



# 7 Experts on Transitioning to Managed Detection and Response

---

Choosing an MDR service provider  
and building a valuable relationship



# INTRODUCTION

As the saga of the 2020 SolarWinds supply chain hack unfolded, many were surprised to learn that the offending malware had been deployed more than a year before it was discovered. Dwell time was and continues to be a central issue in IT security.

For this reason, many choose a managed detection and response (MDR) solution. MDR is a security service specifically designed to rapidly detect, respond to, and mitigate cyberattacks. It is an evolutionary step in cyber security, which is more important than ever now that so many people are working remotely.

It is not always clear when a company should move to MDR or how it can get the greatest value from an MDR service. That's why, with the generous support of GoSecure, we asked seven security experts the following question:

**Based on your experience with MDR, what advice can you offer organizations trying to decide whether MDR is a good choice for them?**

The experts agree that companies must first understand the gap between their current security capabilities and what they need to adequately address security risks.

Cyber security is more than simply a technology challenge. So, if you are considering an MDR solution or already work with a security provider, this ebook offers sound advice about evaluating potential MDR partners so that you can get the most out of those relationships.



**David Rogelberg**  
Editor  
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.

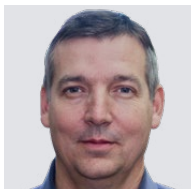
Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

# FOREWORD

Cybersecurity is constantly evolving, with technology adaptations quickly following new breach techniques. Attackers are increasingly exploiting the blind spots in traditional security technologies, such as antivirus tools, to breach endpoints, forcing cybersecurity teams to reevaluate their time-tested approaches.

These attacks can take place at any time, so cybersecurity teams must remain vigilant for suspicious activity, analyze event information quickly, and then respond accordingly. Breaches succeed when cybersecurity teams miss something within this visibility-analysis-response pyramid. They are more likely to miss something when their resources—people, time, or money—are limited.

GoSecure was founded on the belief that a new approach to cybersecurity was required, one purpose-built to redefine detection and response. Starting with a core behavior-based approach rather than the traditional binary indicators of compromise that many solutions use, our managed detection and response (MDR) approach added the key element: people. From the beginning, we realized that successful managed security requires collaboration and cooperation. As you are about to see from the experts in this ebook, a strong relationship with your MDR provider is vital to success. We invite you to learn more about how GoSecure MDR works with you to deliver the right security outcomes for your organization.



**Neal Creighton**

CEO  
GoSecure





**GoSecure** is recognized as a leader and innovator in cybersecurity solutions. The company is the first and only to integrate endpoint, network, and email threat detection into a single Managed Detection and Response (MDR) service. The GoSecure detection and response platform delivers predictive multi-vector detection, prevention, and response by applying a unique combination of behavioral analysis, memory forensics, machine learning, and reputational techniques to counter the most advanced threats. GoSecure MDR is designed to detect and respond in less than 15 minutes, rapid response and active mitigation services that directly touch the customers' network and endpoints. Together, these capabilities provide the most effective response to the increased sophistication of continuously evolving malware and malicious insiders that target people, processes, and systems.



# DETECT AND RESPOND TO THREATS FASTER

With 24/7 visibility into your environment to identify, track and stop advanced threats, GoSecure Managed Detection and Response dramatically reduces your company's risk.

## Why GoSecure?

-  **Visibility:** 150 unique event types across endpoint, network, email and user behavior compared to industry average of less than 50
-  **Analysis:** ML / AI, combined with human review, to correlate behaviors and events with attack strategies

-  **Response:** Mitigating attacks on average in less than 15 minutes, compared to average dwell time of almost 80 days
-  **Experience:** Over 6 years of experience operationalizing the MDR connection between people, processes, and technology



**GOSECURE**

Learn more at [www.gosecure.net](http://www.gosecure.net)

# MEET OUR EXPERTS



**BRIAN SHEA**  
**Revolution Group**

Chief Information Officer and  
Practice Director,  
Technical Services  
pg. 6



**ERICA WILSON**  
**Cass Information Systems**

Vice President, Chief  
Information Security Officer  
pg. 9



**ROBERT L. PACE**  
**Invitation Homes**

Chief Information Security  
Officer and Vice President,  
Information Security  
pg. 12



**ANATOLY CHIKANOV**  
**Enel X North America**

Director of Information  
Security  
pg. 15



**CHRISTOPHER KOZLOV**  
**Lake Forest Academy**

Director of Information  
Technology  
pg. 18



**HEMANT DESAI**  
**CIO**

Guilford County  
pg. 21



**SCOTT WOOD**  
**Opis Senior Services Group**

Executive Vice President/  
Chief Information Officer  
pg. 24



**Brian Shea, Revolution Group,**  
Chief Information Officer and  
Practice Director, Technical Services

Based in Columbus, Ohio, Brian Shea is the chief information officer (CIO) of Revolution Group, and is a dynamic IT executive. He has more than twenty-five years of IT experience and focuses on IT strategy, infrastructure and operations, compliance, and cybersecurity. He is the former CIO and chief compliance officer of MBX Medical Billing Experts and the chief technology officer of Riverside Radiology and Nationwide Children's Hospital.



**“An underlying driving force behind MDR is the need to spot threats earlier, respond to them faster, and mitigate them before they become serious incidents.”**

## **When Considering MDR, Think about What You Need to Accomplish**

The big difference between a managed detection and response (MDR) service and traditional security services is that MDR does more than monitor, detect, and provide alerts. MDR service providers automate responses in real time through their security stack, their security operations center, and staff expertise.

Many organizations that are considering MDR are doing so in response to an incident—something that forced them to rethink their security practice. In security, it is usually the thing you don't know that gets you, and people are reevaluating their security technology and practices to see what they are missing. An underlying driving force behind MDR is the need to spot threats earlier, respond to them faster, and mitigate them before they become serious incidents.

When considering an MDR service, think about what you are trying to accomplish. Security practice should start with a security maturity matrix that covers everything from endpoints to the edge. With that you can evaluate your strengths and weaknesses, and then avoid acquiring redundant capabilities. For example, many MDR solutions include layered protection for endpoints so

that if you use the full, encompassing MDR service, you may be able to phase out the antivirus/antimalware applications and services you are currently using. MDR not only improves your ability to detect and respond to things quickly but offers an opportunity to consolidate security functions under one vendor, simplifying security management overall.

**“The more visibility MDR providers have into the workflow tools that employees are using, regardless of the endpoint, the better.”**

Key capabilities that an MDR provider should be able to provide include response automation and visibility. Automation is critical because the amount of data generated at endpoints in a networked environment is far too much for humans to digest. People are good at detecting trends and helping the system learn so that it generates fewer false positives, but the reality is that the data flow is so great—in fact, rising all the time—that the more automation you can apply to detection and response, the better. The most successful MDR providers are those with the technology stack best able to consume a lot of data and make decisions quickly.

Visibility into the environment is also vital. You can have the best technology stack in the world, but if email phishing attacks and ransomware attempts get through, bad things will happen. The more visibility MDR providers have into the workflow tools that employees are using, regardless of the endpoint, the better. The right kind of

**GoSecure’s visibility is unmatched. We have 150 unique event types across the endpoint, network, email and user behavior compared to the industry average of less than 50.**



MDR service can be effective at catching threats early. We have recently seen several health care practices and hospital networks targeted with ransomware. The MDR service was successful in remediating these incidents before they could become successful attacks.

To get the most out of an MDR service, choose carefully and trust in the provider's ability to perform. A lot of factors come into play, such as the type of industry you are in, the regulatory environment in which you operate, and your organization's security maturity. As a consumer of these services, I lean toward allowing the MDR service to do the job it is designed to do. You may need to build that trust, starting with the incident or drivers that motivated you to turn to MDR initially. Watch how the MDR provider performs. If the process is sound, the service is grounded in a good technology stack, and the service provides good reporting, the MDR solution's effectiveness should quickly show through.



**Brian Shea, Revolution Group,**  
Chief Information Officer and Practice Director,  
Technical Services



## Key Points

- 1 MDR not only improves your ability to detect and respond to things quickly but offers an opportunity to consolidate security functions under one vendor, simplifying security management overall.
- 2 To get the most out of an MDR service, choose carefully and trust in the provider's ability to perform. Allow the service to do the job it was designed to do, but expect results.





**Erica Wilson, Cass Information Systems, Vice President, Chief Information Security Officer**

Erica Wilson has more than twenty years of IT experience, primarily in cybersecurity. She has worked in various industries, including manufacturing, higher education, and financial services. Erica is currently the chief information security officer of Cass Information Systems, where she is responsible for all aspects of the company's cybersecurity program, including security strategy, policies and procedures, technologies, and training.



**“By having the ability to extend your staff with a trusted partner that can provide additional analytics and faster response times . . . , you are working toward a more mature security program.”**

## **An MDR Service Provider Must Fit with Your Organization's Goals**

In the cybersecurity industry, you can never have enough resources to assist with threat detection. By having the ability to extend your staff with a trusted partner that can provide additional analytics and faster response times to security events in your environment, you are working toward a more mature security program.

Deciding whether you need managed detection and response (MDR) resources—and what kind of resources you need—requires taking a hard look at your own detection and response capabilities. It may be that a specific incident causes you to examine whether you have gaps in your ability to identify threats. Or, you may have constraints on existing resources that you know limit your capabilities, not only with technology and skills but the level of work that people can take on day to day. You have to take a step back and determine whether an opportunity exists to improve your detection capabilities because in today's world, it's easy to miss real threats. An MDR service provider can extend your staff with threat-handling expertise and tools. It can also develop a broader picture of the threat landscape, and that experience adds value to the advice and information the provider can share with you.

The biggest challenge in making an MDR decision is deciding which service provider to partner with. Many providers operate with the best technology and threat intelligence, top skill sets, and similar detection capabilities. Ideally, you want a trusted partner that fits well with your organization's long-term goals and can provide essential security information in one clear single pane of glass. Key factors in the decision are the cultural fit with your organization and the vendor's ability to fully integrate with your technology.

**“Information visibility and reporting of key performance metrics are also important considerations, especially if you are a regulated business subject to compliance auditing.”**

On the technology side, integration with your technology is essential. If the MDR service provider cannot pull in logs from key resources and systems in your environment, its benefit to you is limited. Information visibility and reporting of key performance metrics are also important considerations, especially if you are a regulated business subject to compliance auditing.

Similarly, cultural fit is critical because an MDR partner is a resource that supports and acts as an extension of your team. As such, vendor staff need to work well with your team in terms of skill sets and communication preferences and styles. A single point of contact at the vendor is also essential—someone you can get to know and who understands your organization, appreciates your expectations for response times, and knows how quickly you will respond when an issue comes up.

**In a recent IDC Brand Perceptions Study of Managed Security Service Providers in Canada, GoSecure was the top-ranked vendor on overall perception score as ranked by customers. The top 3 buying criteria identified by the organizations were highly responsive staff, incident response and competitive price.**

Good two-way communication is essential for nurturing the relationship with the vendor and gaining trust in the provider's ability to detect issues and respond. Schedule regular meetings to discuss monitored activities and what is happening in the industry as a whole. The more actions a provider can take on for you, the faster you will be able to respond to incidents, but what you allow the vendor to do depends on trust and the nature of your business. It should be a risk-based decision based on the nature of the alerts, the systems involved, and the kinds of mitigating controls you have on the actions you would take. As the MDR relationship grows and the vendor learns more, it may have the ability to do more, but it takes time to build that level of trust.




**Erica Wilson**, Cass Information Systems,  
Vice President, Chief Information Security Officer



## Key Points

- 1 Deciding whether you need MDR resources—and what kind of resources you need—requires taking a hard look at your own detection and response capabilities. Key factors are the cultural fit with your organization and its ability to fully integrate with your technology.
- 2 The more actions a provider can take for you, the faster you will be able to respond to incidents. What you let the vendor do, however, depends on trust, the nature of your business, the type of alerts received, the systems involved, and the kinds of mitigating controls you have for the actions you would take.



“When evaluating an MDR service provider, recognize that the relationship will be more than just monitoring. The provider can take actions, too.”

**Robert L. Pace**, Invitation Homes,  
Chief Information Security Officer  
and Vice President, Information  
Security

Robert Pace is the vice president, Information Security, and chief information security officer for Invitation Homes, where he leads the Information Security program. Robert’s career spans twenty years leading global teams in the delivery of IT security operations. He holds degrees from Michigan State University and Walsh College as well as CISSP, CISM, CICISO, and ITILv3 certifications.



## **Be Clear in Your Objectives and Transparent with Your MDR Service Provider**

Security is all about how quickly you can detect, identify, isolate, mitigate and remediate issues. To do those things well, you must be on guard 24/7/365. The fundamental question you must ask yourself and your team is, Do you have that 24/7 capability? If you do not, then you need to bring in a vendor that has access to the right threat intelligence and can be on call 24/7, watching over your systems. You want a provider that you know has already looked at something before it gets to you, one that can respond quickly and enable you to take action. That is how you get ahead of the curve. Just having someone from your team on call does not give you the agility needed in today’s environment. You need eyes on the monitor at all times. These are the capabilities you want from a managed detection and response (MDR) service provider.

Before engaging with an MDR service provider, list your clear objectives: Making the vendor relationship work requires being transparent with the vendor about your goals and expectations. That transparency works both ways, too. You should expect the service provider to be open with you about what it can do to improve your security practice. To set those objectives,



work with your organization's leadership team to evaluate the company's security situation, and then work with the MDR service provider's team to develop a full view of your organization's IT environment.

When evaluating an MDR service provider, recognize that the relationship will be more than just monitoring. The provider can take action, too. You must understand which actions the vendor is capable of taking and which actions you want it to take. To that end, conduct full evaluation of people, processes, and technology—both yours and the vendor's. Ultimately, you want to integrate the MDR service provider into your organization so that its staff can generate tickets, remediate problems, and send critical issues to the right places.

**“With a strong MDR service provider relationship, you can improve your ability to quickly detect and respond to threats.”**

An MDR service provider needs visibility into your environment, and with all that high-velocity security data, it is important that you thoroughly work out processes for detection and remediation. With those processes in place, the provider can quickly take corrective actions, many of which can be automated. Take care in this area, however, because depending on your industry or data configurations, there may be critical systems that you do not want the provider to touch. When the MDR service provider takes actions in response to events it detects, those actions should be based on playbooks that you have carefully worked out and reviewed.

**With client agreement, GoSecure will own mitigation. We back that with mitigating attacks on average in less than 15 minutes, compared to an average dwell time of almost 80 days.**

A successful MDR service provider–company relationship goes back to transparency between you and the vendor so that everyone has clear expectations and objectives and you feel confident that the MDR service provider will work closely with you and your team. A key part of the relationship is measuring performance—for example, the vendor’s ability to close tickets, or time to remediation, or trend data that indicates that you are meeting key objectives. Meet regularly with the provider to evaluate operations and performance. Ideally, you want the vendor’s service delivery lead to be dedicated to your account.

With a strong MDR service provider relationship, you can improve your ability to quickly detect and respond to threats, which is essential for staying ahead of today’s cyberthreats.



## Key Points

- 1 Security is all about how quickly you can detect, identify, isolate, mitigate and remediate events. To do those things well, you need to be on guard 24/7/365. The fundamental question you must ask yourself and your team is, Do you have that 24/7 capability?
- 2 When the MDR service provider takes actions in response to events it detects, those actions should be based on playbooks that you have carefully worked out and reviewed.



**Robert L. Pace**, Invitation Homes,  
Chief Information Security Officer and Vice President,  
Information Security



**Anatoly Chikanov**, Enel X North America, Director of Information Security

Anatoly Chikanov is director of information security at Enel X North America, where he is responsible for maintaining operational security and DevSecOps. Anatoly uses his positive energy to encourage others to work in a smart, secure way to protect clients and the company as well as provide high-level security. Anatoly inspires change through security awareness education and mentoring for people considering information security careers.



**“For smaller and midsized organizations that do not have huge security teams to staff a 24/7 SOC, an MDR service makes sense.”**

## **Choosing and Working with an MDR Service Provider Involves Risk Management**

The first step in deciding whether you need a service—and exactly what kind of service you need—is to evaluate your current capabilities. Look at how those capabilities mesh with the reality of the risks you face and your current ability to meet them, and see where you have gaps.

A reputable managed detection and response (MDR) service typically has security operations centers (SOCs) located in different geographies or that run 24/7 so that they can provide full coverage and continuous, proactive monitoring of all your endpoints. This coverage is important because of where and when people work, and it has become even more critical since the COVID-19 pandemic, which has really changed how people work. You no longer have the standard set of people coming into the office from eight to five, and remote workers don't have the robust network security controls found in the corporate offices.

We began looking at MDR services seriously when our business expanded to Europe. It was not an easy decision for us because we already had an internal security information and event management (SIEM) system and an

internal SOC. We already managed data coming from all the endpoints through the SIEM system, and we were getting alerts. The big question was, How do we scale that? Now we would be ingesting twice as much security data. We would need to staff up so we could run 24/7 because of the different time zones of our operations. In addition, we would have to plan for security people taking vacations. Even with that, how effective would the night shift be at 3:00 or 4:00 a.m.?

**“To have a successful relationship with an MDR service provider, you need a good account executive and a good solutions engineer you can reach at any time.”**

Making this kind of decision becomes a numbers game, where you look at your internal resources and capabilities, how much you can cover, how many endpoints you have, and how many potential alerts come in, and then you determine the budget needed to add staff who can do all that. Then, you look at the cost and scalability of an MDR service and its ability to scale up or down, and it makes sense. It depends on the business and its capabilities. For smaller and mid-sized organizations that do not have huge security teams to staff a 24/7 SOC, an MDR service makes sense.

**Experience matters.**  
GoSecure MDR features a dedicated hunt team with over 500,000 hours of experience. We also have over 6 years of experience operationalizing the MDR connection between people, processes, and technology.



We have found value in relying on the MDR service to detect events faster, having better threat intelligence, and the service provider's broader perspective on security. When you focus on your own business, you work in your own security bubble. An MDR service provider works with a variety of clients, so it can bring a broader perspective to the things we see and make recommendations about what works in different organizations.

To have a successful relationship with an MDR service provider, you need a good account executive and a good solutions engineer you can reach at any time. You must keep them in the loop about changes in your environment; if they roll out new tools and capabilities, they should tell you about those things.

You also need to make decisions about what kinds of actions you will allow them to take and develop confidence they can perform those actions well. We take a risk management approach to that process. You must balance the risk of interruptions caused by false positives against the risk of not taking any action. Part of this calculation involves categorizing your IT assets based on how critical they are to operations. Finally, good communications channels with the MDR service provider are crucial to success.



**Anatoly Chikanov**, Enel X North America,  
Director of Information Security



## Key Points

- 1 Deciding to work with an MDR service provider becomes a numbers game where you look at your internal resources and capabilities, determine how much you can cover, calculate how many endpoints you have, determine how many potential alerts come in, and then come up with the budget you would need to add staff to do all that.
- 2 To decide on the remediation actions you allow the MDR service provider to take for you, use a risk management approach that balances the risk of interruptions caused by false positives against the risk of not taking any action at all.



**Christopher Kozlov**, Lake Forest Academy, Director of Information Technology

Christopher Kozlov is dedicated to facilitating the design, implementation, and support of IT services ranging from the visionary to the mission critical. He has 25 years of experience with technology in the financial, distribution, and education sectors. Christopher is the IT director for a private boarding school in Illinois, where he designs systems for users with wildly varying abilities and needs.



**“When evaluating an MDR service provider, it’s important to match the provider’s technology and staffing offerings to your technology, usage patterns, and security needs.”**

## **Can Your MDR Service Provider Deliver What You really Need?**

All organizations face the challenges of increasing complexity in the technical environment they must defend and the growing sophistication of attacks. Meeting these challenges requires new tools and skills—tools and skills that can stretch an organization financially. As an educational institution, our IT environment consists of a variety of technologies that support a range of user scenarios. We are not in a position to offer big salaries for top security expertise; instead, we rely fully on an in-house team to defend our infrastructure. That is why we use a managed detection and response (MDR) service.

When evaluating an MDR service provider, it’s important to match the provider’s technology and staffing offerings to your technology, usage patterns, and security needs. Some providers have special expertise in particular types of network technology; others have a broader range of technical capabilities.

Another key factor is a clear understanding of exactly which services the MDR service provider offers beyond detection and alerting. Look beyond threat

acknowledgement to what happens next. Does the vendor just give you a ping, or is it doing something more? Does it open a ticket? Who does the follow-up work to mitigate the threat? Who does the necessary forensic work? How do you get the incident information you need? Then what happens? Now that the vendor has detected the threat, who are the people helping you figure out the details of that threat? Are those people up to the task, or are they going to get stuck?

**“The value you realize from an MDR service provider depends a lot on the trust you have in that provider’s ability to perform those response actions you want it to take.”**

These key questions relate to whether the MDR service provider is going to take you from start to finish with the threat response, including helping you mitigate it. Is there someplace along the way where the vendor’s services stop? If the vendor just provides an alerting service, that may not be of much value to you. Then, underlying all these questions about the depth of services a vendor can provide and who on the vendor’s team provides them, there is the question of false positives. How well does the provider understand the actual threat it detects? This is important because it goes to the heart of how much trust you can put in the vendor’s ability to respond to real threats.

**GoSecure MDR was built to do one thing – detect and respond in less than 15 minutes. And, most importantly, mitigate attacks with zero false positives. In 2020 alone, we mitigated over 200 ransomware attacks for our clients. With no false positives.**

Finding the right MDR service provider has helped us close gaps in what our technicians see from a networking perspective. It has helped them understand the environment, from the desktop through the network and everything in between it. It has improved our security practice and helped with internal knowledge transfer. It also gives my staff a place to go to ask questions about things that come up, which means that I don't have to play that forensic cop so much. That is helpful to me as I am the last line of defense for every problem we run into.

The value you realize from an MDR service provider depends a lot on the trust you have in that provider's ability to perform those response actions you want it to take. Vendor staff must prove themselves, as well. We let them work on things as long as we're confident they're not operating in the false-positive range. Collaboration with our security team is important, as is vendor staff members' willingness to learn when they need to be careful about turning things off for certain critical people and operations. The key is having that good, two-way working relationship.



**Christopher Kozlov**, Lake Forest Academy,  
Director of Information Technology



## Key Points

- 1 A key factor in evaluating an MDR service provider is having a clear understanding of exactly which services the vendor offers beyond detection and alerting. Look beyond threat acknowledgement to what happens next.
- 2 You need a solid two-way relationship with your MDR service provider, one in which the vendor's staff are willing to learn the uniqueness of your environment, and one in which you can gain confidence in their ability to respond correctly to incidents.





**Hemant Desai, CIO,**  
Guilford County

As CIO of Guilford County, North Carolina, Hemant Desai creates strategic plans for countywide IT needs, aligns IT initiatives with county's goals and objectives, and identifies opportunities to enhance operational efficiencies. With more than thirty years in IT, his love of working with talented team members motivates him every day. He strives to improve by learning from his staff, customers, and subject matter experts.



**“In reviewing our strengths and weaknesses, we determined that our greatest risks came from having limited internal resources.”**

## **Evaluating an MDR Provider Begins with Understanding Your Own Security Gaps**

After outsourcing IT security to a managed security service provider for several years, we brought all IT security in house so that we could have more control. Now, several factors are causing us to evaluate extending our current security practice with a monitoring detection and response (MDR) service provider.

As the IT department for a county government, my team and I support many county operations including law enforcement, and Health and Human Services (DHHS). Now, with the coronavirus disease 2019 (COVID-19), we are supporting DHHS and the county's vaccination efforts. We have an internal security team who manage cybersecurity for approximately 2,500 employees. The security team operates with a security incident and response plan that includes risk assessment for IT assets, risk mitigation, and continuity of operations.

Because of the growing complexity of IT security and the increasing pressure on our in-house resources, combined with the fact that in recent months, many organizations including government entities have experienced ransomware attacks, we know we need to continue to evolve our security strategy and extend our capabilities. We are in the early stages of evaluating our resource gaps to determine the best way to fill them.

Before you can even begin to evaluate specific service providers, it is important to understand your current security posture in key risk areas. We do this by leveraging standard frameworks such as the National Institute of Standards and Technology (NIST) security framework, as recommended by our state. In reviewing our strengths and weaknesses, we determined that our greatest risks came from having limited internal resources and comprehensive assessment and mitigation if necessary of

**“Determining who is authorized to take different actions will be coordinated between the MDR organization and our internal IT team.”**

security threats. Therefore, we drafted a list of key requirements for an MDR provider: early detection capabilities, some preventative techniques to enable us to get ahead of a threat before it actually penetrates our firewall, 24/7 monitoring to support our operations, and dynamic dashboard-type reportings.

We expect that the greatest benefit of working with an MDR provider will be having an extension of our security team that can fill in resource gaps, in addition to providing our team with additional insight into what they are seeing in the environment.

We are still in the assessment phase and deciding how to go forward with an MDR provider. Once we establish that relationship, we will clearly define responsibilities in operating agreements. For instance, the MDR may be able to take certain actions for

**Because every organization is different, we collaborate closely with security teams to better understand their people, processes and technology so we become an extension of the team. With our focus on detecting and responding to advanced threats 24/7, organizations are able to maximize their security resources by allowing them to focus on what matters most.**

us, but it depends on the type of action. Being a government agency, we cannot have a third party take action on behalf of our county employees, especially when it comes to law enforcement. Determining who is authorized to take different actions will be coordinated between the MDR organization and our internal IT team.

Security is never a one-and-done operation, and that is true now more than ever. With an MDR relationship in place, our posture would be strengthened, our stakeholders will gain comfort from knowing that we have somebody looking out for us, and hopefully we will sleep better at night.



**Hemant Desai, CIO,**  
Guilford County



## Key Points

- 1 Key benefits of working with an MDR include: extension of our security team in addition to providing our team with additional insight into what they are seeing in the environment.
- 2 Security is never a one-and-done operation, and that is true now more than ever. With an MDR relationship in place, you can strengthen your security posture, better satisfy your security auditors, and hopefully sleep better at night.



“What I need to see from the service provider, in addition to its technical capabilities, is that . . . its staff must act like they’re part of my team.”

**Scott Wood**, Opis Senior Services Group, Executive Vice President/Chief Information Officer

Scott Wood is a technical lead with extensive experience guiding technology program and enablement functions. As an analytics professional, he uses his skills to identify trends, performance indicators, and operational gaps to enhance bottom-line factors. His talent for providing transformational leadership across functions, driving the execution of quality outcomes, has driven his success.



## **An MDR Provider Should Feel Like Part of Your Team**

The ability to detect and automatically respond to incidents in real time is essential in today’s threat environment of ransomware and viruses. If you do not have this ability now, you already have a problem managing cyber-risk.

We have a layered approach that starts with monitoring router activity, then monitoring network and endpoint activity, followed by monitoring servers and applications. The system displays alerts, and then sends email alerts. If the system detects a threat or suspicious activity, it automatically shuts down nodes.

We currently do all this monitoring in house. We began beefing up our detection and response capabilities several years ago, after a couple of ransomware attacks that, although they did not cause us material losses, were disruptive because we had to restore data and re-image machines. We are a small shop. Our IT team, which handles all IT support and security, consists of five people who watch over fourteen locations, 1,200 machines, and 2,500 users. The security tools we currently use make this work possible, and they work well for us, but we do not have the staff to continuously watch security monitors. We depend on the tools to automatically block threats, which so far has happened quickly and reliably. It’s often the case that we first learn of an



issue when users call in to tell us they are unable to get into the system. Then, we go to the security tools, determine what happened, and correct it.

Even though the tools work for us now, we are anticipating an expansion that will require us to cover forty locations—a serious stretch for our team. The expansion will require that we either hire additional staff or contract with a managed detection and response (MDR) service provider.

**“If an MDR service provider makes me confident that I can trust its ability to detect issues and respond quickly, . . . then I can sell it internally.”**

For an MDR service provider to work for us, it must fit our budget. If I can avoid hiring additional staff and maybe offset the cost of some of the tools we use—and if I’m confident that the provider can deliver the services we need—then it may make sense. What I need to see from the service provider, in addition to its technical capabilities, is that it is customer oriented. The provider has to be a team player, and its staff must act like they’re part of my team. We currently work with a couple of specialized cloud-based software services that include a person dedicated to us who can respond to our immediate needs. This relationship is essential for security, too, and should be part of what an MDR service provider offers. A close relationship is the key to making an MDR service effective at protecting your assets.

“

They [GoSecure] were the only MDR provider that delivered such extensive coverage. And their ability to work closely with our team to create custom run books was truly unique. After performing a thorough review of the MDR landscape, it was GoSecure’s unique combination of visibility, operational experience and customized service delivery that convinced ECPI University to choose GoSecure.

**Jeff Arthur,**  
ECPI University CIO.

”

Of course, the provider must also understand and be able to work with your technology stack and the products you use. I have spoken to service providers that would like us to change our infrastructure so that we use the technology with which it's familiar, but that would not be practical. When looking for a service provider, be sure that it can work with the technology you have in place.

If an MDR service provider makes me confident that I can trust its ability to detect issues and respond quickly, that we can have a close working relationship, that it understands our systems—and it makes economic and business sense for us—then I can sell it internally. I can make the pitch to my organization that this is what we need to do to protect our data and our business.



## Key Points

- 1 If you do not currently have the ability to detect and automatically respond to incidents in real time, then you already have a problem managing cyber-risk.
- 2 An MDR service provider should make you confident that it can detect issues and respond quickly, that you can have a close working relationship with its staff, and that those staff understand your technology.



**Scott Wood**, Opis Senior Services Group,  
Executive Vice President/Chief Information Officer

