



Consideraciones sobre seguridad de las impresoras

Aspectos de seguridad importantes a la hora de evaluar soluciones de impresión

Índice

Los dispositivos de impresión e imagen no protegidos son la norma	2
Cinco aspectos principales de la seguridad de las impresoras	2
Proceso de arranque seguro	2
Integridad del código del firmware	2
Detección de intrusiones en el tiempo de ejecución.....	3
Verificación continuada de los ajustes de la política de seguridad.....	3
Detección y análisis de amenazas en tiempo real	3
Dispositivos compatibles con FutureSmart y disponibilidad de las funciones.....	4

Los dispositivos de impresión e imagen no protegidos son la norma

El departamento de IT trabaja continuamente para proteger la información confidencial, que incluye los datos de los empleados y los clientes, en múltiples dispositivos. Esta necesidad de atender a una amplia variedad de usuarios con diferentes estilos de trabajo en una misma empresa hace que las amenazas de seguridad informática imprevistas supongan un desafío constante.

Aunque muchos departamentos de IT aplican medidas de seguridad rigurosas a los ordenadores y la red de la empresa, a menudo los dispositivos de impresión e imagen quedan desatendidos y sin protección. Sin embargo, las amenazas de seguridad son reales, porque a medida que los dispositivos de impresión e imagen se vuelven cada vez más sofisticados, ofrecen más oportunidades a los atacantes para poner en peligro el dispositivo o toda la red.

Cinco aspectos principales de la seguridad de las impresoras

El objetivo de este documento no es solo ofrecerle un marco de trabajo, sino también explicar los aspectos más específicos de la seguridad de la impresión que debe tener en cuenta a la hora de comprar, implementar o utilizar impresoras y soluciones de impresión. Las impresoras de HP compatibles con las tres grandes funciones de seguridad (HP Sure Start, listas blancas y detección de intrusiones en el tiempo de ejecución) presentadas en otoño de 2015 cumplen todos los criterios de los siguientes apartados (cuando se combinan con JetAdvantage Security Manager y ArcSight¹). Los dispositivos con FutureSmart que no son compatibles con HP Sure Start cumplen estos criterios, excepto los indicados en el apartado 1 (proceso de arranque seguro). Consulte la tabla de la página 4 para ver los detalles de compatibilidad de las funciones de seguridad.

Debe centrarse en cinco áreas clave de seguridad de las impresoras:

1. Proceso de arranque seguro
2. Integridad del código del firmware
3. Detección de intrusiones en el tiempo de ejecución
4. Verificación continuada de los ajustes de la política de seguridad
5. Detección y análisis de amenazas en tiempo real

Proceso de arranque seguro

A continuación, puede ver los aspectos relacionados con un proceso de arranque seguro que HP recomienda para maximizar la seguridad:

- Cuando se enciende, el dispositivo debe validar la integridad del BIOS.
- El dispositivo debe recuperar automáticamente un BIOS infectado sustituyéndolo por la copia maestra protegida por hardware del BIOS.
- El dispositivo debe notificar cualquier incidencia al administrador mediante mecanismos de eventos estándar, que incluyen los sistemas SIEM.
- El dispositivo debe recuperarse a un estado seguro conocido después de detectar un BIOS infectado y sustituirlo por la copia maestra.

Integridad del código del firmware

Los siguientes aspectos relacionados con la integridad del código del firmware deberían incluirse en las propuestas para los clientes:

- El dispositivo debe verificar la integridad del código del firmware en el momento de cargarlo y permitir que solo se ejecute firmware seguro conocido.
- El dispositivo debe notificar cualquier incidencia al administrador mediante mecanismos de eventos estándar, que incluyen los sistemas SIEM.

Detección de intrusiones en el tiempo de ejecución

A continuación, puede ver los aspectos relacionados con la detección de intrusiones en tiempo de ejecución que HP recomienda para maximizar la seguridad:

- El dispositivo debe ofrecer una supervisión continuada de los ataques de inyección de malware en la memoria.
- El dispositivo debe notificar cualquier incidencia al administrador mediante mecanismos de eventos estándar, que incluyen los sistemas SIEM.
- El dispositivo debe detener su funcionamiento normal cuando detecta una anomalía y reiniciarse a un estado seguro conocido.
- El algoritmo de detección de intrusiones debe insertarse de forma aleatoria en diferentes partes de la imagen del código para prevenir que se detecte a sí mismo.

El algoritmo de detección de intrusiones debe ejecutarse con una frecuencia suficiente para detectar las inyecciones de malware antes de que pongan en peligro la integridad del dispositivo.

Verificación continuada de los ajustes de la política de seguridad

La verificación continua de los ajustes de la política de seguridad se realiza principalmente mediante el uso de una herramienta de cumplimiento de seguridad. A continuación, puede ver los aspectos relacionados con una herramienta de cumplimiento de la seguridad que HP recomienda para maximizar la seguridad:

- La herramienta de cumplimiento de seguridad debe aplicar la política de seguridad a las impresoras y equipos multifunción que no la cumplen.
- La herramienta de cumplimiento de seguridad debe detectar automáticamente los dispositivos nuevos o reiniciados de la red y aplicarles inmediatamente la política de seguridad.
- La herramienta de cumplimiento de seguridad debe incluir un editor de políticas de seguridad intuitivo que ayude al administrador a configurar los ajustes de seguridad adecuados indicándole los posibles conflictos.
- La herramienta de cumplimiento de seguridad debe gestionar e instalar los certificados mediante un proceso automático en toda la flota de impresoras y equipos multifunción.

Detección y análisis de amenazas en tiempo real

La detección y análisis de amenazas en tiempo real se realiza generalmente mediante el uso de un sistema de gestión de eventos de seguridad de la información (SIEM). A continuación, puede ver los aspectos relacionados con un sistema SIEM que HP recomienda para maximizar la seguridad:

- El SIEM debe recopilar los eventos de seguridad importantes de las impresoras.
- El SIEM debe permitir a los analistas de seguridad personalizar los informes y alertas mediante mensajes que avisen de las amenazas en tiempo real.
- El SIEM debe integrarse con otros equipos de IT de la red (servidores, enrutadores, etc.) que están siendo supervisados para permitir la detección de amenazas en tiempo real.
- El SIEM debe transformar los Big Data en inteligencia de seguridad aplicable empleando una correlación en tiempo real, combinada con potentes análisis de seguridad.
- El SIEM debe detectar el comportamiento anormal de los usuarios y prevenir las amenazas a los datos confidenciales.

Dispositivos compatibles con FutureSmart y disponibilidad de las funciones

La siguiente tabla muestra cuáles de las nuevas funciones de seguridad integradas son compatibles con la flota de dispositivos HP Enterprise FutureSmart desde finales de otoño de 2015. Todos los nuevos dispositivos FutureSmart presentados a partir de otoño de 2015 son compatibles con las tres nuevas funciones de seguridad integradas (HP Sure Start, listas blancas y detección de intrusiones). Debido a las limitaciones del hardware, algunas funciones no son compatibles con determinadas plataformas antiguas.

Categoría de la propuesta		Proceso de arranque seguro	Integridad del código del firmware	Detección de intrusiones en el tiempo de ejecución	Verificación continuada de los ajustes de la política de seguridad	Detección y análisis de amenazas en tiempo real
Plataforma de dispositivo (incluye todos los paquetes y opciones gestionadas)	Disponibilidad de las nuevas funciones de seguridad integradas	HP Sure Start	Listas blancas	Detección de intrusiones en el tiempo de ejecución	HP JetAdvantage Security Manager	Integración con HP ArcSight
HP LaserJet Enterprise MFP M527	Otoño 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M577	Otoño 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M506	Otoño 2015	✓	✓	✓	✓	✓
HP Color LaserJet Enterprise M552 y M553	Otoño 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise M604, M605 y M606	Otoño 2015	✓	✓	✓	✓	✓
HP LaserJet Enterprise 700 Color MFP M775	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 Color MFP M575	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise 500 MFP M525	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise MFP M725	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise Flow MFP M830	Primavera 2016	⊘	✓	✓	✓	✓
HP LaserJet Enterprise M806	Primavera 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise M855	Primavera 2016	⊘	✓	✓	✓	✓
HP Color LaserJet Enterprise Flow MFP M880	Primavera 2016	⊘	✓	✓	✓	✓
HP OfficeJet Enterprise Color MFP X585	Primavera 2016	⊘	✓	✓	✓	✓

Categoría de la propuesta		Proceso de arranque seguro	Integridad del código del firmware	Detección de intrusiones en el tiempo de ejecución	Verificación continuada de los ajustes de la política de seguridad	Detección y análisis de amenazas en tiempo real
Plataforma de dispositivo (incluye todos los paquetes y opciones gestionadas)	Disponibilidad de las nuevas funciones de seguridad integradas	HP Sure Start	Listas blancas	Detección de intrusiones en el tiempo de ejecución	HP JetAdvantage Security Manager	Integración con HP ArcSight
HP OfficeJet Enterprise Color X555	Primavera 2016	⓪	✓	✓	✓	✓
HP Color LaserJet Enterprise M651	Primavera 2016	⓪	✓	✓	✓	✓
HP Color LaserJet Enterprise MFP M680	Primavera 2016	⓪	✓	✓	✓	✓
HP LaserJet Enterprise MFP M630	Primavera 2016	⓪	✓	✓	✓	✓
HP LaserJet Enterprise 700 M712	Primavera 2016	⓪	✓	✓	✓	✓
HP Color LaserJet Enterprise M750	Primavera 2016	⓪	✓	✓	✓	✓
HP LaserJet Enterprise 600 M601, M602 y M603	Primavera 2016	⓪	✓	✓	✓	✓
HP LaserJet Enterprise Color M551	Primavera 2016	⓪	✓	✓	✓	✓
HP LaserJet Enterprise M4555 MFP	No compatible	⓪	⓪	⓪	✓	✓
HP Color LaserJet CM4540 MFP	No compatible	⓪	⓪	⓪	✓	✓
HP LaserJet Enterprise CP5525	No compatible	⓪	⓪	⓪	✓	✓
HP Digital Sender Flow 8500 fn1	No compatible	⓪	⓪	⓪	✓	✓
HP ScanJet Enterprise 7000n	No compatible	⓪	⓪	⓪	✓	⓪

¹ Para activar las funciones de seguridad puede ser necesaria una actualización del paquete de servicios de HP FutureSmart.

Regístrese y reciba las actualizaciones
hp.com/go/getupdated



© Copyright 2015 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin aviso previo. Las únicas garantías para los productos y servicios HP se establecen en las declaraciones expresas de garantía que acompañan a dichos productos y servicios. Ninguna información contenida en este documento debe interpretarse como una garantía adicional. HP no se hace responsable de los errores técnicos o editoriales ni de las omisiones que pueda contener este documento.

4AA6-3571ESE, diciembre de 2015

