Forcepoint® ONE Web Edition Rapid Deploy

DESCRIPTION

Maximum protection provided by the Forcepoint® ONE solution requires a high level of knowledge and experience. That is why Adistec offers the Forcepoint® ONE Rapid Deploy service, this service consists of a set of activities and procedures that following the best practices of the industry allows to deploy the solution efficiently, optimizing resources and ensuring performance while securing your infrastructure.

SCOPE OF OUR SERVICE

Design	→ Scope definition workshop
	    o Smart Agent
	    o Using the Authentication Portal
	→ Define authentication methods
	    o Policy design

Testing	→ Test Environment Deployment and Configuration
	→ Policy settings
	    o Up to three (03) data leak policies
	    o Up to three (01) ZTNA access control policies
	       Up to three (03) navigation policies
	→ Importing or synchronizing user accounts

Deployment	→ Agent deployment in production environment up to 5 devices o Agent Deployment Case Explained → Exception Case Handling

Integration	→ Integration with up to one (01) Proxy or Firewall for Shadow-IT Reports:
	    o Bluecoat
	    o Mcafee
	    o Symantec
	    o Websense
	    o Culm
	    o Checkpoint
	    o Fortinet
	    o Juniper
	    o Palo Alto
	    o Splunk
	    o Mapping logs to the Bitglass Discovery engine

SCOPE OF OUR SERVICE (Continued)

QA

→ Functional test
→ Skill Transfer
  o Duration: up to four (04) hours

SERVICE DETAILS
Modality: On-Line
Estimated Duration: 120 hours

PART NUMBER

P/N	Description
APS-FCP-ONEWERD	Forcepoint® ONE Web Edition Rapid Deploy

LIMITATIONS AND OUT OF SCOPE

The service does not include the configuration of the built-in RBI feature. The service only includes the configuration of a single cloud according to the official compatibility matrix. SAML Relay services are not included. The client is responsible for providing the necessary prerequisites for the execution of this service such as (but not limited to) servers, databases, networking modifications, etc. Adistec will not be able to ensure the level of performance of the solution, these metrics may be related to the hardware, networking or software components of third parties and the client must analyze such behaviors with their suppliers or the corresponding manufacturers. The filtering and protection policies are based on the data dictionaries or templates that are incorporated by default in the solution, they are out of scope of the service to make customizations such as scripts or modifications to the templates by default. Certain configurations may require the client to have acquired the corresponding license, in case it does not have it this does not oblige Adistec to carry out the implementation or configuration of said features or modules and generates some partial refund to the client.