SOLUTION BRIEF

FortiResponder Services Turn Alerts Into Actions

Executive Summary

Due to advancements in the threat landscape, security breaches are inevitable. At some point, every organization is faced with a security incident that needs investigation, a response, and/or remediation. Even worse, a surprising number of organizations may already have active threats operating inside their network. Beyond threats growing in volume and sophistication, security operations teams lack the skill sets to identify and address network breaches—not to mention face an acute cybersecurity skills shortage. Fortinet offers security leaders two types of incident response services—FortiResponder Managed Detection and Response (MDR) Service and FortiResponder Incident Response Service—that enable them to turn security alerts into real action. These two services enable security operations teams to stop breaches and to improve incident detection, investigation, and response capabilities, which in turn reduce operational costs and disruptions.

Mapping the Right Response to the Threat Landscape

The evolution of the threat landscape—volume, velocity, and sophistication—makes it increasingly difficult for security operations teams to monitor threats, triage alerts, proactively hunt for threats, and respond to incidents. Security leaders, as a result, need to be able to:

- **Prepare to respond to advanced threats.** Successful security compromises are inevitable, regardless of the security solutions an organization has implemented. As a result, security leaders must have incident response processes in place that reduce the impact and costs of security incidents.
- **Find the right security expertise.** There is a significant cybersecurity skills shortage. It is exacerbated as a result of the growth in security tools that organizations use, as well as a threat landscape that is increasingly more advanced. As a result, staff in the security operations center (SOC) are overstretched and lack the skill sets needed to address these new challenges.

The global cybersecurity workforce needs to grow 145% to meet the demand for cybersecurity talent.[5]

- **Reduce the mean time to detect and respond.** It takes an average of 197 days before a breach is discovered, and 69 days to contain it.[1] As cyber criminals often begin to exploit data in days, hours, or even minutes, these response times create huge risk exposures. Bandwidth-constrained security operations teams need help to identify and respond to these breaches.
- **Deal with information overload and alert fatigue.** Security professionals face too many events and alerts. Indeed, on average, a security analyst can realistically investigate 20 to 25 alerts in a standard workday.[2] But with the average organization's SOC receiving over 10,000 alerts per day, organizations simply cannot keep pace.[3] It makes sense that nearly 40% of security leaders list missing threats and attacks as their top challenge.[4] All this amounts to a huge productivity drain and distracts from threat-hunting activities.

FortiResponder Services: An Extension of Your Team and Technology

To help security leaders address these challenges, Fortinet offers **FortiResponder Services**. FortiResponder Services enable organizations to achieve continuous monitoring as well as incident response and forensic investigation.

The FortiResponder Services team is staffed with professionals who possess years of training and experience in malware hunting and analysis, reverse engineering, multiple scripting languages, forensics, incident response processes, and the tactics, techniques, and procedures of bad actors. FortiResponder is available as two separate services:

FortiResponder Managed Detection and Response (MDR) Service

The FortiResponder Managed Detection and Response (MDR) Service is designed for customers of the FortiEDR advanced endpoint security platform. FortiResponder MDR provides organizations with 24x7 continuous threat monitoring, alert triage, and incident handling by experienced analysts and the platform. FortiResponder MDR is designed to help organizations defeat even the most advanced attacks.

In order to do so, Fortinet focuses on monitoring the alerts produced by FortiEDR for customers. This team of threat experts reviews and analyzes every alert, proactively hunts threats, and takes actions on behalf of customers to ensure they are protected according to their risk profile. Additionally, the FortiResponder team provides guidance and next steps to incident responders and IT administrators.

Some of the key capabilities of FortiResponder MDR include:

- **24x7 monitoring and response.** This around-the-clock coverage helps customers' security teams focus on more strategic tasks.
- **Alert triage with guided response.** The FortiResponder MDR team supplements a customer's SOC team, acting as senior SOC analysts for customer SOC teams.
- **Guided remediation instructions** as well as remote remediation and rollback.

FortiResponder Forensics and Incident Response Service

While many incidents can be addressed by FortiEDR and the FortiResponder MDR Service, sometimes organizations will need more customized services, which are available through FortiResponder Forensics and Incident Response Service.

The FortiResponder Forensics and Incident Response Service assists customers with the analysis, response, containment, and remediation of security incidents to reduce the time to resolution, limiting the overall impact to an organization. In addition to serving FortiEDR customers (whether or not they have subscribed to the FortiResponder MDR Service), FortiResponder Forensics and Incident Response Service can also help organizations that have not deployed FortiEDR for specific incident or breach investigation.

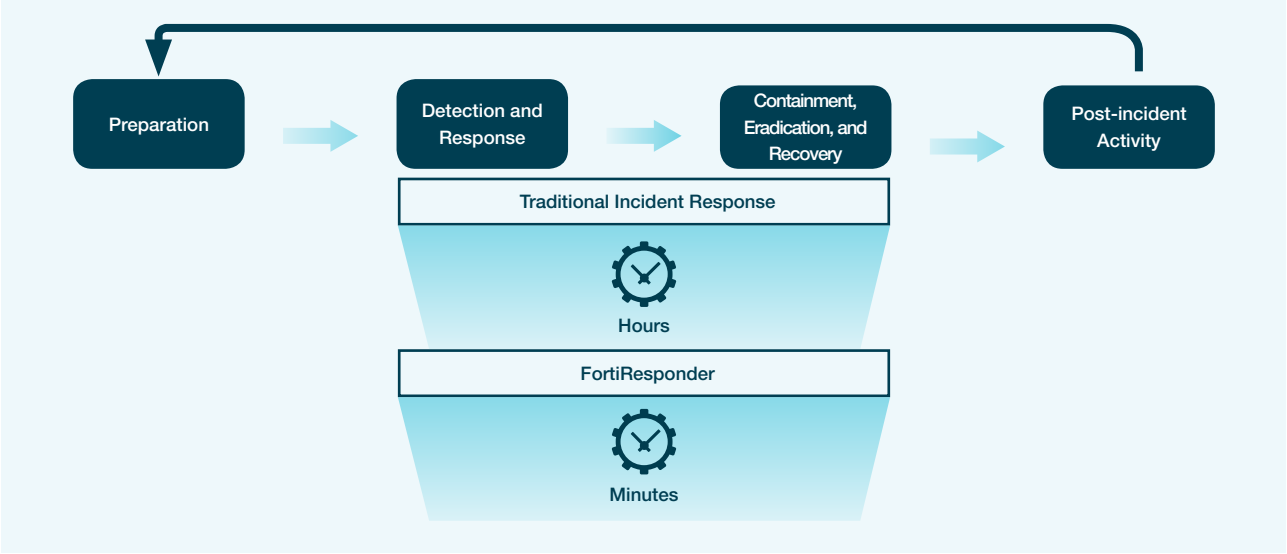

Figure 1: FortiResponder Services transform traditional incident response from hours to minutes.

Key Benefits of FortiResponder Services

Organizations needing to accelerate their SOC maturity benefit from the combination of advanced endpoint security delivered through FortiEDR and FortiResponder Services; they get 24x7 coverage and the ability to scale existing SOC resources. In doing so, they can better respond to threats, operationalize incident response processes, and avoid alert fatigue without worrying about missed detection. These services lend bench strength to the SOC team, enabling junior SOC personnel to take on more sophisticated tasks so that organizations can do more with the talent they already have in place, addressing threats and bad actors. In addition, daily coverage from an external provider gives overextended security teams an essential backup, enabling them to scale while reducing mean time to detect and respond.

[1] "Cost of a Data Breach Report 2019," Ponemon Institute and IBM Security, April 2019.

[2] Moazzam Khan, "Security Analysts Are Overworked, Understaffed and Overwhelmed—Here's How AI Can Help," Security Intelligence, July 13, 2018.

[3] "How Many Daily Cybersecurity Alerts does the SOC Really Receive?" Bricata Blog, October 2, 2018.

[4] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[5] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019, (ISC)², accessed January 9, 2020.

Copyright © 2020 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. 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.

January 15, 2020 1:45 AM

575788-0-0-EN

D:\Fortinet\Solution Briefs\teal solution briefs\FortiResponder\sb-FA-fortiresponder-services-turn-alerts-into-actions\sb-FA-fortiresponder-services-turn-alerts-into-actions