Informe técnico empresarial

Mantenga los datos del punto de venta totalmente seguros

HP Client Security proporciona protección de varios niveles

Índice

Los detalles del cliente tienen valor y presentan riesgos 2
Seguridad de varios niveles de HP 3
Figura 1: HP Client Security 3
Proteja los dispositivos y los datos en el núcleo 3
Figura 2: HP Sure Start 4
Mantenga a los usuarios confiables productivos y a los intrusos afuera 4
Proteja y administre todos los dispositivos con facilidad 5
Figura 3: Información personal identificable 5
Retire los dispositivos y los datos de forma segura 5
Siéntase tranquilo con la ayuda de un líder confiable 6
Tabla 1: Conjunto de recursos de seguridad HP 7

Los detalles del cliente tienen valor y presentan riesgos

Las tecnologías existentes en los entornos de punto de venta (PDV) actuales capturan más datos de los clientes que nunca —y datos más valiosos—, lo que permite que los operadores de comercio, hospedaje y alimentación proporcionen experiencias fluidas y altamente personalizadas a los clientes.

Desde encuestas y actividades interactivas ofrecidas en kioscos en la tienda hasta programas de fidelidad en los que se pueden inscribir al pagar, los sistemas de computación de PDV inteligentes crean beneficios atractivos tanto para los comerciantes como para los clientes. El acceso instantáneo a información de pago y envío permite ofrecer un servicio más rápido y más preciso. Los detalles sobre la edad, los intereses, el histórico de compras y otras características de los clientes ayudan a las empresas a personalizar su marketing para construir una conexión emocional más fuerte con cada cliente.

Sin embargo, almacenar y administrar toda esta información confidencial personal identificable también genera un riesgo potencial mayor. Una fuga accidental o un ataque malintencionado pueden erosionar rápidamente la confianza y la fidelidad que le costó tanto trabajo obtener.

Ninguna empresa, grande ni pequeña, puede darse el lujo de subestimar el riesgo de sufrir ataques. En 2015, comerciantes de todo el mundo sufrieron por lo menos 370 violaciones de seguridad de datos, 70% de las cuales tuvieron por objetivo sistemas de PDV.[1] Los analistas prevén que para el 2020 más de **1,5 mil millones** de personas en todo el mundo serán afectadas por violaciones de datos.[2]

Los hackers por detrás de esas intrusiones están usando métodos cada vez más sofisticados y tecnologías cada vez más poderosas para robar información personal identificable, incluso información financiera. Los comerciantes y las empresas del sector de alimentación y hospedaje deben invertir en medidas de seguridad y tecnología capaces de proteger los datos en todas las capas de computación y permitirles recuperarse con rapidez, y con daños mínimos, de cualquier violación de datos.

El 70% de las violaciones de seguridad en el sector de comercio ocurrieron en PDV.[1]

El 73% de las violaciones de seguridad en el sector de entretenimiento ocurrieron en PDV.[1]

El 91% de las violaciones de seguridad en el sector de hospedaje ocurrieron en PDV.[1]

[1] *2015 Data Breach Investigations Report (Informe sobre investigaciones de violaciones de datos en 2015),* Verizon.

[2] Christian A. Christiansen et al., *IDC FutureScape: Worldwide IT Security Products and Services 2016 Predictions*, International Data Corporation, noviembre de 2015.

Seguridad de varios niveles de HP

HP tiene el marco de seguridad de PC profundo y amplio, respaldado por nuestros servicios de soporte y herramientas de gestión eficientes líderes del sector, para ayudar a su comercio a mantenerse seguro.

Nuestra estrategia de seguridad del cliente incluye la creación de varios niveles de protección en los dispositivos, los datos y la identidad. Junto con las herramientas de seguridad que se proporcionan a través de software, como HP Client Security y HP Sure Start, proporcionamos recursos adicionales en el hardware y sólidas protecciones incorporadas en todos los niveles descendentes hasta el BIOS. Los gerentes de TI pueden configurar, implementar y actualizar estas herramientas sin interrumpir la productividad de los empleados.

Figura 1. HP Client Security proporciona protección integral en todos los niveles del entorno de TI de la empresa.

Proteja los dispositivos y los datos en el núcleo

Los ataques al BIOS, que van más allá del nivel del sistema operativo, están entre los más difíciles de detectar y prevenir. En el momento en que se descubren, sus dispositivos y sus datos de clientes ya pueden estar comprometidos. Sin embargo, el monitoreo y la solución de problemas constantes para mantener los dispositivos seguros requieren dedicar tiempo y dinero a tareas de rutina en lugar de permitir que el área de TI se concentre en las iniciativas estratégicas y de productividad para hacer avanzar a la empresa.

HP BIOSphere proporciona protección optimizada integral contra ataques malintencionados y errores accidentales que puedan afectar el BIOS. Ofrece una arquitectura de autorreparación diseñada para prevenir, detectar y reparar ataques. Fácil de configurar y personalizar, HP BIOSphere ayuda a su empresa a optimizar las tareas de gestión y a proteger el firmware de los dispositivos para que pueda mantenerse productivo mientras protege la información delicada. La solución puede integrarse con las protecciones de seguridad existentes, configuradas de forma remota, y administradas con facilidad mediante actualizaciones automatizadas.

HP Sure Start —una solución de tecnología de autorreparación a nivel del BIOS— actúa junto con HP BIOSphere para proporcionar un nivel de seguridad agregado. Ayuda a asegurar que todos los sistemas y los datos estén protegidos antes de iniciar el proceso de arranque. HP Sure Start almacena una versión limpia del BIOS en la memoria a la que software o firmware de terceros no puede acceder. La solución basada en hardware también protege los datos únicos de un dispositivo, como su número de serie y las configuraciones de fábrica. Y con la capacidad de registro de auditoría de HP Sure Start, puede obtener información detallada sobre intentos de ataques al BIOS.

Figura 2. HP Sure Start recupera el BIOS para proporcionar productividad ininterrumpida, en todo momento y en todo lugar.

Mantenga a los usuarios confiables productivos y a los intrusos afuera

La autenticación falsa del usuario puede producirse en varios puntos en los sistema de PDV comerciales, exponiendo sus sistemas y sus datos a un uso indebido. Los datos no cifrados también son vulnerables ya que residen en las unidades de disco duro del dispositivo o circulan entre sistemas. HP Client Security crea una barrera sólida contra este tipo de intrusiones.

HP Trusted Platform Module (TPM) es un chip estándar del sector que almacena de forma segura información de identificación del usuario (como contraseñas, certificados o claves de cifrado) para autenticar los dispositivos y asegurarse de que no sufrieron violaciones de seguridad. Esta tecnología sella automáticamente los datos sensibles en la unidad de disco duro del dispositivo si la configuración de la plataforma se altera mediante un acceso no autorizado.

Windows 10 Credential Guard[3] permite autenticación de múltiples factores para evitar el acceso no autorizado o la eliminación de datos en sistemas de PDV al mantener la información delicada solo en software con privilegios. Por ejemplo, la seguridad basada en virtualización mantiene las credenciales en un entorno separado del SO, lo que permite que estén protegidas de amenazas avanzadas.

La tecnología de unidad de autocifrado (SED) de HP cifra y descifra los datos más rápido y de forma más segura que las soluciones basadas en software. Cuando se necesita, la SED puede borrar los datos en segundos, a diferencia de los métodos de eliminación tradicionales que pueden tardar horas.

Windows 10 Device Guard[4] permite que los gerentes de TI creen reglas para ejecutar solo aplicaciones firmadas, confiables y aprobadas en el sistema de PDV para ayudar a proteger contra ataques walk-up y de bajo nivel a través de puertos USB.

[3] Windows 10 Enterprise y Device Guard solo están disponibles para la instalación a través de los servicios de integración personalizados HP para clientes de empresa con una licencia por volumen para usar Windows 10 Enterprise. Credential Guard no está disponible con Windows 10 Pro.

[4] Windows 10 Enterprise y Device Guard solo están disponibles para la instalación a través de los servicios de integración personalizados HP para clientes de empresa con una licencia por volumen para usar Windows 10 Enterprise. Device Guard no está disponible con Windows 10 Pro.

Proteja y administre todos los dispositivos con facilidad

La realización de tareas de seguridad y auditorías de rutina puede ser una distracción costosa para el personal de TI ocupado y puede afectar su presupuesto limitado. HP ofrece soluciones de seguridad al cliente que ayudan a automatizar y optimizar la administración del día a día para que el equipo de TI pueda concentrarse en dar soporte a los empleados y crear mejores experiencias para sus clientes.

HP Client Security Manager proporciona mejoras en el inicio de sesión en Windows® y capacidades de inicio de sesión única para sitios web. Los administradores pueden usar estas herramientas para administrar recursos de seguridad exclusivos para sistemas de PDV, además de monitorear y diagnosticar problemas dentro del hardware. HP Client Security Manager también le permite evaluar la fortaleza de las contraseñas y usar credenciales de huellas digitales para proteger dispositivos dentro de su sistema.

La implementación remota de herramientas de HP lo ayuda a ahorrar tiempo y dinero al administrar e implementar configuraciones de seguridad para sus sistemas de PDV. Los administradores de TI pueden capturar las configuraciones actuales en un dispositivo central y replicarlas en el resto de los sistemas de la empresa. Así, los administradores de TI pueden monitorear dispositivos, actualizar firmware e incluso obtener informes avanzados y más, todo de manera remota.

El control de puerto de entrada/salida de HP lo ayuda a configurar y administrar con facilidad los puertos de los dispositivos. La capacidad de bloqueo y desbloqueo de puertos controlada por el BIOS ayuda a proteger contra ataques a través de unidades de almacenamiento de medios portátiles.

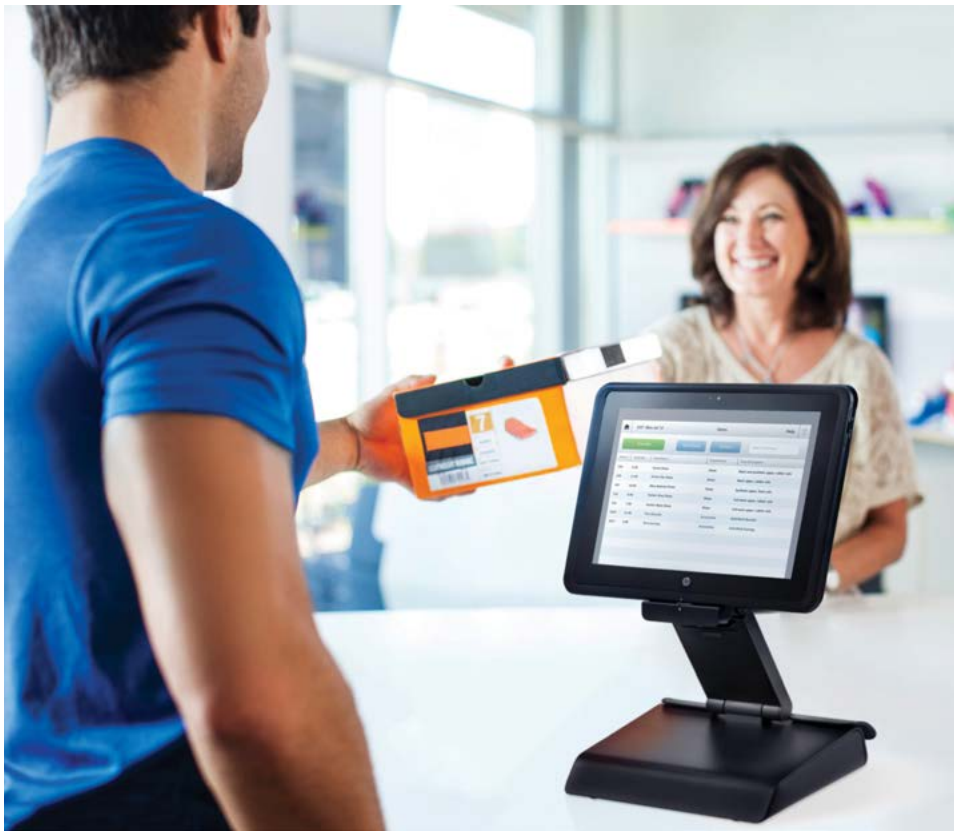
Figura 3. Los atacantes buscan más que simplemente los datos de las tarjetas de crédito. La información personal identificable tiene un ciclo de vida de meses, días, años o incluso décadas.

Retire los dispositivos y los datos de forma segura

Como parte de la recopilación de información que usted necesita para construir relaciones sólidas con el cliente y mejores resultados de negocios, es esencial eliminar los datos de forma segura cuando ya no son más necesarios. HP ofrece dos herramientas para ayudarlo a destruir con facilidad y seguridad datos antiguos para mantener sus dispositivos, su reputación y las identidades de los clientes seguros.

HP Secure Erase sobrescribe todos los datos en una unidad de estado sólido (SSD) Intel® o en una unidad de disco duro estándar, sin posibilidad de recuperación. Simplemente seleccione "Secure Erase" en el menú de seguridad y confirme la unidad que desea borrar.[5]

[5] Para los casos de uso indicados en el suplemento 5220.22-M del Departamento de Defensa (DoD). No es compatible con SSD. Requiere Windows en sistemas para comercio. No disponible en BIOS de desktops empresariales. Se requiere una conexión de red con el servidor de administración. Con Windows 8.1, el usuario debe apagar el modo de protección mejorada en IE11 para el recurso de cierre con eliminación de historial del explorador.



Siéntase tranquilo con la ayuda de un líder confiable

Ganarse y mantener la fidelidad del cliente es esencial para ayudar a que su comercio prospere. Mientras mejor conozca a sus clientes, más oportunidades y experiencias personales podrá ofrecer.

Mantenga esa confianza —estando siempre un paso al frente de los hackers, los ladrones y los usuarios no autorizados— con seguridad incorporada, no agregada con posterioridad. Los recursos de HP Client Security lo ayudan a rechazar un mundo de amenazas en cambio constante con protección para cubrir múltiples puntos de entrada, desde el BIOS y el hardware hasta las aplicaciones de software de PDV. Nuestros experimentados consultores pueden ayudarlo a identificar sus necesidades de seguridad específicas y a recomendar soluciones personalizadas adecuadas a su entorno.

Contacte a su representante de HP para comenzar u obtenga más información aquí.

Tabla 1. Recursos de seguridad HP.

Función	Descripción	Dispositivo	Datos	Identidad
HP BIOSphere con Sure Start	Solución de tecnología de autorreparación a nivel del BIOS creada para proteger contra malware y ataques a la seguridad orientados al BIOS	•	•	•
HP Client Security Manager	Estructura para administrar y configurar recursos de seguridad disponibles en PDV comerciales y plataformas de PC empresariales		•	•
Control de puertos de entrada/salida HP	Bloqueo/desbloqueo de puerto controlado por el BIOS para prevenir ataques desde medios USB de arranque	•	•	•
Implementación remota de herramientas de HP	Capture la imagen actual y replíquela en el conjunto de programas de administración de todos los otros sistemas.	•	•	
HP Secure Erase[5]	Recurso que destruye de forma permanente los datos de la unidad de disco duro para prepararla para la eliminación/redespliegue. Todos los datos en unidades SSD o de disco duro estándar son totalmente sobrescritos y no pueden recuperarse, incluso con herramientas avanzadas de recuperación		•	•
Unidad de autorreparación (SED) HP	Solución basada en hardware que cifra y descifra los datos a medida que se escriben o leen de la unidad de disco duro; esto protege los datos y minimiza la sobrecarga		•	•
Módulo de plataforma segura (TPM)	Procesador criptográfico que valida la integridad de la plataforma y proporciona almacenamiento de credenciales seguro para ayudar a garantizar la conformidad de interconexión de componentes periféricos	•	•	•
Windows 10 Credential Guard[3]	Recurso basado en Windows que utiliza el TPM para posibilitar autenticación de múltiples factores, lo que aumenta la protección contra el robo de credenciales	•	•	
Windows 10 Device Guard[4]	Seguridad basada en Windows 10 IOT Enterprise Virtualization que permite un bloqueo del cliente de PDV para que solo ejecute aplicaciones firmadas, confiables y aprobadas	•	•	•

Regístrese para recibir actualizaciones
hp.com/go/getupdated

Compartir con colegas

4AA6-9038SPL, enero de 2018