DELL Technologies

솔루션 브리프

Dell EMC PowerEdge의 UEFI 보안 부팅 맞춤 구성

데이터 센터 서버 환경은 기존에는 운영 체제, 애플리케이션, 네트워크 수준의 보안 작업에 주로 집중했습니다. 하드웨어 인프라스트럭처 보안 문제가 계속해서 늘어남에 따라 IT 보안 관리자가 담당해야 할 작업의 복잡성도 가중되고 있습니다. 서버 및 보안 IT 팀에 근본적으로 필요한 것은 신뢰할 수 있는 컴퓨팅 기반을 구축하고 운영 체제 및 애플리케이션으로 이러한 신뢰 구조를 확장하는 것입니다. 일반적으로 가장 중요하게 보호해야 할 애플리케이션 및 데이터 세트를 위한 보호 수단으로 맞춤형 인프라스트럭처 보안이 빠르게 부각되고 있습니다. 서버 하드웨어에 대한 위협이 날로 진화함에 따라 UEFI 보안 부팅 맞춤 구성을 비롯하여 신뢰할 수 있는 기반을 강화하는 더욱 포괄적인 접근 방식이 필요합니다.

이러한 접근 방식은 iDRAC(Integrated Dell Remote Access Controller)가 로드되기 전에 이에 대한 BIOS 및 펌웨어를 검증하는 Dell EMC의 사이버 회복탄력성을 갖춘 아키텍처를 기반으로 합니다. 또한 저장된 암호화 인증서를 사용하여 다른 중요 구성 요소에 대한 펌웨어가 검증되므로 신뢰할 수 있는 펌웨어가 서버에서 실행되도록 합니다.

사이버 회복탄력성을 갖춘 Dell EMC 아키텍처

효과적인 보호

- 칩 내장형의 하드웨어 RoT(Root of Trust)
- 서명된 펌웨어 업데이트
- 시스템 잠금
- 기본 암호 보안

신뢰할 수 있는 탐지

- 구성 및 펌웨어 변동 탐지
- 사용자 활동을 비롯하여 지속적인 이벤트 로깅
- 보안 알림

신속한 복구

- 자동 BIOS 복구
- 빠른 OS 복구
- 시스템 삭제

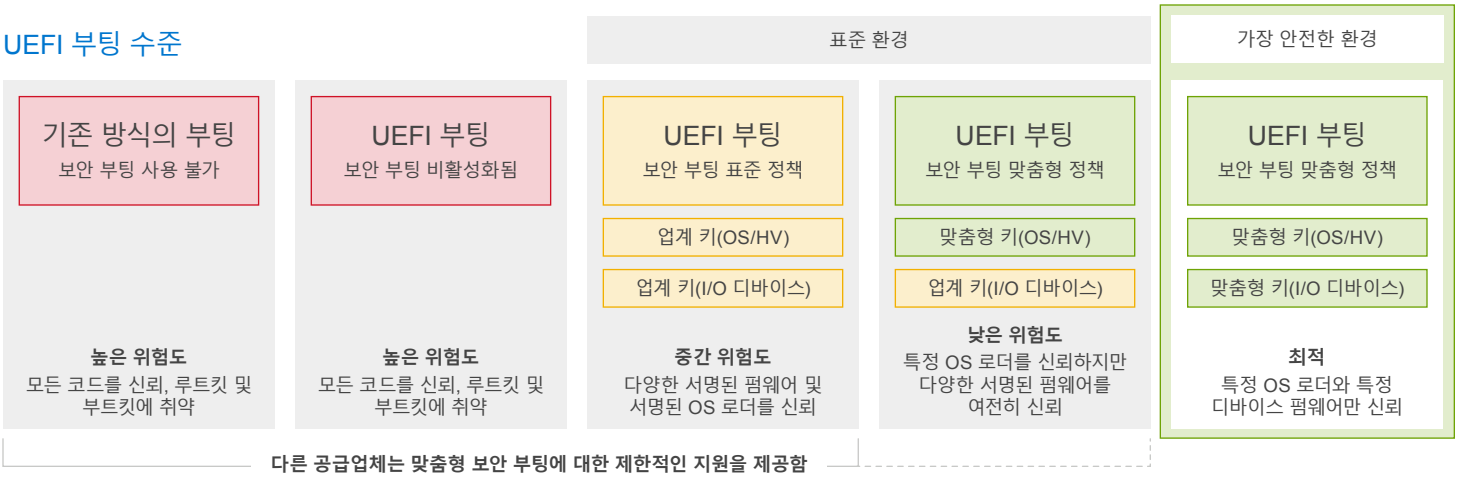
기존 BIOS 구성 및 시작 컨트롤을 대체하는 최신 기술인 UEFI 보안 부팅은 하이퍼바이저 또는 운영 체제가 시작되기 전에 서버의 기본 기능을 초기화합니다. PowerEdge 서버는 UEFI 보안 부팅을 활용하여 UEFI 드라이버 및 운영 체제 부팅 로더에 대해 암호화 방식으로 생성된 인증서를 검사합니다. 이것이 바로 PowerEdge 서버가 다음을 검증할 수 있는 "핵심 기능"입니다.

- PCIe 카드에서 로드된 UEFI 드라이버
- 대용량 스토리지 디바이스에서 로드된 UEFI 드라이버 및 실행 파일
- 운영 체제 부트 로더 - 일반적으로 Linux 또는 Microsoft Windows

이 검증 프로세스는 운영 체제가 시작되기 전에 코드가 무단으로 초기화되지 않도록 서버를 보호하는 데 중요한 역할을 합니다. UEFI 펌웨어 검증 프로세스는 부트 로더, 커널 및 기타 사용자 공간 코드 서명을 확인하여 서명되지 않은 소프트웨어가 시스템에서 실행되는 것을 방지하도록 설계되었습니다.

Dell EMC PowerEdge의 UEFI 보안 부팅 맞춤 구성은 Microsoft 이외의 인증 기관에서 생성하고 서명한 맞춤형 인증서를 지원하는 고유 기능도 제공합니다. Microsoft는 UEFI에서 지원되는 디바이스 및 운영 체제에 대한 기본 인증 기관입니다. 대부분의 표준 Linux 배포 환경에서는 Microsoft 인증서를 구현했습니다. 표준이 아닌 Linux 환경이 사용되는 경우(예: 전용 커널 또는 드라이버 수정) 부트 로더를 자체 검증하고 하드웨어-소프트웨어 신뢰 체인을 유지하려면 맞춤형으로 생성되고 사용자가 암호화 방식으로 서명한 인증서가 필요합니다.

UEFI 부팅 수준



성능 저하 없이 서버 보안 강화

부팅 프로세스는 모든 디바이스에서 보안의 기반이 됩니다. 이 프로세스는 디바이스의 구성 요소와 주변 기기가 어떻게 초기화되고 운영 체제가 어떻게 로드되는지를 제어하는 다양한 펌웨어를 사용합니다. 코드가 빨리 로드될수록 권한을 더 많이 가지며, 먼저 인증되지 않은 경우 위험이 더 커집니다. 부팅 프로세스가 손상되면 공격자가 보안 컨트롤을 무력화하여 시스템의 다양한 부분에 대한 무단 액세스 권한을 효과적으로 확보할 수 있습니다. 이로 인해 악성 UEFI 부트 로더를 사용하여 서버가 부팅될 때 서버를 제어하고, 컴퓨터를 재구성하며, 데이터를 암호화하고, 문제를 초래하는 랜섬웨어가 생성될 수도 있습니다.

위험 완화

최신 컨트롤 및 구성 옵션을 활용하면 이전보다 더 효과적으로 펌웨어 또는 부트 로더 공격으로부터 서버를 보호할 수 있습니다. Dell EMC PowerEdge의 UEFI 보안 부팅 맞춤 구성은 기존의 BIOS 기반 부팅 방법을 뛰어넘어 서버 인프라스트럭처의 보안을 강화합니다. 미국 정부 소속 NSA(National Security Agency)의 최근 권고에서는 서버 하드웨어 보안 강화를 주제로 다루었으며, PowerEdge UEFI 보안 부팅 맞춤 구성을 사용하는 것이 여러 운영 체제를 지원하는 유연성과 함께 훨씬 높은 수준의 보안을 제공하는 방법으로 특별히 언급되었습니다. NSA의 관련 CyberSecurity Technical 보고서에서 주목할 내용은 "맞춤 구성 모드를 통해 시스템 소유자는 신뢰할 수 있는 하드웨어 및 소프트웨어 솔루션의 선택지를 좁히거나 넓힐 수 있다..."는 것이며, Dell EMC의 내장형 UEFI 구성 유틸리티를 사용하여 이를 어떻게 실현할 수 있는지를 시사합니다[1]. 이러한 세부적인 제어로 잘못된 구성, 변조 및 멀웨어로 인한 위협을 완화하거나 완전히 차단할 수 있습니다. 시스템 관리자는 새로운 부팅 위협에 더욱 신속하게 대응할 수 있으며, 공급업체가 범할 수 있는 잠재적인 인증서 서명 실수의 영향을 받지 않습니다.

맞춤 구성된 인증서를 사용하는 UEFI 보안 부팅의 특징

기능	설명	이점
보안 부팅	• 주요 구성 요소 및 펌웨어 검증	• 기존 BIOS의 한계 및 보안 위협에서 벗어나 최신 펌웨어 검증 방식 채택
자체 서명된 인증서	• 서버 운영 전반에 걸쳐 안전한 펌웨어, 부트 로더 및 운영 체제 초기화 유지	• 고도로 안전한 배포 환경에서 맞춤형 OS 빌드 지원 • 맞춤형 하드웨어 및 관련 펌웨어를 구축할 때 기본 서명 기관에 구속되지 않음
보안 지침 준수	• 서버 부팅 프로세스, 펌웨어 검증 및 맞춤형 인증서 관리에 대한 보안 표준에 부합	• 서버 하드웨어 및 펌웨어 보안에 대한 표준 정립 • 중요 환경에서 향후 서버 보안 지침을 준수할 수 있도록 서버 운영 준비
iDRAC 및 TPM과의 통합	• PowerEdge 서버와 이미 통합된 기존 하드웨어 및 펌웨어 보안 기능 활용	• 통합 보안 기능의 가치를 극대화하여 포괄적인 하드웨어 RoT(Root of Trust) 구축

[1] 대부분의 시스템 설정과 마찬가지로 관리자는 시스템 설정 이외에 다른 툴을 사용하여 보안 부팅 표준 정책을 활성화할 수 있습니다. Dell Technologies의 DTK(Deployment Toolkit™), Lifecycle Controller™, OpenManage™ 툴, RACADM 콘솔, WS-MAN 콘솔로도 보안 부팅 표준 정책을 활성화할 수 있습니다.

PowerEdge 서버에 대해 자세히 알아보기

Dell EMC OpenManage Enterprise에 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