DELL Technologies

Resumo da solução

Verificação de componentes protegidos da Dell Technologies para PowerEdge

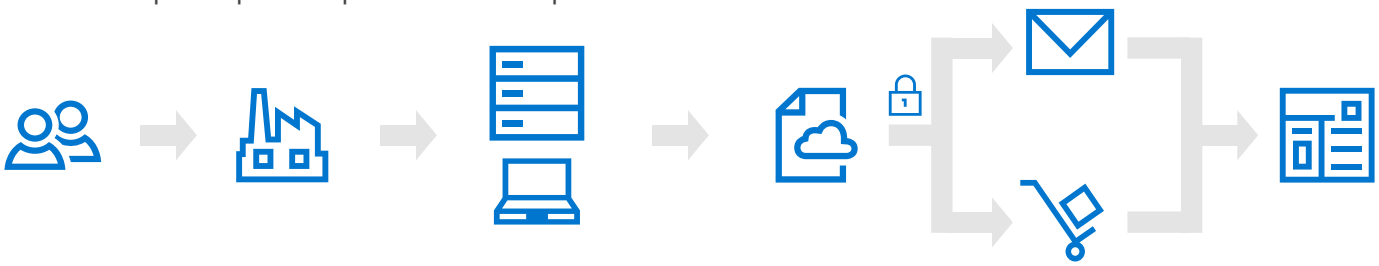
A defesa contra ataques de segurança cibernética continua a desafiar as equipes de operações e segurança de TI em todos os níveis de sua infraestrutura. Embora os comprometimentos de aplicativos e sistemas operacionais sejam o vetor de ataque mais comum, utilizando malware e ransomware, os ataques de hardware também estão aumentando. Devido a essa crescente ameaça, cada vez mais atenção está sendo dada aos servidores e à garantia de que nada na configuração de hardware de servidor foi alterado entre o momento em que o sistema é construído e o momento em que o sistema é implantado. Não é de se admirar que 84% dos entrevistados de uma pesquisa da Forrester Research[1] consideraram a segurança de hardware/cadeia de suprimentos como essencial ou muito importante para seus negócios.

A Verificação de componentes protegidos da Dell Technologies fornece a verificação da configuração de hardware integrada para os servidores PowerEdge. A verificação permite que você implante com confiança novos servidores em seu datacenter sabendo que a configuração de hardware fornecerá uma base sólida para seus aplicativos essenciais. A verificação de componentes protegidos está alinhada com as diretrizes emergentes do governo dos EUA para a segurança da cadeia de suprimentos de tecnologia.

Implante servidores com confiança

A Verificação de componentes protegidos da Dell Technologies, agora parte integrante da linha de servidores Dell EMC PowerEdge, permite que os administradores de TI validem com segurança seus sistemas entregues antes da implementação. As organizações podem garantir que seus novos servidores sejam entregues com os mesmos componentes instalados nas instalações de fabricação da Dell Technologies.

Quando o sistema está pronto para envio, os componentes do servidor e seus IDs exclusivos são avaliados, e os dados resultantes são protegidos criptograficamente usando um certificado assinado. O inventário criptografado é incorporado ao servidor e enviado com o sistema para o datacenter. Depois que o sistema for recebido, o administrador de TI conduzirá um inventário do sistema entregue usando a ferramenta SCV fornecida e autenticará esse inventário com o certificado armazenado no sistema. Depois da autenticação e da verificação da correspondência dos componentes, o sistema estará pronto para ser provisionado e implementado.



Pedir

O cliente faz um pedido de produto de servidor

Criar

O pedido é enviado para a fábrica para construção

Nenhuma alteração no pedido existente

→

Processo de construção

Coletar

Os dados de componentes do sistema são coletados, criptografados e um certificado de plataforma é criado e assinado por um HSM (High Security Module)

Armazenar

O certificado da plataforma é armazenado em um local central (DL para serviços) e no servidor (iDRAC)

Entregar

O certificado assinado pela Dell é entregue ao cliente no servidor (IDRAC)

Validar

O cliente valida a autenticidade dos componentes por meio da ferramenta de gerenciamento de sistema local

[1] Fonte: Forrester Research, Inc., The Next Frontier for Endpoint Protection

© 2020 Dell Inc. ou suas subsidiárias

A necessidade de uma cadeia de suprimentos de tecnologia segura torna-se evidente

O governo dos EUA, em colaboração com seus parceiros comerciais globais, continuou a refinar sua orientação para a segurança cibernética. No que diz respeito à infraestrutura de servidores, recentemente eles focaram mais atenção na validação dos componentes do servidor e na autenticidade do firmware nesses servidores. Em seu documento mais recente, o National Cybersecurity Center of Excellence (NCCOE), parte do National Institute of Standards and Technology, ilustrou claramente o desafio: todos os OEMs de servidores estão trabalhando com vários fornecedores de componentes e subsistemas. Embora todos tenham instituído programas de verificação da cadeia de suprimentos para garantir a qualidade e a segurança dos componentes de seus fornecedores, não existia uma maneira fácil para o usuário final validar que o que foi instalado na fábrica é exatamente o que ele recebeu. A Dell Technologies está colaborando com o NCCoE no Supply Chain Assurance Building Block Consortium para desenvolver abordagens de segurança cibernética práticas e interoperáveis que atendam às necessidades reais dos sistemas complexos de tecnologia da informação (TI).[2]

Verificação de componentes protegidos da Dell Technologies - uma base segura para aplicativos confiáveis

No atual ambiente de segurança cibernética em evolução, em que o software e o hardware são alvos de penetração em potencial, há claramente uma necessidade de maior garantia e confiança na infraestrutura do servidor. Para acompanhar a crescente demanda por mais rapidez no desenvolvimento, no teste e na implementação de aplicativos, novos recursos, como a Validação de componentes seguros, precisam ser incorporados ao ciclo de vida da infraestrutura. Com a SCV, as equipes de operações e segurança de TI podem ter a certeza de que seus sistemas entregues estão alinhados com as especificações de seus servidores e sua estrutura de segurança, eliminando um possível vetor de ataque para que as equipes concentrem sua energia nos resultados comerciais.

Recursos e benefícios da Verificação de componentes protegidos:

- Certificados de inventário assinados criptograficamente disponíveis no portfólio de servidores PowerEdge
- Garantia da fábrica ao rack - a autoverificação segura garante a integridade total do hardware durante o trânsito para o datacenter
- Integração com scripts existentes para facilitar o processo de validação, tornando a implementação confiável um processo que pode ser automatizado
- Alinha-se aos padrões emergentes de segurança da cadeia de suprimentos, importantes para setores em que a segurança cibernética é a prioridade principal

[2] O NIST não avalia produtos comerciais deste consórcio e não endossa nenhum produto ou serviço usado. Informações adicionais sobre esse consórcio podem ser encontradas em: https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

Descubra mais sobre os servidores PowerEdge

Saiba mais sobre a Verificação de componentes protegidos da Dell Technologies

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

© 2020 Dell Inc. ou suas subsidiárias. Todos os direitos reservados. Dell, EMC e as demais marcas comerciais são de propriedade da Dell Inc. ou de suas subsidiárias. Outras marcas comerciais podem pertencer a seus respectivos proprietários.

DELL Technologies