FACT SHEET

FortiGuard Managed Detection and Response Service

Introduction

Fortinet boasts one of the largest security research and analyst teams in the industry with over 215 expert researchers and analysts around the world. For many years our dedicated experts have continuously been on the lookout for breaking threats and new tactics, techniques, and procedures of the threat actors—studying every critical area of the threat landscape including malware, botnets, mobile, and zero-day vulnerabilities. Leveraging that vast experience and expertise, Fortinet is offering to its customers a Managed Detection and Response (MDR) Service. This 24/7 service provides organizations with continuous monitoring, alert triage, threat hunting, and incident handling by our team of experienced analysts and the FortiEDR Platform.

An add-on service to FortiEDR, FortiGuard Managed Detection and Response Service focuses on monitoring the alerts and suspicious threats detected by FortiEDR. The goal is to ensure all customer alerts are acknowledged and addressed accordingly. 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 FortiGuard team provides guidance and next steps to incident responders and IT administrators. The following is a list of activities delivered as part of the MDR service.

Service Features and Deliverables

Continuous Threat Detection and Analysis

Our team of experts will work around the clock to monitor and hunt for threats and analyze events that may have entered your environment, leveraging alerts from the FortiEDR Platform. Activities include but are not limited to:

- Analyzing malware both static and dynamic
- Analyzing memory for malicious processes
- Identifying potential vulnerable and unwanted programs
- Environment tuning—setting micro exceptions for clean applications
- Retrieval and analysis of additional forensic artifacts such as:
  - Windows Event Log Records
  - AmCache File
  - Host File
  - Scheduled Task Log File
  - Browsers Artifacts

Containment and Remediation

Once a compromised host(s) has been identified, the FortiGuard team will provide the initial tactical containment options with the goal of isolating the threat without impacting business operations. These options leveraging the FortiEDR technology can include:

- Stopping a process from writing to the disk
- Blocking communications to another device

Benefits

Organizations needing to accelerate their SOC maturity benefit from the combination of advanced endpoint security delivered through FortiEDR and FortiGuard Managed Detection and Response Service; 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.

- Accelerate SOC Maturity
- Scale the Existing SOC
- Reduce Analyst Burnout

Some of these containment options may already be automated through our technology IR playbooks. If not, the team can assist with additional configurations with playbooks as well as group/security policies.

In addition, based on our threat analysis we will provide guidance for remediation steps, which can include both tactical and strategic steps. Some short-term options that can be both manual and automated are:

- Terminating a process
- Removal of a file
- Removing persistency from the registry

Reporting and Alerting

Our team will ensure you have the right information to make educated decisions about security issues we discover. Every security event that is triggered by our FortiEDR technology is handled within 24 hours. If the issue is critical, we will respond appropriately. Once the event is analyzed, the team will send an incident email notification explaining the threat and recommendations for review and/or remediation steps.

Customers may also escalate a request for more information and/or guidance about an incident or event through email. Our team of experts are available 24/7 to assist with those requests. Depending on the criticality, the communications can be via phone or web conference call.

As the engagement progresses, customers may want to know more about their environment regarding the platform health and/or specific threats or trends. Annually our consulting solution architects and our FortiGuard team will provide an environment assessment. This assessment can include:

- Device coverage and FortiEDR license usage
- FortiEDR platform health
- Malware and vulnerable or unwanted program findings
- Overall threat trends and recommendations
- Process questions and issues
- Address remediation issues as needed
- Address training requirements as needed

Training

As part of the onboarding process, our team of experts will conduct an initial training focused on how to review and analyze events within the FortiEDR Platform.

Eligibility and Purchasing

The service is available for purchase by authorized Fortinet resellers and distributors globally. The service is delivered to the customer or end-user of Fortinet products as referenced in the purchase order placed with Fortinet by a customer or Fortinet authorized partner or distributor.

The service may be purchased through FortiEDR bundles or as a stand-alone add-on to FortiEDR. The service is priced per endpoint for the entire endpoint estate protected by FortiEDR.

Unit	SKU	Description
Managed Detection and Response	FC1-10-FEDR0-340-01-DD	FortiGuard Managed Detection and Response Service, 1-year: 24x7 threat monitoring and incident triage email notifications, on-demand reports, guided remote remediation, orchestrated response playbook setup