DELL Technologies

解决方案简介

# Dell EMC PowerEdge UEFI 安全启动自定义

传统上，为了确保数据中心服务器环境的安全，IT 安全管理员的工作重点通常会放在操作系统、应用程序和网络层面上。随着硬件基础架构安全问题不断增加，他们的任务也日渐复杂。服务器和安全 IT 团队的一项基本需求就是建立一个可信赖的计算基础，继而将这样的信任延伸到操作系统和应用程序。自定义基础架构安全机制通常是留给最安全、最敏感的应用程序和数据集使用的，但它正被快速、广泛地采用。服务器硬件面临着不断变化的威胁，因此需要采用更加全面的方法（包括 UEFI 安全启动自定义）来增强这一可信赖的基础。

这项工作的起点就是 Dell EMC 网络弹性体系结构，它会在加载 Integrated Dell Remote Access Controller (iDRAC) 之前验证 BIOS 和固件。同样，其他关键组件的固件也会使用存储的加密证书进行验证，从而确保服务器上运行的是可信固件。

## Dell EMC 网络弹性体系结构

### 有效的保护

- 基于硅片的硬件信任根
- 签名固件升级
- 系统锁定
- 安全的默认密码

### 可靠的检测

- 配置和固件偏差检测
- 持久事件日志记录，包括用户活动
- 安全警报

### 快速恢复

- 自动 BIOS 恢复
- 快速操作系统恢复
- 系统擦除

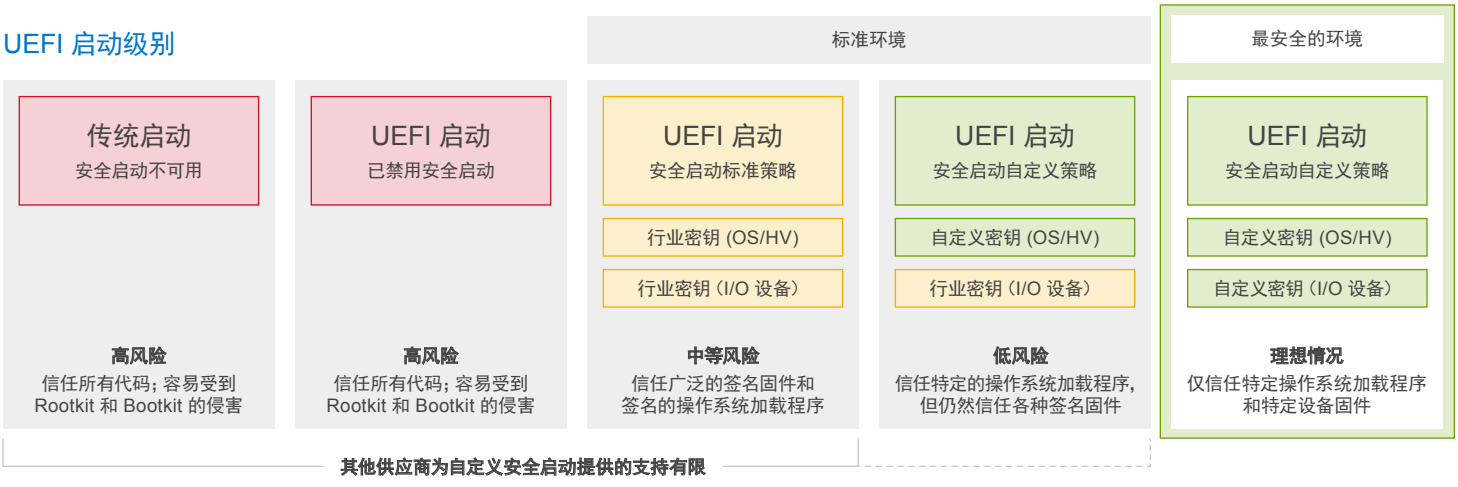
作为传统 BIOS 配置和启动控件的现代替代产品，UEFI 安全启动可在虚拟机管理程序或操作系统启动之前初始化服务器的基线功能。PowerEdge 服务器利用 UEFI 安全启动，以检查 UEFI 驱动程序和操作系统启动加载程序的通过加密方式生成的证书。这些证书就像是让服务器能够验证以下内容的“密钥”：

- UEFI 驱动程序是从 PCIe 卡加载的
- UEFI 驱动程序和可执行文件是从大容量存储设备加载的，
- 操作系统启动加载程序 — 通常是 Linux 或 Microsoft Windows。

这个验证过程至关重要，可以在操作系统启动之前实施保护机制，并避免有未经授权的代码在服务器上初始化。UEFI 固件验证经过精心设计，能够检查启动加载程序、内核和其他用户空间代码的签名，从而禁止未签名的软件在系统上运行。

Dell EMC PowerEdge UEFI 安全启动自定义还具有独特的功能，可支持由 Microsoft 以外的其他证书颁发机构生成和签名的自定义证书。Microsoft 是支持 UEFI 的设备和操作系统的默认证书颁发机构。许多标准 Linux 发行版均已实施 Microsoft 证书。在使用非标准 Linux 环境（例如，专有内核或驱动程序修改）的情况下，则需要使用自定义生成的证书（由用户加密签名），以便自行验证启动加载程序，并维护“从硬件到软件”的信任链。

## UEFI 启动级别



## 在不做妥协的情况下增强服务器安全性

启动过程是所有设备的安全基础。它依赖于多种固件，可控制设备组件和外围设备的启动方式，还会加载操作系统。代码加载的时机越早，获得的特权就越多，如果未首先对其执行身份验证，那么就有可能造成更严重的破坏。如果启动过程遭遇入侵，攻击者可以彻底破坏安全控制机制，从而有效地获得对系统各个部分未经授权的访问。攻击者甚至可以使用恶意的 UEFI 启动加载程序创建勒索软件，从而在服务器启动时接管服务器控制权，重新配置计算机，加密数据并造成严重破坏。

## 降低风险

借助现代化的控制和配置选项，您可以比从前更好地保护服务器，防止固件或启动加载程序的攻击。Dell EMC PowerEdge UEFI 安全启动自定义增强了服务器基础架构的安全性，同时超越了基于 BIOS 的传统启动方法。美国国家安全局 (NSA) 最近的一份建议记录了提高服务器硬件安全性的主题，其中特别指出可以将 PowerEdge UEFI 安全启动自定义作为方法之一，以显著提高安全性并灵活地支持多种操作系统。在美国国家安全局的相关网络安全技术报告中提到：“自定义模式允许系统所有者缩小或扩展受信任硬件和软件解决方案的选择范围...”，并且说明了如何使用戴尔嵌入式 UEFI 配置实用程序[1] 来实现这一目标。这种精细的控制可以降低或消除错误配置、篡改和恶意软件的威胁。系统管理员可以更快地响应新的启动威胁，并且可以避免由供应商造成的证书签名错误。

## 使用自定义证书的 UEFI 安全启动的功能

| 功能 | 说明 | 优势 |
|---|---|---|
| 安全启动 | • 验证关键组件和固件 | • 采用现代固件验证方法，摆脱传统 BIOS 的限制和安全威胁 |
| 自签名证书 | • 在整个服务器操作中确保固件、启动加载程序和操作系统初始化的安全 | • 支持在高度安全的部署中使用自定义的操作系统内部版本<br>• 在实施自定义构建的硬件和相关固件时，不依赖于默认的签名机构 |
| 安全准则合规性 | • 符合有关服务器启动流程、固件验证和自定义证书管理的安全标准 | • 设定服务器硬件和固件安全性的标准<br>• 为敏感环境中的服务器操作做好准备，使之能够遵守未来的服务器安全准则 |
| 与 iDRAC 和 TPM 集成 | • 利用已经与 PowerEdge 服务器集成的现有硬件和固件安全功能 | • 尽可能提升集成式安全功能的价值，以建立全面的硬件信任根 |

[1] 像处理大多数系统设置时一样，管理员可以使用除系统设置程序以外的其他工具来启用安全启动标准策略。戴尔的 Deployment Toolkit™ (DTK)、Lifecycle Controller™、OpenManage™ 工具、RACADM 控制台和 WS-MAN 控制台也能启用安全启动标准策略。

## 了解有关 PowerEdge 服务器的详细信息

详细了解 Dell EMC OpenManage Enterprise

详细了解我们的系统管理解决方案

搜索我们的资源库

关注 Twitter 上的 PowerEdge 服务器

联系 Dell Technologies 销售或支持专家



DELL Technologies