DELL Technologies

Resumo da solução

Personalização do UEFI Secure Boot do Dell EMC PowerEdge

Tradicionalmente, os ambientes de servidor de data center concentram muito de suas iniciativas de segurança no nível de sistema operacional, aplicativo e rede. A complexidade para os administradores de segurança de TI aumenta, pois os problemas com a segurança da infraestrutura de hardware continuam aumentando. Uma necessidade fundamental das equipes de TI de servidores e segurança é estabelecer uma base de computação confiável e estender essa confiança aos sistemas operacionais e aos aplicativos. A segurança personalizada da infraestrutura, normalmente reservada para os aplicativos e os conjuntos de dados mais seguros e confidenciais, está rapidamente sendo colocada em primeiro plano. A ameaça em constante evolução contra o hardware de servidor exige uma abordagem mais abrangente, incluindo a personalização do UEFI Secure Boot, para fortalecer essa base confiável.

Tudo começa com a arquitetura com resiliência cibernética da Dell EMC, que valida o BIOS e o firmware para o iDRAC (Integrated Dell Remote Access Controller) antes que ele seja carregado. O firmware para outros componentes essenciais também é validado com o uso de certificados criptográficos armazenados para garantir a execução do firmware autêntico no servidor.

Arquitetura com resiliência cibernética da Dell EMC

Proteção efetiva

- Raiz de confiança de hardware baseada em silício
- Atualizações de firmware assinadas
- System Lockdown
- Senhas padrão seguras

Detecção confiável

- Configuração e detecção de desvio de firmware
- Log de evento persistente, incluindo atividade do usuário
- Alerta de segurança

Recuperação rápida

- Recuperação automática do BIOS
- Rapid OS Recovery
- System Erase

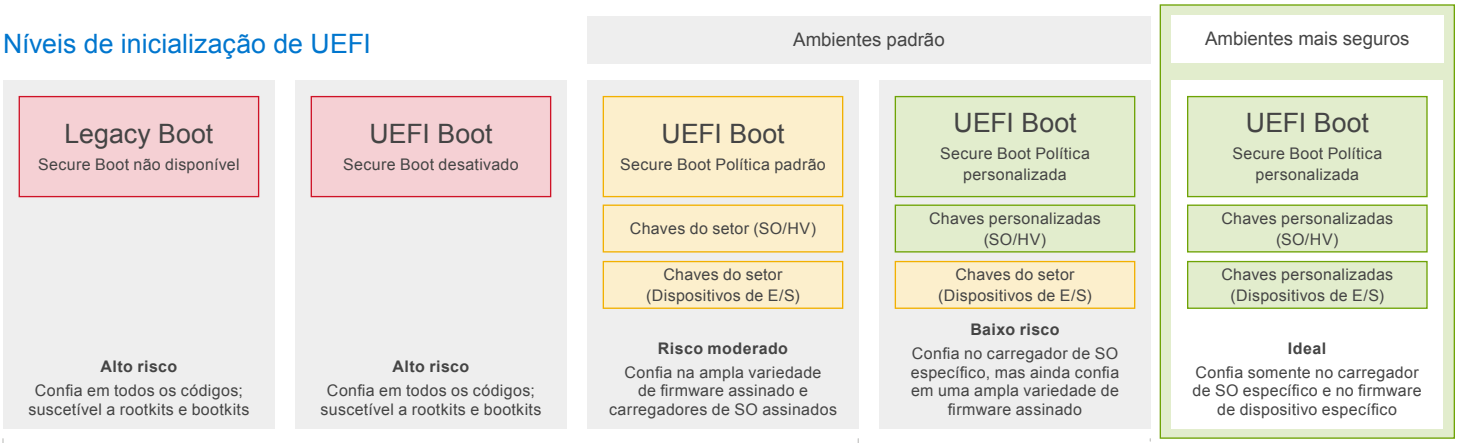
Como a substituição moderna dos controles de inicialização e configuração do BIOS preexistente, o UEFI Secure Boot inicializa as funções de linha de base do servidor antes que um hypervisor ou sistema operacional seja iniciado. Os servidores PowerEdge utilizam o UEFI Secure Boot para verificar os certificados, gerados de maneira criptográfica, dos drivers de UEFI e dos carregadores de inicialização do sistema operacional. Essas são as "chaves" que permitem que o servidor valide:

- Os drivers de UEFI carregados de placas PCIe;
- Os drivers de UEFI e os arquivos executáveis carregados de dispositivos de armazenamento em massa;
- Os carregadores de inicialização do sistema operacional, geralmente Linux ou Microsoft Windows.

Esse processo de validação é essencial para proteger o servidor contra a iniciação de código não autorizado antes da inicialização do sistema operacional. A validação de firmware de UEFI foi projetada para proibir a execução de software não assinado no sistema, verificando a assinatura do carregador de inicialização, do kernel e de outros códigos de espaço do usuário.

A personalização do UEFI Secure Boot do Dell EMC PowerEdge também tem a capacidade exclusiva de oferecer suporte a certificados personalizados gerados e assinados por uma autoridade que não seja a Microsoft. A Microsoft é a autoridade de certificação padrão para sistemas operacionais e dispositivos compatíveis com a UEFI. Muitas distribuições Linux padrão implementaram um certificado Microsoft. Nas situações em que se usa um ambiente Linux não padrão (ou seja, modificações de driver ou kernel proprietário), há a necessidade de gerar certificados personalizados, assinados de maneira criptográfica pelo usuário, para autovalidar o carregador de inicialização e manter a cadeia de confiança hardware para software.

Níveis de inicialização de UEFI



Melhorar a segurança do servidor sem causar danos

O processo de inicialização é a base da segurança para qualquer dispositivo. Ele depende de uma grande variedade de firmware que controla a forma como os componentes e periféricos de um dispositivo são iniciados, bem como o carregamento do sistema operacional. Quanto mais cedo o código for carregado, mais privilegiado ele será e mais danos ele poderá causar se não for autenticado primeiro. Se houver danos no processo de inicialização, os invasores poderão corromper os controles de segurança, obtendo, de maneira eficaz, o acesso não autorizado a várias partes do sistema. Talvez até seja possível criar ataques de ransomware usando carregadores mal-intencionados de inicialização de UEFI para assumir o controle dos servidores na inicialização deles, reconfigurando o computador, criptografando dados e causando destruição.

Reduzir os riscos

Com opções de configuração e controles modernos, você está mais bem equipado do que nunca para proteger seus servidores contra ataques de carregadores de inicialização ou de firmware. A personalização do UEFI Secure Boot do Dell EMC PowerEdge aumenta a segurança de sua infraestrutura de servidores e deixa para trás os métodos de inicialização baseados em BIOS preexistente. Um informativo recente da NSA (National Security Agency, Agência de Segurança Nacional) do governo dos EUA documenta o aumento da segurança de hardware de servidor, citando especificamente o uso da personalização do UEFI Secure Boot do PowerEdge como um método que oferece um nível de segurança significativamente maior, além de flexibilidade para dar suporte a vários sistemas operacionais. Em um relatório técnico de segurança cibernética relacionado da NSA, nota-se que "o modo Custom permite que o proprietário do sistema restrinja ou expanda a seleção de soluções confiáveis de hardware e software...". Além disso, é ilustrado como esse processo pode ser realizado com o utilitário[1] de configuração de UEFI incorporado da Dell. Esse controle específico pode reduzir ou eliminar a ameaça de configuração incorreta, violação e malware. Os administradores do sistema podem reagir mais rapidamente a novas ameaças de inicialização e isolarem-se de possíveis erros de assinatura de certificado cometidos pelos fornecedores.

Recursos do UEFI Secure Boot com certificados personalizados

Recursos	Descrição	Benefícios
Secure Boot	• Valida os principais componentes e o firmware	• Adoção de uma validação de firmware moderna, deixando para trás as limitações e as ameaças à segurança do BIOS preexistente
Certificados autoassinados	• Mantêm a segurança do firmware, do carregador de inicialização e da iniciação do sistema operacional em toda a operação do servidor	• Suporte para compilações de SO personalizadas em implementações altamente seguras • Independência da autoridade de assinatura padrão ao implementar hardware personalizado e o firmware associado
Conformidade com as diretrizes de segurança	• Alinha-se aos padrões de segurança quanto ao processo de inicialização do servidor, à validação de firmware e ao gerenciamento de certificados personalizados	• Definição do padrão da segurança de firmware e hardware de servidor • Posicionamento das operações do servidor para fins de conformidade com as futuras diretrizes de segurança do servidor em ambientes confidenciais
Integração com iDRAC e TPM	• Aproveita os recursos de segurança de firmware e hardware existentes já integrados aos servidores PowerEdge	• Aumento do valor dos recursos de segurança integrados para estabelecer uma raiz de confiança de hardware abrangente

[1] Assim como na maioria das configurações do sistema, um administrador pode usar outras ferramentas, além do System Setup, para ativar a política padrão do Secure Boot. O DTK (Deployment Toolkit™) da Dell, o Lifecycle Controller™, as ferramentas do OpenManage™, o console RACADM e o consoles WS-MAN também podem ativar a política padrão do Secure Boot.

Descubra mais sobre os servidores PowerEdge

Saiba mais sobre o Dell EMC OpenManage Enterprise

Saiba mais sobre nossas soluções de gerenciamento de sistemas

Pesquise em nossa biblioteca de recursos

Siga servidores PowerEdge no Twitter

Entre em contato com um especialista da Dell Technologies em vendas ou suporte

DELL Technologies