CyberMaxx

WHY A PURPOSE BUILT MDR IS THE ANSWER TO YOUR INTEGRATION CHALLENGES

Even best of breed security products and systems are extremely complex to manage. Without proper orchestration, you could be wasting valuable company resources on solutions that aren't working together, ultimately leaving your organization vulnerable.

WHY BEST OF BREED SOLUTIONS FALL FLAT WHEN IT COMES TO ORCHESTRATION

In the mid-2000s, many IT security shops went out and bought the best of breed for each area of need in their respective security domains (firewall, IPS, SIEM, endpoint monitoring, and AV technologies, etc.) The general idea was to ensure the very best was protecting their subsequent corners of the world. This thought process is still prevalent today throughout many organizations, both small and enterprise. While the approach has some intuitive benefits, it also has many drawbacks, especially today when there are so many different security tools required to ensure complete visibility and enforcement capabilities in all IT security facets. This trend has accelerated even faster with the adoption of IAAS and SAAS services that add another complexity level to the mix. Lack of integrations, orchestration, and siloing of capabilities and subsequent knowledge between security products and systems became apparent, leaving organizations taking this approach vulnerable and overwhelmed.

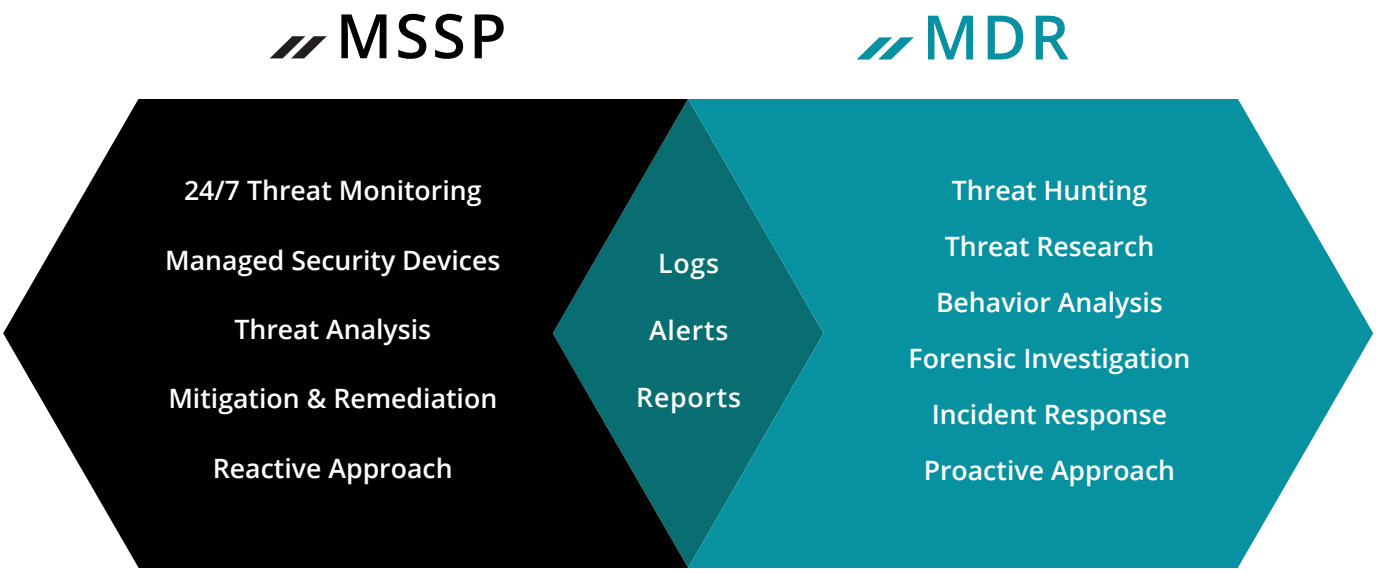
USERS CAN'T SUSTAIN TWO SYSTEMS NOT DESIGNED TO INTEGRATE

Eventually, manufacturers caught on to this and started trying to buy up adjacent security products with the idea they could integrate them, which worked with varying degrees of success. Other companies partnered with adjacent companies' products to try and build out integrations. For example, a SIEM solution might integrate with a firewall to automatically create a security rule based on a SIEM event.

Both of these approaches, while having many benefits, often fell short. The root of this problem is if two systems are not designed from the ground up to integrate, then doing so after the fact becomes next to impossible to sustain. There are several reasons why these integrations did not work well, but it was primarily due to updates and format changes that occur during any product's software lifecycle; what these companies once orchestrated eventually broke due to updates. These issues created a need for a more coordinated integration path.

MSSPs essentially offered to offload some of the requirements for customers to manage what had become an unwieldy security initiative of having an orchestrated security practice. They then tried to scale that process out to hundreds and sometimes thousands of companies. Traditional MSSPs suffered from the same fate as many of their customers—they took the same approach of trying to marry different vendors' products together in an orchestrated fashion. A tighter coupled solution was required to scale and allow for tailored security fit for each customer.

With companies asking for a proactive and interactive posture from their MSSPs, MDR (Managed Detection and Response) solutions formed and created the concept that an MSSP was an extension of an organization's security team. Instead of just telling a customer there was an incident, an MDR will proactively seek avenues of attack and indicators of an already active breach, as well as remediate the problem. While this approach has merit, the same limitations on the solution's efficacy will be present if the MDR does not have a well-thought-out and orchestrated security platform.



HOW PROPRIETARY SOLUTIONS SET MODERN MDRS APART

Modern MDR solutions often take a different approach of custom building many of their tools to allow for manageable integrations and orchestration capabilities—tools built to work together collaboratively and protect organizations from all sides. Extending orchestration capabilities to both monitoring and enforcing is vital to any successful MDR solution. The more automation on the backend, the faster the MTTR an incident will be. This speed is critical, especially to healthcare organizations that experienced a 470% increase in ransomware attacks from 2019 to 2020, impacting more than 18 million patient records. To truly create a custom security solution for each customer, orchestration is an absolute requirement. When talking with an MDR provider, one of the first questions to ask is if the provider has a custom-built platform or if they opted for a best-of-breed approach that has not played out well historically.

For more information about MAXX MDR, CyberMaxx's combination of three proven technologies that drive deeper analysis and more proactive prevention, visit **CyberMaxx.com/maxx-mdr** to learn more and schedule a call.

ABOUT CYBERMAXX

We built CyberMaxx with one goal in mind: to be the industry's leading trusted partner in preventing, detecting, and responding to cyber attacks.

We're proud to provide a team of leading cybersecurity professionals focused solely on protecting our customers 24/7/365. When evaluating cybersecurity vendors, we know that the team members you'll work alongside matter. That's why we're passionate about serving as your trusted partner and extension of your security team.

With more than 15 years of experience, we've discovered that there are three areas of focus that must be preformed with precision in order to prevent, detect, and respond to cyber attacks effectively. This approach is based on the equal importance of three distinct pillars of cybersecurity: people, process, and technology.