DELL Technologies

Présentation de la solution

Dell Technologies Secured Component Verification pour PowerEdge

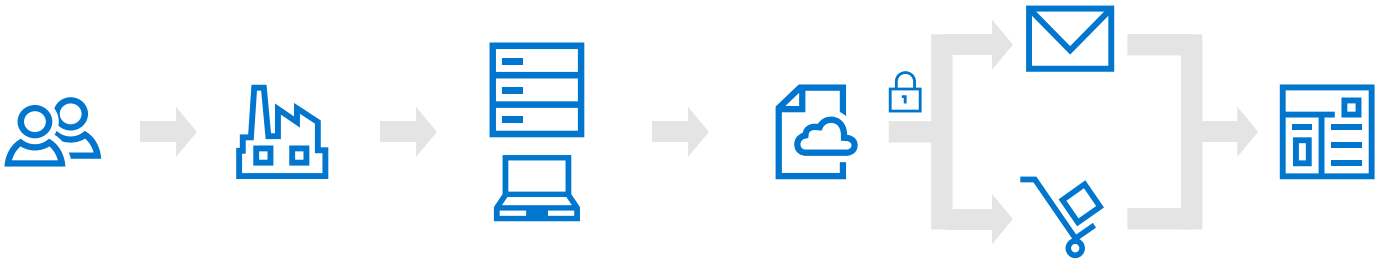
La défense contre les attaques de cybersécurité reste un défi pour les équipes des opérations et de sécurité IT à tous les niveaux de leur infrastructure. Alors que les compromissions des applications et des systèmes d'exploitation sont les vecteurs d'attaque les plus courants, via des logiciels malveillants et des programmes de rançon, les attaques matérielles sont également en hausse. En raison de cette menace en pleine expansion, l'attention se porte de plus en plus sur les serveurs et l'assurance que la configuration matérielle du serveur n'a fait l'objet d'aucune altération entre la création et le déploiement du système. Il n'est pas étonnant que 84 % des personnes interrogées dans le cadre de l'enquête Forrester Research[1] aient considéré la sécurité du matériel/de la chaîne d'approvisionnement comme essentielle ou importante pour leur entreprise.

Dell Technologies Secured Component Verification permet de vérifier la configuration matérielle intégrée de vos serveurs PowerEdge. La vérification vous permet de déployer en toute confiance de nouveaux serveurs dans votre datacenter, car vous savez que la configuration matérielle vous fournira une base solide pour vos applications essentielles. Secured Component Verification est aligné sur les directives émergentes du gouvernement américain concernant la sécurité de la chaîne d'approvisionnement.

Déployez vos serveurs en toute confiance

Dell Technologies Secured Component Verification, qui fait désormais partie intégrante de la gamme de serveurs Dell EMC PowerEdge, permet aux administrateurs IT de valider en toute sécurité les systèmes livrés avant le déploiement. Les entreprises peuvent s'assurer que leurs nouveaux serveurs sont livrés avec les mêmes composants installés que dans les sites de fabrication de Dell Technologies.

Lorsque le système est prêt à être expédié, les composants du serveur et leurs ID uniques sont évalués et les données obtenues sont sécurisées par chiffrement à l'aide d'un certificat signé. L'inventaire chiffré est intégré au serveur et livré avec le système au datacenter. Une fois le système reçu, l'administrateur IT effectue un inventaire du système livré à l'aide de l'outil SCV fourni et authentifie cet inventaire avec le certificat stocké sur le système. Une fois l'inventaire authentifié et la correspondance des composants vérifiée, le système est prêt à être configuré et déployé.



Commande
Le client commande un produit de serveur

Créer
La commande est envoyée à l'usine à des fins de fabrication

Collecter
Les données des composants du système sont collectées, chiffrées et un certificat de plate-forme est créé et signé par un module HSM (High Security Module)

Stockage
Le certificat de plate-forme est stocké dans un emplacement central (DL pour les services) et sur le serveur (iDRAC)

Livraison
Le certificat signé Dell est livré au client sur le serveur (iDRAC)

Valider
Le client valide l'authenticité des composants via l'outil de gestion des systèmes locaux

La commande existante reste inchangée

Processus de création

[1] Source : Forrester Research, Inc., The Next Frontier for Endpoint Protection

La nécessité d'une chaîne d'approvisionnement technologique sécurisée s'impose

Le gouvernement américain, en collaboration avec ses partenaires commerciaux internationaux, a continué à peaufiner ses conseils en matière de cybersécurité. En ce qui concerne l'infrastructure de serveurs, il a récemment axé son attention sur la validation des composants de serveur et sur l'authenticité des firmware présents sur ces serveurs. Dans son projet de document le plus récent, le National Cybersecurity Center of Excellence (NCCoE), qui fait partie du National Institute of Standards and Technology, a clairement illustré ce défi : tous les fabricants de serveurs collaborent avec de nombreux fournisseurs de composants et de sous-systèmes. Bien qu'ils aient tous mis en place des programmes d'assurance de la chaîne d'approvisionnement pour garantir la qualité et la sécurité des composants de leurs fournisseurs, l'utilisateur final n'est pas en mesure de confirmer facilement que les composants installés en usine correspondent exactement à ce qu'il a reçu. Dell Technologies collabore avec le NCCoE dans le cadre du Supply Chain Assurance Building Block Consortium pour développer des approches de cybersécurité pratiques et interopérables qui répondent aux besoins réels des systèmes des technologies de l'information (IT) complexes.[2]

Dell Technologies Secured Component Verification : une base sécurisée pour des applications de confiance

Dans l'environnement de cybersécurité en constante évolution, dans lequel les logiciels et le matériel sont des cibles de pénétration potentielles, il est évident qu'il est nécessaire d'accroître l'assurance et la confiance dans l'infrastructure de serveurs. Pour suivre le rythme de la demande croissante en matière de développement, de test et de déploiement d'applications plus rapides, les nouvelles fonctionnalités telles que la validation des composants sécurisés doivent être intégrées au cycle de vie des infrastructures. Avec SCV, les équipes chargées des opérations et de la sécurité IT peuvent être assurées que leurs systèmes livrés sont alignés sur les spécifications de leurs serveurs et sur leur cadre de sécurité, éliminant ainsi un vecteur d'attaque potentiel afin de concentrer leur énergie sur les résultats opérationnels.

Fonctionnalités et avantages de Secured Component Verification :

- Certificats d'inventaire signés par chiffrement disponibles dans toute la gamme de serveurs PowerEdge
- Assurance de l'usine au rack : la vérification automatique sécurisée garantit une intégrité matérielle complète pendant le transit vers votre datacenter
- Intégration avec les scripts existants pour faciliter le processus de validation, transformant ainsi le déploiement fiable en processus pouvant être automatisé
- S'aligne sur les normes émergentes en matière de sécurité de la chaîne d'approvisionnement, ce qui est important pour les secteurs dans lesquels la cybersécurité est la priorité absolue

[2] NIST n'évalue pas les produits commerciaux dans le cadre de ce consortium et ne soutient aucun produit ou service utilisé.
Pour des informations complémentaires sur ce consortium, consultez le site suivant : https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

En savoir plus sur les serveurs PowerEdge

En savoir plus sur Dell Technologies Secured Component Verification

En savoir plus sur nos solutions de gestion des systèmes

Effectuer une recherche dans notre bibliothèque de ressources

Suivre les serveurs PowerEdge sur Twitter

Contacter un expert Dell Technologies pour une question sur les ventes ou le support

DELL Technologies