DELL Technologies

솔루션 브리프

PowerEdge를 위한 Dell Technologies 보안 구성 요소 검증

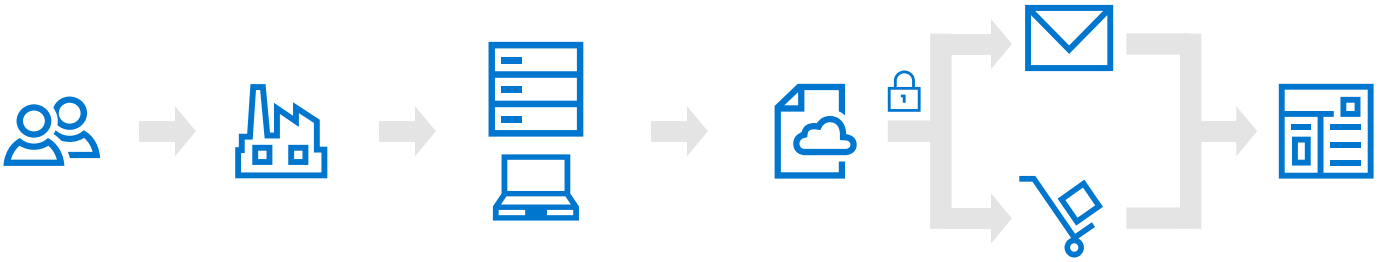
IT 운영 및 보안 팀은 인프라스트럭처의 모든 레벨에서 사이버 보안 공격을 방어하는 데 있어서 지속적인 어려움을 겪고 있습니다. 애플리케이션 및 운영 체제 손상이 멀웨어 및 랜섬웨어를 활용하는 가장 일반적인 공격 벡터이지만, 하드웨어 공격도 증가하고 있습니다. 이처럼 증가하는 위협으로 인해, 서버에 대한 관심이 점점 더 높아지고 있으며 시스템을 제작할 때와 구축할 때 사이의 시간에 서버 하드웨어 구성이 전혀 바뀌지 않았다는 것에 대한 확신이 요구됩니다. Forrester Research 설문조사[1] 응답자 중 84%가 하드웨어/공급망 보안이 비즈니스에 핵심적이거나 매우 중요하다고 생각하는 것은 당연한 결과입니다.

Dell Technologies 보안 구성 요소 검증은 PowerEdge 서버의 하드웨어 구성이 처음 그대로라는 것을 검증해 줍니다. 이 검증 덕분에 하드웨어 구성이 미션 크리티컬 애플리케이션을 위한 탄탄한 기반을 제공할 것임을 확신하면서 데이터 센터에서 새 서버를 자신 있게 구축할 수 있습니다. 보안 구성 요소 검증은 기술 공급망 보안에 대한 미국 정부의 새로운 지침에 부합합니다.

자신 있게 서버 구축

이제 Dell EMC PowerEdge 서버 라인의 필수적인 부분인 Dell Technologies 보안 구성 요소 검증은 IT 관리자가 배송된 시스템을 구축하기 전에 안전하게 검증할 수 있도록 해줍니다. 조직은 새로운 서버가 Dell Technologies의 제조 시설에서 설치한 구성 요소가 그대로 배송되었는지를 확인할 수 있습니다.

시스템이 배송 준비가 되면 서버 구성 요소와 해당 고유 ID가 평가되고, 최종 데이터는 서명된 인증서를 사용하여 암호화 방식으로 보호됩니다. 암호화된 인벤토리가 서버에 내장되고 시스템과 함께 데이터 센터로 배송됩니다. IT 관리자는 시스템을 수령한 후 제공된 SCV 툴을 사용하여 배송된 시스템의 인벤토리를 살펴보고, 해당 인벤토리를 시스템에 저장된 인증서와 비교하여 인증할 수 있습니다. 구성 요소가 일치하는 것이 확인되고 인증되면 시스템을 프로비저닝하고 배포할 준비가 된 것입니다.



주문
고객이 서버 제품을 주문함

제작
제작을 위해 주문이 공장에 전달됨

기존 주문에 변경 사항 없음
→
제작 프로세스

수집
시스템의 구성 요소 데이터가 수집되어 암호화되고 플랫폼 인증서가 생성되어 HSM(High Security Module)에 의해 서명됨

저장
플랫폼 인증서가 중앙 위치(Services의 경우 DL) 및 서버(iDRAC)에 저장됨

제공
Dell 서명 인증서가 서버(iDRAC)에 포함되어 고객에게 전달됨

검증
고객이 로컬 시스템 관리 툴을 통해 구성 요소가 정품인지 검증함

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

보안 기술 공급망의 필요성 대두

미국 정부는 글로벌 무역 파트너들과 협력하여 사이버 보안에 대한 지침을 지속적으로 개선해 왔습니다. 서버 인프라스트럭처와 관련하여, 최근에는 서버 구성 요소의 검증과 해당 서버 펌웨어의 신뢰성에 초점을 맞추고 있습니다. 미국 국립표준기술원(National Institute of Standards and Technology) 산하 NCCoE(National Cybersecurity Center of Excellence)는 가장 최근의 초안 백서에서 당면 과제를 명확히 설명했습니다. 모든 서버 OEM은 수많은 구성 요소 및 서브시스템 공급업체와 협력하고 있습니다. 모든 기업들이 공급업체 구성 요소의 품질과 보안을 보장하기 위해 공급망 보증 프로그램을 도입했지만, 최종 사용자의 입장에서는 공장에서 설치한 그대로의 제품을 받고 있는지를 검증할 수 있는 손쉬운 방법이 없었습니다. Dell Technologies는 NCCoE에서 진행하는 공급망 보증 빌딩 블록 컨소시엄에 참여하여 복잡한 IT(Information Technology) 시스템의 실제 요구 사항을 해결하는 실용적이고 상호 운용 가능한 사이버 보안 접근 방식을 개발하고 있습니다.[2]

Dell Technologies 보안 구성 요소 검증 - 신뢰할 수 있는 애플리케이션을 위한 안전한 기반

소프트웨어와 하드웨어가 잠재적인 침투 대상이 되는 오늘날의 진화하는 사이버 보안 환경에서는 서버 인프라스트럭처에 대한 보증과 신뢰도를 높일 필요가 분명히 있습니다. 더 빠른 애플리케이션 개발, 테스트, 배포에 대한 수요가 점점 커지고 있으며 이에 보조를 맞추려면 보안 구성 요소 검증과 같은 새로운 기능을 인프라스트럭처 수명주기에 통합해야 합니다. IT 운영 및 보안 팀은 SCV를 사용하여 배송된 시스템이 서버 사양 및 보안 프레임워크에 부합한다는 것을 확인하고 잠재적인 공격 벡터를 없앰으로써 비즈니스 성과에 집중할 수 있습니다.

보안 구성 요소 검증의 특징 및 이점:

- PowerEdge 서버 포트폴리오 전반에서 암호화 방식으로 서명된 인벤토리 인증서 사용 가능
- 공장에서 랙까지 보장 - 안전한 자체 검증을 통해 데이터 센터로 운송되는 동안 완전한 하드웨어 무결성 보장
- 기존 스크립트와의 통합을 통해 검증 프로세스를 용이하게 만들고, 신뢰할 수 있는 구축을 자동화 가능한 프로세스로 전환
- 새로운 공급망 보안 표준에 부합(사이버 보안이 최우선 순위인 업계에서 중요함)

[2] NIST는 이 컨소시엄에 속한 상업용 제품을 평가하지 않으며 사용된 제품 또는 서비스를 보증하지 않습니다. 이 컨소시엄에 대한 추가 정보는 다음 링크에서 확인할 수 있습니다. https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

PowerEdge 서버에 대해 자세히 알아보기

Dell Technologies 보안 구성 요소 검증에 대한 자세한 정보

시스템 관리 솔루션에 대한 자세한 정보

리소스 라이브러리 검색

Twitter에서 PowerEdge 서버 팔로우

Dell Technologies 영업 및 지원 전문가에게 문의

DELL Technologies