DELL Technologies

Zero-Trust
La transition vers une cybersécurité renforcée

Commencez votre transition vers une approche Zero-Trust avec un partenaire expérimenté en matière de technologies et de sécurité.

Les organisations qui font progresser leur maturité en matière de cybersécurité conçoivent une feuille de route exploitable. Elle leur permet d'identifier des moyens de réduire la surface d'attaque, de détecter et de répondre aux cybermenaces, et de mettre en œuvre diverses manières de récupérer après une cyberattaque, le tout avec des fonctionnalités d'adoption d'une approche Zero-Trust.

Pour faire face à des cybermenaces de plus en plus sophistiquées, Dell s'appuie sur les fonctionnalités de sécurité intégrées dans nos solutions ainsi que nos partenaires pour aider nos clients à atteindre une approche Zero-Trust qui s'aligne sur les objectifs métier de nos clients.

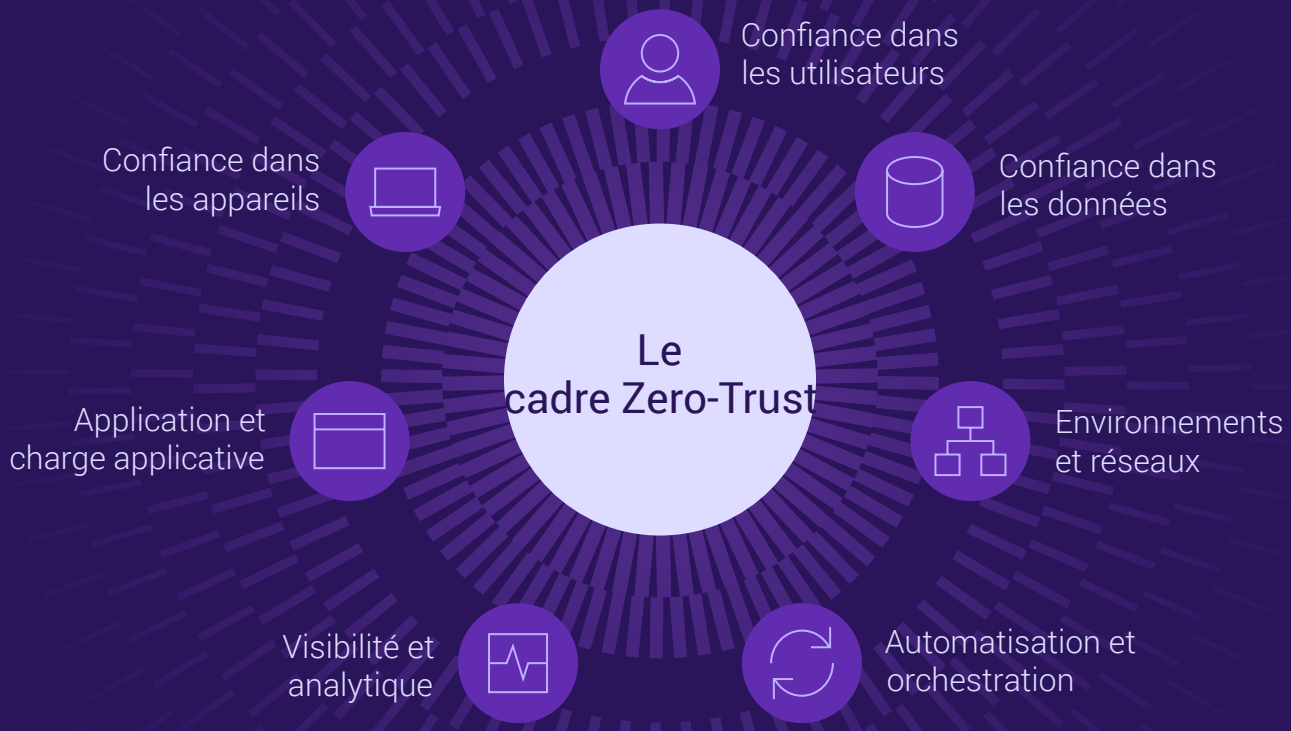
Qu’est-ce qu’une approche Zero-Trust ?

Imaginez que votre réseau soit un château. Une fois le pont-levis baissé, si quelqu’un entre, il peut se déplacer librement à l’intérieur. Il est temps de passer d’un modèle de sécurité de défense basé sur le périmètre vers un cadre Zero-Trust plus moderne et plus sécurisé.

Une stratégie Zero-Trust est une approche architecturale de la sécurité plutôt qu’un produit que vous achetez. Elle ne fait jamais confiance et vérifie toujours la légitimité d’une utilisation professionnelle avant d’accorder à quiconque ou à quoi que ce soit l’accès aux ressources.
Cela signifie que les utilisateurs et les appareils ne sont pas considérés comme fiables par défaut, même s’ils sont connectés à un réseau autorisé et même s’ils ont été préalablement vérifiés.

Ne jamais faire confiance, toujours vérifier.

Les principes fondamentaux d'un écosystème IT sécurisé.



Le cadre Zero-Trust, tel que défini par le NIST (National Institute of Standards and Technologies), a été adopté et intégré dans une architecture par le département de la Défense des États-Unis.

Il comprend sept piliers interdépendants qui orientent la prise de décision de Dell Technologies dans les différents domaines de sécurité. Une fois combinés, les piliers offrent une architecture intégrée multifacette pour une approche de sécurité complète qui protège les données de votre organisation et son infrastructure.

L'adoption d'une approche Zero-Trust s'est avérée difficile en raison de la complexité de l'intégration de diverses fonctionnalités de sécurité et du choix entre différentes options fragmentées parmi un certain nombre de fournisseurs de sécurité.

NIST

U.S. Department of Defense

DELL Technologies

Renforcez la maturité de votre approche Zero-Trust.

Quel que soit le niveau d'avancement de votre transition, Dell propose des solutions pour vous aider.

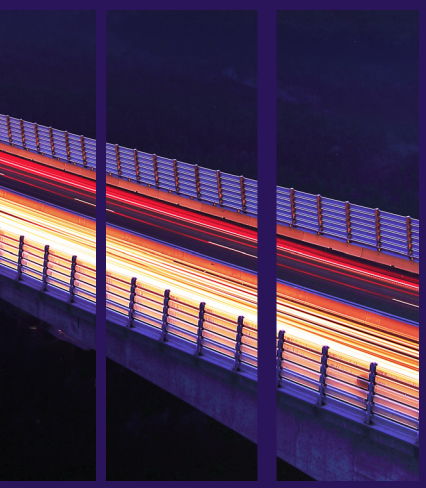
Dell Technologies offre le choix et la flexibilité à votre organisation. Si vous cherchez à faire progresser votre maturité en matière de cybersécurité, nous proposons des solutions de sécurité avec des fonctionnalités Zero-Trust afin d'améliorer votre capacité de renforcement, de détection, de défense et de restauration contre les cyberactivités malveillantes.

Activez les principes d'une approche Zero-Trust.

Favorisez la diversité des choix et la flexibilité pour faire progresser votre maturité en matière de cybersécurité.

Dell Technologies propose des solutions de sécurité avec des fonctionnalités Zero-Trust afin d'améliorer votre capacité de renforcement, de détection, de défense et de restauration contre les cyberactivités malveillantes. Et ce grâce aux éléments suivants :

- Des protections intégrées qui améliorent l'automatisation, l'intelligence sur les menaces, l'authentification, la visibilité et plus encore
- Des services permettant de développer une feuille de route, d'intégrer des technologies clés et des fonctionnalités de gestion proactive pour soutenir l'approche Zero-Trust
- Des services de conseils professionnels, managés et de sécurité
- Un vaste écosystème de partenaires



Simplifiez radicalement l'adoption d'une approche Zero-Trust.

Ne faites pas les choses à moitié et optez pour une architecture entièrement intégrée.

Une stratégie Zero-Trust est une approche architecturale de la sécurité, il ne s'agit pas d'un produit unique. Cela nécessite une synergie soigneusement planifiée entre les solutions. Dell allège le fardeau de l'intégration d'une approche Zero-Trust. Voici comment :

- Dell crée la première et unique architecture Zero-Trust entièrement intégrée conçue, testée et validée par le département de la Défense des États-Unis

DELL Technologies

Activez les principes d'une approche Zero-Trust.

Adoptez une approche Zero-Trust qui s'appuie sur votre écosystème de sécurité spécifique.

Dell contribue à faire progresser la maturité en matière de cybersécurité en favorisant les stratégies Zero-Trust, ce qui permet de réduire la surface d'attaque, d'améliorer la détection et d'accélérer la restauration face aux cybermenaces.

Chacun des piliers Zero-Trust illustrés se compose de technologies, de processus et de personnes alignés sur des domaines stratégiques où la sécurité et les politiques professionnelles sont nécessaires pour protéger votre organisation. Les services de sécurité Dell peuvent vous aider avec les éléments suivants :

- Maturité en matière de sécurité, approche Zero-Trust et évaluations des risques
- Développement d'une stratégie et d'une feuille de route
- Services managés de fonctionnalités Zero-Trust clés

DELL Technologies

Les bases d'une approche Zero-Trust.

Nous proposons des solutions de sécurité avancées et intégrées qui vous donnent un avantage dans votre démarche d'adoption d'une approche Zero-Trust.

Dell Data Protection

Coffre-fort Cyber Recovery | PowerProtect Data Manager | CyberSense Transparent Snapshots | CloudIQ | System Lockdown | Détection des écarts | Gestion sécurisée des clés d'entreprise | TLS 1.3 | IPv6 | Authentification multifacteur | Authentification unique | Accès basé sur les rôles | CloudIQ

Serveurs Dell PowerEdge

Nomenclature logicielle | Vérification sécurisée des composants | Racine de confiance au niveau de la puce | System Lockdown | Drift detection | Gestion sécurisée des clés d'entreprise | TLS 1.3 | IPv6 | Authentification multifacteur | Authentification unique | Accès basé sur les rôles | CloudIQ

Plateformes de stockage Dell

Isolement des données | Immuabilité des données | Détection des menaces | Authentification par contrôle d'accès | Chiffrement des données | Renforcement STIG | Racine de confiance matérielle | Secure Boot | Firmware signé numériquement | Accès basé sur les rôles | Snapshots sécurisés

Dell HCI/CI

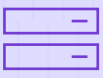
Racine de confiance matérielle | Chaîne de confiance Secure Boot | Mises à jour signées numériquement | Gestion des clés | Journalisation sécurisée | Commutateurs virtuels distribués | Isolement des machines virtuelles | Authentification et autorisation | Connecteurs d'écosystème | États validés en continu | Intégrité du code logiciel | Matrice de compatibilité électronique

PC professionnels Dell

Sécurité du BIOS/firmware | Sécurité matérielle | Assurance de la chaîne logistique | Logiciels de gestion des menaces (EDR, XDR, VDR) | Logiciels de protection des données réseau et Cloud

Solutions de périphérie Dell

Attestation matérielle, logicielle et des machines virtuelles | Intégration sécurisée | Chaîne de confiance | Livraison d'OS/d'applications | Gestion des droits numériques



Commutateurs réseau Dell

SmartFabric | CloudIQ | SD-WAN | Segmentation VLAN | Enterprise SONiC | Listes de contrôle d'accès | RADIUS | TACACS+ | Chiffrement | Renforcement des commutateurs | Microsegmentation | Routage et transfert virtuels

DELL Technologies

Notre approche accélérée.

Rapide et complet, Project Fort Zero intègre l'approche Zero-Trust dans l'ensemble de votre organisation.

Project Fort Zero offre une méthode validée pour immédiatement atteindre un niveau de maturité avancé en matière d'approche Zero-Trust, en réduisant le temps d'adoption, les interruptions et en gérant les coûts.

Forte de son expertise et de sa présence reconnue au sein du secteur, Dell Technologies a été sollicitée par le ministère de la Défense des États-Unis pour accélérer le taux d'adoption de l'approche Zero-Trust. Pour aider les organisations des secteurs privé et public à simplifier l'adoption et à faire évoluer l'architecture Zero-Trust à l'échelle mondiale, Dell crée un écosystème et dirige l'intégration de plus de 30 sociétés technologiques et de sécurité leaders sur le marché. Nous sommes à la pointe du développement et du déploiement à l'échelle mondiale de l'architecture Zero-Trust pour les organisations privées et publiques du monde entier. Cela témoigne de l'engagement de Dell envers les objectifs du département de la Défense des États-Unis pour atteindre une approche Zero-Trust.

Sur site

Dans les datacenters pour les organisations où la sécurité et la conformité des données sont primordiales.

À distance ou à l'échelle régionale

Dans des sites tels que les boutiques, où l'analyse sécurisée en temps réel des données clients peut offrir un avantage concurrentiel.

La périphérie amovible

Dans des lieux tels que les avions ou les véhicules avec une connectivité intermittente, où une implémentation temporaire est nécessaire pour assurer la continuité opérationnelle.

DELL Technologies

Nous vous aiderons à accélérer l'adoption d'une approche Zero-Trust en déployant les **152** activités énoncées par le département de la Défense des États-Unis pour une approche Zero-Trust d'un niveau avancé.

Outils d'exécution

Doctrine | Organisation | Formation | Ressources | Leadership et éducation | Personnel | Locaux | Politique

Niveau cible d'une approche Zero-Trust

Confiance dans les utilisateurs

- Inventaire des utilisateurs
- Autorisation basée sur les applications
- Accès dynamique basé sur les règles pt. 1
- Authentification multifacteur/fournisseur d'identités internes à l'organisation
- Implémentation du système et limitation des privilèges des utilisateurs pt. 1
- Gestion du cycle de vie des identités de l'organisation
- Stratégie de refus par défaut des utilisateurs
- Authentification unique
- Implémentation du système et limitation des privilèges des utilisateurs pt. 2
- Gestion du cycle de vie des identités de l'entreprise pt. 1
- Implémentation d'outils UEBA
- Authentification régulière
- Infrastructure à clé publique/fournisseur d'identités d'entreprise pt. 1

Confiance dans les appareils

- Analyse des lacunes de l'outil d'aide aux appareils
- Intégration d'outils d'antivirus de nouvelle génération avec C2C
- Appareils sous gestion de moteur de traitement réseau/infrastructure à clé publique sous gestion
- Stratégie de refus par défaut des appareils
- Implémentation d'UEDM ou d'outils équivalents
- Gestion des appareils d'entreprise pt. 1
- Implémentation d'outils de détection/réponse aux points de terminaison et intégration avec C2C
- Implémentation d'outils de gestion des ressources, des failles de sécurité et des correctifs
- Fournisseur d'identités d'entreprise pt. 1
- Implémentation de C2C/autorisation réseau basée sur la conformité pt. 1
- Implémentation du contrôle des applications et d'outils de surveillance de la conformité des fichiers
- Support BYOD et IOT géré et limité
- Gestion des appareils d'entreprise pt. 2
- Implémentation d'outils de détection étendue des menaces et intégration avec C2C pt. 1

Application et charge applicative

- Identification de l'application/du code
- Autorisation des ressources pt. 1
- Création d'usine logicielle DevSecOps pt. 1
- Fichiers binaires/code approuvés
- Programme de gestion des failles de sécurité pt. 1
- Autorisation de ressources SDC pt. 1
- Autorisation de ressources pt. 2
- Création d'usine logicielle DevSecOps pt. 2
- Automatisation de la sécurité des applications et des mesures correctives pour le code pt. 1
- Programme de gestion des failles de sécurité pt. 2
- Validation continue
- Autorisation des ressources SDC pt. 2

Confiance dans les données

- Analyse des données
- Journalisation et analyse des points d'application DLP
- Journalisation et analyse des points d'application DRM
- Définition des normes de balisage des données
- Implémentation d'outils de balisage et de classification des données
- Surveillance des activités liées aux fichiers pt. 1
- Implémentation de DRM et d'outils de protection pt. 1
- Mise en œuvre de points d'application
- Normes d'interopérabilité
- Développement d'une politique SDS
- Balisage manuel des données pt. 1
- Surveillance des activités liées aux fichiers pt. 2
- Implémentation de DRM et d'outils de protection pt. 2
- Application de DLP via des balises de données et l'analytique pt. 1
- Intégration de l'accès DAAS avec politique SDS pt. 1
- Application de DRM via des balises de données et l'analytique pt. 1
- Intégration de solution(s) SDS et de politiques avec fournisseur d'identités d'entreprise pt. 1

Environnements et réseaux

- Définition de règles d'accès au contrôle granulaire pt. 1
- Définition des API SDN
- Définition de règles d'accès au contrôle granulaire pt. 2
- Mise en œuvre d'une infrastructure programmable SDN
- Macrosegmentation des datacenters
- Mise en place d'une microsegmentation
- Intégration des segments dans la gestion des contrôles et les plans de données
- Macrosegmentation B/C/P/S
- Microsegmentation des applications et des appareils
- Protection des données en déplacement

Automatisation et orchestration

- Inventaire et développement des politiques
- Analyse de l'automatisation des tâches
- Analyse de l'automatisation des réponses
- Analyse de la conformité des outils
- Profil d'accès de l'organisation
- Implémentation d'outils SOAR
- Appels et schémas d'API standardisés pt. 1
- Enrichissement des workflows pt. 1
- Profil de sécurité d'entreprise pt. 1
- Intégration d'entreprise et provisionnement des workflows pt. 1
- Implémentation d'outils ML de balisage et de classification des données
- Appels et schémas d'API standardisés pt. 2
- Enrichissement des workflows pt. 2

Visibilité et analytique

- Considérations relatives à l'échelle
- Analyse des logs
- ID d'actif et corrélation des alertes
- Alerte sur les menaces pt. 1
- Implémentation d'outils d'analytique
- Programme d'intelligence sur les cybermenaces pt. 1
- Analyse du journal
- Alerte sur les menaces pt. 2
- Référentiels utilisateurs/appareils
- Définition du référentiel de comportement de l'utilisateur
- Référentiel et profilage pt. 1
- Programme d'intelligence sur les cybermenaces pt. 2

Total des activités cibles : 91

Source : Publication DoD Zero Trust Strategy, 7 novembre 2022

DELL Technologies

Approche Zero-Trust avancée

Confiance dans les utilisateurs

- Accès dynamique basé sur des règles pt. 2
- Rôles et autorisations d'entreprise pt. 1
- Autre authentification multifacteur flexible pt. 1
- Approbations en temps réel d'analytique JIT/JEA pt. 1
- Gestion du cycle de vie des identités d'entreprise pt. 2
- Surveillance de l'activité des utilisateurs pt. 1
- Authentification continue pt. 1
- Authentification continue pt. 2
- Infrastructure à clé publique/fournisseur d'identités d'entreprise pt. 3
- Rôles et autorisations d'entreprise pt. 2
- Autre authentification multifacteur flexible pt. 2
- Approbations en temps réel et analytique JIT/JEA pt. 2
- Gestion du cycle de vie des identités d'entreprise pt. 3
- Surveillance de l'activité des utilisateurs pt. 2
- Infrastructure à clé publique/fournisseur d'identités d'entreprise pt. 2

Confiance dans les appareils

- Fournisseur d'identités d'entreprise pt. 2
- Implémentation de C2C/autorisation réseau basée sur la conformité pt. 2
- Surveillance des activités de l'entité pt. 1
- Intégration complète de sécurité des appareils Slack avec C2C
- Infrastructure à clé publique d'entreprise pt. 1
- Support BYOD et IOT géré et complet pt. 1
- Implémentation d'outils de détection étendue des menaces et intégration avec C2C pt. 2
- Surveillance des activités de l'entité pt. 2
- Infrastructure à clé publique d'entreprise pt. 2
- Support BYOD et IOT géré et complet pt. 2

Application et charge applicative

- Enrichissement d'attributs pour l'autorisation des ressources pt. 1
- Enrichissement d'attributs pour l'autorisation des ressources pt. 2
- Autorisation de fonctionnement continu (ATO) pt. 1
- Automatisation de la sécurité des applications et des mesures correctives pour le code pt. 2
- Microsegmentation de l'API REST
- Autorisation de fonctionnement continu (ATO) pt. 2

Confiance dans les données

- Balisage manuel des données pt. 2
- Surveillance des activités liées aux bases de données
- Balisage et support des données automatisés pt. 1
- Application de DRM via des balises de données et l'analytique pt. 2
- Application de DLP via des balises de données et l'analytique pt. 2
- Intégration de l'accès DAAS avec politique SDS pt. 2
- Intégration de solution(s) SDS et de politiques avec fournisseur d'identités d'entreprise pt. 2
- Intégration d'outil SOS et/ou intégration avec outil DRM pt. 1
- Balisage et support des données automatisés pt. 2
- Surveillance complète des activités liées aux données
- Application de DRM via des balises de données et l'analytique pt. 3
- Application de DLP via des balises de données et l'analytique pt. 3
- Intégration de l'accès DAAS avec politique SDS pt. 3
- Intégration d'outil SDS et/ou intégration avec outil DRM pt. 2

Environnements et réseaux

- Découverte et optimisation des ressources réseaux
- Décisions d'accès en temps réel
- Microsegmentation des processus

Automatisation et orchestration

- Profil de sécurité d'entreprise pt. 2
- Intégration d'entreprise et provisionnement des workflows pt. 2
- Implémentation d'outil d'automatisation par IA
- Enrichissement des workflows pt. 3
- Modifications A&O déterminées par l'IA qui se base sur l'analytique
- Implémentation de playbooks
- Workflows automatisés

Visibilité et analytique

- Alerte sur les menaces pt. 3
- Référentiel et profilage pt. 2
- Support référentiel UEBA pt. 1
- Support référentiel UEBA pt. 2
- Accès réseau optimisé par l'IA
- Contrôle d'accès dynamique optimisé par l'IA

Total des activités avancées : 61

Dell Technologies peut simplifier la réalisation rapide des objectifs en matière de maturité d'une approche Zero-Trust.

Source : Publication DoD Zero Trust Strategy, 7 novembre 2022

DELL Technologies

Répondre aux besoins de toutes les organisations.

Renforcez la maturité de votre approche Zero-Trust.

Zero-Trust est un cadre défini et un ensemble de principes qui guident l'approche de la sécurité. Sa mise en œuvre peut s'appuyer sur diverses fonctionnalités. Que vous vous lanciez corps et âme dans l'adoption d'une approche Zero-Trust ou que vous visiez des améliorations ciblées, en respectant les principes Zero-Trust, Dell est un partenaire de sécurité expérimenté qui vous aidera à faire progresser votre transition vers la sécurité.

Industrie chimique	Technologies de l'information	Communications	Intervenants des services d'urgence
Alimentation & Agriculture	Défense	Services de santé et santé publique	Fabrication
Finances	Réacteurs nucléaires	Professionnel	Secteur public
Énergie	Transport	Eau et eaux usées	Barrages

DELL Technologies

DELL Technologies

Un partenaire technologique et de sécurité expérimenté pour le processus de transition vers une approche Zero-Trust de votre organisation.

Renforcez la cybersécurité à long terme avec la mise en œuvre d'une approche Zero-Trust.

Les services de sécurité Dell proposent :

Une évaluation par des experts de la maturité en matière de sécurité et de risque global.

Le développement d'une feuille de route Zero-Trust.

Une gestion continue des activités de sécurité.

DELL Technologies

Dell.com/SecuritySolutions

Demander que l'on vous rappelle

Chatter avec un conseiller en sécurité

Appelez le 1-800-433-2393