UNCOMMONX

4 Benefits of Hiring a Managed Detection and Response Provider

I hear from IT leaders constantly about issues they face trying to protect their organizations at a time when cyberattacks are growing and evolving at an exponential rate. One of the most significant challenges is they don't have the in-house expertise to combat the many threats coming at them on a 24/7 basis. They realize that tracking risks and fighting evolving threats is a round-the-clock job.

It takes a fully committed focus by experienced people who live and breathe cybersecurity working with the right technology to protect companies successfully. Except many midsize companies don't have the budget to hire (and rehire) and train full-time security teams or install the devices they need. Even if they could afford the optimal personnel, there is a severe lack of security pros available for hire today.

That's why companies are looking outside for help from security providers. Of those, managed detection and response (MDR) companies are proving to be the best option for many. Gartner defines an MDR as a company that provides "customers with remotely delivered modern security operations center (MSOC) functions. These functions allow organizations to rapidly detect, analyze, investigate, and actively respond through threat mitigation and containment. This process allows for investigation by experts skilled in threat hunting and incident management that deliver actionable outcomes."

Here are four reasons why organizations are choosing MDRs to be their remote

cybersecurity department.

1. Ready-to-go, cost-effective security teams

MDRs already have highly trained security personnel in place with knowledge in areas like threat hunting, endpoint management, ransomware, incident response, and security awareness/phishing. They can provide the exact scalable services you need in days, not weeks or months. They can also do much more for much less, eliminating the need to invest in in-house personnel (salary, training, benefits, office space, etc.) or costly security tools and licensing.

Partnering with a full-service MDR can also help you avoid the increasing costs of an attack. In a recent survey conducted by UncommonX, 80% of the respondents said they had to spend up to $249 thousand to recover. The remaining 20% shelled out between $250 thousand and $3.5 million. That doesn't even include the financial impact to your business due to lost revenue and a sullied reputation. Compared to those figures, the price of working with an MDR to prevent attacks in the first place is well worth the investment.

2. 24/7 customized full service when you need it

Even in today's security environment with ransomware attacks at the top of the threat list, some businesses still put security at the bottom of their priorities list. But many others understand the importance of full-time protection. They know that having a modern strategy to safeguard their organizations against threats and a plan to mitigate them once identified can often be the difference between surviving an attack or sifting through the digital rubble. That's the level of defense MDRs can deliver.

An MDR provider is responsible for staying up-to-¬¬date with the latest strategies for securing organizations of all kinds. The security tools they deploy and the people they hire stand as a fortress against threat actors. They also have the knowledge and expertise to stay up-to-the-minute on the current vulnerabilities and global hazards. This enables them to point out any gaps or shortfalls in your

infrastructure. Then they can provide guidance on what you and your IT team (regardless of size) can do to resolve your specific issues.

3. Faster response time is critical

Because they have their SOC staffed with the necessary experts around the clock, an MDR provider can detect, investigate, respond, and mitigate security incidents quicker than most in-house teams. They can view all portions of your organization (depending on the vendor), helping to understand the full nature of risks and threats in near real time.

Companies that utilize an MDR supplier will benefit from faster mean time to detect (MTTD) and mean time to respond (MTTR), able to resolve security incidents rapidly. MDR providers can coordinate responses, quarantine devices, and block hashes as needed. They can even focus on quickly identifying and mitigating threats before they arise.

4. Offensive versus defensive security posture

Instead of your IT team putting out fires and calling for an "all-hands-on-deck" response to incidents, your MDR provider can manage security situations, pulling you in at a time you have predetermined as ideal. They proactively manage ongoing threats compared to a managed services provider (MSP) that generally offers support only after an incident occurs.

Plus, because the MDR is monitoring and managing security situations full-time, your people won't have to. Instead, they're free to proactively focus on your company business goals and other important responsibilities.

To learn more about the benefits of managed detection and response providers, visit UncommonX.

UNCOMMONX

About the author

John Guzman is Sales Director for North America at UncommonX. His experience includes over 30 years of development of strategic sales plans, sales growth, and customer satisfaction/retention nationally and globally. He has over 20 years of security and cloud experience assisting Fortune 500 and Global 2000 clients and clients of all sizes build their network and infrastructure securely. He is an accomplished public speaker and published author. He has worked for industry leaders like AT&T, Verizon, Nuspire Networks, and Delta Risk/Motorola Solutions, winning multiple companies' President's Award for Sales and Service. He has consulted for KPMG and Accenture and holds multiple certifications in cloud infrastructure, sales, and security.

Contact Us Today, Be Safer Tomorrow

Talk to our experts today about your specific needs. Call **866-405-9156**, email us at **sales@uncommonx.com** or visit us at **uncommonx.com**.