Dell Technologies

Solution Brief

Dell EMC PowerEdge UEFI Secure Boot Customization

Datacenter server environments have traditionally focused much of their security efforts at the operating system, application, and network level. As hardware infrastructure security concerns continue to rise, the complexity for IT security administrators increases. A fundamental need for Server and Security IT teams is to establish a trusted computing foundation and extend that trust to the operating systems and applications. Typically reserved for the most secure and sensitive applications and datasets, customized infrastructure security is rapidly coming to the fore. The evolving threat to server hardware requires a more comprehensive approach, including UEFI Secure Boot Customization, to strengthen this trusted foundation.

It starts with the Dell EMC Cyber Resilient Architecture, that validates the BIOS and firmware for the Integrated Dell Remote Access Controller (iDRAC) before it is loaded. Firmware for other critical components is likewise validated using stored cryptographic certificates to ensure that authentic firmware is running on the server.

Dell EMC Cyber Resilient Architecture

Effective Protection

- Silicon-based Hardware Root of Trust
- Signed Firmware Updates
- System Lockdown
- Secure Default Passwords

Reliable Detection

- Configuration and Firmware Drift Detection
- Persistent Event Logging including user activity
- Secure Alerting

Rapid Recovery

- Automatic BIOS Recovery
- Rapid OS Recovery
- System Erase

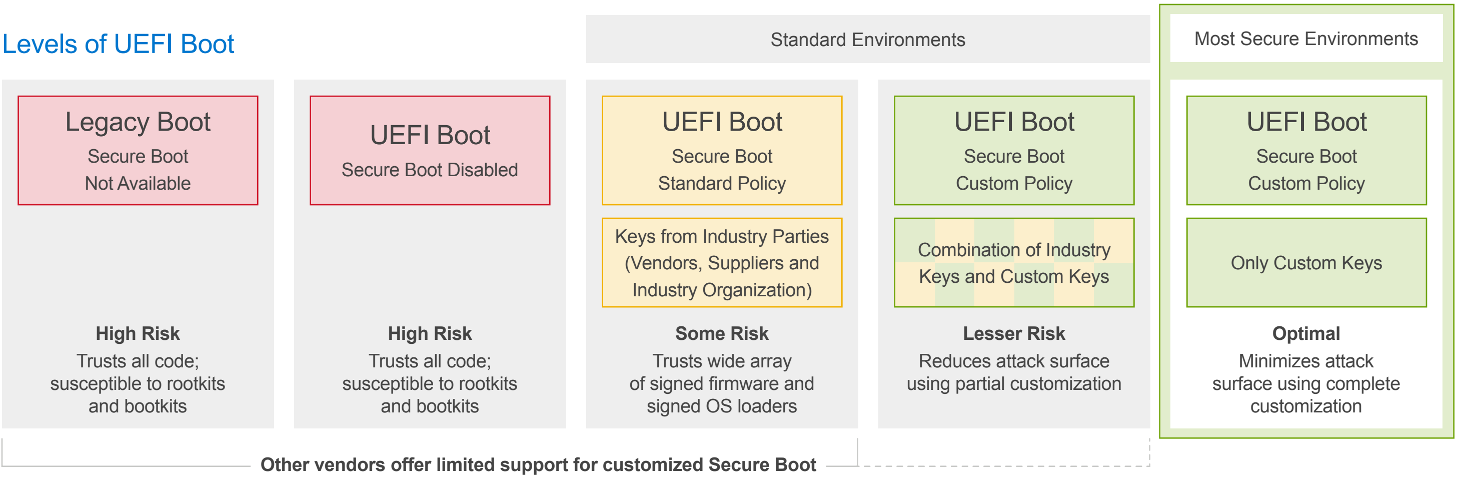
As the modern replacement for legacy BIOS configuration and startup controls, UEFI Secure Boot initializes the server's baseline functions before a hypervisor or operating system is started. PowerEdge servers utilize UEFI Secure Boot to check the cryptographically generated certificates of the UEFI drivers and operating system boot loaders. These are the “keys” that enable the server to validate the following:

- UEFI drivers loaded from PCIe cards
- UEFI drivers and executables loaded from mass storage devices,
- Operating System boot loaders – typically Linux or Microsoft Windows.

This validation process is critical to protecting the server from unauthorized code initiation prior to the launching of the operating system. By checking the signature of the bootloader, kernel, and other userspace code, UEFI firmware validation is engineered to prohibit unsigned software from running on the system.

Dell EMC PowerEdge UEFI Secure Boot Customization also has the unique capability of supporting customized certificates generated and signed by an authority other than Microsoft. Microsoft is the default certificate authority for UEFI supported devices and operating systems. Many standard Linux distributions have implemented a Microsoft certificate. In situations where a non-standard Linux environment is being used (i.e. – proprietary kernel or driver modifications) there is a need for custom generated certificates, cryptographically signed by the user, to self-validate the boot loader and maintain the hardware to software chain of trust.

Levels of UEFI Boot



		Standard Environments		Most Secure Environments
Legacy Boot Secure Boot Not Available	UEFI Boot Secure Boot Disabled	UEFI Boot Secure Boot Standard Policy	UEFI Boot Secure Boot Custom Policy	UEFI Boot Secure Boot Custom Policy
		Keys from Industry Parties (Vendors, Suppliers and Industry Organization)	Combination of Industry Keys and Custom Keys	Only Custom Keys
High Risk Trusts all code; susceptible to rootkits and bootkits	**High Risk** Trusts all code; susceptible to rootkits and bootkits	**Some Risk** Trusts wide array of signed firmware and signed OS loaders	**Lesser Risk** Reduces attack surface using partial customization	**Optimal** Minimizes attack surface using complete customization

Other vendors offer limited support for customized Secure Boot

Enhance Server Security Without Compromise

The boot process is the foundation of security for any device. It relies on a multitude of firmware that controls how a device's components and peripherals are initiated as well as loading the operating system. The earlier code is loaded, the more privileged it is and the more damage it can do if it is not authenticated first. If the boot process is compromised, attackers can subvert security controls, effectively gaining unauthorized access to various parts of the system. It could even be possible to create ransomware using malicious UEFI bootloaders to take control of servers when they are booting-up, reconfiguring the computer, encrypting data, and causing havoc.

Reduce Risk

With a modern controls and configuration options, you are better equipped than ever to protect your servers from firmware or boot loader attacks. Dell EMC PowerEdge UEFI Secure Boot Customization increases the security of your server infrastructure while leaving legacy BIOS-based boot methods behind. A recent advisement from the U.S. Government's National Security Agency (NSA) documents the topic of increased server hardware security, specifically citing the use of PowerEdge UEFI Secure Boot Customization as a method that provides a significantly higher level of security along with the flexibility to support multiple operating systems. In a related CyberSecurity Technical report from the NSA, it is noted that "Custom Mode allows the system owner to narrow or expand the selection of trusted hardware and software solutions…" and illustrates how this can be accomplished using the Dell embedded UEFI configuration utility[1]. This granular control can reduce or eliminate the threat of misconfiguration, tampering, and malware. System administrators can react faster to new boot threats and are insulated from potential certificate signing mistakes made by vendors.

Features of UEFI Secure Boot with Customized Certificates

Features	Description	Benefits
Secure Boot	• Validation of key components and firmware	• Adoption of a modern firmware validation, leaving behind the limitations and security threats of legacy BIOS
Self-Signed Certificates	• Maintain secure firmware, bootloader and operating system initiation across the entire server operation	• Support for customized OS builds in highly secure deployments • Independence from default signature authority when implementing custom built hardware and associated firmware
Security Guideline Compliance	• Aligned with security standards for server boot process, firmware validation, and customized certificate management	• Sets the standard for server hardware and firmware security • Positions server operations for compliance with future server security guidelines in sensitive environments
Integration with iDRAC and TPM	• Leverage existing hardware and firmware security features already integrated with PowerEdge servers	• Maximize the value of integrated security features to establish a comprehensive hardware root of trust

[1] As with most system settings, an administrator may use other tools besides System Setup for enabling the Secure Boot standard policy. Dell's Deployment ToolkitTM (DTK), Lifecycle ControllerTM, OpenManageTM tools, RACADM console, and WS-MAN consoles can also enable the Secure Boot standard policy.

Discover more about PowerEdge servers

Learn more about Dell EMC OpenManage Enterprise

Learn more about our systems management solutions

Search our Resource Library

Follow PowerEdge servers on Twitter

Contact a Dell Technologies Expert for Sales or Support

DELL Technologies