SOLUTION BRIEF

Hasten Endpoint Protection with the Fortinet Managed Detection and Response Service

Augment Your Capabilities and Efficiently Protect Your Endpoints

It's no secret that every security and IT practitioner's to-do list keeps getting longer as the threat landscape grows increasingly complex. Combined with the ongoing cybersecurity talent shortage, new demands from cyber insurers, and other hurdles, organizations have numerous challenges to manage.

At the same time, there are core technologies and processes that must be used to effectively protect your endpoints. To take full advantage of the technologies you've deployed, such as an endpoint detection and response (EDR) tool, you need time to fully understand the technology, tune the solution, and monitor the alerts generated. While this may sound straightforward, these activities require ample time and advanced knowledge, both of which are often in short supply among small and overburdened IT and security teams.

That's why many organizations rely on Fortinet Managed Detection and Response (MDR) Service to augment their internal capabilities with a new level of security expertise and protection. Whether it's tuning your technology, understanding your environment in order to address anomalous activity, conducting ongoing monitoring, or performing threat hunting based on the latest threat intelligence, our 24×7×365 MDR service helps keep your organization safer. Our MDR experts can also respond to alerts on your behalf, if desired, or we can advise your team on the proper next steps to take. You choose the level of our team's involvement.

Get Quick Protection from Your EDR Technology with Our Experts

As is the case when deploying any new technology, it takes time and expertise to take full advantage of an EDR deployment. Your staff needs to learn how to accurately tune the tool to balance user access with the right level of protection, and then needs time to understand and assess the context of alerts to determine the appropriate next steps. Many businesses that adopt EDR for improved endpoint protection don't have the level of resources needed to run and maintain the technology, and, in many cases, they don't have the ability to hire new practitioners or make time for an existing team member to complete necessary trainings.

EDR works differently than traditional antivirus solutions, yet having this type of protection across your environment is table stakes as the threat landscape grows increasingly complex.

Many businesses incorrectly assume that they can seamlessly move from one solution to the other, using the same staff to do what is thought to be the same level and type of work. But the solutions approach endpoint security differently, which is why there's often a sizeable learning curve when implementing an EDR tool.

"Misconfiguration and mismanagement of workload and endpoint security tools can increase the attack surface, hinder operational effectiveness, and lead to security breaches."[1]

"MDR providers help security teams reduce the inherent asymmetric advantage attackers operate with by enhancing the security team's ability to protect the customers, employees, partners, suppliers, and investors that make up their business ecosystem."[2]

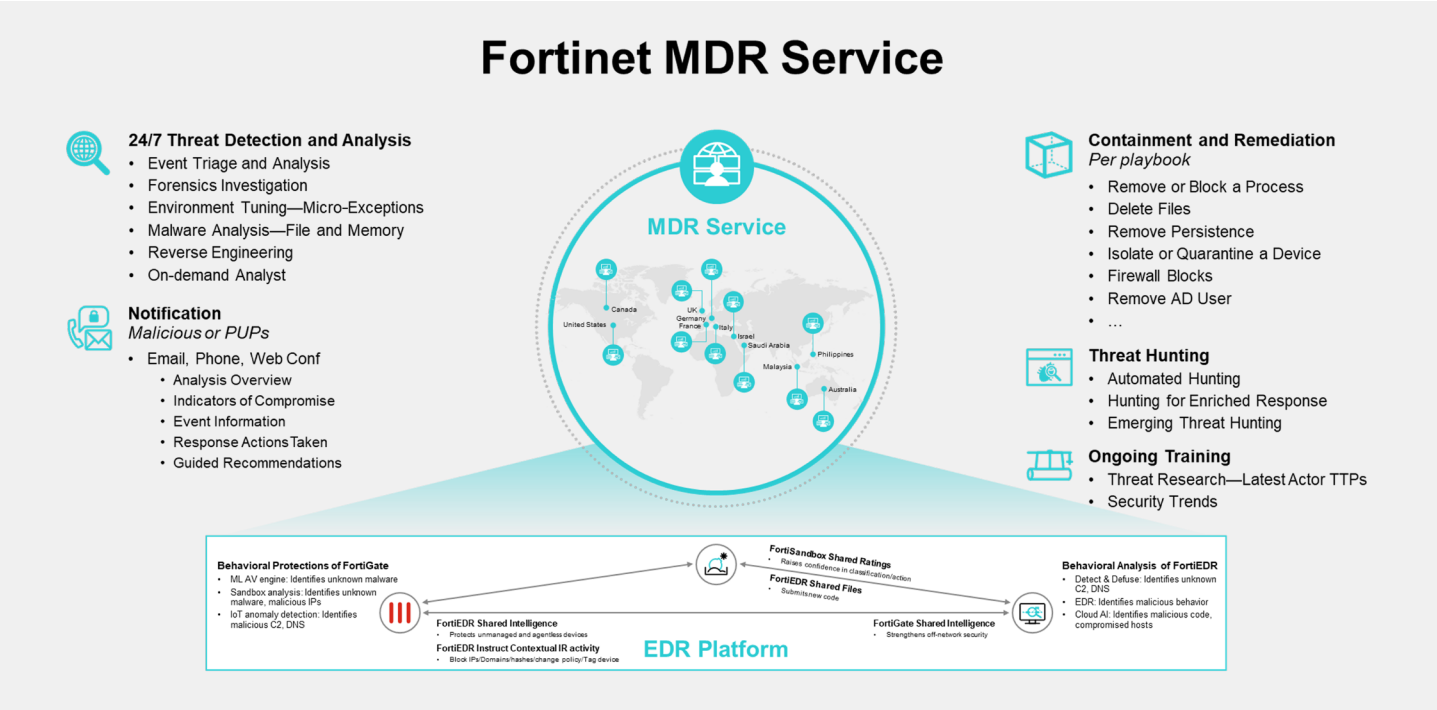
Today's attackers are using legitimate business applications to hide their tracks and operate in plain sight within your network, making strong processes and ongoing EDR tuning crucial to risk management. This means that you must have disciplined processes of logging unusual application behavior and recognizing how to tune your EDR solution to accommodate your users, all while ensuring your organization is secured. EDR also offers additional powerful benefits, such as the ability to enhance threat hunting. However, most businesses don't have the resources in house to take full advantage of EDR technology. To deploy this new technology quickly and effectively and begin seeing the benefits of it right away, many business leaders turn to an MDR provider to augment their internal capabilities.

Embrace MDR Services to Fully Protect Your Endpoints

For practitioners who want support with activities such as monitoring and triaging an incident, conducting playback analysis to understand and fix security gaps, and tuning their environment, an MDR service is the optimal choice. The Fortinet MDR Service offering provides you with all of this and more so that your IT and security professionals can focus on more strategic priorities.

Fortinet MDR Service provides five key services that work in conjunction with your existing FortiEDR or FortiXDR (extended detection and response) deployments:

- **24×7×365 threat detection and analysis:** Leave it to our MDR team to do your environment tuning, setting any micro-exceptions needed to balance usability and security. Managed detection and response experts conduct event triage and analysis, as well as malware analysis, reverse engineering, forensics investigation, and on-demand analysis.
- **Threat hunting and analysis:** Our threat hunters are experts at their craft, looking for malicious activity and emerging or trending threats. Embracing threat hunting offers organizations an additional layer of protection, yet most teams don't have time for this important activity.
- **Containment and remediation:** Our MDR service contains threats as they're discovered. Knowing that organizations have different needs, these containment actions are predetermined with you and your team when we kick off our service. The division of responsibility is codified in playbooks developed in partnership with your staff. The MDR expertise provides guided remediation of actions to take, both short- and long-term. Containment actions can include (but are not limited to) removing or blocking a process, deleting files, removing persistence, isolating or quarantining a device, or removing a user.
- **Notifications and recommendations:** The team provides escalations to you for any suspected malicious activity, along with an expert analysis of the threat. With each notification, you'll receive the indicators of compromise, event information, response actions taken, and recommended next steps.



- **Forensic requests:** When you need clarification on something our team has observed and reported or you want us to analyze malware, files, or scripts, you're able to open tickets for forensic requests. Our team acts as an extension of your own, and they anticipate such requests.

Fortinet MDR Service Outcomes, Benefits, and Differentiators

Many MDR providers leave it to you to tune appropriately while they merely monitor your product for alerts, while others charge extra for threat hunting. Our comprehensive MDR service does all of this for you, providing you with a single vendor directly responsible for your FortiEDR platform with one comprehensive service to manage it all. With the Fortinet MDR Service, you'll get:

- Swift time-to-protection with expert analysis and containment
- Optimization of scarce team resources
- Cost predictability
- Ongoing product tuning to balance usability and security
- Proactive protection with skilled threat hunting
- Faster team onboarding, when desired

"Rapid growth in tools like endpoint detection and response [...] reveals the understanding that educating employees isn't sufficient to protect against hacks—you need to find advanced solutions to counteract new attack techniques."[3]

In addition to the above, the right MDR provider can offer complementary incident readiness services through proactive activities. These services can help develop your incident response plans and keep your organization secure from and ready to respond to ransomware and other common attacks. The Fortinet MDR and FortiGuard Incident Response (IR) teams work together in a symbiotic way that's advantageous to your enterprise. We have the ability to provide a one-hour turnaround to cyber incidents found elsewhere in your network—all from the provider already familiar with your network.

Get Maximum Flexibility with Our MDR Service

Fortinet offers maximum flexibility for customers by offering our MDR services by the hour. For organizations already using FortiEDR or FortiXDR that are unsure about making a long-term investment in an MDR offering, this is a helpful way to test the value and effectiveness of the service in order to justify the budget for such a service. Organizations that are just getting started with a new technology such as FortiEDR can also take advantage of this hourly service to help onboard and train the team, tune the technology, implement the right level of endpoint protection, or augment threat hunting or analysis capabilities.

Conclusion

As ransomware continues to proliferate and cyber insurers mandate new requirements in order to achieve coverage, organizations of all shapes and sizes must adopt EDR in order to enhance their security strategy. Adopting new security tools doesn't need to stretch your resources to their limits. By using the Fortinet MDR Service to manage your FortiEDR or FortiXDR deployment, you'll gain more robust security, faster and more comprehensive endpoint protection, greater peace of mind, and more flexibility for you and your staff members to focus on your organization's most strategic priorities.

[1] Peter Firstbrook and Chris Silva, "2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms," Gartner, December 31, 2022.

[2] Jeff Pollard, et al., "The Managed Detection and Response Landscape, Q1 2023," Forrester, January 30, 2023.

[3] "How Enterprises Plan to Address Endpoint Security Threats in a Post-Pandemic World," Dark Reading, February 2022.

FORTINET

www.fortinet.com

March 30, 2023 2:08 PM
2032137-0-0-EN