MSPs: 5 Tips for Assessing XDR Solutions

The ability to quickly uncover and control threats that put your customers at risk has never been more critical. Extended detection and response (XDR) collects and automatically correlates data across multiple security layers—so you can see more and respond faster.

1. Identify Solutions With **Broad Coverage**

In order for managed service providers (MSPs) to ensure their entire customer base is secure, they need complete and holistic coverage. When identifying potential XDR vendors, MSPs should look for solutions that can:

- Correlate several vectors like endpoint, email, server, and network. Ensure that full activity data is being collected—not just alerts or detections.
- Deliver the full scope of detection, investigating, and response features across all layers. Robust cross-layered detection rules/analytics can detect threats that the individual layers cannot.
- Take action for other areas directly from the console. Ask if investigation views and response actions are still siloed to the endpoint.

2. Choose the **Right Fit** for Your Customer's Environment

Select a fully integrated XDR threat-defense solution that has the flexibility to fit within and augment the current ecosystem. An XDR solution must always add value to existing process and workflows and should allow MSPs to reduce blind spots, increase efficiencies, and implement immediate controls to improve the time to detect and respond.

3. Remember: **Less is More**

Your security team is bombarded with thousands of alerts every day, making it difficult for them to decide what's important and how alerts are related. Choose an XDR solution that can offer fewer, but more cohesive and high-confidence alerts that allow analysts to quickly understand critical detections, the scope and severity of the attack, and act immediately to neutralize the risk.

4. Select a Solution That **Scales With Your Business**

Not all XDR delivery models are created equal. When evaluating vendors, look for providers that allow your organization to easily extend and adjust detection and response support to the layers that are most important to you. At any given time, your customers may have changing security requirements or a desire to adjust priorities—your XDR vendor should be able to serve those needs.

5. Invest in the **Vision**

It's vital to look beyond the flashy technology claims and consider the nuances to determine the true threat detection and response value of an XDR offering. Finding an XDR solution that leans more toward "partner," not "vendor", with a solid long-term vision and ability to identify the who, where, and why of an attack will empower you to defend your customers with confidence and speed.

Next steps

Want a solution that's tailor-made for MSPs and checks each box? Check out **Trend Micro™ Worry-Free™ Services** and discover how you can start to see more and respond faster.

[IG00_5 Tips For Assessing XDR_Solutions_WF_MSP_210518US]

TREND MICRO™