Secureworks

SOLUTION BRIEF

Evaluating a Managed Detection and Response Provider

What's Inside?

This Brief details the key requirements you should consider when evaluating managed detection and response services. It then shows how MDR powered by Red Cloak uses a combination of security analytics software, deep threat intelligence, and leading security expertise to significantly improve threat detection and response times. Links to useful MDR resources like reports, papers, and webinars are included throughout to give you quick access in case you have additional questions or want to see third-party data.

Security teams of all sizes and maturity levels are struggling with larger attack surfaces, disparate tools, and insufficient staff and skills. Managed Detection and Response (MDR) solves these challenges but not all MDR providers are equal in today's market. Read this Brief to learn what requirements to look for in an MDR solution and how Secureworks stands out in a crowded, changing market landscape.

Detection and Response Challenges

76%

of cybersecurity professionals in a recent survey by ESG[1] found that threat detection and response is more difficult than two years ago. Our experience with customers shows this is a result of amplified threat volume, staff shortages, excessive manual work, and a widening attack surface.

89%

of respondents in the ESG[1] survey said they plan to increase funding for threat detection and response activities. But choosing a provider to partner with isn't easy. The number of vendors in the market attempting to address detection and response has increased dramatically. But most of these providers are missing the mark.

[1] Source: ESG Master Survey Results, The Threat Detection and Response Landscape, April 2019

MDR Buyer Requirements Table

The following table outlines how any MDR solution you're evaluating must meet certain minimum requirements to solve the challenges above.

Component	Description	Vendor Vetting Questions
Software-Driven Detection Speed	Analytical speed is a powerful weapon in security operations. Any proposed solution needs to be architected around the latest analytics technology, even if you're not directly using it. Be on the lookout for true cloud-native architectures that incorporate data science methods such as machine and deep learning.	1. Describe how quickly you detect <insert threat here> and can you show us how you will respond to it on our behalf? 2. Explain how your cloud-native analytics technology works. Was it built in-house or are you just partnered with another vendor? 3. Discuss how you incorporated data science into your software development process.
Software-Driven Detection Precision	Quickly detecting a false alarm is not very effective. Precise detections fuel precise responses. AI-based Detectors should be purpose-built and used in the provider's daily operations. These Detectors are used to find behavioral anomalies such as command and control, brute force attempts, and stolen credentials.	1. Describe how accurately you can detect <insert threat here> and can you show us how you will respond to it on our behalf? 2. Tell us about the experience you have in responding to and evicting threats from organizations? 3. Can you show me a demo of how your solution will apply that experience to keep us safe? 4. Is your software proprietary or via a third party? Does our team get access to your software as part of the solution?
Diversity of Threat Data and Research	When a threat actor has infiltrated your environment, they often use legitimate tools to evade detection by traditional security controls. In fact, our research shows that the average dwell time of attackers is 111 days. Detecting and evicting these threats requires a vast amount of threat data combined with a deep understanding of how threats behave.	1. How many professionals do you have keeping up to speed on the threat landscape? 2. Show us how your software infuses a diversity of data on historical, current, and potential threats. 3. Does the solution adapt to new attack patterns or is it a static set of rules that are easy to figure out and bypass? 4. Describe the process for how you find threats on other customer environments and feed that data into our defense posture.
Proactive Threat Hunting	Collaboration and transparency between the provider and your team is a key success factor. There needs to be collaborative investigation capabilities and open channels of communication. Threats don't sleep, and neither should your provider's ability to keep you up to speed on a risk to your business.	1. Please show us a demo of the user interface you provide to support co-hunting and collaborative investigations. 2. Describe what happens when we have questions – can we call or live chat with you at any time. 3. Describe how you know what to search for in our environment and what would trigger a hunt with us? Can we initiate a request for help in this area?
Incident Response Support	Your team needs to be able to rely on experienced security professionals to help during critical events. Any provider should provide evidence on how exactly remote incident response hours are a part of their MDR solution without any hidden fees or costs.	1. Are incident response hours included in the MDR solution? 2. How quickly will you respond in the event of a validated incident? 3. Tell us more about the experience your incident response team has – are they recognized by industry analysts?

Click Here to Request a Demo of Our Security Analytics Software

OR

Click Here to Watch a Webcast to learn more

"Prioritize providers that own their MDR intellectual property"

Forrester Research Inc. Now Tech: Managed Detection And Response (MDR) Services, Q2 2018, Jeff Pollard

Read the Report

Read the following IDC Analyst Connection paper on MDR

by Martha Vazquez

Read the Paper

To download a Data Sheet on MDR powered by Red Cloak, click here.

The answers to these questions will reveal if the proposed MDR solution can improve your defense posture, or if it will waste your limited time and resources. Of course, each environment has unique variables to consider, such as staff size, existing technology investments, and industry or geographic nuances. But this basic list of considerations will help you avoid making a regrettable decision.

MDR powered by Red Cloak™

Getting MDR right requires a software-driven formula. Our MDR solution is built on a highly powerful security analytics application called Red Cloak™ Threat Detection and Response. It was built using advanced data science techniques to reliably expose adversaries that would otherwise go undetected.

A combination of machine and deep learning trained using our proprietary threat intelligence and customer data powers behavioral threat analytics.

The software includes built-in detection use cases, simple investigation workflows, and automated containment actions across your endpoint, network, and cloud environments (see Figure 1).

Secureworks fuses human and machine intelligence to improve security for organizations of all sizes. Click any of the following links to learn more about our capabilities.

- MITRE ATT&CK mapping
- Incident response and threat hunting expertise
- Threat intelligence and research
- 20-year history of service excellence
- Watch how our experts understand the mindset of an attacker

MDR powered by Red Cloak enables your team, however advanced, to deal with an increasing workload and threat volume. We bring our expertise into your daily operations. Your team can collaborate with us on hunts, chat with our analysts, and periodically assess your security posture.

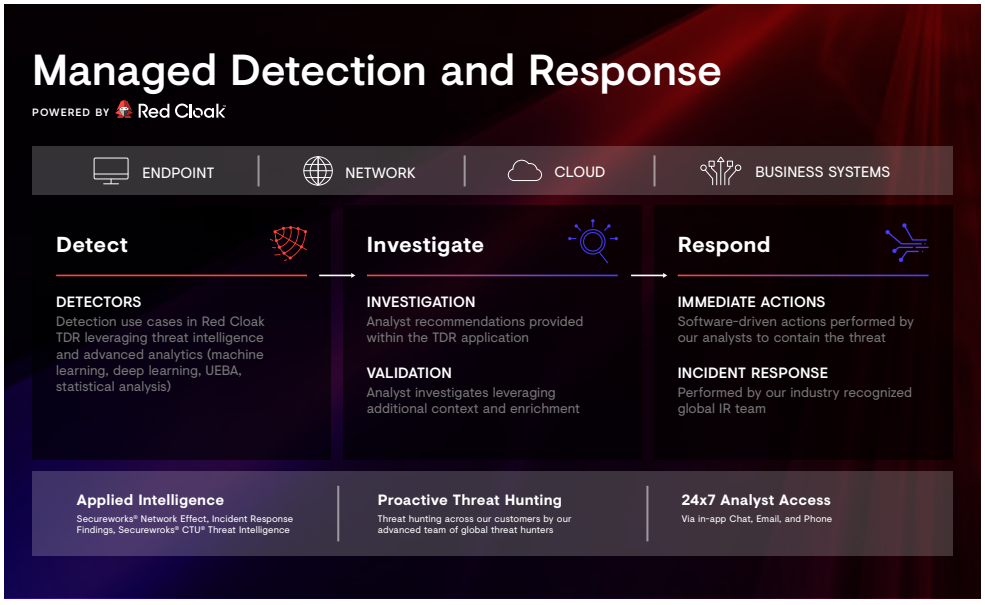

Figure 1. MDR powered by Red Cloak

Secureworks®

Experiencing an Incident?

If your organization needs immediate assistance for a potential incident or security breach, please contact us directly on our Incident Response Hotline.

United States & Canada:
1-877-884-1110

United Kingdom:
0808-234-1203

For more information, call to speak to a Secureworks security specialist.

United States & Canada:
1-877-838-7947

United Kingdom:
+44 0-131-260-3040

secureworks.com/mdr

10 Reasons To Consider Secureworks for Your MDR Needs

1 **Benefit from over 20 years of expertise**

Partner with a security organization that uses 20 years of security operations expertise to expose, contain, and resolve advanced threats.

2 **Partner on investigations**

Raise the skill level of your team by partnering on investigations with our experts.

3 **Live Chat with our security analysts**

Instantly pull up a chat window to get expert help whenever you need it.

4 **Enhance your security posture with frequent reviews**

Continuous improvements to your security posture with periodic reviews and reports.

5 **See more threats with unmatched data diversity**

Act on threat knowledge from over 1,000 IR engagements, a team of 70 threat researchers, and our experience protecting over 4,000 customers globally.

6 **Act with confidence – backed by human and machine intelligence**

Save time and increase effectiveness through automation of basic tasks and collaborative investigations.

7 **Detect and respond to unknown threats**

Find evasive threats like fileless malware and know exactly how to respond.

8 **Hunt threats proactively to check anomalies**

Our experts help you hunt for persistence mechanisms, threat actor tactics, anomalous user activity, anomalous network communications, and anomalous application usage.

9 **Incident response is included**

Incident response hours are included for added peace of mind.

10 **Protect your cloud deployments**

Use our cloud-native architecture to detect and respond to events from your AWS, Office 365, and Azure environments.

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Secureworks®