Crowe

Smart decisions. Lasting value.™

October 2019

Top 10 Reasons Why Your MSP Should **Not** Be Your MDR Provider

An article by C. Glen Combs

Cybercrimes are rampant, and smart businesses understand that it is not a matter of if – it is a matter of when – a cyberattack will compromise an organization. Many businesses understand the need to engage external parties to assist in navigating the complexities of a cyberattack, but they often don't understand the distinct ways in which each type of provider can contribute to cybersecurity protection.

Why MDR is different

Managed service providers (MSPs) provide basic services to monitor servers, firewalls, and other critical IT infrastructure and applications from a central location. MSPs have proven to be a cost-effective way of obtaining technical resources without having to attract and retain them directly. However, to provide these services in the most efficient manner, the depth of MSP services is vastly less specialized in cybersecurity and significantly less equipped to respond to and mitigate cyberattack costs.

In contrast, managed detection and response (MDR) providers offer:

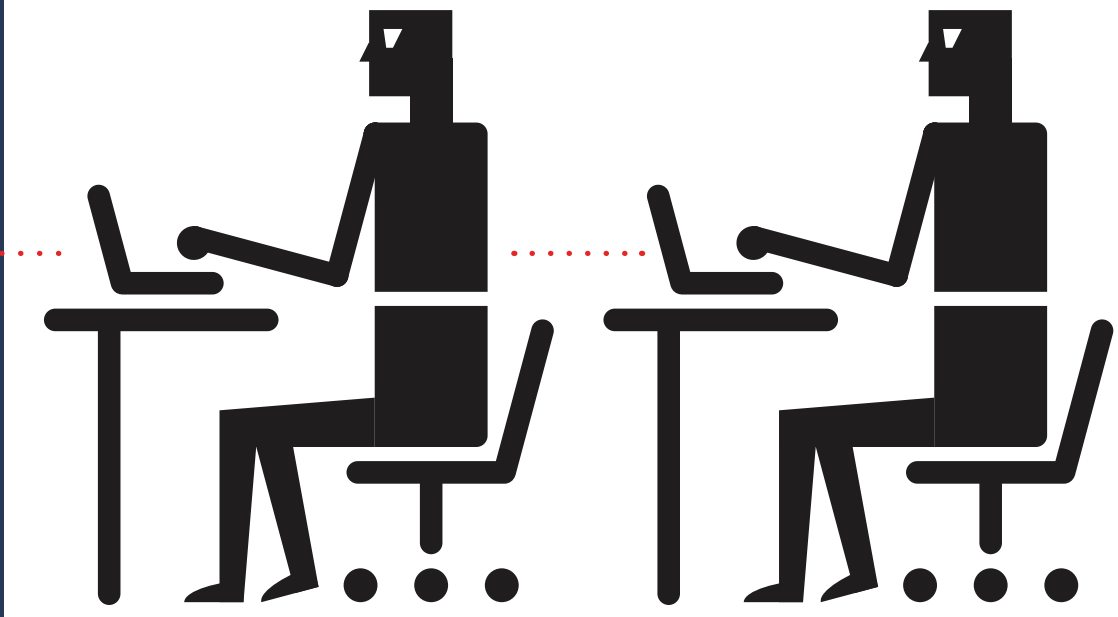
- 24/7 security operations
- Real-time detection
- Proactive threat hunting
- Customized threat detection
- Customized and automated playbooks
- Incident response and resolution support
- Post-breach investigation
- Cyberresilience benchmarks
- Program maturity insights

MSPs do not have the expertise or specialization to address cyberthreats in the ways that MDR providers can.

10 reasons why an MSP should not take the place of an MDR provider:

1. Security
2. Prevention & mitigation
3. Training
4. Technology
5. Surveillance
6. Detection
7. Nuance
8. Holistic approach
9. 24/7 coverage
10. Customization

Bonus 11. Accountability



1 SECURITY

MSP protection stops at operations, but MDR protection goes beyond operations to security resilience.

The job of the MSP is to keep the digital environment operating at its peak technical efficiency. But the job of an MDR provider is to monitor the business and digital environment for threats, detect them quickly, and respond in a prescribed manner.

2 PREVENTION & MITIGATION

An MSP focuses on end-user experiences, but MDR focuses on cyberthreat prevention, identification, and mitigation.

MSP professionals are focused on making technology work and making end users happy. On the other hand, MDR specialists are curious hunters. Their mission is to find issues that others cannot and to stop them before they damage the business environment.

3 TRAINING

MDR and MSPs have different training requirements.

MSP teams are composed of specialists in end-user and application support as well network design and operational engineering. MSPs generally have information technology and network administration educational backgrounds. The most competent MDR professionals acquire education that equips them to understand advanced threats, how to recognize them, and how to build security operation strategies that reduce the risk of successful attacks. In addition to specialization in cybersecurity, MDR professionals often have computer and data science backgrounds.

4 TECHNOLOGY

MSPs apply technology operationally, but MDR applies technology strategically.

MSPs focus on learning networking protocols, solution selection, operations, and keeping abreast of technologies that solve business operational problems. MDR focuses on big data analytics, artificial intelligence, and machine learning. Solid business processes are critical for both MDR and MSPs.

5 SURVEILLANCE

MSPs provide efficient operation, whereas MDR offers surveillance and detection aimed at secure operations.

MDR provides another set of eyes into an organization's environment. MDR surveillance is focused on identifying threats and providing real actionable data to the MSP whose responsibility is to use all information available to keep the equipment and processes up and running.

6 DETECTION

An MSP is a target for bad actors, but MDR is a watchdog.

MSPs are an increasingly popular target for attack because they hold complete access to most of their clients' systems. The MDR provider does not hold a level of access that can be threatened. Instead, the MDR solution is designed to help detect threat actors who want to access an organization's data and resources.

7 NUANCE

An MSP applies formulaic service, whereas MDR understands nuances.

An MSP focuses on certain business-critical applications and infrastructure to keep clients performing at a high level. The MDR provider learns what constitutes normal and abnormal behavior within a business and evaluates events through that lens.

8 HOLISTIC APPROACH

MSP services are à la carte. In contrast, MDR services are holistic.

MSPs provide basic log retention services at an additional fee and do not include the monitoring, detection, and response services organizations need for cyber protection. Many MDR solutions include the technology and processes necessary to assist organizations in meeting regulatory compliance requirements.

9 24/7 COVERAGE

MSP coverage is reactionary, but MDR provides 24/7 coverage.

Most MSPs do not have security specialists available after normal working hours. True MDR providers have analysts working around the clock, not analysts who are asleep until they receive a notification from a pager or call service.

10 CUSTOMIZATION

An MSP generally offers an off-the-shelf solution, reselling someone else's technology and sometimes even services.

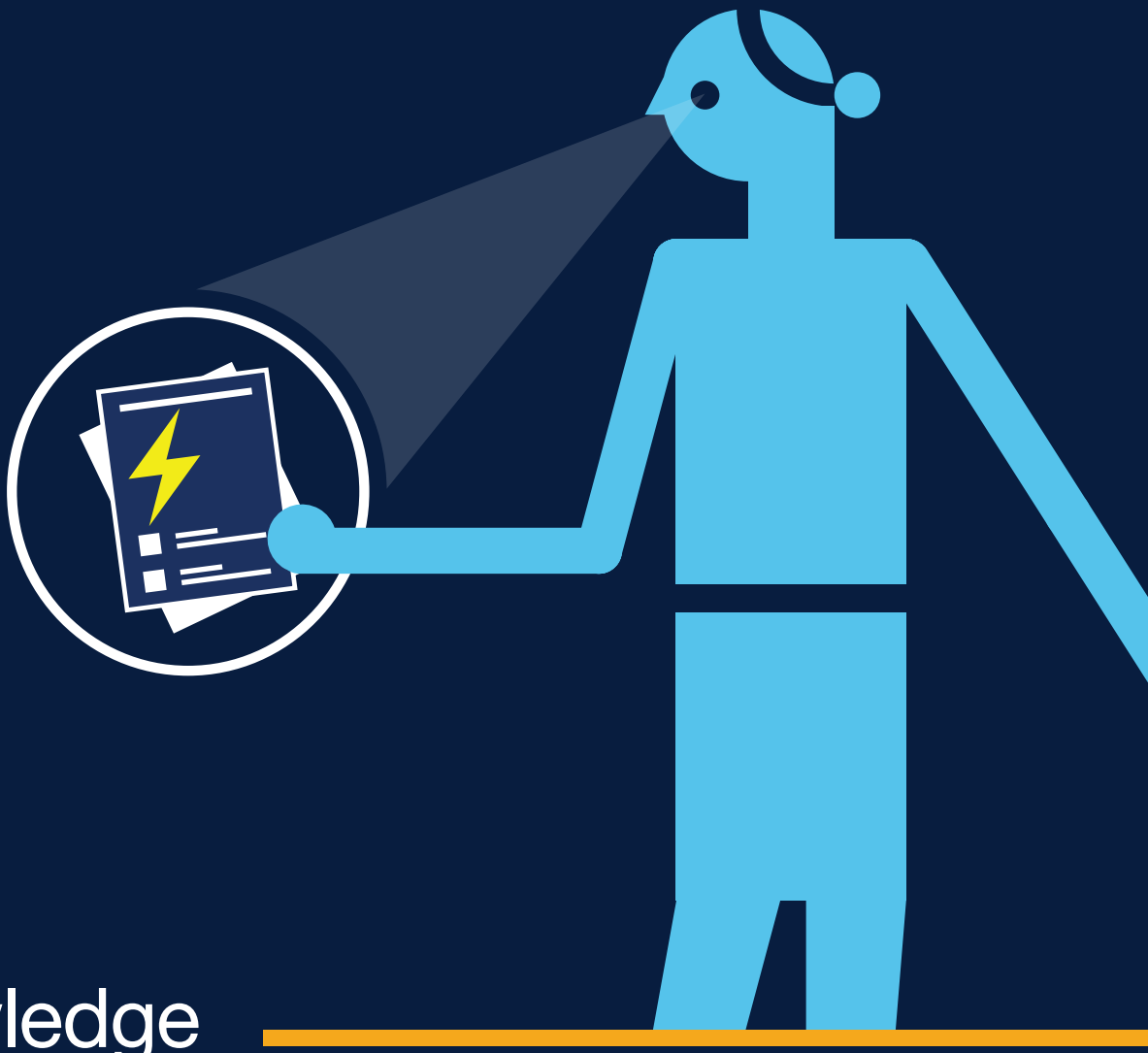
Customization is generally limited to "bending the rules" to support legacy client technology. The best MDR providers customize their solutions from day one – data that's ingested, threat detection rules and alerts, case management, and response services.

BONUS

11 ACCOUNTABILITY

Larger organizations generally separate their IT and security functions.

A contributing factor is the accountability offered by having a security team that is independent of those charged with architecting, maintaining, and supporting the technical infrastructure. Separating the MSP from the MDR function provides this same accountability to businesses that depend on outsourcing for one or both roles.



Acknowledge the “when”

Addressing gaps in cybersecurity protection should be a top priority for any organization. Learning more about how MDR can bridge those gaps can be one step toward strengthening defenses and mitigating damage when – not if – a cyberattack occurs.

LEARN MORE

C. Glen Combs
Partner
+1 859 264 3168
glen.combs@crowe.com

crowe.com

CC2062-010A