



HP DaaS Proactive Security



Ventajas del servicio

- Aumenta la seguridad de los puntos de conexión
- Evita sitios web y archivos adjuntos maliciosos
- Protege tus datos y dispositivos

Aspectos destacados del servicio

- Tecnología avanzada de aislamiento para protegerse del malware²
- El análisis de HP TechPulse proporciona informes y observaciones sobre seguridad
- La evaluación Aon CyQu facilita la comprensión de tu posición actual de seguridad³

Descripción general del servicio

Mejora las funcionalidades de gestión segura de HP Device as a Service (DaaS) con HP DaaS Proactive Security.¹ Proporciona protección contra el malware en tiempo real para los puntos de conexión, análisis de seguridad y amenazas, y experiencia específica en ese terreno para reforzar tu seguridad. La tecnología de aislamiento de amenazas ayuda a protegerse del malware a través del correo electrónico, de los navegadores y de archivos PDF y de Office. Amplía los informes y observaciones de seguridad proporcionados por el análisis de HP TechPulse. De esta forma podrás protegerte, entender mejor y responder a las amenazas.

Características y especificaciones

Tecnología de aislamiento avanzada

Los virus, el ransomware y demás malware son una amenaza constante para las infraestructuras de IT. Ve más allá de las soluciones antivirus basadas en definiciones con la tecnología de aislamiento de amenazas en tiempo real, basada en máquinas virtuales (VM) para contener ataques de correo electrónico de día cero, navegador y archivos, evitando así que entren en la red.² Los usuarios pueden ver archivos adjuntos y sitios web sin comprometer la seguridad de su red, sin interrumpir su trabajo ni alterar sus rutinas.

Análisis de HP TechPulse

Recibe información y una visión global del estado de protección de los dispositivos con informes detallados de los ataques bloqueados por HP TechPulse, todo desde un único panel de control en el portal de HP DaaS.

Expertos de servicio de HP

Refuerza tu seguridad, anticipáte a los ataques y evita el impacto negativo en tu empresa gracias a la asistencia de nuestros expertos, encargados de supervisar informes, analizar amenazas y ayudarte en la planificación. Los expertos de servicio de HP realizan análisis de amenazas de seguridad trimestrales y responden a las alertas de seguridad.⁴

Aon

Ofrecemos soluciones de seguridad cibernética adicionales en colaboración con Aon que incluyen servicios de evaluación, respuesta ante incidencias y seguros. La herramienta de autoevaluación Aon Cyber Quotient (CyQu) y la calificación de seguridad ayudan a evaluar tu posición de seguridad en relación a otras empresas de tu mismo sector. Aon ofrece respuesta a incidencias sin costes adelantados en un máximo de una hora en caso de aparición de una brecha de seguridad.³

Planes de DaaS Proactive Security

Características del servicio	Plan Estándar (autogestionado)	Plan Avanzado (gestionado por HP)
Protección ante amenazas de archivos adjuntos de correo electrónico, enlaces de phishing y descargas	✓	✓
Observaciones de seguridad de HP TechPulse	✓	✓
Evaluación con Aon CyQu, respuesta a incidencias y elegibilidad para seguros ³	✓	✓
Aplicación de políticas de aislamiento: Los expertos de servicio de HP pueden gestionar una protección avanzada del estado de la tecnología	—	✓
Análisis: Los expertos de servicio de HP realizan un análisis de seguridad de las amenazas aisladas y ofrecen recomendaciones sobre las prácticas recomendadas para usuarios y dispositivos con un gran volumen de amenazas, según sea necesario	—	✓
Investigación de eventos de seguridad y notificaciones: Los expertos de servicio de HP te notificarán cuándo los dispositivos no dispongan de protección debido a su manipulación por los usuarios finales o por cambios en la configuración del sistema	—	✓

Especificaciones de entrega

Opciones del servicio

- **Estándar:** La versión estándar autogestionada de DaaS Proactive Security está disponible en los planes DaaS Estándar, Avanzado y Premium. En la opción autogestionada, asumes la responsabilidad de registrar tus dispositivos y de ponerte en contacto con HP en caso de necesitar soporte.
- **Avanzado:** La versión avanzada de DaaS Proactive Security solo está disponible si tienes un plan DaaS Avanzado o Premium. Con el plan Avanzado, un gerente de incorporación de HP te ayudará con la instalación y configuración del servicio; los expertos de servicio de HP se encargarán de proporcionar soporte y supervisión.

Responsabilidades de HP

Responsabilidades de los expertos en servicio de HP para los planes Estándar:

- Solución de problemas de instalación y aspectos de conectividad.
- Proporcionar asistencia y respuestas a las preguntas relacionadas con el servicio.
- Añadir nuevas URL a las listas blancas de páginas web específicas de la empresa.

Responsabilidades de los expertos de servicio de los planes Avanzados:

- Asegurar que la tecnología de aislamiento avanzada está instalada y activada.
- Proporcionar informes trimestrales de análisis de seguridad de amenazas.
- Investigar alertas de seguridad y tomar las medidas apropiadas.
- Supervisar el servicio y coordinar la asistencia y resolución de problemas.
- Proporcionar soporte de nivel 2 y 3 y coordinación con tu servicio de atención al cliente.

Responsabilidades del cliente

- Revisar paneles, informes e incidencias en el panel de control de gestión proactiva HP DaaS.
- Revisar informes de seguridad y realizar acciones según corresponda.
- Solicitar y proporcionar URL de páginas web para la confección de listas blancas.
- Llevar a cabo las tareas básicas de solución y clasificación de los problemas de soporte más comunes de los usuarios finales antes de escalarlos al servicio de soporte de HP.
- Renovar, cambiar o cancelar la cuenta de HP DaaS.
- Responder a la encuesta en línea de CyQu.³

Requisitos del sistema

- DaaS Proactive Security requiere dispositivos cliente multiproveedor con Windows 10 1703 o posterior, con una memoria mínima de 8 GB y 6 GB de espacio libre en disco duro.
- DaaS Proactive Security requiere HP TechPulse, incluido en cualquier plan HP DaaS o HP DaaS Proactive Management. El plan Avanzado de HP DaaS Proactive Security requiere que los clientes contraten un plan HP DaaS Avanzado o Premium.
- La comunicación entre los dispositivos gestionados y el servicio de gestión en la nube HP requiere una conexión a Internet activa.
- Visita hpdaas.com/requirements para ver más información.

Especificaciones de entrega (continuación)

Incorporación

La incorporación se refiere al proceso de integración en la solución DaaS Proactive Security de los dispositivos cubiertos. Si tienes un plan HP DaaS Avanzado o Premium, se te asignará un gerente de incorporación para supervisar el proceso. Si tienes un plan Estándar autogestionado, será un experto de servicio de HP el encargado de crearte una cuenta y proporcionar la información necesaria en un correo electrónico de bienvenida, junto a las instrucciones para recibir asistencia técnica en caso necesario.

Requisitos de incorporación

Antes de que tus dispositivos realicen la transición a DaaS Proactive Security, debes proporcionar la siguiente información a tu gerente de incorporación, gestor de cuentas HP y/o partner de servicio:

- Información principal de contacto (nombre, correo electrónico, teléfono, y ubicación)
- Domicilio de la empresa
- Nombre del dominio DNS del directorio activo
- Lista de administradores de informes
- Una lista de dispositivos que se supervisarán con HP Proactive Management, que incluye el modelo y el número de serie (solo para planes DaaS Avanzado o Premium)

Proceso de incorporación

- **Fase 1: Registro:** Recibirás una clave de licencia y un enlace a un formulario de registro.
- **Fase 2: Recopilación de información:** Se te asignará un gerente de incorporación para supervisar el proceso. Se programará una llamada para proporcionar recomendaciones sobre cómo seguir.
- **Fase 3: Recomendaciones y creación de cuenta:** HP creará una cuenta en la plataforma de seguridad HP DaaS, activará la configuración inicial de seguridad y añadirá las URL que necesites a una lista blanca.
- **Fase 4: Implementación:** El gerente de incorporación se reunirá contigo para comenzar el registro de dispositivos y resolver cualquier problema.
- **Fase 5: Transición al servicio de soporte y supervisión (solo plan Avanzado):** Al finalizar la incorporación, el servicio pasará a manos de los expertos de servicio de HP, que proporcionarán soporte y supervisión durante el periodo contratado.

Responsabilidades del gerente de incorporación

- Crear la cuenta DaaS Proactive Management.
- Añadir o eliminar usuarios del panel HP DaaS Proactive Management.
- Otorgar accesos a cuentas de usuario.
- Reunir y consolidar la información de entorno requerida.
- Proporcionar documentación y asistencia para implementar el agente de análisis.
- Desarrollar e implementar el proyecto del plan de incorporación.
- Proporcionar actualizaciones de progreso.
- Verificar que la implementación sea un éxito.
- Realizar la transición de la atención al cliente de la funcionalidad HP DaaS Proactive Management a los expertos de servicio de HP.
- Diagnosticar y resolver problemas de instalación.
- Proporcionar asistencia continuada.

Limitaciones del servicio

- Disponibilidad de expertos de servicio de HP para el plan Avanzado DaaS Proactive Security:
 - **América del Norte:** asistencia en inglés disponible de lunes a viernes (excepto los días festivos de HP) de 6:00 a 18:00 MT.
 - **América Latina:** asistencia en inglés y español disponible de lunes a viernes (excepto los días festivos de HP) de 7:00 a 18:00 GMT - 5.
 - **Europa, Oriente Medio y África:** asistencia en inglés, francés y alemán disponible de lunes a viernes (excepto los días festivos de HP) de 8:00 a 18:00 CET.
 - **Asia, Pacífico y Japón:** asistencia en inglés y chino disponible 24 horas al día; asistencia en japonés de 9:00 a 21:00, hora estándar de Japón, 7 días a la semana (excepto los días festivos de HP).
- Los servicios de Aon solo se encuentran disponibles en los Estados Unidos.
- Las plataformas HP DaaS Proactive Management y HP DaaS Proactive Security están alojadas en Amazon Web Services (AWS).

Términos y condiciones

Consulta los [términos y condiciones](#) de HP DaaS.

Más información

Ponte en contacto con el representante de ventas de HP o partner de canal local para ampliar información, o visita hp.com/go/DaaS.

Regístrate para recibir actualizaciones
hp.com/go/getupdated



Compartir con compañeros

1. Los requisitos de sistema para implementar HP DaaS Proactive Security son: dispositivos cliente multiproveedor con Windows 10 1703 o posterior, con una memoria mínima de 8 GB y 6 GB de espacio libre en disco duro para instalar el software cliente. HP DaaS Proactive Security requiere HP TechPulse, incluido en cualquier plan HP DaaS o HP DaaS Proactive Management. El plan Avanzado de HP DaaS Proactive Security requiere que los clientes se registren en un plan Avanzado o Premium de HP DaaS o HP DaaS Proactive Management.
2. La tecnología HP Sure Click Advanced está incluida en HP DaaS Proactive Security y requiere Windows 10. Es compatible con Microsoft Internet Explorer, Google Chrome y Chromium. Entre los archivos adjuntos compatibles se incluyen los archivos de Microsoft Office (Word, Excel, PowerPoint) y los archivos PDF, siempre y cuando se haya instalado Microsoft Office o Adobe Acrobat.
3. Los servicios de Aon solo se encuentran disponibles en los Estados Unidos.
4. Los expertos en servicio solo están disponibles en el plan Avanzado de Proactive Security.

© Copyright 2019 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de HP quedan establecidas en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. Nada de lo aquí indicado debe interpretarse como una garantía adicional. HP no se responsabiliza de los errores u omisiones técnicos o editoriales que puedan existir en este documento. Adobe y Acrobat son marcas comerciales de Adobe Systems Incorporated. Google, Chrome y Chromium son marcas comerciales de Google Inc. Microsoft y Windows son marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

4AA7-4656ESE, marzo de 2019

