

Dell Technologies Secured Component Verification para PowerEdge

La defensa contra los ataques de ciberseguridad continúa siendo un desafío para los equipos de Operaciones y Seguridad de TI en cada nivel de su infraestructura. Si bien el vector de ataque más común corresponde a impactos en los sistemas operativos y las aplicaciones, en vista de que utilizan malware y ransomware, los ataques de hardware también están en auge. Debido a esta amenaza creciente, se está poniendo cada vez más atención a los servidores y la garantía de que no se hayan producido alteraciones en la configuración del hardware del servidor entre el momento en que se desarrolla el sistema y el momento en que se implementa. No es de extrañar que el 84 % de los encuestados en una encuesta de Forrester Research¹ considerara que la seguridad del hardware/cadena de suministro es crítica o muy importante para su negocio.

Dell Technologies Secured Component Verification realiza una verificación de la configuración de hardware conforme a como se desarrolló para sus servidores PowerEdge. La verificación le permite implementar con confianza nuevos servidores en su centro de trabajo, de modo que tiene la certeza de que la configuración de hardware le proporcionará una base sólida para sus aplicaciones de misión crítica. Secured Component Verification está alineada con las pautas emergentes del Gobierno de EE. UU. para la seguridad de la cadena de suministro de tecnología.

Implemente servidores con confianza

Dell Technologies Secured Component Verification, que ahora es una parte integral de la línea de servidores Dell EMC PowerEdge, permite a los administradores de TI validar de manera segura los sistemas desarrollados antes de la implementación. Las organizaciones pueden asegurarse de que sus nuevos servidores se desarrollen con los mismos componentes instalados en las instalaciones de fabricación de Dell Technologies.

Cuando el sistema está listo para el envío, se evalúan los componentes del servidor y sus ID únicos, y los datos resultantes se protegen de forma criptográfica mediante un certificado firmado. El inventario cifrado está integrado en el servidor y se envía con el sistema al centro de datos. Después de que se recibe el sistema, el administrador de TI realizará un inventario del sistema desarrollado mediante la herramienta SCV que se proporcionó y autenticará ese inventario con el certificado almacenado en el sistema. Una vez autenticado, y los componentes verificados para garantizar que coincidan, el sistema está listo para su aprovisionamiento e implementación.



¹ Fuente: Forrester Research, Inc., The Next Frontier for Endpoint Protection

La necesidad de una cadena de suministro de tecnología segura adquiere importancia

El Gobierno de EE. UU., en colaboración con sus partners comerciales globales, ha continuado perfeccionando su orientación respecto a la ciberseguridad. En relación con la infraestructura de servidores, recientemente se han enfocado más en la validación de los componentes de servidor y la autenticidad del firmware en esos servidores. En su documento preliminar más reciente, el National Cybersecurity Center of Excellence (NCCoE), parte del Instituto Nacional de Estándares y Tecnología (NIST), planteó claramente el desafío: todos los OEM de servidores están trabajando con numerosos proveedores de componentes y subsistemas. A pesar de que todos han implementado programas de garantía de la cadena de suministro para que la calidad y la seguridad de los componentes de sus proveedores estén aseguradas, no ha existido una manera sencilla de que el usuario final valide que lo que se instaló en la fábrica sea exactamente lo que recibió. Dell Technologies está colaborando con el NCCoE en el Supply Chain Assurance Building Block Consortium para desarrollar enfoques de ciberseguridad prácticos e interoperables que abordan las necesidades del mundo real de los sistemas complejos de tecnología de la información (TI)².

Dell Technologies Secured Component Verification: una base segura para las aplicaciones de confianza

En el entorno de ciberseguridad actual, que está en constante evolución y donde el software y el hardware son objetivos potenciales de penetración, hay una clara necesidad de mayor garantía y confianza en la infraestructura de servidores. Para seguir el ritmo de la creciente demanda de desarrollo, pruebas e implementación de aplicaciones con mayor rapidez, se deben incorporar nuevas funciones, como Secured Component Verification, en el ciclo de vida de la infraestructura. Con SCV, los equipos de Operaciones y Seguridad de TI pueden estar seguros de que sus sistemas conforme a como se entregaron están alineados con las especificaciones de su servidor y su infraestructura de seguridad, lo que elimina un posible vector de ataque, de modo que enfocan su energía en los resultados del negocio.

Características y beneficios de Secured Component Verification:

- Certificados de inventario firmados criptográficamente disponibles en todo el portafolio de servidores PowerEdge
- Garantía de fábrica a rack: la verificación automática segura garantiza la integridad total del hardware durante el tránsito hacia el centro de datos
- Integración con scripts existentes para facilitar el proceso de validación, lo que hace que la implementación de confianza sea un proceso que se puede automatizar
- Conformidad con los estándares emergentes para la seguridad de la cadena de suministro, lo que es importante para las industrias en las que la ciberseguridad es la principal prioridad

² NIST no evalúa productos comerciales en virtud de este consorcio y no avala ningún producto o servicio utilizado.

Puede encontrar información adicional sobre este consorcio en: <https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance>

Obtenga más información acerca de los servidores PowerEdge



Obtenga más información
sobre Dell Technologies
Secured Component
Verification



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