

ADISTEC PROFESSIONAL SERVICES

FortiEDR Rapid Deploy

DESCRIPTION

FortiEDR® Rapid Deploy for FortiEDR Cloud and On-Premises is a set of activities and procedures that, following industry and Fortinet® best practices, help you minimize installation times for FortiEDR®, optimizing configuration and ensuring proper production deployment. Applies to the FortiEDR® and FortiEDR Cloud® family.

SCOPE OF OUR SERVICE

- Infrastructure Review
 - Configure up to five (5) Security Policies
 - Using Defaults
 - Execution Prevention
 - Exfiltration Prevention
 - Ransomware Prevention
 - Device Control
 - Extended Detection
 - Configure up to five (5) Clones of the Security Policies
 - In Simulation Mode for troubleshooting
 - Define up to three (3) Playbook Policies
 - Including the Default Playbook
 - Define up five (5) Communication and Control Policies
 - Configure IOT Scanning (if necessary)
 - Configure up to five (5) Collector Groups
 - Ensure at least 4 collectors are successfully assigned to each group
- Configuration**
- Ensure legitimate applications are not being blocked by FortiEDR
 - Add up to five (5) exceptions
 - Train the client to create further exceptions
- Tuning**

SERVICE DETAILS

Mode: On-Line

Estimated Duration: 24 hours

PART NUMBER

P/N	Description
APS-FRT-FTEDRRD	FortiEDR Rapid Deploy

LIMITATIONS AND OUT OF SCOPE

The client is responsible for ensuring that the FortiEDR is installed/deployed. Adistec will not perform the deployment tasks of the platform and additionally it is required that remote access be provided for configuration via the internet. Integration with authentication services and validation/authentication of users is excluded. Integration of the Cloud Service or On-Premise deployments to the Security Fabric is not included. Some features of the service require the customer to have the appropriate license purchased.