

ADISTEC PROFESSIONAL SERVICES

Kaspersky Endpoint Security Cloud Rapid Deploy

DESCRIPCIÓN

Kaspersky Endpoint Security Cloud Rapid Deploy es un conjunto de actividades y procedimientos que, siguiendo las mejores prácticas de la industria y del fabricante, le permiten tener la plataforma Endpoint Security Cloud habilitada en la nube en un breve plazo, minimizando los tiempos de instalación en los dispositivos de los usuarios, optimizando la configuración y asegurando la correcta puesta en producción.

ALCANCES DE NUESTRO SERVICIO

→ KickOff

- Validación de pre-requisitos
- Listado de usuarios
- Definición de administrador del servicio

→ Configuración

- Inicialización del tenant
- Configuración del portal
- Creación de hasta un (01) grupo
 - Asignación de usuarios
- Configuración de hasta dos (02) perfiles de seguridad
 - Configuración de hasta un (01) security settings por perfil
 - File Threat Protection
 - Mail Threat Protection
 - Web Threat Protection
 - Network Threat Protection
 - Firewall
 - BadUSB Attack Prevention
 - Scan of removable drives
 - Behavior Detection
 - Configuración de hasta un (01) perfil Web por perfil
 - Configuración de hasta tres (03) excepciones
 - Configuración de hasta un (01) perfil Aplicaciones
 - Configuración de hasta tres (03) excepciones por perfil
 - Configuración de hasta un (01) Vulnerabilidad Assessment por perfil
- Configuración de hasta un (01) notificación de eventos.
- Configuración de hasta un (01) Endpoint Detection and Response Alerts (*según licenciamiento adquirido*)

→ Despliegue de hasta veinte (20) agentes

- Modalidad de despliegue
 - Stand-Alone desde la consola
 - Asistencia para generación de GPO
- Sistemas Operativos cubiertos:
 - Microsoft® Windows
 - MacOS
 - iOS
 - Android

ALCANCES DE NUESTRO SERVICIO (Continuación)

- Testing
 - Pruebas de hasta un (01) servidor Windows.
 - Pruebas de hasta una (01) estación de trabajo Windows.
 - Pruebas de hasta una (01) estación de trabajo Mac.
 - Pruebas de hasta un (01) dispositivo móvil Android.
 - Pruebas de hasta un (01) dispositivo móvil IOS.

- Skill Transfer
 - Hasta cuatro (04) horas de duración
 - Hasta dos (02) participantes

DETALLES DEL SERVICIO

Modalidad: On-Line

Duración Estimada: 32 horas

PART NUMBER

P/N	Descripción
APS-KAS-ENDCLDRD	Kaspersky Endpoint Security Cloud Rapid Deploy

LIMITACIONES Y FUERA DE ALCANCE

Adistec no podrá asegurar el nivel de performance de la solución, estas métricas pueden estar relacionadas con los componentes de hardware, networking o software de terceros y el cliente deberá analizar dichos comportamientos con sus proveedores o los correspondientes fabricantes. Ciertas configuraciones pueden requerir que el cliente tenga adquirido el licenciamiento correspondiente, en caso de que no lo posea esto no obliga a Adistec a realizar la implementación o configuración de dichas características o módulos y no genera derecho alguno de reembolso parcial al cliente. Esta fuera del alcance del servicio la instalación, configuración o modificación de Active Directory. Se recomienda que los dispositivos de los usuarios no tengan ninguna protección de antivirus instalada. Esta fuera del alcance del servicio la desinstalación del agente de antivirus en los dispositivos de los usuarios. Adistec brindará un apoyo razonable dentro de la duración del servicio para asistir al cliente a remover el cliente de antivirus. Adistec no asegura el correcto funcionamiento en caso de que el cliente tenga acceso a internet a través de una VPN. Por default se asigna el nivel de seguridad "medium" en la configuración de los módulos de "Security Settings". En caso de que el cliente desee realizar un despliegue masivo de agentes a través de políticas de GPO de Active Directory, Adistec brinda apoyo para la generación de las políticas, pero queda fuera del alcance la creación de estas en la consola de GPO. Adistec no asegura y garantiza la instalación de agentes a través de Active Directory con el uso de GPO. Sin embargo, Adistec brindará un apoyo razonable dentro de la duración del servicio para asistir al cliente a realizar un troubleshooting en caso de falla de la política de GPO. Queda fuera del servicio la configuración de herramientas de terceros para (pero sin estar limitado a) desinstalar los clientes de antivirus, instalaciones masivas de software o similares. El usuario debe contar con acceso a su Apple ID para la configuración del agente para iOS.