could occur," says Smith. Given the unlimited time and resources available to determined attackers, Smith believes a proactive security strategy is the better approach against an enemy that has a built-in advantage.

> *"The objective is to observe, catch unusual behaviors as fast as possible, and perform threat analysis based on the possible damage that could occur."*

In addition to a traditional defensive stack, Smith employs multilevel accounts in which more privileged ones have more access and controls, to limit access as far as possible to what's needed for a particular task. He also uses application whitelisting to block any unrecognized or unapproved applications.

In defending user endpoints, Smith takes a somewhat different approach. "From my perspective, I can't look at it as just an endpoint, because the endpoints are part of one giant, integrated system," he explains. "They're talking to data servers and email servers.

There are many avenues for lateral attack. To me, an endpoint is just another piece of our network that has to be protected. Even though it's just an end-user machine, I treat it like any other server."

At the same time, he recognizes that the mobility of some user endpoints makes them even more dangerous as potential attack vectors, and this calls for special defensive strategies.

For example, much of the user functionality that faces university assets is accessed through virtual desktops. This limits what user endpoints can do when they engage with university assets by moving most of the functionality into the cloud and turning the user endpoint into something like a dumb terminal. Still, they run agents on user endpoints that monitor application activity and combine that data with other data collected across the network. "We see all the traffic from end users going out and coming in, and we do behavioral and predictive analysis at that level," says Smith. He correlates all that activity with firewall events and other network activity. "You should have heuristic scanning. You need to look beyond simple definition-based, signature-based patterns to behavioral patterns. The attackers are smart. They know what you're going to look for," he says. ›

> "You need to look beyond simple definition-based, signature-based patterns to behavioral patterns. The attackers are smart. They know what you're going to look for."

Smith also advocates using technology to trigger flags and actions based on abnormal behavior. As a simple example, to prevent phishing attacks from using legitimate email accounts to send out spam, they implemented a trigger that automatically forces email account password changes any time they detect unusual volumes of outbound email from a particular account.

Using this security strategy that combines activity monitoring, automated triggers, and limits to user endpoint functionality, Smith is able to quickly sacrifice endpoints to limit the spread of an attack. "They're kind of like pawns in a chess game," he says. "You don't really defend the endpoints at that level. You defend the data."

## KEY POINTS

1 **Given the unlimited time and resources available to determined attackers, an active security strategy is the better approach against an enemy that has a built-in advantage.**

2 **A security strategy that combines activity monitoring, automated triggers, and limited endpoint functionality can quickly sacrifice endpoints to limit the spread of an attack.**

## KATRINA BISCAY

Director of Information Security
University of Cincinnati

Katrina Biscay is a seasoned information security professional with experience in government and higher-education sectors. She specializes in incident response, digital forensics, threat intelligence, SOC leadership, e-discovery, and vulnerability management. Biscay holds a bachelor's degree in Computer Science from Xavier University and a master's in Digital Forensic Science from Champlain College, and is a certified paramedic.

in
Linkedin

For Katrina Biscay, a director of information security and manager of incident response at the University of Cincinnati, a layered approach to security remains the best strategy in an increasingly dangerous cyber environment. "Unfortunately things like fileless malware and polymorphic malware are not new, but a lot of organizations have lacked preparedness," she says. "Now it's costing the organization, from ransomware and the fees and recovery costs associated with that, to reputation impact, and compliance fees and reporting guidelines which are much stricter now than they ever were before."

> *"Unfortunately things like fileless malware and polymorphic malware are not new, but a lot of organizations have lacked preparedness."*

In an open university environment that Biscay characterizes as something of a free-for-all, where students and researchers come and go and 60 percent of the devices connecting to the network are not owned or controlled by the university, she strongly advocates a layered strategy that includes a lot of monitoring and more training for SOC analysts. "The best approach is the layered defense where antivirus and endpoint management are tools in your toolbox," she says. "I think training is the most important thing that you can do for your SOC. It's the one thing I cannot emphasize strongly enough. The skills to detect, alert, and respond to new threat types are what's required to really get your return on investment from your SOC." >

An established SOC already has many of the necessary skills in place, but there needs to be an adjustment of focus so that analysts understand not only what the malware is doing, but also its impact on the business. “They need to focus more analysis on how the malware impacts their environment, not necessarily every tiny thing that a piece of malware does,” Biscay says. “That way they can prioritize their response based on what something will actually do to their organization.” This requires a broader versus deeper malware analysis. More people in the SOC should be trained in this kind of analysis, rather than having one person be the expert analyst.

New tools are important as well, particularly those that monitor activity across the network, including endpoints, perimeter alerts, communications with command and control servers, and memory activity. “There are quite a few tools that do proactive detection,” notes Biscay. “They can look for things like abnormal power shell execution, abnormal detection of administration commands, file integrity monitoring and any unauthorized changes to system files, DLL injection monitoring in memory and its behavioral analysis, system resource usage. These are things that should be alerted and investigated.” ›

> “They need to focus more analysis on how the malware impacts their environment, not necessarily every tiny thing that a piece of malware does.”

Looking for abnormal behaviors requires having a baseline of normal behaviors. "You need to know what normal is for your organization," explains Biscay. "That is unique to each agency. You can't adapt it across companies or industries. You need to know what you are expecting to see in your environment." This involves training the tools to minimize false positives and avoiding the very real problem of alert fatigue. "A mistake I see a lot of organizations make is an out-of-the box approach. You start out of the box, but then you fine-tune it to your environment and your baseline."

Biscay also says to focus on your most critical assets. "I recommend focusing on things that are critical to your business. That's what's going to cost you in a breach. Focus on what you can control and monitor well. Then as you mature your security program, expand to other areas."

## KEY POINTS

1 **Many companies run behavior-analysis tools with out-of-the-box settings. You need to start out of the box, then you fine-tune it to your environment and your baseline.**

2 **An established SOC has many of the necessary skills in place, but it needs to adjust its focus so that analysts understand not only what the malware is doing, but also its impact on the business.**

# BIMODALITY AND DIGITIZATION CAN HELP YOU DETECT THE UNKNOWN THREAT

## KEVIN MCLAUGHLIN

Director, Deputy CISO
& Adjunct Professor
American Public University
System (APUS)

Dr. Kevin McLaughlin has more than 35 years of corporate and cybersecurity experience. Over the course of his career, he's been involved in creating three cybersecurity operations centers, implementing cybersecurity architecture for three Fortune 500 companies. An army veteran, McLaughlin has led over 800 cyber investigations, was a SWAT team leader, conducted anti-terrorism activities, and has provided solid executive management.

Linkedin I Twitter I Website I Blog

Kevin McLaughlin, cybersecurity expert and associate professor at American Public University, is a strong believer in defense in depth, but he also recognizes that in today's threat environment, traditional defenses are not enough. "You still need to have your core components on the endpoint," he says. "But the bad guys are so good, you really have to start looking at your next steps."

> "What we are talking about is the digitization of security."

The challenge is that no matter what tools you use to block the bad guys, intrusions will occur, often through insider activities that create unintended vulnerabilities. In many cases, these intrusions are designed to resemble normal network activities or they have patterns never seen before, which makes them very difficult to detect. You need to find those threats as quickly as possible before they cause damage or data loss. But new fileless attacks that work in memory and operate using legitimate operating system components are difficult to detect even for tools designed to find them. It requires more intense monitoring and analysis. "What we are talking about is the digitization of security," says McLaughlin.

To do this, you need tools that detect suspicious activity on endpoints, skill sets, and methods for investigating that activity, and a corporate culture that accepts the need to respond immediately. These are the hallmarks of a modern endpoint detection and response (EDR) capability. >

EDR tools monitor activity and apply machine learning, predictive analytics, and artificial intelligence to detect threats that human analysts are likely to miss. “It’s a machine-learning process where the tool monitors computer functions and learns a normal operational stance,” McLaughlin explains. “If something outside those norms happens, the tool raises an alert.” AI takes that further by not only teaching itself what is normal, but also teaching itself malware behavior patterns and predicting the likelihood of activity being a threat.

McLaughlin believes it’s a mistake to set alert thresholds manually, preferring to let the tool teach itself what is normal. “I like having the machine learn by itself in default mode and establish the norm. I might set a wrong boundary, and then I’ll be the next big exploit,” he says. EDR tools can also automatically initiate response actions beyond sending alerts. “If the tool knows it’s getting hit by something on a port, I want it to shut down the port automatically. I want it to take that proactive action and then notify me after,” says McLaughlin.

In addition to having the right tools, McLaughlin says organizations need to build threat-hunting teams. This requires a different skill set than that of a traditional analyst. “In my operation, a known piece of malware goes to my SOC [security operations center], my level one and two analysts,” he explains. “They can handle that.

> “I like having the machine learn by itself in default mode and establish the norm. I might set a wrong boundary, and then I’ll be the next big exploit.”

If it’s something unknown, that goes to my threat hunter. They are a talented certified ethical hacker, and they will dig in to see how great a risk it is and what is the best mitigation approach.

Not every organization has the resources to build out its tools and security teams. For those who do not, McLaughlin recommends considering managed detection and response (MDR) services. He also notes that it’s not always the biggest players who offer the best MDR services. “There are really good, low-cost MDR services out there,” he says. “The important thing is to recognize you need to invest a couple of weeks upfront training the MDR team, on your environment, your policies and process, your handoff points, and what you expect to see happening.” ■

## KEY POINTS

1 **In addition to having the right tools, organizations need to build threat-hunting teams. Threat hunting is a different skill set than that of a traditional analyst.**

2 **When working with an MDR vendor, spend time teaching them your environment, your policies and process, your handoff points, and what you expect to see from them.**

# MORE DATA MAKES THE BEHAVIORAL ANALYSIS MORE ACCURATE

## LESTER GODSEY

Chief Information Security Officer
City of Mesa, Arizona

CISO for the City of Mesa, Arizona, Lester Godsey has more than 24 years of public-sector IT experience, and has presented on topics ranging from telecommunications to project management to cybersecurity. Godsey has taught technology and project management at the collegiate level. A published author, he holds a BA in Music and an MS in Technology from Arizona State University.

in
Linkedin

For Lester Godsey, chief information security officer (CISO) of the City of Mesa, a key consideration when executing a security strategy is the business context of the infrastructure and data you are defending. For instance, some organizations have fast-changing environments that support high volumes of transactional activity. Other environments are less dynamic and may not expose business-critical or sensitive data. These differences impact everything from the resources you use to secure your assets to how you analyze threats.

When it comes to taking a more active approach to securing endpoints, Godsey offers several pieces of advice:

> “We prefer tools with a client that has a hook into the operating system kernel so we have that deep level of insight.”

- **Catching attacks early**—The low profile of some attacks, such as fileless attacks that work inside known, legitimate applications, and fast-acting attacks such as ransomware, puts a premium on identifying and neutralizing these incursions as quickly as possible. Doing that requires continuously analyzing a lot of endpoint activity and responding to suspicious behaviors. “We’ve turned to tools that work to address fileless malware and zero-day attacks and look at more behavior as opposed to signature-based indicators,” says Godsey. “We prefer tools with a client that has a hook into the operating system kernel so we have that deep level of insight.” >

- **Monitoring the right activity data**—If you haven't taken a comprehensive and holistic approach to knowing what data assets you have available to you for threat management, and you're not capturing that data, you've already lost before you've begun. "Security folks tend to focus just on log collection," explains Godsey. "Log data is not the only source of data that allows you to more actively manage threats. Security operations center (SOC) people need to be aware of this, because data comes from all over the place, and it may not always be structured."
- **Predictive Detection and False Positives**—Certain patterns are predictive. Determining the likelihood that an observed behavior is part of a threat pattern involves a calculation. "Your [endpoint detection and response] EDR discovers something that looks unusual compared to a baseline, there's a higher degree of a probability that something weird is going on. There are predictive aspects to that," Godsey says. But he also points out that the same calculation can generate false positives. "EDR solutions looking for fileless malware and zero-day stuff that they've never seen depend on algorithms," he says. "If you change one aspect of your environment, you're changing something that can affect that calculation." He believes that although collecting more data makes the analysis more accurate, you can never completely eliminate the possibility of false positives. Then it becomes a risk-benefit judgement. ›

> "Our advanced endpoint solution has the ability to automatically quarantine or remove an endpoint from the network if we so choose."

“I’m never going to hit zero, so at what point is my threshold such that I’m comfortable automatically quarantining a device? At what point does the benefit outweigh the risk of hitting a false positive?”

The ultimate goal is being able to respond quickly to detected threats, because having all the insight does you no good if you cannot act on it. This often requires automation, because many threats progress too quickly for humans to respond.  “Our advanced endpoint solution has the ability to automatically quarantine or remove an endpoint from the network if we so choose. We’re not totally there yet. We’re still fine tuning that capability,” concludes Godsey.

## KEY POINTS

1 **SOC leaders should look beyond just log data for anomalies. Threat insights can be found in data can comes from many sources, and it is not always structured.**

2 **The ultimate goal is being able to respond quickly to detected threats, because having all the insight does you no good if you cannot act on it.**

# MOVING FROM FILE LOCKING TO BEHAVIOR LOCKING

## PAUL HEFFERNAN

Group CISO
Unipart Group

Paul Heffernan is the CISO for Unipart Group. With experience in cybersecurity, he engages with the business at board level to enable trusted secure commerce. He is a regular speaker at international conferences, such as the e-Crime Congress and CISO 360 Barcelona. Heffernan is proud to have been recognized at the Cyber Security Awards in London as "Highly Commended" CISO of the Year 2017.

Linkedin I Twitter I Website I Blog

In the past, a "set-it-and-forget-it" security strategy had a certain appeal. The role of security has always been to reduce risk to the company without obstructing business. The goal was to be a business enabler. The approach made it possible to provide security at the pace of business operations.

But attacks have become more complex, and signature-based security solutions cannot possibly keep up with malware. Traditional security practices are further challenged by an increasingly rigorous regulatory environment. And then there are customer expectations. "Our customers buy from us because they trust us to do a better job of securing their data," explains Paul Heffernan, group chief information security officer (CISO) at Unipart. "We're in an interesting position where security is becoming a competitive advantage, and it's adding value to the business."

> *"The first thing we are doing is applying the principle of least privilege to behavioral locking and restriction, rather than file locking and restriction."*

All of these factors are making effective security practices more critical than ever. "And with so many new malware files being released every day, we're reaching a point where antivirus vendors and other technologies that alarm signatures are unable to keep databases large enough to hold all the signatures. Clearly this approach isn't enough," Heffernan says. >

To respond to these challenges, Heffernan sees a fundamental shift in the application of the principle of least privilege. “From my perspective, the very first thing we are doing is applying that principle to behavioral locking and restriction, rather than file locking and restriction,” he says. “Instead of looking for signatures, we need to look at what actions and behaviors happen on the system that indicate malware where we don’t have a file or we don’t have a signature to detect a file.”

There are other things system administrators can do to make that principle of least privilege even more powerful, such as locking administrative tools. “A typical corporate laptop will have power shell enabled by default. Most users don’t use those technologies. They’re designed for system administrators. The bad guys know this, so simply disabling these tools can improve security” notes Heffernan.

An increased reliance on behavior analytics requires new tools to keep up with the scale and speed of this challenge. “Tooling around automation and orchestration, particularly on behavioral analysis, will play a big part in this,” says Heffernan. He sees machine learning and artificial intelligence as critical tools for early threat detection, but they still require help from humans. >

> “Security operations center analysts need access to tools that can do that behavioral analysis to scale.”

“I have seen some movement in the vendor space on unsupervised machine learning,” he says. “The problem historically is those tools tend to generate lots of false positives simply because they are having to do a lot of work to determine what is abnormal. In the early stages that requires some human intervention.”

Still, these tools are becoming essential for the SOC analyst. “SOC analysts need access to tools that can do that behavioral analysis to scale,” Heffernan says. He also sees SOC analysts needing to adjust their skill sets. “You need people who have got that natural sense of curiosity. They should probably have some background in programming or system development-type problem solving, because they’re going to be more likely to put those puzzle pieces together.”

Ultimately, these analysts will rely on behavior analytics tools to allow them to focus on what is important. “People’s brains are naturally hardwired for pattern sourcing and problem solving. What we want to do is remove the noise from the activity SOC analysts see, and give them what naturally suits their capabilities. This brings patterns to life and helps them think about how a particular problem needs to be solved,” concludes Heffernan. ■

## KEY POINTS

1 **With malware variants being generated far faster than any signature-based security solution can possibly keep up with, signature detection is not enough.**

2 **Machine learning and artificial intelligence are critical tools for early threat detection, but they still require help from humans.**

# 'SET AND FORGET' IS LAZY SECURITY

## DR. REBECCA WYNN

Head of Information Security<br>& Data Protection Officer
Matrix Medical Network

Dr. Rebecca Wynn has a proven track record of taking companies to the next level of excellence in many sectors, including government, financial services, fintech, healthcare, information technology, legal, semiconductors, and retail. Named 2017 Cybersecurity Professional of the Year at the Cybersecurity Excellence Awards, she is a "big-picture" thinker with nearly 20 years of experience in information security, assurance, and technology.

Linkedin I Twitter I Website I Blog

As head of information security & data protection officer for Matrix Medical Network, Dr. Rebecca Wynn is responsible for assuring compliance with regulations related to personal identity and health information. Just as importantly, she must protect data and systems against any kind of breach that could seriously hurt the business. To accomplish that, she oversees a defense-in-depth strategy that includes endpoints and continuous monitoring. She is also a strong believer in active threat management. "I hate 'set and forget,' or checkbox risk management. All that does is let the security team sit back and say, 'Hey, the bells and whistles didn't go off, so I don't have a problem,'" she says. Wynn believes this lazy approach to security provides an opening for attacks that traditional defenses won't detect.

> *"People shouldn't fool themselves that something hasn't happened on their network. It's happening, but being blind to it is what gets you in the news."*

A simple example might be an employee who is lured into clicking on malvertising that strips data off the network by looking at whatever is in that user's memory cache. "You wouldn't catch that in traditional endpoint protection," she says. "You wouldn't catch it in the data loss prevention either. The firewall might see something happening, maybe you have some sort of trap on the top layer that might catch it, but maybe not. ›

You really don't know what's in the cache for that employee. Maybe it's PCI [payment card industry] data, or HIPAA [Health Insurance Portability and Accountability Act] data. Maybe it's company financial data. Maybe it's junk. Who knows?"

To catch these kinds of threats, Wynn looks at what applications are doing as well as what is happening in memory and data feeds, everything that's going out, and the reasons it is going out. She believes it's necessary to monitor and analyze this continuously, and to address anything out of the ordinary immediately. "You want to try and catch any issue as close to zero day as possible," she says.

> "You want to try and catch any issue as close to zero day as possible."

To accomplish that, Wynn employs EDR (endpoint detection and response) and data loss prevention tools, and uniform security monitoring tools that correlate data across the infrastructure. "People often have different vendors monitoring just databases or managing just file servers," she explains. "Things happening by themselves in those silos may not seem significant, but when you correlate them, they suddenly look really bad. Being able to correlate things through a uniform security management system is important." ›

Transitioning to a more active endpoint-security practice requires investing in tools, learning how to use them effectively, and retraining or remaking security teams to change their old “set and forget” habits. But Wynn says with some of the new tools that are becoming available, this does not have to be a big, costly proposition. “With these new tools, you can be smart about how you do this. You really need to partner with vendors that have more holistic vendor solutions.”

She also believes taking this step is something organizations need to do in the face of modern cyber threats. “People shouldn’t fool themselves that something hasn’t happened on their network,” Wynn says. “It’s happening on your network, but being blind to it is what gets you in the news. It’s not a matter of when something bad will happen. It’s how quickly you resolve it and how quickly you get to zero day. You’re only going to do that by being active.”

## KEY POINTS

1 **“Set and forget” is a lazy approach to endpoint security that provides an opening for attacks traditional defenses won’t detect.**

2 **Active endpoint security requires investing in tools, learning how to use them effectively, and retraining security teams to change their old “set and forget” habits.**

# TO SECURE ENDPOINTS, YOU NEED A COMPLETE VIEW OF THREATS

## STEVE STONEBRAKER

Principal Security Architect
Guaranteed Rate

With 10 years of information-security experience, Steve Stonebraker believes that basic IT hygiene, next-generation technology, and a mature cyber program are needed to protect organizations effectively. He specializes in securing networks, applications, and systems in public and private clouds. Previously, he managed DevOps, Systems-Engineering, and Performance-Engineering teams. He holds an MS in Computer Information Network Security from DePaul University and is a Red Hat Certified System Administrator.

Linkedin | Twitter | Website | Blog

When it comes to securing endpoints in today's threat environment, early detection and quick response are the rules of the game. And Steve Stonebraker, who has worked in companies with both highly mature and less mature security practices, says that antivirus alone just doesn't cut it. "I've been in environments where you only have basic antivirus. And one of the issues with that is you don't have all the pieces of the puzzle." He likens antivirus to the check-engine light on your car. When the light goes on, you have no idea why, and you have no information for diagnosing the problem.

> "With a fileless attack, the exploit can sit inside of explore.exe and the hash is totally normal for that file. It's all about behavior."

For example, a typical antivirus might send a generic trojan alert if it detects a file exhibiting suspicious behavior. To really diagnose that, you need to know where it came from, what websites or other interactions were involved, and whether it is persistent on the network. This is what an advanced endpoint detection and response solution allows you to do. "If you have advanced EDR, it actually records every single website the end user goes to, and it records every single file that's written to disk," Stonebraker says. "I can see the moment that suspicious file was written to disk and the website the end user went to that caused that file to download. I can even search for a generic string and it will show me every single machine that has that string, which is great for figuring out if an attack is moving across the network. Basically, the EDR enables you to respond quickly." ›

Stonebraker notes that EDR tools increasingly use behavioral analysis to identify anomalies that are otherwise difficult to detect. “With a fileless attack, if I go to a bad site and it’s a drive-by download, my machine is exploited,” he explains. “The exploit can sit inside of explore.exe and the hash is totally normal for that file. In that case it’s all about behavior. Explore.exe may spawn a PowerShell or Windows command prompt instance.  From there an attacker may start adding administrative users to the machine and try to scan your Active Directory for additional machines to exploit.  At this point, alarm bells should be going off. A standard user has no reason for that type of behavior”

Another key capability in modern endpoint security is the ability to respond quickly to detected threats. “You need a tool that can quarantine machines that are showing malicious activity, and then have the right folks looking at it,” Stonebraker says, and one of the best ways to do that is to utilize your vendor’s incident response team or a third party Managed Security Service Provider (MSSP). “Otherwise you’re going to hire staff, and hiring security experts to do all of this in-house is awfully expensive in today’s environment.”

This is an important consideration, because hunting down threats not only requires special expertise, but cannot be practically done if you are unable to distinguish real threats from false positives. >

> “You need a tool that can quarantine machines that are showing malicious activity, and then have the right folks looking at it.”

Once again, this is where working with an EDR vendor or managed security service provider can be a big help. “The best way to eliminate false positives is to contract with your vendor to do all the first- and second-tier investigation reports,” says Stonebraker. “To go with advanced EDR, you need to be ready for the transition. You should have the tools in place, and you need people dedicated to investigating alerts if you’re not paying for a service provider to do it.” ■

## KEY POINTS

1 **To diagnose an alert properly, you need to know where it came from, what websites or other interactions were involved, and whether it is persistent on the network.**

2 **Hunting down threats not only requires special expertise, it cannot be practically done if you are unable to distinguish real threats from false positives.**

# A SECURITY PRACTICE NEEDS TO DEMONSTRATE CONTINUOUS IMPROVEMENT

## TODD SPIGHT

Chief Information Officer
Columbia College Chicago

In his more than 20 years in IT, Todd Spight has specialized in leading business strategy, cybersecurity, and business system modernization and consolidation. With experience in multiple industries, including food, healthcare, insurance and banking, Spight has held senior positions at Smalley, Medela, and Preferred Meals. He has a BS in Computer Science from Illinois State University and an MS in Information Technology from Northwestern University.

in
Linkedin

Information sharing is crucial in educational environments, especially higher education, and their networks must support this. Open networks, however, present a special challenge for IT security organizations. "In higher education, we typically have networks that transmit a lot of data very fast," says Todd Spight, chief information officer (CIO) at Columbia College. "And you find a lot of high-end computers. We attract attackers who are looking for free firepower. So it's not about just prevention anymore—it's about detecting, and being able to respond and recover. You have to change your priority from prevention being number one to detection being number one."

> *"Progressive security operations centers need to extend their reach into endpoint devices, including desktops and phones."*

This is not a small task in network like Columbia College's, which has over 60,000 devices on the network at any given time. "Progressive SOCs [security operations centers] need to extend their reach into endpoint devices, including desktops and phones," says Spight. This involves acquiring tools that enable you to monitor and correlate endpoint activity, and developing a baseline of expected activity, which serves as a reference for defining anomalies. "You have to have a good understanding of how a device is actually being used on a day-to-day basis, so that when an anomaly occurs, the technology recognizes that anomaly, logs it, and blocks it," he explains. >

Using predictive threat detection that involves scoring anomaly risk is an important part of addressing active endpoint security. For example, with good endpoint-detection capabilities you may see something happening on your network that's not an immediate problem, but you can tell someone is trying to do something. "Maybe they're getting to step 7, but they need to get to step 10 to be successful. The fact that they're getting to step 7 should raise a flag for you because you really don't want them to get past step 2," says Spight. He adds that if you were using a "set and forget" approach to endpoint security, you wouldn't even know there was something happening until they got to 10.

This requires a change in the security team's attitude, because in the old "set and forget" approach, the SOC teams waited for the technology to tell them what to do. In active detection and response, it's different. "Now you're looking at things like zero day, and you have patterns that are changing minute by minute," says Spight. "They're now doing reconnaissance, which requires new skills and training so that individuals understand the possibilities of these events they are seeing." ›

> "Now you're looking at things like zero day, and you have patterns that are changing minute by minute. Security teams are now doing reconnaissance."

One of the goals of any security strategy is to demonstrate the security practice is continuously improving, which is necessary to stay ahead of more aggressive and sophisticated threats. Whether you acquire tools and skills for successfully engaging in active endpoint security, or you contract those capabilities through a managed security services provider, the teams must continuously improve. This involves establishing performance metrics that demonstrate this, but also setting the expectation of what you need the teams to deliver.

You have to really understand what the team or the managed security service provider (MSSP) is bringing to the table, and make sure you're getting the reporting and metrics that measure your continuous improvement programs. "It isn't just about sending a report of everything that you stopped," says Spight. "That's not bad because that's what you are paying them to do. But it's not enough. That's table stakes. You want them to go further. You want to see what's changing. You need to see how it is improving your security." ■

## KEY POINTS

1 **Using predictive threat detection that involves scoring anomaly risk is an key element of active endpoint security.**

2 **Active threat detection requires new skill sets, because you are no longer waiting for something to happen. Teams need to understand the possibilities of events they are seeing.**