SERVICE DESCRIPTION
FORTIEDR™ & MDR SERVICES

1. Introduction

FortiEDR™ Services are available to the end-user (the "Customer") as two (2) lines of service:

- FortiEDR is a cloud-based software as a service, which provides an end-point protection platform, based on alerts communicated by collectors deployed in the Customer's network (the "FortiEDR Service"). The FortiEDR Service delivers threat protection both pre- and post-infection in real time. The FortiEDR Service incorporates techniques to: prevent malware infection, detect and defuse security threats and to provide automated response and remediation with customisable playbooks.
- The FortiResponder™ Managed Detection and Response Service adds alert management with the aim to assure all customer alerts are acknowledged and addressed accordingly ("MDR Service"). The MDR Service provides round the clock monitoring in order to provide protection for the Customer's risk profile. For malicious alerts, Fortinet will actively contact the Customer to provide guidance to mitigate the threat.

2. Service Features and Deliverables

2.1 FortiEDR Service Bundles

The FortiEDR Service is delivered through the FortiEDR cloud platform which is managed by Fortinet on a twenty-four (24) hours a day by seven (7) days a week basis. FortiEDR cloud platform is monitored for server availability, service capacity, and network resource utilization and is based on the Google Cloud Platform for hosted services and computing infrastructure. Customers may choose the geographic region in which their FortiEDR platform components are located from the then-current available regions (currently, US Central, US East, US West, West Europe, East Europe, North America, South America, Asia East, Asia South, Asia Southeast, Asia Northeast and Australia).

The FortiEDR Service is available for purchase with a minimum of five hundred (500) end-point collectors with increments of twenty-five (25), five hundred (500) or ten thousand (10,000) end-point collectors.

Fortinet will use reasonable efforts to ensure the FortiEDR Service is offered bundled with the following security features:

- Predict & Protect*:* Pre-infection prevention engine based on Fortinet Next Generation Anti-Virus (NGAV) capabilities; post-infection real time protection; proactive risk mitigation that includes discovery of communicating applications and IoT devices, vulnerability management and application rating empowering attack surface reduction; orchestrated incident response that includes automated investigation and remediation capabilities.
- Protect & Response: Pre-infection prevention engine based on Fortinet NGAV capabilities; post infection real-time protection; threat hunting capabilities with a six (6) month data retention; forensics overview and control that includes attack graph with code tracing and orchestrated incident response that includes automated investigation and remediation capabilities.
- Predict, Protect and Response: Pre-infection prevention engine based on Fortinet NGAV capabilities; post-infection real time protection; proactive risk mitigation that includes discovery of communicating applications and IoT devices, vulnerability management and application rating empowering attack surface reduction; threat hunting capabilities with a six (6) months data retention; forensics overview and control that includes attack graph with code tracing and orchestrated incident response that includes automated investigation and remediation capabilities.

All FortiEDR Service bundles provide:

- Service availability target of 99.9%, with platform functionality available for 99.8% in any given calendar month.
- FortiCare™ 24x7 technical support, as outlined in the then-current Fortinet support policies and service description, available on the Support Portal or other site as designated by Fortinet.

2.2 FortiResponder Managed Detection and Response Service

The MDR Service is delivered on a twenty-four (24) hours a day by seven (7) days a week basis. The MDR Service provides threat monitoring and analysis of events in the Customer's environment, as reported to the FortiEDR console. The aim is to respond as detailed below to all alerts within twenty-four (24) hours of the generation of the event, in the FortiEDR console or the receipt of Customer request for assistance. The MDR service provides the following pro-active security elements:

- *Review & analysis* of all customer alerts reported to the FortiEDR console for:
  - Static and dynamic malware.
  - Malicious processes in memory.

  If required, malicious artefacts may be obtained from collector end-points for forensic analysis (e.g. Windows event log records, AMCache and host files, scheduled log files, browser artefacts).
- *Alert management*. Upon reporting of an alert to the FortiEDR console;
  - Validation and classification of known malware.
  - Investigation and reporting on previously unknown malware or, potentially dangerous applications. For any alert of malicious activity or upon identification of a potentially unwanted program, a notification will be sent to the Customer by email to describe the alert, the level of threat, and recommendations for review and/or remediation steps. For events classified as malicious, upon configuration in the console, an email will be generated within sixty (60) minutes of receipt. If required, the Customer may request a conference call to obtain clarification on the analysis and any recommended remedial actions, which may involve assistance to the Customer in configuring a FortiEDR playbook.
- *Annual environment review* will be delivered, via a remote video conferencing tool, by the last quarter of the annual service entitlement with a view to providing an assessment of the Customer environment. This review may include the discussion of the following topics:
  - Device coverage and FortiEDR license usage.
  - FortiEDR environment health.
  - Malware findings.
  - Trends from alert management.

3. Scope and Conditions

3.1 Platform requirements

- The Customer acknowledges and accepts to comply with the system requirements to use the FortiEDR cloud platform. Fortinet may change the platform requirements from time-to-time. The Customer is solely responsible for utilizing the appropriate level of the appropriate supported platform required by the FortiEDR Service. The then-current supported platform requirements are available in the "Installation and Administration Guide" which is available on the website www.fortinet.com.

3.2 Customer Requirements

- In the event that continued provision of the Service to the Customer may compromise the integrity or security of the FortiEDR or Fortinet's systems, networks or reputation, the customer agrees that Fortinet may permanently or temporarily limit or suspend these FortiEDR Service or MDR Service to the Customer at Fortinet's sole discretion.
- Customer agrees to use the FortiEDR Service or MDR Service for legitimate and lawful business purposes only. The FortiEDR Service and MDR Service are provided for the Customer internal business use and shall not be resold to third parties or used for managed services. The Customer is responsible for ensuring that its usage of the Service shall be in accordance with all applicable laws (including, but not limited, privacy and security laws) and proper controls and processes shall be implemented in this respect. Therefore, Fortinet explicitly advises the Customer to always assess and ensure that the usage of the Service complies with local legislation prior to its any deployment.
- Should Fortinet discover any illegal activity, regardless of intent, the FortiEDR Service and MDR Service may be terminated without notice and where appropriate the relevant authorities notified.

- The Customer understands that the FortiEDR Service and the MDR Service are designed to supplement and support, but not to replace, the implementation of an effective end-user computer usage policy by the Customer across its organization.
- Correct technical issues and minimize the recurrence of technical issues, for which the Customer is responsible, that may prevent Fortinet from meeting the service levels or availability targets.
- Accept that Fortinet is not responsible for any loss of connectivity by the Customer, where the FortiEDR or MDR Service will considered as being utilized.
- The Customer is responsible for ensuring that their use of the FortiEDR and MDR Service is in accordance with all applicable privacy and security laws, and the customer will ensure it has in place proper controls and processes in this respect.
- All communication with the Fortinet assigned resources shall be conducted in a professional manner and in accordance with the services provided.

MDR Service requirements

- For first time usage, the pre-requirements for the MDR Service are: (a) purchase and completion of the FortiEDR Deployment Service; and (b) end-point collectors covered by the Service shall be configured into prevention mode to actively monitor threats.
- Through experience, Fortinet has learned that the quality of its services is greatly impacted by Customer participation. Accordingly, the Customer will provide in a timely fashion all information, support, approvals and resources needed by Fortinet team to successfully deliver the MDR Service. In particular, the Customer shall:
  - Provide relevant application knowledge associated with an alert or a request.
  - Provide any other data that Fortinet may reasonably request in order to reproduce operating conditions similar to those present when the relevant alerts or issues occurred.
  - carefully monitor emails from Fortinet on an on-going basis as a requirement for the delivery of the MDR service.
  - To remediate vulnerabilities on protected systems within fourteen (14) days of any threat notification by Fortinet. The Customer agrees that Fortinet's response time targets do not apply to protected systems that are pending remediation for more than fourteen (14) days after initial notification by Fortinet.
- Customer shall provide and maintain with Fortinet a list of up to three (3) designated contacts. No more than one (1) change a quarter may take place to this list. These are the only contacts authorized on the Customer's behalf to make and respond to inquiries regarding alert management services to Fortinet.
- The delivery of the annual review remote session will take place using Fortinet resource during the core business hours of 09:00 to 18:00 in the time zone local where the work is being delivered. For clarity this is based on Eastern Standard Time (EST) and Israel Standard Time (IST).

3.3 General Conditions

- There are regularly scheduled maintenance of the Fortinet infrastructure which takes place on the first and third Sunday of each month between 02.00 and 11.00 (EST). During the maintenance, Fortinet will use reasonable efforts to perform such maintenance without any service disruption. It may occur during these maintenance windows that the FortiEDR central manager is unavailable for up to thirty (30) minutes. During this time, data collection will not be disrupted, and end-points will remain protected.
- In the event that the integrity of the Service is at risk, Fortinet may perform emergency maintenance actions at their sole discretion. Fortinet will use reasonable efforts to inform all affected parties within one (1) hour of the start of the maintenance activity.
- The Customer acknowledges and agrees that: (a) FortiEDR Service and MDR Service are subject to intrinsic reliability and technical limitations; (b) FortiEDR Service and MDR Service help to prevent, find or eliminate malware and security breaches but it is technically impossible to guarantee email or network security as no security device or service can guarantee full security or the blocking of all known malicious activity; and (c) Fortinet accepts no liability for any damage or loss resulting directly or indirectly from any failure of FortiEDR

Service and MDR Service to detect malware, malicious activity or for false positives including security breach, data loss, data corruption, and service interruptions and/or degradations of the Company's network, systems.

- Unless otherwise specified, the FortiEDR and MDR Service will be delivered in English and remotely.
- The scope of the service is limited to the FortiEDR and MDR Service as outlined in this document. Any request by the Customer for services beyond the duration or scope will be provided at Fortinet's discretion and billable at the then-current rate.
- All MDR service levels described in this document are targets which Fortinet will use reasonable efforts to achieve and are measured on receipt of an alert in the FortiEDR console.
- By purchasing the FortiEDR or MDR Service, Customer understands and agrees that Fortinet is not obligated to provide the service if Customer fails to meet the requirements under section 3.
- Fortinet will retain the configuration and any associated data only for a period of fourteen (14) days to allow data collection or service re-initiation following termination or expiration of the Service or the end of agreed Service's evaluation period. Once such period is elapsed, the Customer instance will be deleted along with any associated data.
- Customer represents and warrants that it has all rights, permissions, and consents necessary to: (a) submit personal data to deliver the FortiEDR Service, MDR Service, and necessary support; and (b) grant Fortinet the right to process personal data for the provision of the FortiEDR Service, MDR Service, and support: (i) as required by applicable law; (ii) as reasonably requested by the Customer; (iii) as necessary to provide the FortiEDR Service, MDR Service, and related support, and prevent or address technical problems or violations of the FortiEDR Service, MDR Service; and (iv) as set forth in the following sentence. Fortinet will process the personal data that Fortinet receives through the Service pursuant to: (a) a data processing agreement executed between the parties where required under applicable law, and (b) the provisions of the Fortinet Privacy Policy located at http://www.fortinet.com/aboutus/privacy.html ("Privacy Policy"), updated from time to time at Fortinet's discretion. When the FortiEDR Service or MDR Service provides Customer with new personal data that Customer did not already possess (such as the Service's determination that a particular email poses a security threat), Customer may use this new personal data solely for Customer's lawful internal cybersecurity purposes.
- The FortiEDR and MDR Service are subject to the terms of Fortinet's Service Terms & Conditions located at https://www.fortinet.com/corporate/about-us/legal.html.

3.4 Service Availability Levels

The service availability levels described in this document are targets which Fortinet will use reasonable efforts to achieve and will exclude delays related to Service unavailability or disruption caused by any of following events, without limitation:

- scheduled maintenance or emergency maintenance;
- Customer or MSSP's -initiated changes whether implemented by Customer or Fortinet or a third party on behalf of Customer;
- Customer's failure to adhere to Fortinet implementation, support processes and procedures;
- acts or omissions of the Customer, MSSP. its employees, agents, third party contractors or vendors or any third party accessing the Service;
- any violations of the Customer or Scope & Conditions defined above
- any event not wholly within the control of Fortinet;
- negligence or willful misconduct of the Customer, or others authorized by the Customer to use the Services provided by Fortinet;
- any failure of any component for which Fortinet is not responsible, including but not limited to all Customer or MSSP infrastructure including electrical power sources, networking equipment, computer hardware, computer software or email content;
- any failures that cannot be corrected because the Customer or MSSP, its systems or networks are not reasonably accessible to Fortinet. It is the Customer's and/or MSSP's (if applicable) responsibility to ensure that contact details are kept up to date and to confirm or update the existing the technical contact details.

4. Eligibility & Purchasing

The FortiEDR and MDR service are available for purchase by a Customer through authorized Fortinet resellers and distributors globally. The FortiEDR and MDR service is delivered to the Customer of Fortinet products if and when identified on the purchase order received by Fortinet.

The duration of the FortiEDR and MDR service is three hundred and sixty-five (365) days from service unit activation in accordance with Fortinet's registration policies. The FortiEDR Service and MDR Service may be cancelled by the Customer at any time and for any reason, but in no event will Fortinet refund any prepaid subscription fee. All sales are final.

The MDR Service is available bundled with the "Predict & Protect" FortiEDR Service bundle. It is also available for purchase as an uplift to any FortiEDR Service bundles, with a minimum number of incremental end-point collector licenses in values of twenty-five (25).

Purchasing Information: (available as a subscription on a monthly basis where XX = number of months)

FortiEDR Predict and Protect	FC1-10-FEDR0-350-01-XX
FortiEDR Protect and Response	FC1-10-FEDR0-351-01-XX
FortiEDR Predict-Protect-and-Response	FC1-10-FEDR0-348-01-XX
FortiEDR Predict-Protect-and-Response-Airgap	FC1-10-FEDR0-352-01-XX
FortiEDR Predict-Protect-and-Managed-Response	FC1-10-FEDR0-349-01-XX
FortiEDR Managed Detection and Response Services	FC1-10-FEDR0-340-01-xx