Comparativa de las características de seguridad de Windows 7 y Windows 10

Windows 10 está diseñado para defenderse de las amenazas modernas

Windows 7 ha sido el sistema que más éxito ha tenido y que a más usuarios ha llegado en la historia de Microsoft. Aunque en estos últimos cinco años nos ha funcionado muy bien, la realidad es que no proporciona el nivel de protección necesario contra las nuevas amenazas de seguridad a las que nos enfrentamos. A pesar de que se pueden incorporar niveles de defensa mediante productos de otros fabricantes, conviene tener en cuenta que todas las organizaciones que hemos visto en las noticias también lo hicieron y, sin embargo, no fue suficiente.

Los retos actuales requieren una nueva plataforma, y esa plataforma nos la proporciona Windows 10 mediante algunos de los siguientes mecanismos.

	Windows 7	Windows 10
PROTECCIÓN DE LA IDENTIDAD	Las soluciones multifactor actuales suelen ser complejas y caras.	**Microsoft Passport** es una alternativa a las herramientas multifactor de contraseñas que resulta fácil de usar e implementar.
	Los ataques de suplantación de identidad (phishing) a través de las contraseñas de usuarios son cada vez más fructíferos.	**Windows Hello** utiliza funciones biométricas que proporcionan un mecanismo más seguro para acceder al dispositivo, a Microsoft Passport, a las aplicaciones, a los datos y a los recursos en línea.*
	A través de ataques pass-the-hash, los atacantes pueden robar identidades, atravesar las redes y evitar las medidas de protección.	**Microsoft Azure Active Directory** es una solución integral para administrar el acceso y las identidades en la nube.
PROTECCIÓN DE LOS DATOS	BitLocker proporciona servicios configurables y opcionales para el cifrado de discos.	**BitLocker** contiene numerosas mejoras, resulta muy fácil de administrar y puede aprovisionarse automáticamente en la mayoría de los dispositivos nuevos.
	La prevención de pérdida de datos (DLP) requiere el uso de software adicional y, con frecuencia, funciones de otros fabricantes.	**Enterprise Data Protection** cubre las necesidades de DLP, incluye una solución altamente integrada para la separación de los datos y su inclusión en contenedores, y ofrece funciones de cifrado en el nivel de archivo.
	Las soluciones de DLP suelen menoscabar la experiencia del usuario en beneficio de la seguridad, lo que hace que su adopción sea limitada y que la experiencia difiera en los dispositivos móviles y en los equipos de escritorio.	**Enterprise Data Protection** proporciona a los usuarios una experiencia fluida tanto en dispositivos móviles como en equipos de escritorio y está integrado en Azure Active Directory y Rights Management Services.
RESISTENCIA FRENTE A AMENAZAS	Todas las aplicaciones se consideran de confianza hasta que se determina que constituyen una amenaza o hasta que se bloquean de forma explícita.	**Device Guard** proporciona un servicio de protección del escritorio que es similar a la función de bloqueo de las plataformas móviles (bloqueo completo de las aplicaciones).
	Con más de 300 000 nuevas amenazas al día, intentar bloquearlas mediante mecanismos de detección (bloquear los problemas conocidos) es una batalla perdida.	Con **Device Guard,** las aplicaciones deben demostrar que son de confianza antes de que se puedan ejecutar.
	Windows proporciona una serie de mecanismos de defensa, pero muchas amenazas de malware afectan a los usuarios antes de que los antivirus basados en detección puedan descubrirlas.	**Device Guard** será la función de resistencia contra malware más eficaz que Microsoft haya proporcionado nunca al escritorio.
SEGURIDAD DE LOS DISPOSITIVOS	La seguridad de la plataforma se basa íntegramente en lo que el software puede hacer por sí mismo; una vez infectado, no existe ninguna garantía de que las defensas del sistema puedan actuar sin ser manipuladas.	**La seguridad basada en hardware** y el nivel de confianza que ofrece ayuda a mantener y validar tanto el hardware como la integridad del sistema.
	El malware puede ocultarse en el hardware o en el sistema operativo, y no hay forma de validar su integridad una vez que se ha visto comprometido.	**El arranque seguro de UEFI** ayuda a impedir que el malware se incruste en el hardware o se inicie antes que el sistema operativo. Además, el arranque seguro ayuda a mantener la integridad de los demás componentes del sistema operativo.

*Windows Hello requiere hardware especializado, incluido un lector de huellas digitales, un sensor de infrarrojos iluminado u otros sensores biométricos.

Microsoft