DELL Technologies

Lösungsübersicht

Dell Technologies Secured Component Verification für PowerEdge

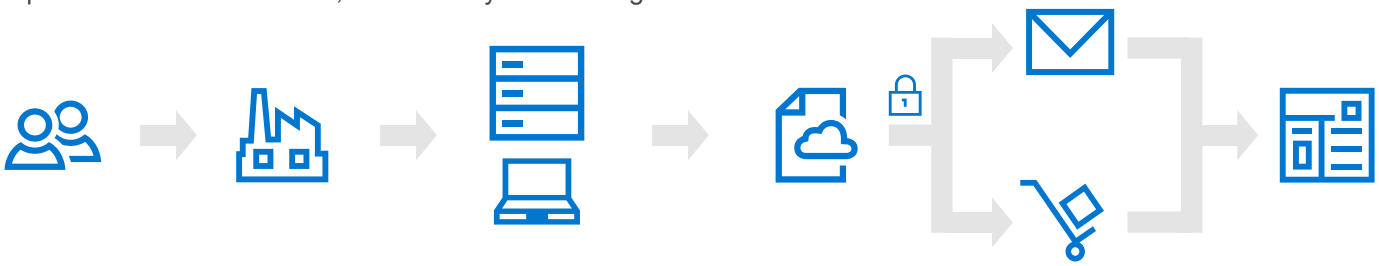
Der Schutz vor Cybersicherheitsangriffen bleibt eine Herausforderung für IT-Betriebs- und -Sicherheitsteams auf allen Leveln der Infrastruktur. Zwar sind Kompromittierungen von Anwendungen und Betriebssystemen die gängigeren Angriffsvektoren, aber auch Hardwareangriffe mithilfe von Malware und Ransomware sind auf dem Vormarsch. Aufgrund dieser wachsenden Bedrohung wird die Aufmerksamkeit immer stärker auf Server und die Absicherung gerichtet, dass die Serverhardwarekonfiguration zwischen dem Zeitpunkt der Systemproduktion und dem Zeitpunkt der Systembereitstellung nicht geändert wurde. Es ist nicht verwunderlich, dass 84 % der Befragten einer Forrester Research-Umfrage[1] die Hardware-/Lieferkettensicherheit als kritisch oder sehr wichtig für ihr Unternehmen einstuften.

Dell Technologies Secured Component Verification bietet eine Verifizierung der As-Built-Hardwarekonfiguration für Ihre PowerEdge-Server. Die Verifizierung ermöglicht Ihnen die zuversichtliche Bereitstellung neuer Server in Ihrem Rechenzentrum mit der Gewissheit, dass die Hardwarekonfiguration Ihnen eine solide Grundlage für Ihre erfolgskritischen Anwendungen bereitstellt. Secured Component Verification ist an den aufkommenden Richtlinien für Sicherheit in der Technologielieferkette der US-Regierung ausgerichtet.

Zuverlässige Bereitstellung von Servern

Dell Technologies Secured Component Verification ist jetzt ein wesentlicher Bestandteil der Dell EMC PowerEdge-Serverproduktreihe. Mit der Lösung können IT-Administratoren ihre gelieferten Systeme vor der Bereitstellung auf sichere Weise validieren. Unternehmen können sicherstellen, dass ihre neuen Server mit denselben Komponenten ausgeliefert werden, die im Dell Technologies Werk installiert wurden.

Wenn das System zur Auslieferung bereit ist, werden die Serverkomponenten und ihre eindeutigen IDs ausgewertet und die resultierenden Daten mithilfe eines signierten Zertifikats kryptografisch gesichert. Der verschlüsselte Bestand ist in den Server integriert und wird mit dem System an das Rechenzentrum ausgeliefert. Nach Eingang des Systems führt der IT-Administrator eine Bestandsaufnahme des gelieferten Systems mithilfe des bereitgestellten SCV-Tools durch und authentifiziert diesen Bestand mit dem im System gespeicherten Zertifikat. Wenn die Authentifizierung erfolgt ist und die Komponenten übereinstimmen, kann das System bereitgestellt werden.



Bestellung

Der Kunde gibt eine Bestellung für ein Serverprodukt auf.

Produktion

Die Bestellung wird zur Produktion an das Werk gesendet.

Keine Änderung an vorhandener Bestellung

→

Produktionsprozess

Erfassung

Die Komponentendaten des Systems werden erfasst und verschlüsselt. Ein Plattformzertifikat wird erstellt und von einem HSM (High Security Module) signiert.

Speicherung

Das Plattformzertifikat wird an einem zentralen Speicherort (DL für Services) und auf dem Server (iDRAC) gespeichert.

Bereitstellung

Das von Dell signierte Zertifikat wird auf dem Server (iDRAC) an den Kunden geliefert.

Validierung

Der Kunde validiert die Authentizität der Komponenten über das lokale Systemmanagementtool.

[1] Quelle: Forrester Research, Inc., „The Next Frontier for Endpoint Protection“

Fokussierung auf die Notwendigkeit einer sicheren Technologielieferkette

Die US-Regierung hat in Zusammenarbeit mit ihren weltweiten Handelspartnern ihre Richtlinien für Cybersicherheit weiter präzisiert. Im Hinblick auf die Serverinfrastruktur hat sie sich kürzlich stärker auf die Validierung von Serverkomponenten und die Authentizität der Firmware auf diesen Servern konzentriert. Das NCCoE (National Cybersecurity Center of Excellence), das zum National Institute of Standards and Technology gehört, hat in seinem neuesten Entwurfspapier die Herausforderung klar herausgestellt: Alle Server-OEMs arbeiten mit zahlreichen Komponenten und Subsystemanbietern. Zwar haben alle Programme für die Absicherung der Lieferkette eingeführt, um die Qualität und Sicherheit der Komponenten ihrer Zulieferer zu gewährleisten, aber der Endnutzer konnte bisher nicht auf einfache Weise validieren, dass sie tatsächlich die werkseitig installierten Komponenten erhalten haben. Dell Technologies arbeitet mit dem NCCoE im Supply Chain Assurance Building Block Consortium zusammen, um praktikable und interoperable Cybersicherheitsansätze zu entwickeln, die auf die realen Anforderungen komplexer IT-Systeme eingehen.[2]

Dell Technologies Secured Component Verification – eine sichere Grundlage für vertrauenswürdige Anwendungen

In der heutigen sich weiter entwickelnden Cybersicherheitsumgebung, in der Software und Hardware potenzielle Durchdringungsziele sind, besteht eindeutig die Notwendigkeit, die Sicherheit und das Vertrauen in die Serverinfrastruktur zu erhöhen. Um mit der wachsenden Nachfrage nach einer Beschleunigung der Entwicklung, Tests und Bereitstellung von Anwendungen Schritt zu halten, müssen neue Funktionen wie Secure Component Validation in den Infrastrukturlebenszyklus integriert werden. Mit SCV können IT-Betriebs- und -Sicherheitsteams sicher sein, dass ihre gelieferten Systeme an ihren Serverspezifikationen und ihrem Sicherheits-Framework ausgerichtet sind. Dadurch wird ein potenzieller Angriffsvektor beseitigt, sodass sie ihre Energie auf die Geschäftsergebnisse konzentrieren können.

Funktionen und Vorteile von Secured Component Verification:

- Kryptografisch signierte Bestandszertifikate, die im gesamten PowerEdge-Serverportfolio verfügbar sind
- Absicherung vom Werk bis zum Rack mit einer sicheren Selbstvalidierung zur Gewährleistung der vollständigen Hardwareintegrität während des Transports zu Ihrem Rechenzentrum
- Integration in vorhandene Skripte zur Vereinfachung des Validierungsprozesses, damit die vertrauenswürdige Bereitstellung zu einem automatisierbaren Prozess wird
- Ausrichtung an aufkommenden Standards für die Lieferkettensicherheit, ein wichtiger Punkt für Branchen, in denen Cybersicherheit höchste Priorität hat

[2] NIST bewertet im Rahmen dieses Konsortiums keine kommerziellen Produkte und gibt keine Empfehlungen für verwendete Produkte oder Services ab. Weitere Informationen zu diesem Konsortium finden Sie unter: https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

Erfahren Sie mehr über PowerEdge-Server.

Weitere Informationen zu Dell Technologies Secured Component Verification

Weitere Informationen zu unseren Systemmanagementlösungen

Durchsuchen Sie unsere Ressourcenbibliothek

Folgen Sie PowerEdge-Server auf Twitter

Wenden Sie sich an einen Dell Technologies Experten für Vertrieb oder Support

DELL Technologies