CXO Insights

MDR vs MSSP

Choosing Managed Risk over Managed Tools

Businesses are continuously stepping up their cybersecurity readiness by adding in more and more tools and resources. Additional tools required more bodies to manage them, so SMBs and middle market enterprises - often budget and resource constrained - turned to managed security services providers (MSSPs) to reduce the strain. MSSPs could manage tools like anti-virus and malware protection, remote device management,and security information and event management (SIEM) configuration. This should free up analyst bandwidth, reducing the requirement to hire staff. **Sounds great, right? Unfortunately, there's more to consider.**

The Shift to MDRs

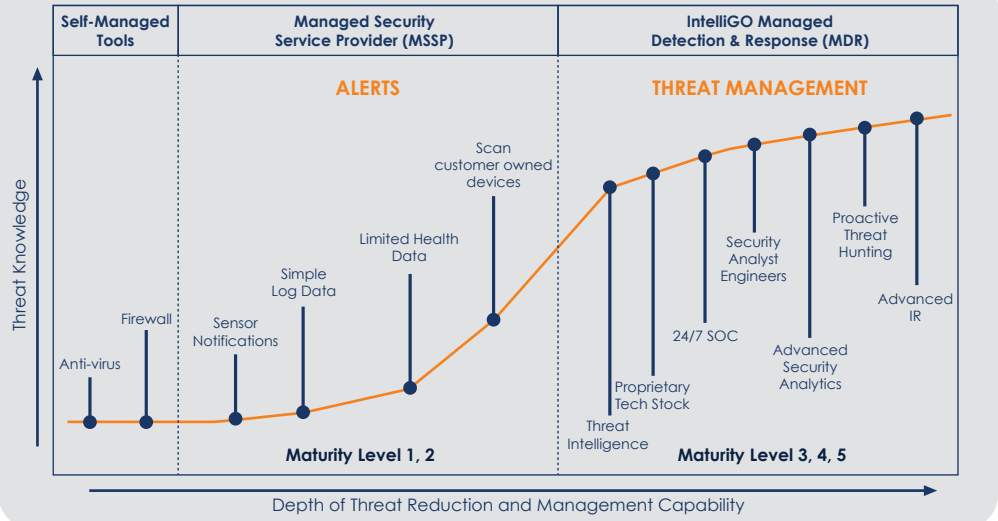
"Many buyers gravitate to the MDR providers because the response capabilities are a differentiator from many MSSPs."

2019 Market Guide for Managed Detection and Response Services

The debate over MDR vs MSSP is not a "Good vs. Bad" conversation. Rather, It's simply a discussion of desired outcome. Business customers are increasingly driven by a need for security outcomes, rather than simply outsourcing SOC operations. They are less willing to trade off security strategy for the endless alert reporting or poor response time they get from MSSPs. Enter Managed Detection and Response (MDR) services. MDRs now compete to provide industry-leading technology, paired with threat hunting and analysis expertise - merging people, processes and technology. As illustrated below in Figure 1, MDRs go well beyond the scope of MSSPs, providing a greater lens into the threat landscape, a better way to manage risk, and an increased focus on strengthening customers' security posture.

MSSPs in MDR Clothing

You might be asking, "My MSSP is now offering MDR services, isn't that enough?" While some MSSPs now claim to offer MDR services, they remain primarily focused on alert management, and usually don't have their own technology. This burdens them with largely fixed costs, and limits their detection and response capabilities. Some do now offer Endpoint Detection and Response as an extended capability, but these are again largely an integrated not owned tool, so the MSSP has little expertise in the solution.



Pure-play MDRs, go well beyond the boundaries of endpoints, analyzing events from other common attack vectors like network and cloud. They eliminate MSSP blind spots in threat intelligence, And, perhaps surprisingly, are a more cost-effective option.

By the Numbers

Finding the right balance between manageable and value-added when it comes to handing your security can be a challenge. There are many concerns about privacy, capability, and scalability. Cost needn't be one of them. Let's compare the costs of securing 500 endpoints with an MSSP (with bolt-on MDR components) to an MDR - We'll use best known approximate annual costs based on previous projects and market intelligence.

Resource	Outsource to MSSP	IntelliGO MDR
Security Operations Centre (SOC) Leader / vCISO	$6,518	$4,000
Managed Detection and Response	$0	$42,900
24/7 Analysts	Usually Included	Included
Threat Hunting / Endpoint Security Analyst	Usually Included	Included
Vulnerability Management	$21,000	Included
Threat Intelligence Feeds	$18,900	Included
Endpoint Detection & Response	$83,940	Included
SIEM (Log Management Fuctionality)	$53,940	Included
Total Estimated Costs	**$184,298**	**$46,9000**

Note: Figures presented are in US dollars, on a 1-year contract for 500 endpoints. Includes optional IntelliGO vCISO service. Model does not include optional Incident Response.

MSSPs cost up to 4X more than MDR, with less capability

MDRs give you a full complement of analysts, threat hunters, and tools, so that you can focus on essential staffing only - saving you considerable

You need more than one threat intelligence feed

MSSPs typically offer a single threat intelligence feed. Supplemental feeds can easily run more than $100K/yr. MDRs use multiple feeds to get you the highest fidelity, and all for one affordable price.

Built-in capability is better than bolt-on features

MSSPs ultimately bring a patchwork of disparate tool management solutions for aleting. MDRs are simply more advanced not only at reporting verified threats, but containing and remediating them.

Want to improve your threat management and security posture? Start now, with IntelliGO Managed Detection and Response.

Toronto Headquarters
207 Queens Quay,
Suite 820
Toronto, ON, Canada M5J 1A7

Seattle Office
925 4th Avenue, 20th Floor
Seattle, WA 98104

Menlo Park Office
2882 Sand Hill Road, Suite 115
Menlo Park, CA 94025

1 (855) 917-4981
info@intelligonetworks.com