Dell NativeEdge

Proteção: opere de maneira confiante com a segurança Zero Trust

Sumário

Conteúdo

Segurança em ambientes distribuídos

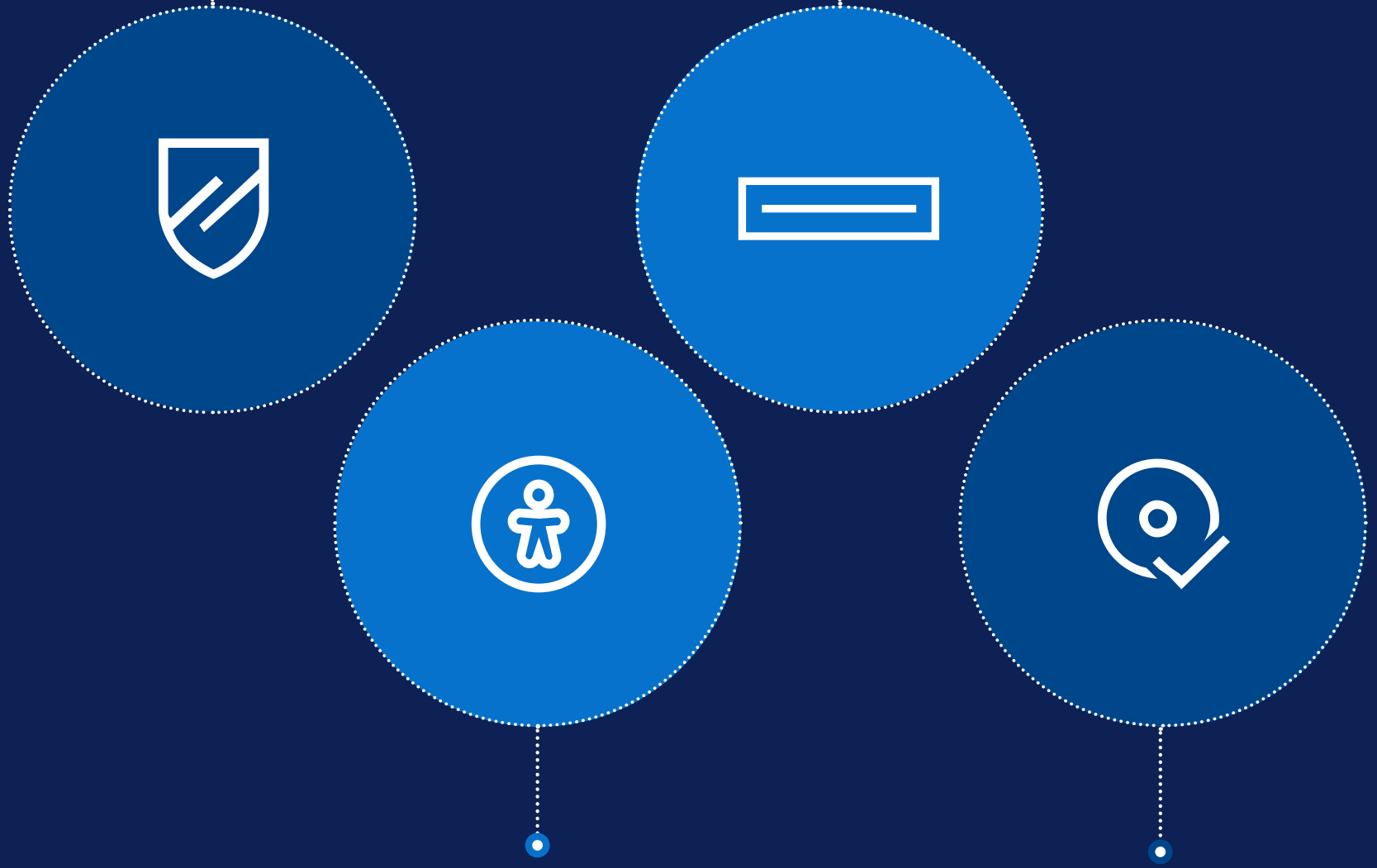
Para atender às preferências dos clientes e à dinâmica do mercado em rápida mudança, as organizações estão implementando novos aplicativos, atualizações e infraestrutura de TI em um volume e velocidade sem precedentes. Essa avalanche de dados, infraestrutura e aplicativos significa que está se tornando cada vez mais essencial proteger os ambientes distribuídos onde essas novas tecnologias residem.

Conforme as empresas ampliam suas operações, elas ficam cada vez mais vulneráveis aos riscos de segurança, que variam desde adulterações de dispositivos físicos a hacking de dados. Além disso, esses sistemas geralmente lidam com dados pessoais confidenciais, colocando mais responsabilidade sobre as empresas para proteger seus clientes.

Para proteger as operações, as empresas precisam

Garantir
a segurança física da infraestrutura implementada em locais distribuídos

Detectar
adulterações de dispositivos e remediar ameaças



Controlar
o acesso de usuários em todos os níveis

Dimensionar
o provisionamento e as atualizações de software em milhares de dispositivos

Dell NativeEdge

Inove onde quer que você atue

Um pacote de soluções completo que centraliza com segurança a implementação, a orquestração e o gerenciamento do ciclo de vida de diversos aplicativos e infraestruturas em data centers distribuídos e na borda.

Simplifique, otimize e proteja ambientes de data centers distribuídos e de borda com recursos, como integração sem intervenção, segurança Zero Trust e orquestração avançada de cargas de trabalho. O NativeEdge utiliza um hipervisor de KVM e um ambiente de execução de contêineres, permitindo que as organizações implementem e gerenciem máquinas virtuais (VMs) e contêineres. Ele é otimizado para orquestrar cargas de trabalho e estruturas de IA, possibilitando a implementação e o gerenciamento otimizados de aplicativos orientados por IA em todos os data centers distribuídos e na borda. O NativeEdge também pode se adaptar a qualquer ambiente de hardware, oferecendo suporte a uma ampla variedade de opções em vários formatos, desde servidores Dell PowerEdge a desktops, bem como infraestruturas de terceiros.

O Dell NativeEdge foi desenvolvido especificamente para atender aos desafios exclusivos de ambientes distribuídos, como complexidade operacional, escalabilidade e segurança. É uma solução personalizada para organizações modernas que desejam aproveitar o poder da computação de borda e, ao mesmo tempo, reduzir custos e melhorar a eficiência.

Simplificar
Acelere os resultados e centralize as operações

Menos de
um minuto
para implementar a infraestrutura e os aplicativos[1]

Otimizar
Obtenha virtualização perfeita e IA escalável

Até
68%
de economia de tempo com a automatização da orquestração de aplicativos de borda[1]

Proteger
Opere de maneira confiante com a segurança Zero Trust

Possibilite as operações de borda
mais seguras
do mundo[2]

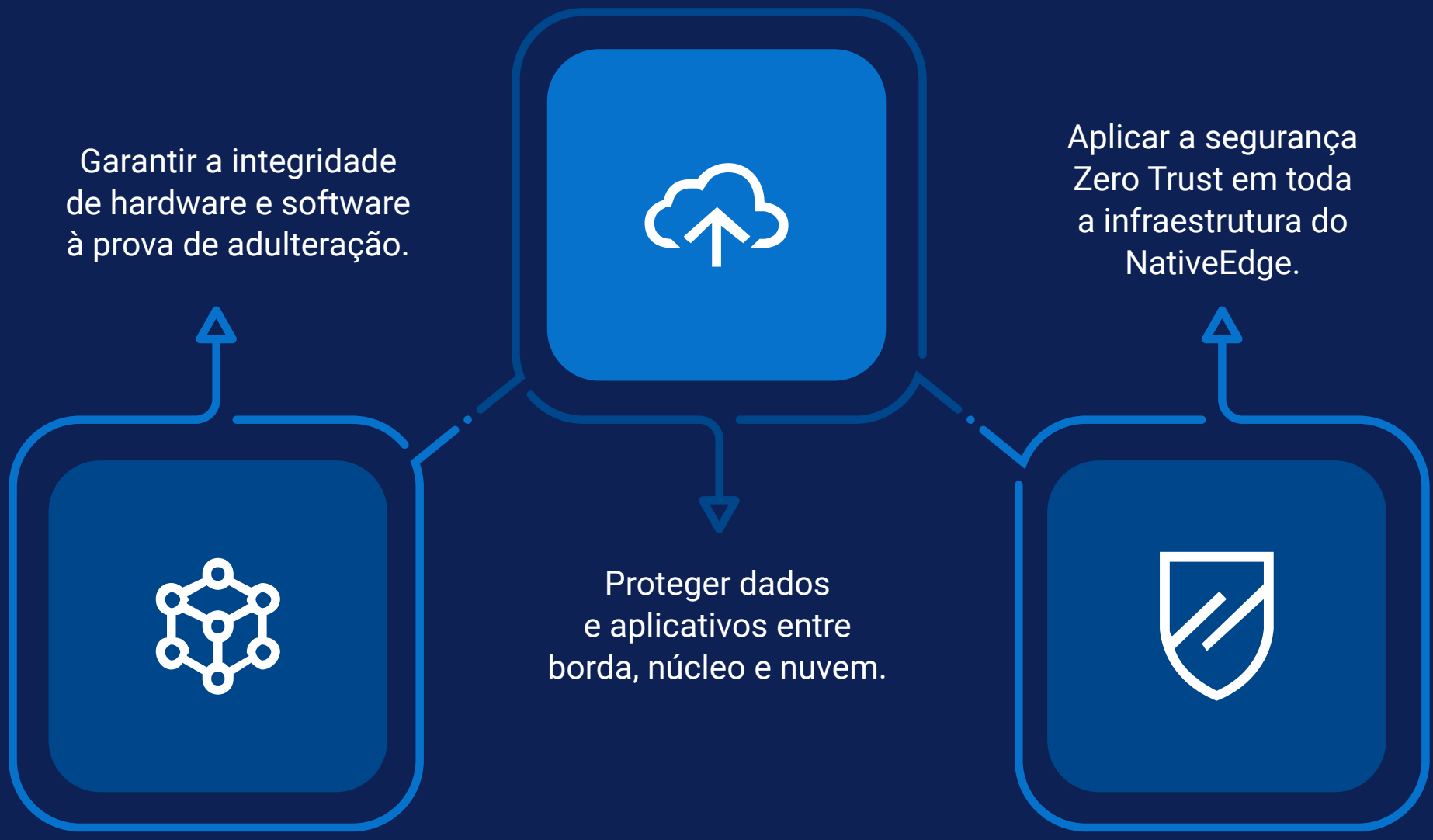
[1] Validação técnica do Enterprise Strategy Group by TechTarget encomendada pela Dell Technologies, "Dell NativeEdge – Edge Operations Software Platform", fevereiro de 2025.

[2] Com base em uma análise interna da Dell Technologies, maio de 2025.

Dell.com/NativeEdge

Proteja suas operações distribuídas em expansão reforçando, de maneira persistente e automática, a segurança da infraestrutura, dos aplicativos, dos dados, da rede e dos usuários, sem qualquer intervenção da TI.

O Dell NativeEdge protege as operações distribuídas ao



Reforçando a segurança Zero Trust

As empresas modernas são responsáveis por gerenciar milhares de aplicativos em locais geograficamente distribuídos e, muitas vezes, dependem de uma combinação heterogênea de infraestrutura. Isso cria uma rede complexa de silos de tecnologia que são ineficientes para gerenciar, difíceis de proteger e lentos para atualizar. À medida que as organizações continuam a implementar novos aplicativos, novos sensores e novos dispositivos em locais distribuídos, a superfície de ataque para possíveis ameaças cibernéticas aumenta.

Como as empresas podem garantir a segurança contínua das operações de dados distribuídos?

O Dell NativeEdge permite que você opere com confiança com uma base de segurança Zero Trust. Desde o momento em que um dispositivo é ligado, uma cadeia de confiança com base no hardware é estabelecida, utilizando recursos como Inicialização segura UEFI e um Virtual Trusted Platform Module (vTPM) para garantir a integridade do dispositivo. Com suporte integrado ao GDPR e a outras exigências globais de soberania de dados, o NativeEdge oferece tranquilidade para ambientes distribuídos. Essa abordagem, combinada com recursos como a microssegmentação zero trust, protege seus aplicativos e dados para que você possa inovar com segurança onde quer que opere.

Segurança Zero Trust

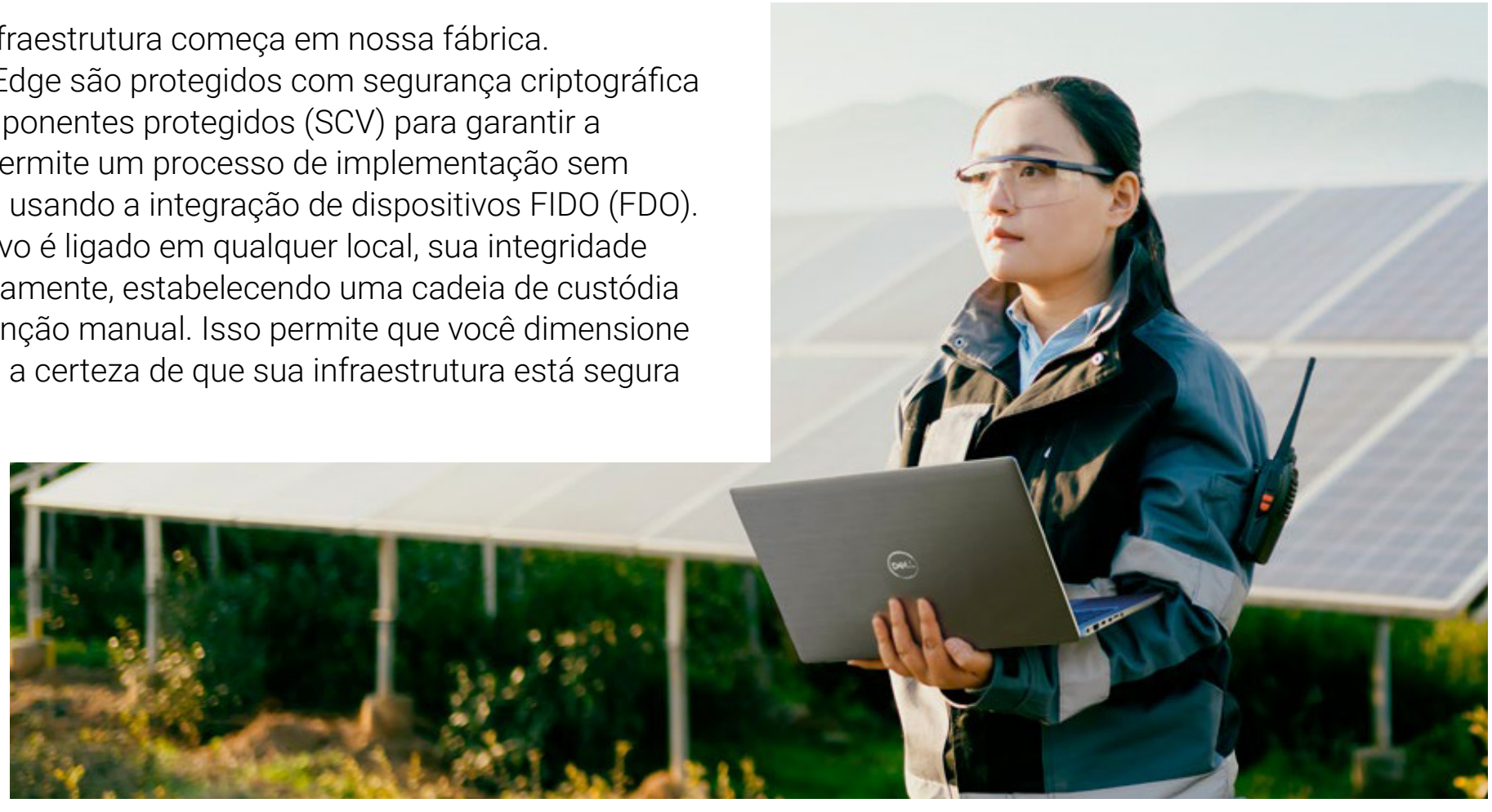
A postura de segurança é ainda mais reforçada pelo monitoramento e compreensão de todas as ações de seus recursos, possibilitados por controles de negócios relevantes, um plano de controle centralizado e uma infraestrutura que trabalha explicitamente em seu nome. Com os princípios de design Zero Trust do NativeEdge, as empresas podem ter certeza de que, à medida que as operações distribuídas se expandem, a integridade de cada recurso conectado é continuamente atestada e validada.

Garantindo a integridade do hardware ao longo da cadeia de suprimentos e seu ciclo de vida

Analisando os exemplos de um varejista ou fabricante com lojas ou fábricas em todo o mundo, torna-se cada vez mais difícil gerenciar e proteger o hardware diversificado que possui especificações e perfis variados com base na localização. Com o tempo, esses dispositivos não são atestados continuamente e a conformidade não pode ser verificada em uma escala de tempo estendida. Esse risco cresce exponencialmente quando várias partes estão envolvidas nas instalações desses dispositivos.

Como você pode proteger consistentemente a infraestrutura distribuída?

A proteção da sua infraestrutura começa em nossa fábrica. Os endpoints NativeEdge são protegidos com segurança criptográfica e Verificação de componentes protegidos (SCV) para garantir a autenticidade. Isso permite um processo de implementação sem intervenção e seguro usando a integração de dispositivos FIDO (FDO). Quando um dispositivo é ligado em qualquer local, sua integridade é validada automaticamente, estabelecendo uma cadeia de custódia segura e sem intervenção manual. Isso permite que você dimensione suas operações com a certeza de que sua infraestrutura está segura desde o primeiro dia.

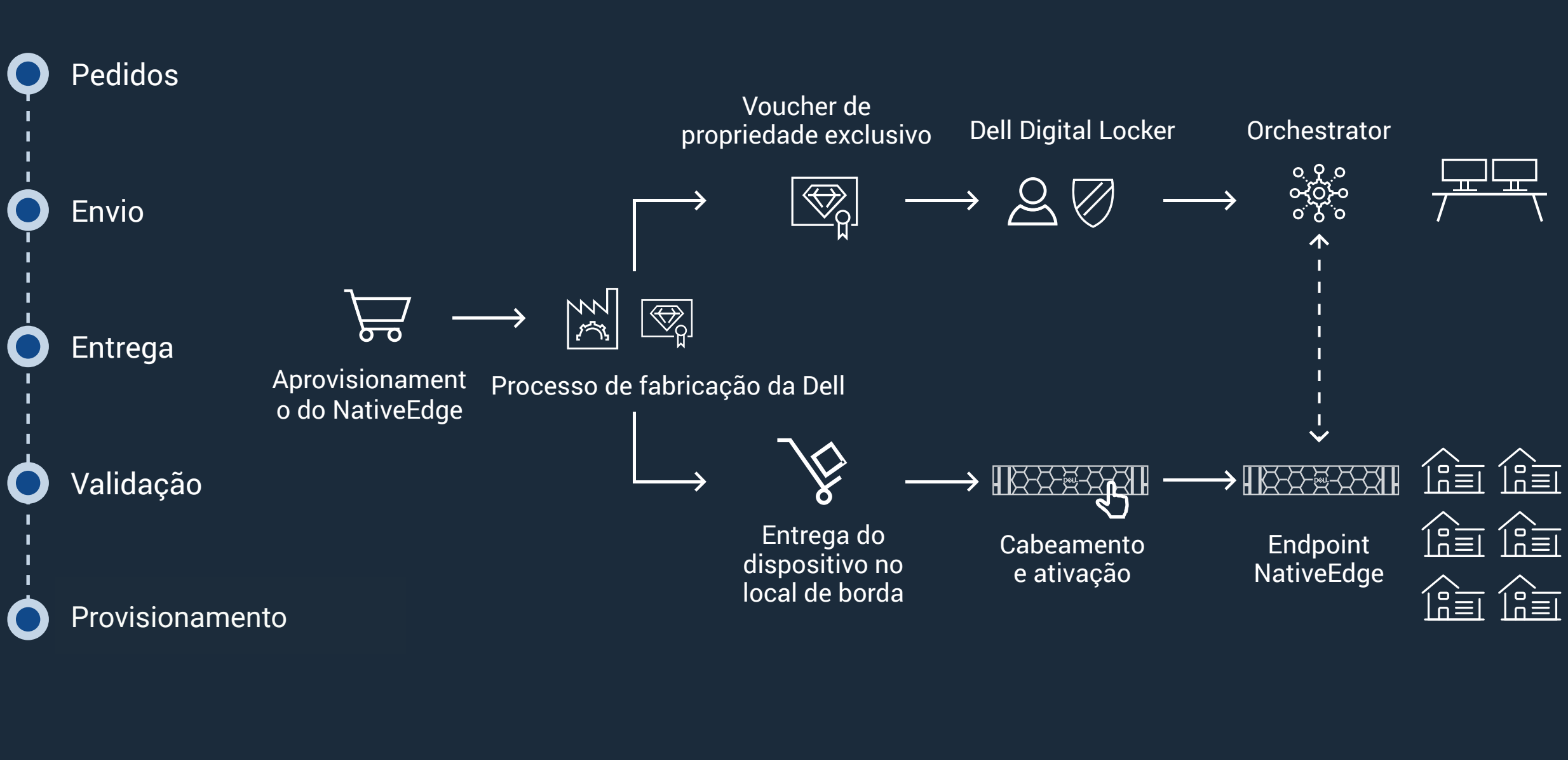


Os endpoints NativeEdge são otimizados para compatibilidade com o NativeEdge e protegidos com segurança criptográfica na fábrica da Dell.

O NativeEdge utiliza o processo de Verificação de componentes protegidos (SCV) para garantir a autenticidade e a integridade dos componentes de hardware. Por meio da SCV, o NativeEdge reforça a integridade da cadeia de suprimentos, a verificação de componentes, a validação de firmware, os processos de inicialização segura e as assinaturas criptográficas para proteger contra acesso não autorizado ou adulteração.

À medida que esses dispositivos passam pelo processo de integração de dispositivos baseada em FIDO, sua integridade é certificada automaticamente, garantindo a segurança desde a produção na fábrica da Dell até o recebimento e a instalação no local da implementação. Se o hardware for adulterado de alguma forma, a plataforma o isola automaticamente, protegendo as operações de elementos prejudiciais.

Integração segura de dispositivos e estrutura Zero Trust

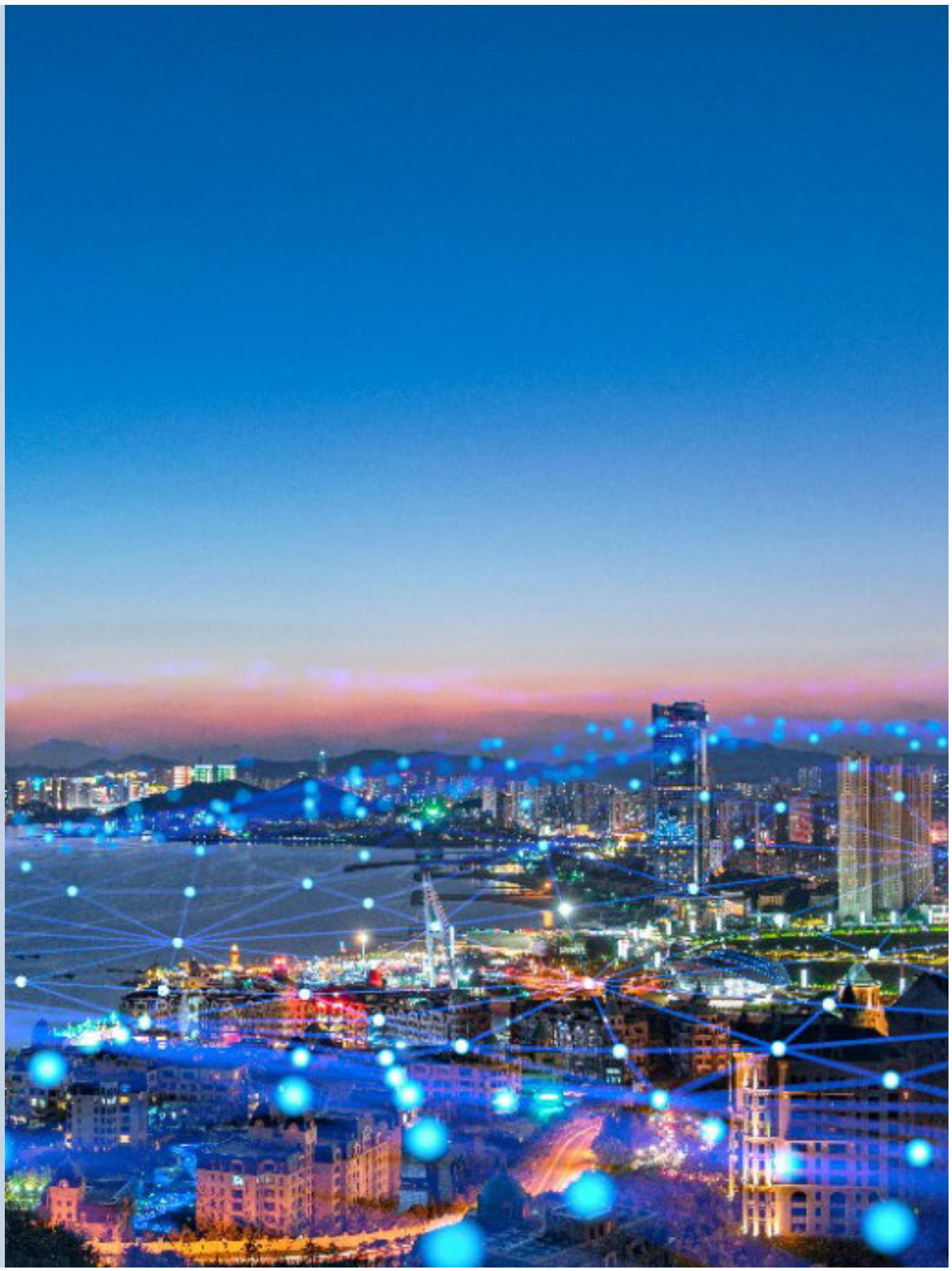


Fortalecendo dados e aplicativos desde a borda até a nuvem

Considere o exemplo de um varejista global. A natureza diversificada e distribuída dos ambientes de varejo significa que as identidades dos usuários que acessam aplicativos e cargas de trabalho podem não ser verificadas rotineiramente. Quando isso ocorre, a verificação é feita localmente para esse ambiente e não fica centralmente visível e nem auditável.

Além disso, os varejistas raramente têm visibilidade da cadeia de suprimentos de software dos aplicativos implementados. Esses serviços geralmente são gerenciados por Prestadores de serviços gerenciados (MSPs) e pode não haver verificações automatizadas visíveis da fidelidade desses aplicativos. Esses aplicativos geralmente são configurados inicialmente pelos mesmos MSPs, com a possibilidade de desvios de configuração ao longo do tempo. Portanto, as partes interessadas não conseguem determinar a conformidade do aplicativo com as políticas de segurança.

No caso dos fabricantes, a equipe de tecnologia operacional (OT) geralmente executa um conjunto diversificado de cargas de trabalho de aplicativos. Alguns desses aplicativos interagem com equipamentos como PLCs e são aplicativos proprietários sem visibilidade interna.



Os recursos da rede de TI não se estendem à rede de tecnologia operacional (OT), que é logicamente separada. Resultado? As cargas de trabalho de infraestrutura e aplicativos dentro das redes de OT dos fabricantes não têm acesso ao nível de controles de segurança de rede necessários para possibilitar um ambiente de OT seguro. Desafios semelhantes relacionados à segurança de aplicativos e dados são comuns em todos os setores.

O Dell NativeEdge ajuda as organizações a proteger o pipeline de dados, desde as fontes de dados até os aplicativos em execução localmente ou na nuvem. Ele combina medidas avançadas de segurança, como criptografia, controle de acesso do usuário, catálogo de modelos de aplicativos, segmentação de rede e orquestração de segurança. O NativeEdge também usa telemetria e lógica analítica para avaliar proativamente a postura de segurança de seus locais distribuídos, sem depender de especialistas com recursos de auditoria para visitar todos os locais.

Medidas avançadas de segurança

Medidas avançadas de segurança garantem operações resilientes

Controle de acesso de usuários

O NativeEdge fornece controle de acesso baseado em função (RBAC) para analisar os níveis de acesso com base nas funções e responsabilidades do usuário. Os usuários dos dispositivos e as cargas de trabalho dos aplicativos implementados são verificados por sessão de acesso, bem como atestados de forma centralizada e visível por meio do gerenciamento de identidade e acesso.

Segmentação de rede

A microssegmentação da rede para os aplicativos facilita o desenvolvimento e o gerenciamento de políticas que visam esses aplicativos para torná-los mais seguros. Essa abordagem reduz os riscos de possíveis violações e a movimentação lateral de ameaças em ambientes virtualizados.

Catálogo de modelos de aplicativos

O NativeEdge foi projetado para tornar os aplicativos mais seguros. Tudo começa com uma cadeia de suprimentos de software segura que utiliza um Catálogo para implementar seus aplicativos usando modelos. O Catálogo é um conjunto de modelos para implementar aplicativos de Fornecedores de software independentes (ISVs) ou modelos pré-validados da Dell, desenvolvidos por empresas, tudo para manter uma cadeia de suprimentos de software segura. Esses modelos, baseados no padrão TOSCA e no formato YAML, automatizam a implementação de aplicativos e estruturas de IA em muitos dispositivos de borda, de uma só vez. O NativeEdge permite que você defina controles de segurança proativos para aplicativos implementados em um nível granular e garante que seus aplicativos sejam implementados de forma consistente e alinhados às suas políticas de segurança. Por fim, as cargas de trabalho dos aplicativos podem ser executadas em endpoints NativeEdge ou em um ambiente multicloud como VMs e contêineres, gerenciados centralmente pelo NativeEdge.

Criptografia e proteção dos dados

O NativeEdge protege seus dados onde quer que estejam, em repouso, em trânsito e em uso, contra violações e acesso não autorizado. O NativeEdge oferece uma robusta criptografia de dados em repouso (DARE), que atende aos padrões de conformidade federais, garantindo que os dados armazenados sejam criptografados e protegidos contra roubos físicos ou adulterações. O NativeEdge controla todos os recursos de dados com princípios de segurança Zero Trust, aplicando um controle de acesso rigoroso, atestando e verificando continuamente o controle de acesso. Isso não apenas protege a integridade dos dados de aplicativos empresariais, mas também aumenta a confiança de todas as partes interessadas da empresa.

Orquestração de segurança

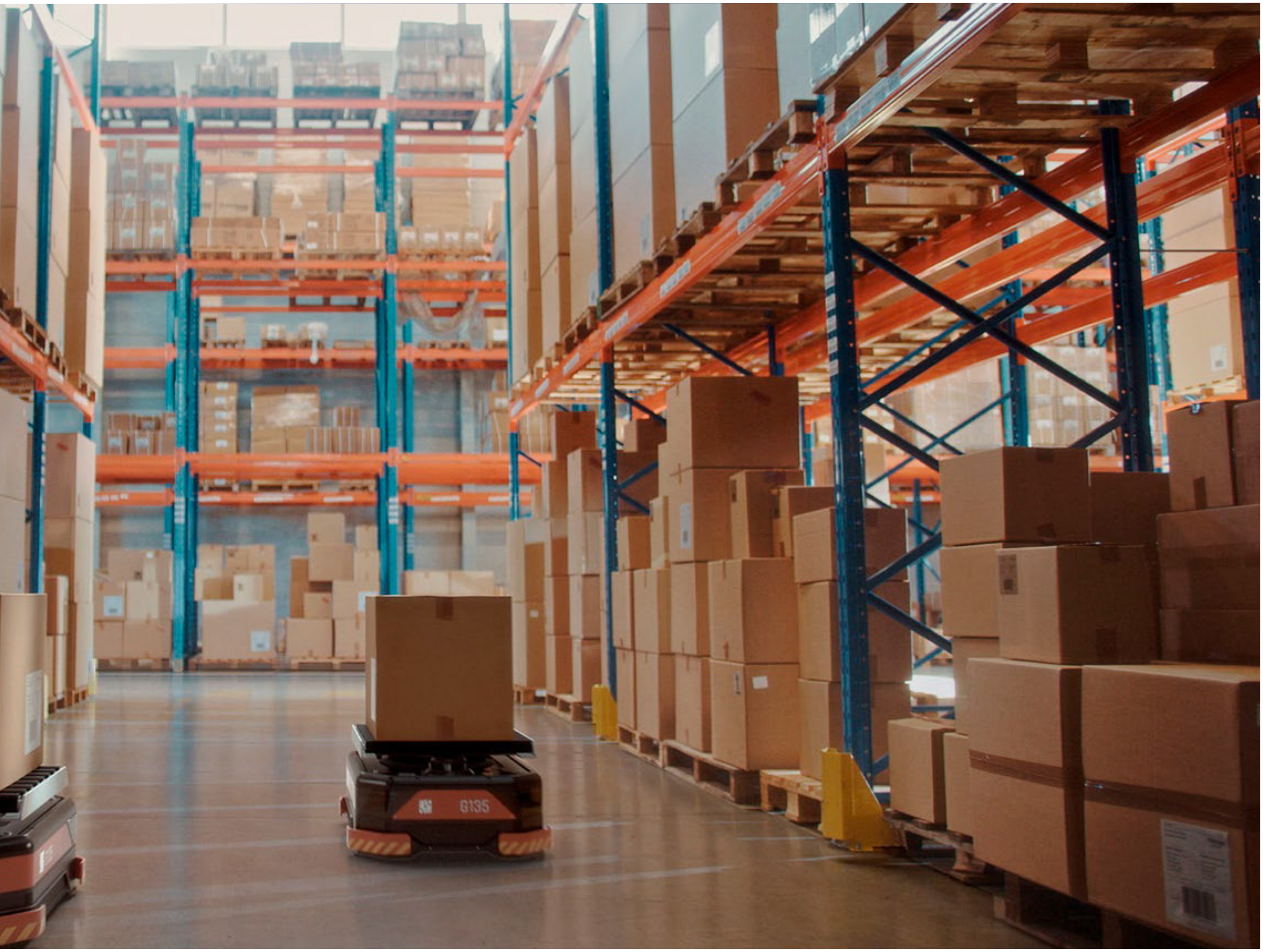
Ações/eventos não autorizados geralmente ocorrem sem serem percebidos e, muitas vezes, nunca são corrigidos. Essa situação apresenta riscos devido aos processos manuais e, muitas vezes, fica em segundo plano em relação a tarefas de negócios de alta prioridade. Além disso, existe variação na integração de TI em torno do Gerenciamento de acessos a identidades (IAM)/Controle de acesso com base em funções (RBAC) e plano de controle.

Isso leva a uma orquestração de segurança desconectada, que geralmente é gerenciada individualmente em cada local. Em muitos casos de tecnologia operacional (OT), esses dispositivos estão em um ambiente máquina a máquina (M2M) que não tem conhecimento do usuário. A orquestração centralizada é crucial para esses ambientes.

O NativeEdge garante orquestração de segurança consistente em todo o ambiente de borda. Com base no conjunto de ações e eventos que acontecem no ambiente de borda, ele oferece uma visão unificada da postura de segurança, permitindo autenticação centralizada e aplicação consistente de políticas em todos os locais. Ele utiliza recursos de IAM e RBAC que permitem o gerenciamento seguro da plataforma usando o princípio de privilégio mínimo, fornecendo assim a granularidade que as empresas precisam. O NativeEdge também simplifica a conformidade com regulamentos como GDPR, PCI e HIPAA, automatizando o registro e o gerenciamento de configuração, ajudando você a operar com confiança em qualquer ambiente com a capacidade de incorporar regras de Governança, risco e conformidade (GRC)/operações de segurança (SecOps).

Telemetria e lógica analítica

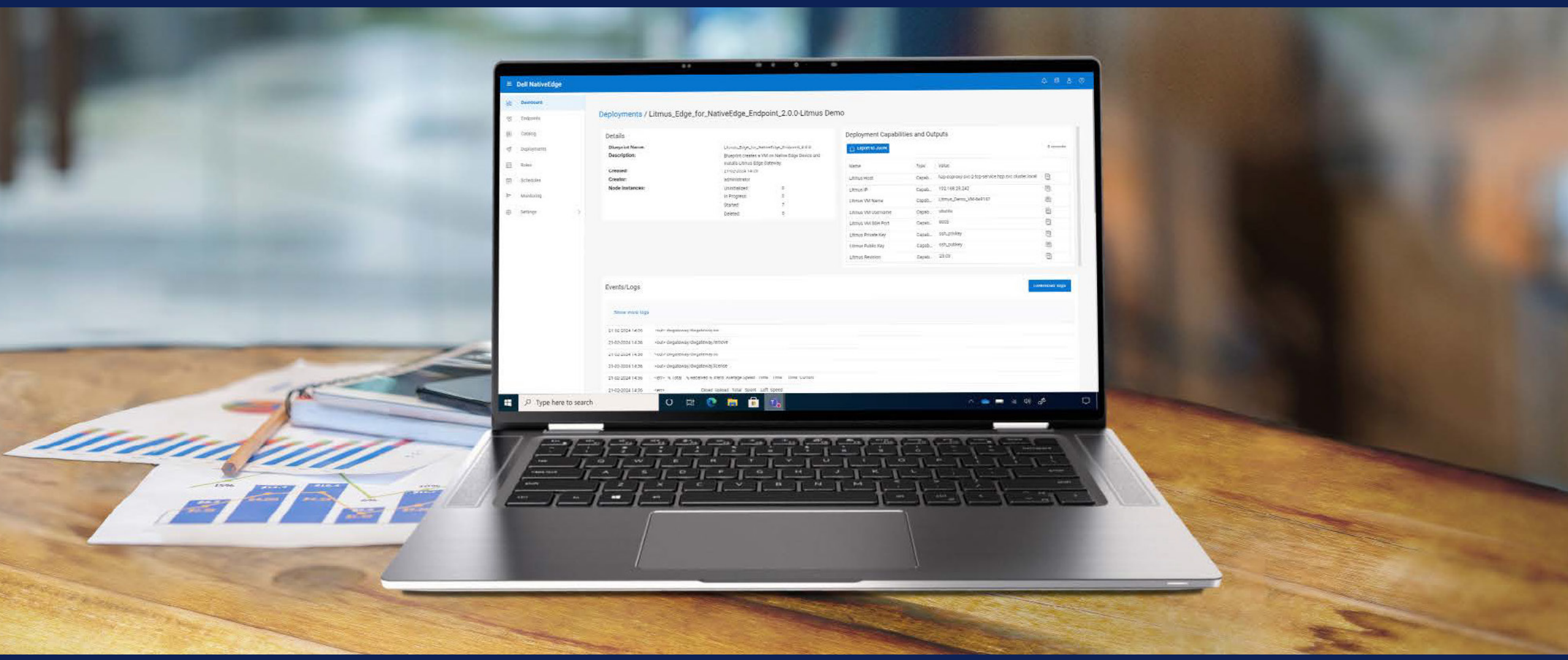
O NativeEdge realiza avaliações de segurança contínuas de acordo com os padrões de conformidade definidos, utilizando telemetria do hardware e do ambiente operacional. Esses dados são usados para detectar desvios de configuração, configurações incorretas e a necessidade de atualizações de segurança.



Proteja sua propriedade de borda

O Dell NativeEdge protege seu patrimônio de borda com princípios de segurança Zero Trust, incluindo integração segura de dispositivos baseada em FIDO, juntamente com um SO NativeEdge reforçado e seguro. Com o Dell NativeEdge, você tem a garantia de que sua infraestrutura, usuários, rede, aplicativos e dados são continuamente atestados e validados em locais distribuídos.

Inove onde quer que você atue



DELL Technologies

Saiba mais em **Dell.com/NativeEdge**