Dell NativeEdge

Protection : travaillez en toute confiance avec une sécurité Zero-Trust

Table des

Table des matières

Sécurité dans tous les environnements distribués

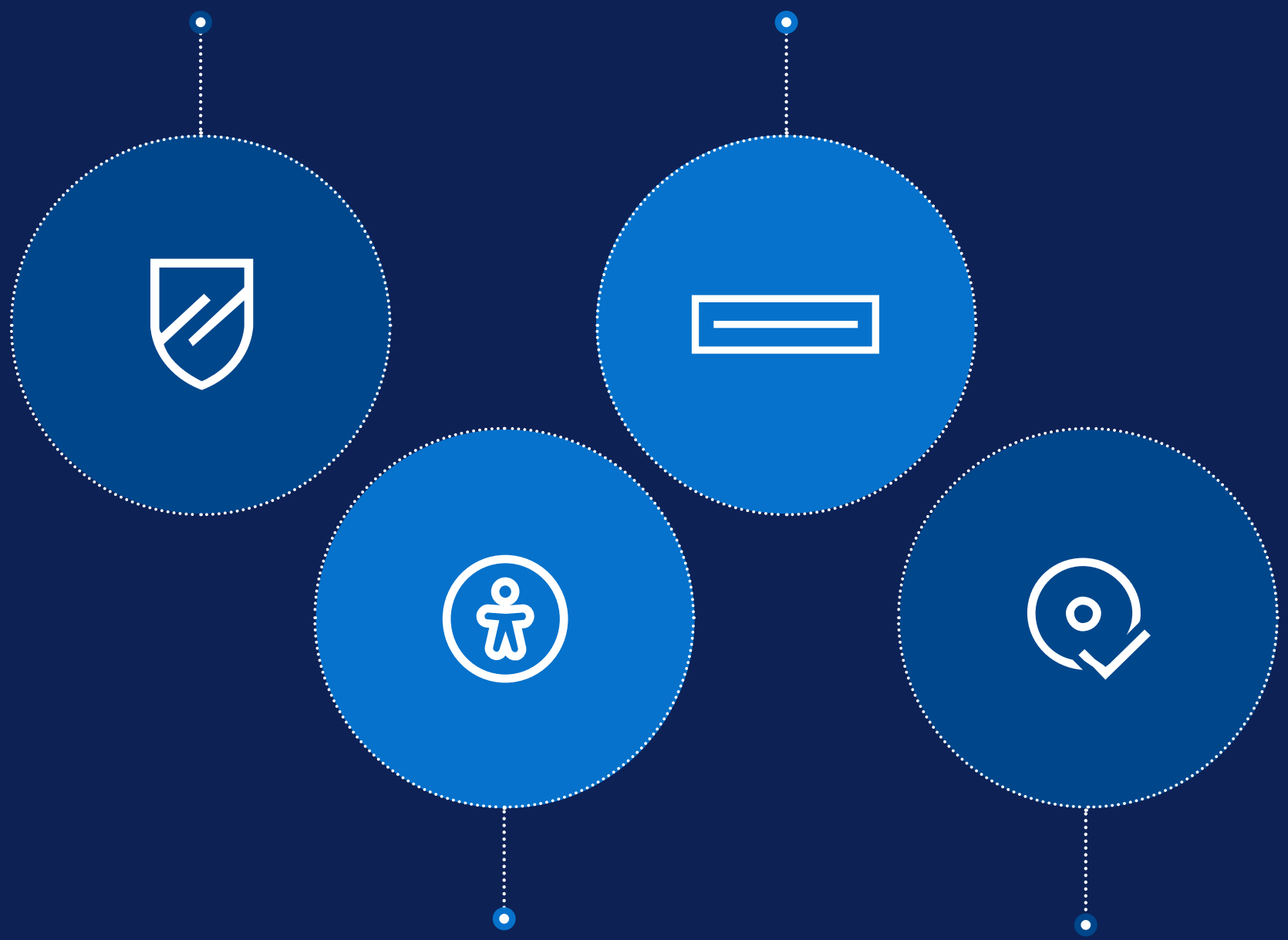
Pour répondre à l'évolution rapide des préférences des clients et de la dynamique du marché, les entreprises déploient de nouvelles applications, mises à jour et infrastructures de calcul à une échelle et une rapidité inégalées. Face à ce déluge de données, d'infrastructures et d'applications, il est de plus en plus essentiel de sécuriser les environnements distribués dans lesquels résident ces nouvelles technologies.

À mesure que les entreprises développent leurs opérations, les risques liés à la sécurité se multiplient : altération d'appareils physiques, piratage de données, etc. En outre, ces systèmes gèrent souvent des données personnelles sensibles, ce qui impose aux entreprises une plus grande responsabilité en matière de protection de leurs clients.

Pour sécuriser les opérations, les entreprises doivent

Assurer
la sécurité physique
de l'infrastructure déployée
sur des sites distribués

Détecter
l'altération des appareils
et neutraliser les menaces



Contrôler
l'accès des utilisateurs
à tous les niveaux

Faire évoluer
le provisionnement et les mises
à jour logicielles
sur des milliers d'appareils

Dell NativeEdge

Innovez où que vous soyez

Une solution complète et de bout en bout qui centralise de façon sécurisée le déploiement, l'orchestration et la gestion du cycle de vie de diverses infrastructures et applications en périphérie et dans l'ensemble des datacenters distribués.

Simplifiez, optimisez et protégez les environnements de périphérie et de datacenters distribués grâce à des fonctionnalités telles que l'intégration sans intervention, la sécurité Zero-Trust et l'orchestration avancée des charges applicatives. NativeEdge utilise un hyperviseur KVM et l'exécution des conteneurs, permettant aux entreprises de déployer et de gérer à la fois des machines virtuelles et des conteneurs. Elle est optimisée pour orchestrer les charges applicatives et les cadres d'IA, ce qui permet un déploiement et une gestion transparents des applications basées sur l'IA à la périphérie et dans l'ensemble des datacenters distribués. NativeEdge peut également s'adapter à n'importe quel environnement matériel, car elle prend en charge un large éventail d'options dans différents formats, des serveurs Dell PowerEdge aux ordinateurs de bureau en passant par les infrastructures tierces.

Dell NativeEdge est spécialement conçue pour relever les défis uniques des environnements distribués, tels que la complexité opérationnelle, l'évolutivité et la sécurité. Cette solution est conçue pour les organisations modernes qui souhaitent exploiter la puissance de l'Edge computing tout en réduisant les coûts et en améliorant l'efficacité.

Simplifier
Accélérez les résultats et centralisez les opérations

Moins
d'une minute
pour déployer l'infrastructure et les applications[1]

Optimiser
Favorisez une virtualisation transparente et une IA évolutive

Jusqu'à
68 %
de gain de temps grâce à l'automatisation de l'orchestration des applications à la périphérie[1]

Protégez
Travaillez en toute confiance avec une sécurité Zero-Trust

Effectuez les opérations
à la périphérie
les plus sécurisées au monde[2]

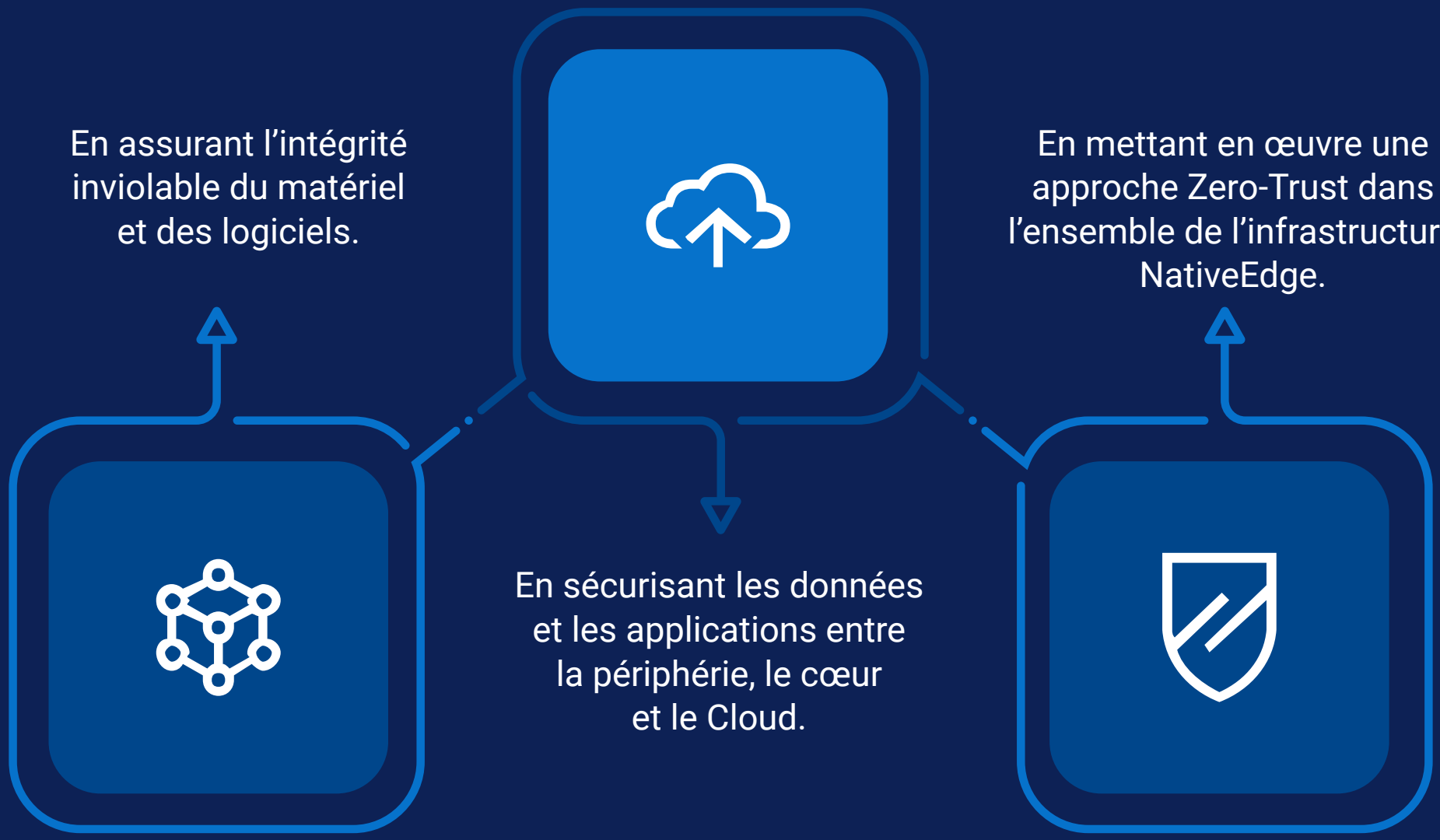
[1] Validation technique par Enterprise Strategy Group de TechTarget Technical réalisée à la demande de Dell Technologies, « Dell NativeEdge - Edge Operations Software Platform », février 2025.

[2] D'après une analyse interne de Dell Technologies datant de mai 2025.

Dell.com/NativeEdge

Sécurisez vos opérations distribuées en pleine expansion en renforçant de manière permanente et automatique la sécurité de l'infrastructure, des applications, des données, du réseau et des utilisateurs, sans aucune intervention IT.

Dell NativeEdge protège les opérations distribuées



Consolidation de la sécurité Zero-Trust

Les entreprises modernes sont responsables de la gestion de milliers d'applications réparties sur des sites géodistribués et s'appuient souvent sur un ensemble d'infrastructures hétérogènes. Cela crée un réseau complexe de silos technologiques qui sont difficiles à gérer et à sécuriser et longs à mettre à jour. À mesure que les entreprises continuent de déployer de nouvelles applications, de nouveaux capteurs et de nouveaux appareils sur des sites distribués, elles sont davantage exposées aux cybermenaces potentielles.

Comment les entreprises peuvent-elles garantir la sécurité continue des opérations de données distribuées ?

Dell NativeEdge vous permet de travailler en toute confiance avec une base de sécurité Zero-Trust. Dès la mise sous tension d'un appareil, une chaîne de confiance basée sur le matériel est établie à l'aide de fonctionnalités telles que UEFI Secure Boot et un module vTPM (Virtual Trusted Platform Module) pour garantir l'intégrité de l'appareil. Conçue pour assurer la conformité au RGPD et à d'autres obligations mondiales de souveraineté des données, NativeEdge permet d'utiliser des environnements distribués sans inquiétude. Cette approche, combinée à des fonctionnalités telles que la microsegmentation Zero-Trust, protège vos applications et vos données afin que vous puissiez innover en toute sécurité, où que vous soyez.

Sécurité Zero-Trust

La posture de sécurité est renforcée par la surveillance et la compréhension de toutes les actions de vos ressources, rendues possibles par des contrôles métier pertinents, un plan de contrôle centralisé et une infrastructure qui fonctionne explicitement en son nom. Avec les principes de conception Zero-Trust de NativeEdge, les entreprises sont assurées que l'intégrité de chaque ressource connectée est constamment attestée et validée à mesure que les opérations distribuées se développent.

Garantie de l’intégrité du matériel tout au long de la chaîne logistique et de son cycle de vie

Pour un détaillant ou un fabricant disposant de magasins ou d’usines dans le monde entier, il devient de plus en plus difficile de gérer et de sécuriser différents types de matériel dont les spécifications et les profils varient d’un site à l’autre. Ces appareils ne sont pas continuellement attestés et la conformité ne peut pas être vérifiée sur une longue période. Lorsque plusieurs parties sont impliquées dans le processus d’installation de ces dispositifs, ce risque augmente de manière exponentielle.

Comment protéger l’infrastructure distribuée de manière cohérente ?

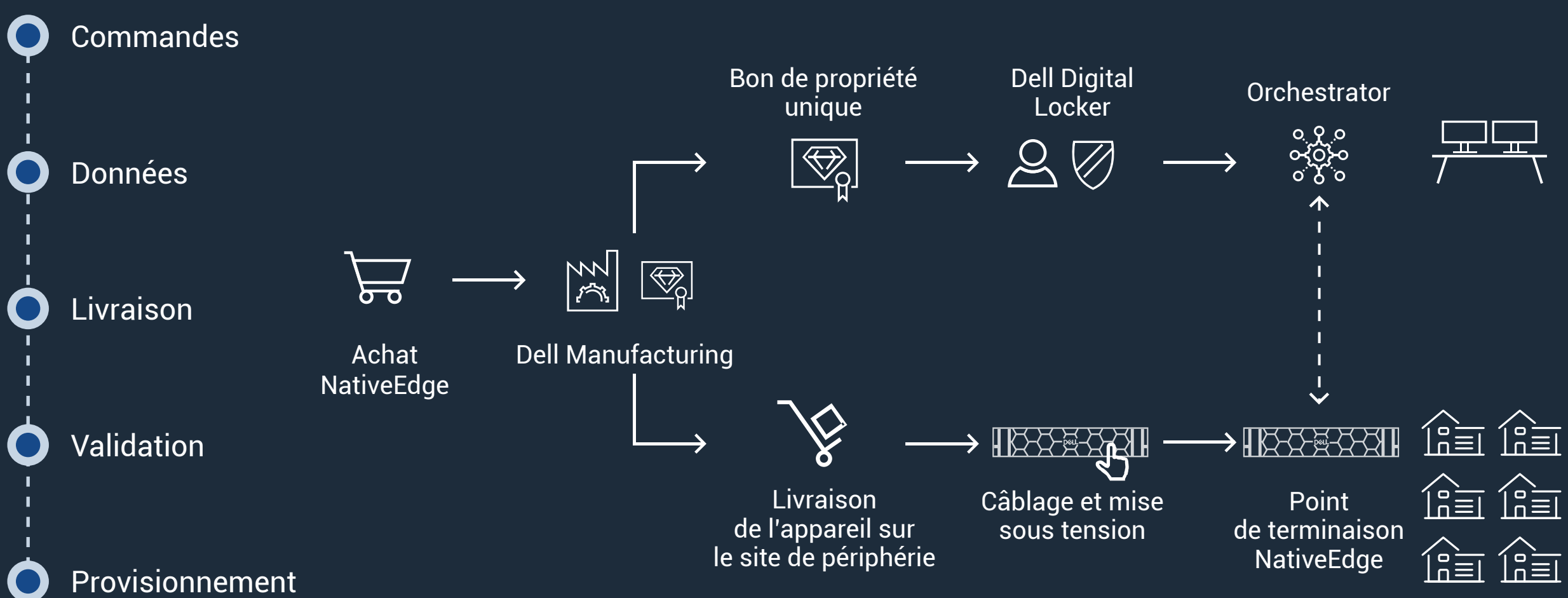
La protection de votre infrastructure commence dans notre usine. Les points de terminaison NativeEdge sont protégés par une sécurité cryptographique et la vérification SCV (Secured Component Verification) pour garantir leur authenticité. Cela permet de mettre en œuvre un processus de déploiement sécurisé et sans intervention à l’aide de la technologie FDO (FIDO Device Onboarding). Lorsqu’un appareil est mis sous tension sur n’importe quel site, son intégrité est automatiquement validée, établissant une chaîne de possession sécurisée sans intervention manuelle. Vous êtes ainsi en mesure de faire évoluer vos opérations tout en sachant que votre infrastructure est sécurisée dès le premier jour.

Les points de terminaison NativeEdge sont optimisés pour une compatibilité avec NativeEdge et sont protégés en usine Dell par une sécurité cryptographique.

NativeEdge utilise le processus SCV (Secured Component Verification) pour garantir l'authenticité et l'intégrité des composants matériels. Via SCV, NativeEdge applique l'intégrité de la chaîne logistique, la vérification des composants, la validation des firmwares, les processus Secure Boot et les signatures cryptographiques afin de vous protéger contre les accès non autorisés ou les altérations.

À mesure que ces appareils sont soumis au processus d'intégration des appareils basé sur FIDO, leur intégrité est certifiée automatiquement, garantissant ainsi la sécurité, de la fabrication dans l'usine Dell jusqu'à la réception et l'installation sur le site de déploiement. Si le matériel est altéré de quelque manière que ce soit, la plate-forme les isole automatiquement, protégeant ainsi les opérations des éléments indésirables.

Intégration sécurisée des appareils et cadre Zero-Trust

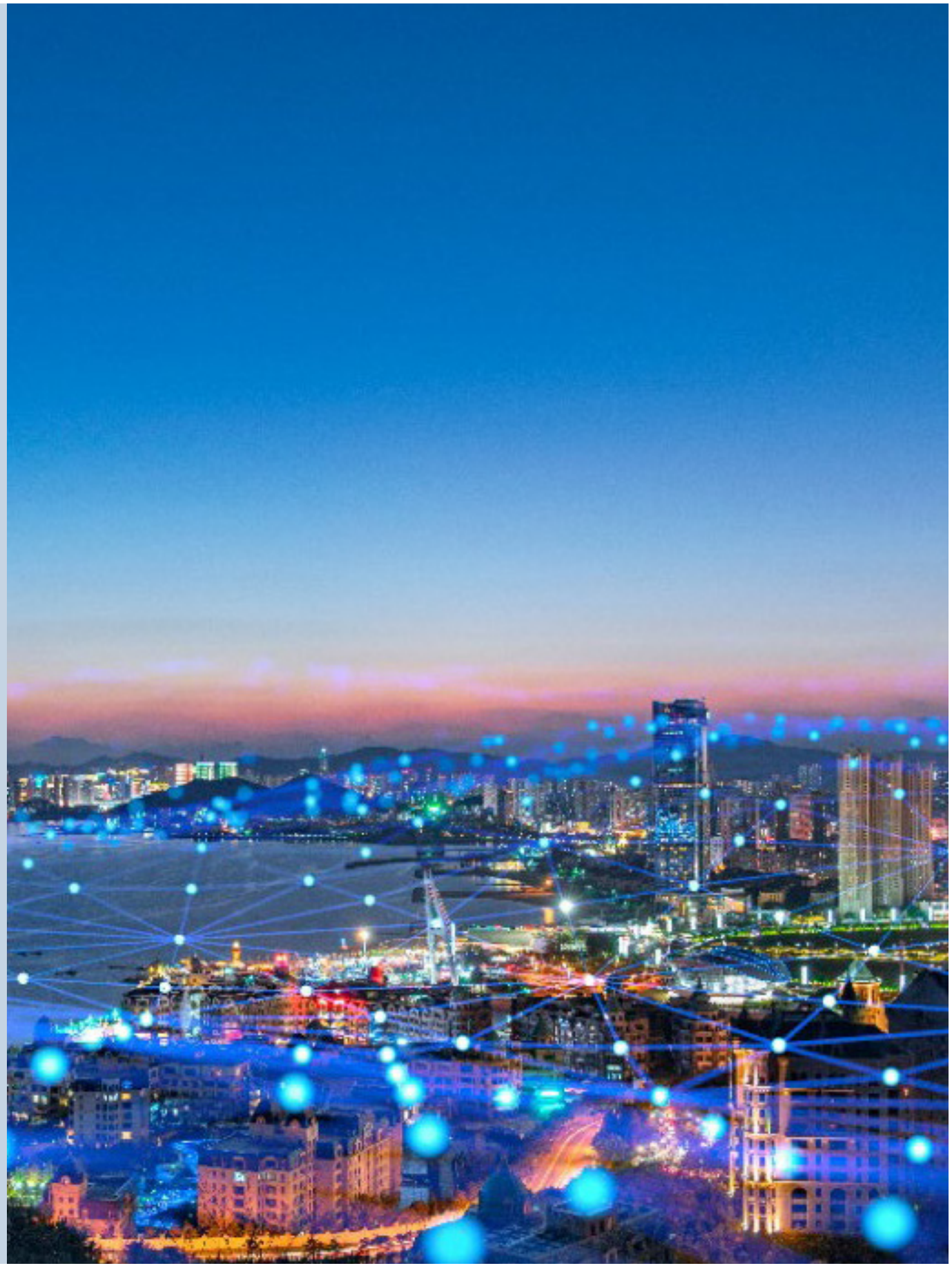


Données et applications renforcées, de la périphérie au Cloud

Prenons l'exemple d'un détaillant international. En raison de la nature disparate et distribuée des environnements de vente au détail, les identités des utilisateurs qui accèdent aux applications et aux charges applicatives peuvent ne pas être vérifiées régulièrement. Si elles le sont, le processus est effectué localement dans cet environnement et ne peut pas être visualisé ni audité de manière centralisée.

En outre, les détaillants disposent rarement de visibilité sur la chaîne logistique logicielle des applications déployées. Ces applications sont souvent gérées par des fournisseurs de services managés (MSP) et leur fidélité peut ne faire l'objet d'aucune vérification automatisée visible. La configuration initiale de ces applications est souvent effectuée par les mêmes MSP, mais des écarts de configuration peuvent apparaître au fil du temps. Les parties prenantes ne sont donc pas en mesure de déterminer la conformité des applications aux règles de sécurité.

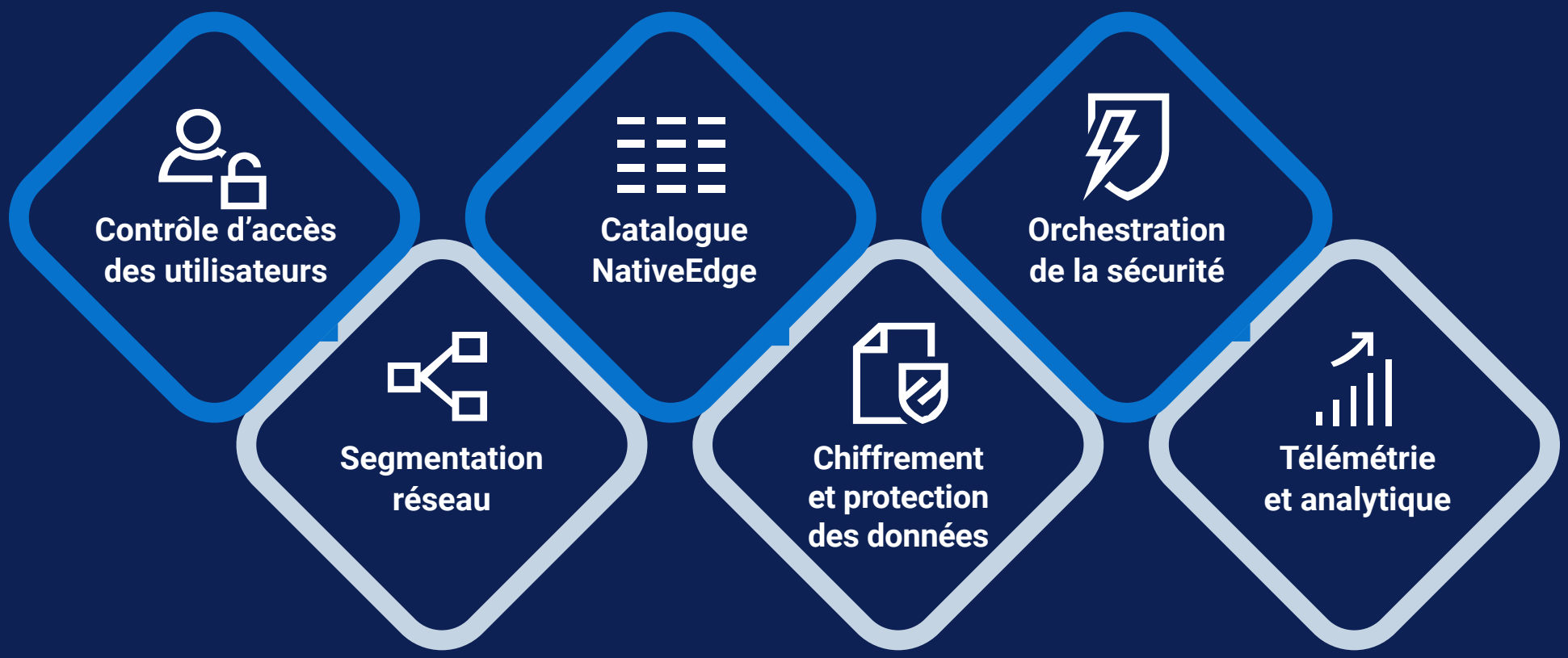
Dans le cas des fabricants, l'équipe des technologies opérationnelles (OT) exécute généralement un ensemble diversifié de charges applicatives. Certaines de ces applications interagissent avec des équipements tels que les automates programmables industriels et sont des applications propriétaires sans visibilité interne.



Les capacités du réseau IT ne sont pas transmises au réseau opérationnel, ce qui crée une séparation logique. Le résultat ? L'infrastructure et les charges applicatives au sein des réseaux OT des fabricants n'ont pas accès au niveau des contrôles de sécurité réseau requis pour sécuriser un environnement OT. Tous les secteurs sont confrontés à des défis similaires liés à la sécurité des applications et des données.

Dell NativeEdge aide les entreprises à sécuriser le pipeline de données, des sources de données aux applications exécutées localement ou dans le Cloud. Cette solution combine des mesures de sécurité avancées telles que le chiffrement, le contrôle d'accès des utilisateurs, le catalogue de blueprints d'applications, la segmentation du réseau et l'orchestration de la sécurité. NativeEdge utilise également la télémétrie et l'analytique pour évaluer de manière proactive la posture de sécurité de vos sites distribués sans qu'il soit nécessaire de faire appel à des experts disposant de fonctionnalités d'audit sur chaque site.

Mesures de sécurité avancées



Opérations résilientes grâce à des mesures de sécurité avancées

Contrôle d’accès des utilisateurs

NativeEdge fournit un contrôle d’accès basé sur les rôles (RBAC) pour analyser les niveaux d’accès en fonction des rôles et des responsabilités de l’utilisateur. Les utilisateurs des appareils et des charges applicatives déployées sont vérifiés par session d’accès et attestés de manière centralisée et visible via la gestion des identités et des accès.

Segmentation réseau

La micro-segmentation du réseau pour les applications facilite le développement et la gestion des règles qui ciblent ces applications afin de les rendre plus sécurisées. Cette approche limite les risques de violation potentielle et de déplacement latéral des menaces au sein des environnements virtualisés.

Catalogue de blueprints d’applications

NativeEdge est conçue pour sécuriser les applications. Tout commence par une chaîne logistique logicielle sécurisée qui s’appuie sur un catalogue pour déployer vos applications à l’aide de blueprints. Le catalogue est un ensemble de blueprints permettant de déployer des applications d’éditeurs de logiciels indépendants (ISV) ou des blueprints prévalidés par Dell développés par des entreprises, le tout dans le but de maintenir une chaîne logistique logicielle sécurisée. Ces blueprints, basés sur la norme TOSCA et le format YAML, automatisent le déploiement simultané d’applications et de cadres d’IA sur de nombreux appareils. NativeEdge vous permet de définir des contrôles de sécurité proactifs pour les applications déployées à un niveau granulaire tout en garantissant que vos applications sont déployées de manière cohérente et alignée sur vos règles de sécurité. Enfin, les charges applicatives peuvent s’exécuter sur des points de terminaison NativeEdge ou dans un environnement multicloud sous forme de machines virtuelles et de conteneurs, gérés de manière centralisée par NativeEdge.

Chiffrement et protection des données

NativeEdge protège vos données, où qu’elles se trouvent (au repos, en transit ou en cours d’utilisation) contre les violations et les accès non autorisés. Notre solution fournit un chiffrement robuste des données au repos (DARE), conforme aux normes de conformité fédérales, garantissant ainsi que vos données stockées sont chiffrées et protégées contre le vol physique ou la falsification. Elle régit chaque ressource de données avec des principes de sécurité Zero-Trust en appliquant un contrôle d’accès strict ainsi qu’en attestant et en vérifiant continuellement le contrôle d’accès. Non seulement l’intégrité des données des applications d’entreprise est ainsi protégée, mais la confiance de toutes les parties prenantes de l’entreprise est également renforcée.

Orchestration de la sécurité

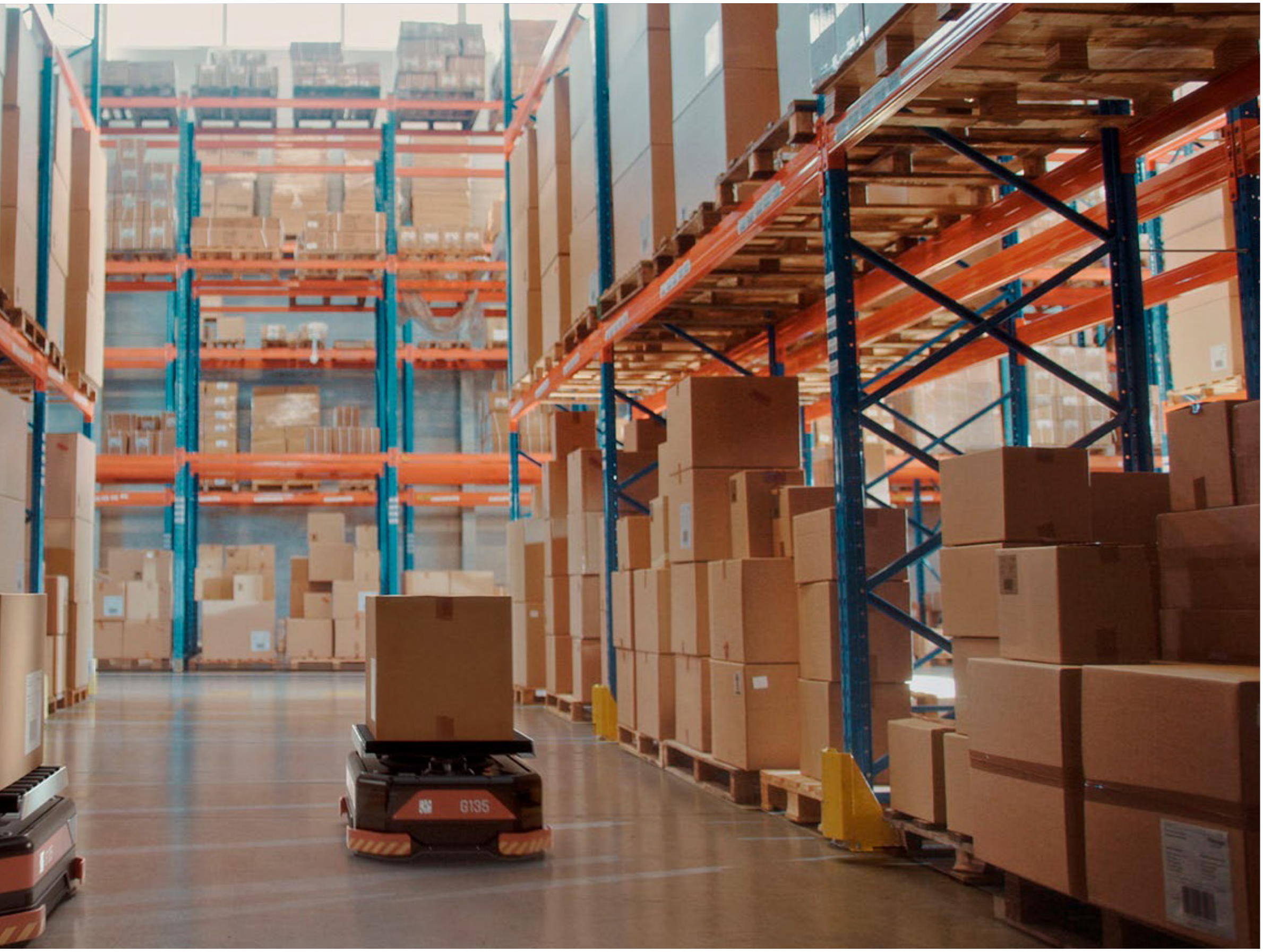
Les actions ou les événements non autorisés se produisent souvent sans être détectés et ne sont généralement jamais corrigés. Ce problème introduit un risque lié aux processus manuels et passe souvent au second plan par rapport aux tâches métiers à priorité élevée. En outre, l'intégration IT varie en matière de gestion des accès et des identités (IAM)/de contrôle des accès basé sur les rôles (RBAC) et de plan de contrôle.

Cela entraîne une orchestration déconnectée de la sécurité, qui est souvent gérée de manière individuelle sur chaque site. Dans de nombreux cas OT, ces appareils se trouvent dans un environnement M2M (machine-to-machine) qui ne prend pas l'utilisateur en compte. L'orchestration centralisée est cruciale pour ces environnements.

NativeEdge garantit une orchestration cohérente de la sécurité sur l'ensemble du parc en périphérie. Basée sur l'ensemble des actions et événements qui se produisent dans l'environnement de périphérie, elle fournit une vue unifiée de votre posture de sécurité, permettant une authentification centralisée et une application cohérente des règles sur tous les sites. Les fonctionnalités IAM et RBAC permettent une gestion sécurisée de la plate-forme à l'aide du principe du moindre privilège, offrant ainsi la granularité dont les entreprises ont besoin. NativeEdge simplifie également la conformité aux réglementations telles que le RGPD, la PCI et la HIPAA en automatisant la journalisation et la gestion de la configuration, ce qui vous permet de travailler en toute confiance dans n'importe quel environnement, avec la possibilité d'intégrer des règles GRC (gouvernance, risques et conformité)/SecOps (Security Operations).

Télémétrie et analytique

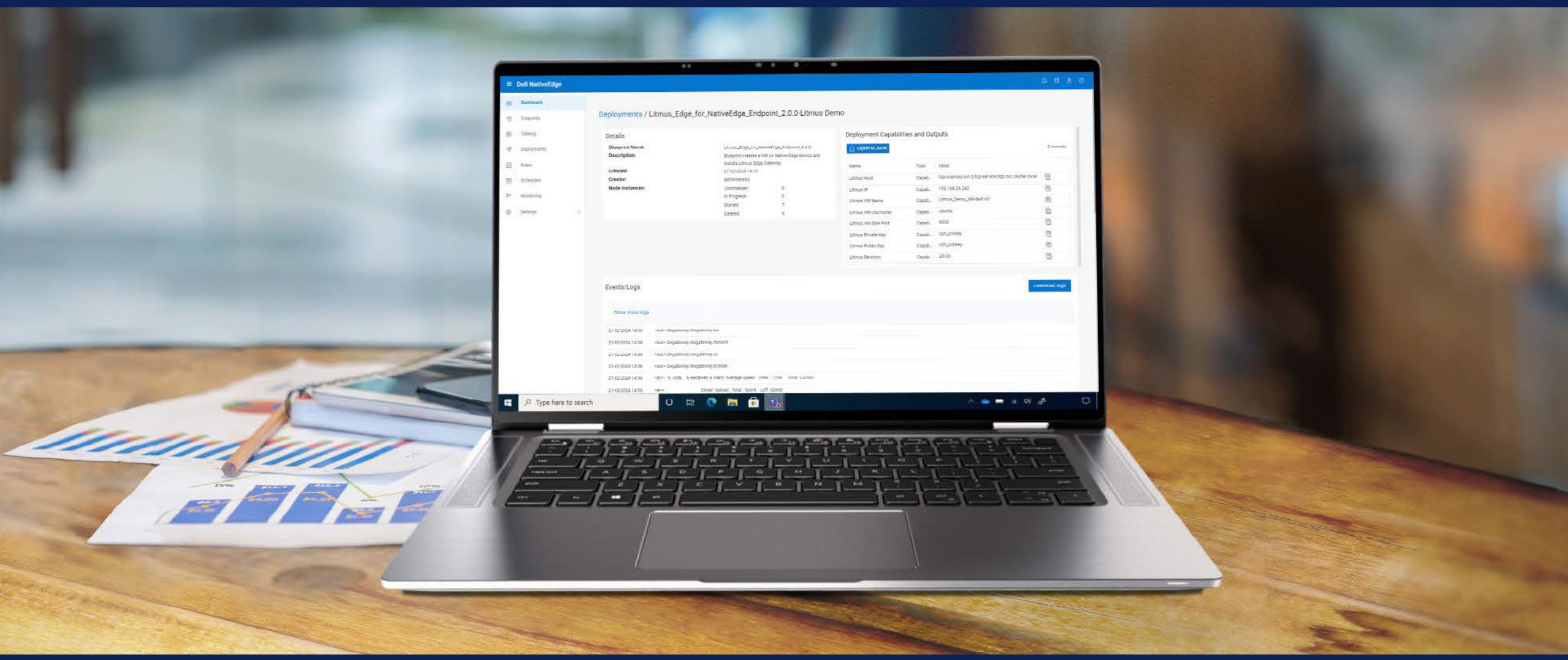
NativeEdge effectue en permanence des évaluations de sécurité alignées sur les normes de conformité définies en s'appuyant sur la télémétrie de l'environnement matériel et d'exploitation. Ces données sont utilisées pour détecter les écarts et les erreurs de configuration, ainsi que pour déterminer la nécessité de réaliser des mises à jour de sécurité.



Protégez l’ensemble de la périphérie

Dell NativeEdge protège votre parc en périphérie avec des principes de sécurité Zero-Trust, notamment l’intégration sécurisée des appareils basée sur la norme FIDO, associée à un système d’exploitation NativeEdge renforcé et sécurisé. Dell NativeEdge garantit que votre infrastructure, vos utilisateurs, votre réseau, vos applications et vos données sont attestés et validés en permanence sur tous les sites distribués.

Innovez où que vous soyez



DELL Technologies

Pour en savoir plus, rendez-vous sur **Dell.com/NativeEdge**