DELL Technologies

Resumen de la solución

Personalización del arranque seguro en UEFI de Dell EMC PowerEdge

Tradicionalmente, en los entornos de servidores de centros de datos se ha enfocado gran parte de las labores de seguridad en los sistemas operativos, las aplicaciones y las redes. Dado que siguen aumentando las inquietudes de seguridad respecto de las infraestructuras de hardware, también se eleva el nivel de complejidad para los administradores de seguridad de TI. Una necesidad fundamental para los equipos de TI de seguridad y de servidores es establecer una base de computación de confianza y extender esa confianza a los sistemas operativos y las aplicaciones. Aunque, generalmente se reserva para las aplicaciones y los conjuntos de datos más seguros y confidenciales, la seguridad personalizada para infraestructuras está llegando rápidamente a la delantera. La amenaza en evolución para el hardware del servidor requiere un enfoque más integral, incluida la personalización del arranque seguro en UEFI, a fin de fortalecer esta base de confianza.

Esto comienza con la arquitectura de resistencia cibernética de Dell EMC, la que valida el BIOS y el firmware para la Integrated Dell Remote Access Controller (iDRAC) antes de que se cargue. El firmware de los demás componentes críticos también se valida mediante el uso de certificados criptográficos almacenados para garantizar que el firmware auténtico se esté ejecutando en el servidor.

Arquitectura de resistencia cibernética de Dell EMC

Protección eficaz

- Raíz de confianza de hardware basada en silicio
- Actualizaciones firmadas de firmware
- Bloqueo del sistema
- Contraseñas predeterminadas seguras

Detección confiable

- Configuración y detección de desviaciones de firmware
- Registro de eventos persistente, incluida la actividad del usuario
- Alertas seguras

Recuperación rápida

- Recuperación automática del BIOS
- Recuperación rápida de SO
- Eliminación del sistema

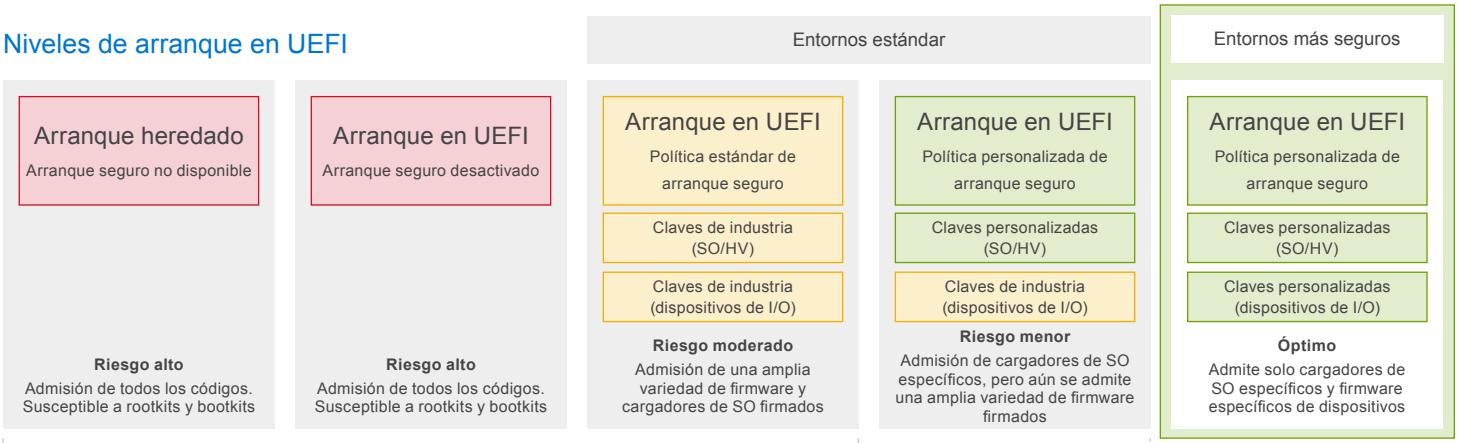
Como el reemplazo moderno para los controles de inicio y la configuración del BIOS heredada, el arranque seguro en UEFI inicializa las funciones base del servidor antes de que se inicie un hipervisor o un sistema operativo. Los servidores PowerEdge utilizan el arranque seguro en UEFI para verificar los certificados generados de forma criptográfica de los controladores de UEFI y los cargadores de arranque del sistema operativo. Estas son las “claves” que permiten que el servidor valide lo siguiente:

- controladores de UEFI cargados de tarjetas PCIe
- controladores y ejecutables de UEFI cargados de dispositivos de almacenamiento masivo
- cargadores de arranque de sistemas operativos; por lo general, Linux o Microsoft Windows

Este proceso de validación es fundamental para proteger al servidor de la iniciación proveniente de códigos no autorizados antes del inicio del sistema operativo. La validación del firmware de UEFI está diseñada para prohibir que un software no firmado se ejecute en el sistema a través de la verificación de la firma del cargador de arranque, el kernel y otros códigos de espacios de usuario.

La personalización del arranque seguro en UEFI de Dell EMC PowerEdge también ofrece la capacidad única de admitir certificados personalizados generados y firmados por una autoridad distinta de Microsoft. Microsoft es la autoridad de certificación predeterminada para los dispositivos compatibles con UEFI y los sistemas operativos. Se ha implementado un certificado de Microsoft en muchas distribuciones de Linux estándar. En los casos en que se emplea un entorno de Linux no estándar (es decir, modificaciones exclusivas del kernel o del controlador), existe la necesidad de contar con certificados generados a la medida, firmados de forma criptográfica por el usuario, con el fin de validar automáticamente el cargador de arranque y mantener el hardware en la cadena de software de confianza.

Niveles de arranque en UEFI



Mejore la seguridad de los servidores sin hacer sacrificios

El proceso de arranque es primordial para la seguridad de cualquier dispositivo. Se basa en una gran cantidad de firmware que controla la forma en que se inician los componentes y periféricos de un dispositivo, así como la carga del sistema operativo. Cuanto más pronto se carga el código, más privilegios tiene y más daños puede causar si no se autentica primero. Si el proceso de arranque se ve comprometido, los atacantes pueden alterar los controles de seguridad, lo que les permite obtener acceso no autorizado a diversas partes del sistema de forma efectiva. Incluso, podría ser posible crear ransomware mediante cargadores de arranque de UEFI maliciosos para tomar el control de los servidores cuando se inician, lo que, a su vez, permite reconfigurar la computadora, cifrar los datos y causar estragos.

Reducción del riesgo

Gracias a las opciones modernas de configuración y control, estará más preparado que nunca para proteger sus servidores de ataques de firmware o de cargadores de arranque. La personalización del arranque seguro en UEFI de Dell EMC PowerEdge permite aumentar la seguridad de la infraestructura de su servidor y, al mismo tiempo, dejar atrás los métodos de arranque de BIOS heredados. En una deliberación reciente de la Agencia de Seguridad Nacional (NSA) del Gobierno de los Estados Unidos, se documenta el tema de contar con una mayor seguridad de hardware en servidores, y se cita específicamente el uso de la personalización del arranque seguro en UEFI de PowerEdge como un método que ofrece un nivel de seguridad significativamente más alto, junto con la flexibilidad para admitir diversos sistemas operativos. En un informe técnico sobre ciberseguridad relacionado de la NSA, se menciona que “el modo personalizado permite que el propietario del sistema estreche o amplíe la selección de soluciones de hardware y software de confianza…” y se demuestra cómo se puede lograr esto mediante la utilidad de configuración de UEFI integrada de Dell[1]. Este control granular permite reducir o eliminar las amenazas de configuraciones erróneas, manipulaciones y la presencia de malware. Los administradores de sistemas podrán reaccionar más rápido a las nuevas amenazas de arranque y estarán protegidos contra posibles errores de firma de certificados cometidos por los proveedores.

Características del arranque seguro en UEFI con certificados personalizados

Características	Descripción	Beneficios
Inicio seguro	• Validación de firmware y componentes clave	• Adopción de una validación de firmware moderna, que permite olvidar las limitaciones y las amenazas de seguridad del BIOS heredado
Certificados autofirmados	• Mantenimiento de la iniciación del sistema operativo, del cargador de arranque y de los firmware seguros en todas las operaciones del servidor	• Soporte para compilaciones de SO personalizadas en implementaciones altamente seguras • Independencia de la autoridad de firmas predeterminada cuando se implementan hardware personalizados y firmware asociados
Cumplimiento de las pautas de seguridad	• Alineación con los estándares de seguridad para el proceso de arranque del servidor, la validación de firmware y la administración de certificados personalizada	• Establecimiento del estándar para la seguridad del firmware y el hardware del servidor • Posicionamiento de las operaciones del servidor para el cumplimiento de las pautas futuras de seguridad de los servidores en entornos confidenciales
Integración en iDRAC y TPM	• Aprovechamiento de las características de seguridad de hardware y firmware actuales e integradas en los servidores PowerEdge	• Aumento del valor de las características de seguridad integradas a fin de establecer una raíz de confianza integral para el hardware

[1] Al igual que con la mayoría de las opciones de configuración de sistema, un administrador puede utilizar otras herramientas, además de la configuración del sistema, para habilitar la política estándar de arranque seguro. En las herramientas Deployment Toolkit™ (DTK), Lifecycle Controller™, OpenManage™ y las consolas RACADM y WS-MAN de Dell, también es posible habilitar la política estándar de arranque seguro.

Obtenga más información acerca de los servidores PowerEdge

Obtenga más información acerca de las soluciones de Dell EMC OpenManage Enterprise

Obtenga más información acerca de nuestras soluciones de administración de sistemas

Busque contenido en nuestra biblioteca de recursos

Siga a los servidores PowerEdge en Twitter

Comuníquese con un experto de Dell Technologies para obtener asistencia de ventas o soporte

DELL Technologies