Extend Your Defense Strategy

Dell Technologies and Polyverse join forces to protect your agency and mission.

The first line of defense—Secure Boot

Secure Boot is a boot-integrity feature that is part of the Unified Extensible Firmware Interface (UEFI) industry standard. Most modern computer systems have a standard Secure Boot policy installed, which is the first line of defense in securing compute resources and applications. Only Dell Technologies provides select Dell EMC PowerEdge servers with the UEFI configuration GUI and RACADM CLI mechanisms for capturing hashes, as noted by the NSA in their published report.

Faced with ever-evolving cyberattacks, federal agencies and other critical enterprises work tirelessly to provide secured applications and systems against sophisticated actors. Cyber-operators, however, are overwhelmed, and the scale and complexity of attacks make it impossible to investigate all identified incidents.

IT decision-makers at all levels understand how crucial comprehensive cybersecurity measures are to the future success of their agencies or departments. They're dealing with risks like the insertion of malware, boot-level exploits, insider threats, buffer overflows, memory exploits, CPU timing and other techniques used to expose vulnerabilities. While many organizations recognize the importance of keeping software up to date with well-established patching plans, all enterprises still face a critical patch gap. This gap is the time between a vulnerability's public disclosure (when attackers begin rapid exploit development) and the moment that a system is entirely protected against it.

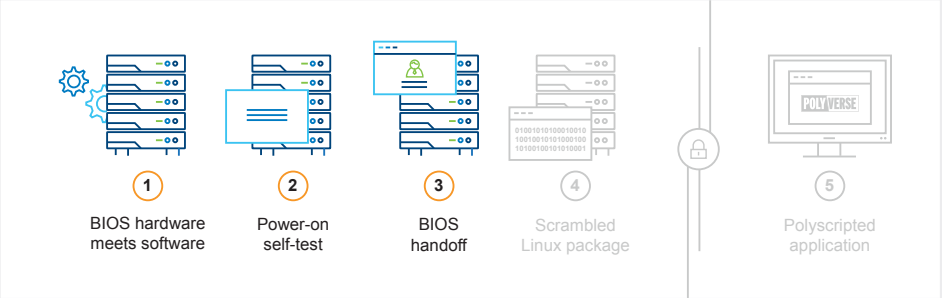
The good news is that Dell Technologies and Polyverse are working together to deliver an innovative and integrated approach to mitigate many zero-day and supply-chain attacks. The first line of defense begins with comprehensive Secure Boot capabilities in Dell EMC PowerEdge servers. That capability is extended with Polyverse® Polymorphing, protecting your operating system (OS) and other applications.

Why does Custom UEFI Secure Boot matter?

Technology solutions without Secure Boot may be vulnerable to firmware rootkits and bootkits, which are what attackers use to hide malicious code.

Secure Boot guards against these attacks by preventing execution of unauthorized preboot code. UEFI Secure Boot allows for customization to remove third-party certificate risks, while an effective UEFI implementation verifies the integrity of non-BIOS code modules.

As the Dell EMC PowerEdge server goes through the Secure Boot process (see diagram), it hands over control to the OS to continue the process of startup and continuous runtime.



Solution brief

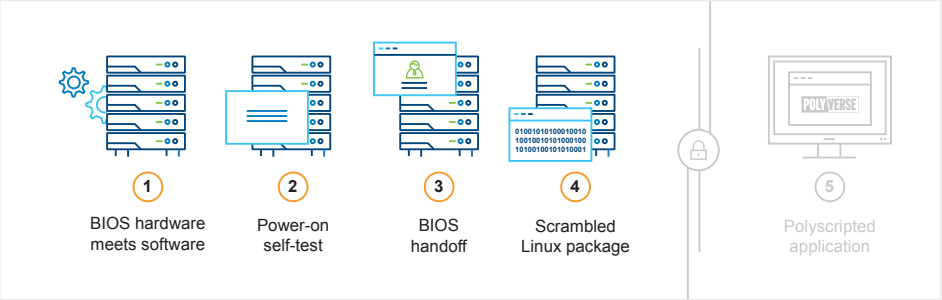
Polyverse Polymorphing mitigates

70% to 80%

of memory-based vulnerabilities.

Polyverse reinforces Secure Boot.

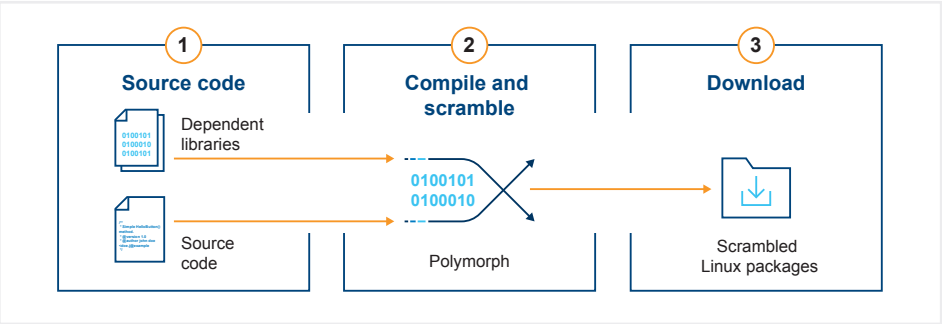
Following the Secure Boot process, your operating systems are loaded or upgraded to support production applications. These standard versions of operating systems have inherent vulnerabilities in them from day zero. This is where Polyverse mitigates your security risk.



Polyverse Polymorphing eliminates 70% to 80% of vulnerabilities that need an immediate patch, significantly reducing your risk of being exploited during any patch gap. Polymorphing compiles, scrambles and serves unique hardened Linux® distributions that mitigate known and undisclosed memory-based attacks.

Polyverse does not change the source code of the operating system in any way — only the compiled binary OS image. This approach drastically reduces the attacker's attack surface yet requires no changes to developer or user behavior. The difference is that attackers cannot apply common memory and register assumptions to each operating system attack.

Secure Boot's defense against malicious activity becomes more robust with the extended security capability of loading a polymorphic version of the operating system after the Secure Boot process is complete.



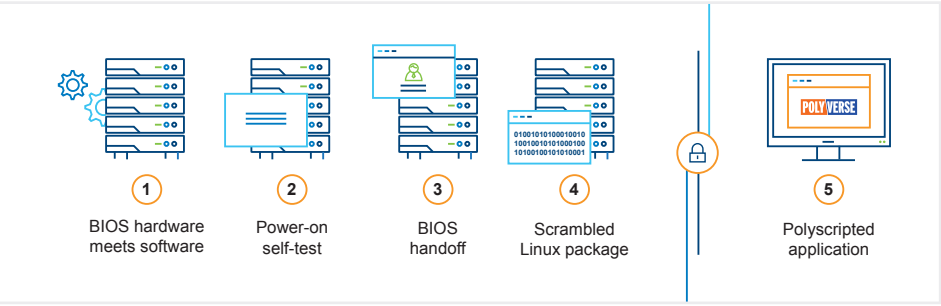
Put your agency on the offense.

Cyberthreats are real and devastating to any organization — and especially to federal agencies that manage citizen data and other sensitive information. Minimize your attack surface with integrated solutions from Dell Technologies and Polyverse.

Secure the foundation of DevSecOps.

As Rapid Application Development, Agile and other development methodologies become more widely used, we cannot overlook the need for protection at all levels of the software stack. Dell Technologies and Polyverse understand that, to guarantee reliability, availability and predictability of mission-critical systems and applications, teams need solutions that enable proactive security measures without disrupting their current DevOps processes and workflows.

Organizations aren't limited to just securing their server and OS deployments with Dell Technologies and Polyverse. With these technologies, administrators and application developers can apply zero-trust software principles to their Kubernetes® clusters, container environments, compute hardware, HPC clusters and edge devices.



Polyscripting counters code-injection attacks.

Polyscripting is another powerful solution from Polyverse that is designed to eliminate code-injection attacks directed at web servers and the applications running on them. Code-injection attacks that target unpatched systems are the top security risk for web-based applications, especially where the most popular server-side scripting languages are involved. Polyscripting works by scrambling the syntax and grammar of the programming language, effectively giving each website a unique and exclusive instance of the language. The result keeps any maliciously injected code from executing, making the website immune to attack. With this technique, there is absolutely no impact to functionality, performance or interoperability.

Take action today.

To learn more about how Dell Technologies and Polyverse can better protect your agency, contact Jennifer_Talley@dell.com.

Published in the USA 04/21 Solution brief

DELL Technologies