CHECKLIST

Ten Considerations to Help You Choose the Right Managed Detection and Response (MDR) Provider

Implementing endpoint detection and response (EDR) capabilities will help your organization to improve the security of your network. But do you have the time, budget, or around-the-clock resources to effectively manage the technology? Working with a managed detection and response (MDR) provider will help to ensure that you're covered, even if it's just for the first year that you have EDR technology in place.

Use an MDR provider for improved endpoint security to:

- Orient to this new way of approaching endpoint security versus using traditional antivirus (AV) capabilities
- Familiarize your team with the right tuning needs for your specific applications, and help them learn how to recognize the malicious use of otherwise legitimate applications
- Get on-the-job training from experts in an OpEx model if you plan to ultimately manage EDR in house
- Have 24×7 dedicated security expert coverage so that your own team can focus on the most strategic priorities
- Understand and accurately interpret the context of various threats and alerts
- Learn from experts on how, why, and when to conduct threat hunting

When you're ready to select an MDR provider, consider the following questions to ensure you're choosing the vendor that best meets your needs:

- ☑ Will the vendor provide accurate tuning, adjusting your policies as needed so that they're neither too lax nor too restrictive?
- ☑ Can they act as an extension of your team and provide human-based analysis and monitoring?
- ☑ Are they readily available to respond to your questions about alerts, threat actor activity, or anything else related to the security of your environment?
- ☑ Is the vendor equipped with more extensive security expertise to analyze, contain, and remediate when you're ready to collect, normalize, and correlate data across your security controls?
- ☑ Do they have an established process that allows you to choose how much or how little control you want to have over your day-to-day EDR operations?
- ☑ Do they have expert threat hunters on staff?
- ☑ Do they have a threat intelligence capability that gives you both insights about the latest threat actors and emerging tactics, techniques, and procedures (TTPs) to inform threat hunting and detection strategies?
- ☑ Do they offer an incident response retainer service?
- ☑ Do they offer proactive readiness services to help you ensure that your processes are updated and that the right people have the correct training?
- ☑ Do they offer exposure management services that help you more broadly understand your risks and address any gaps?

It's crucial to choose the right MDR provider to ensure you get the most from your new investment while maintaining and improving the security of your entire network.

Have additional questions about what to look for in a provider? Send us a note today.

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

March 3, 2023 2:03 PM
1850517-0-0-EN