DELL Technologies

intel®

Cyber-résilience

Luttez contre les menaces avec une posture de sécurité rigoureuse qui commence par les serveurs Dell PowerEdge, avec les processeurs Intel® Xeon® Scalable.

Commencer

Sommaire

Cliquez sur les icônes ou les titres de chapitre ci-dessous pour accéder aux sections spécifiques. Utilisez les boutons fléchés en haut pour naviguer page par page. Utilisez le bouton Accueil dans le coin supérieur gauche pour revenir au début.

Partie 1 : Le paysage de la cybersécurité

Évolution des menaces

Les cybermenaces et les attaques deviennent de plus en plus néfastes et répandues, et les prévisions annoncent une accélération. En 2020, Cybersecurity Ventures estimait que les coûts de la cybercriminalité mondiale devraient augmenter de 15 % par an au cours des cinq prochaines années, pour atteindre 10 500 milliards de dollars par an en 2025, contre 3 000 milliards en 2015.[1] Les données étant accessibles sur l'ensemble des appareils, sur site et dans le Cloud, les violations de données à fort impact continuent de se multiplier. Pour maintenir un environnement plus sécurisé, les entreprises doivent adopter une approche plus complète.

La transformation numérique a été le mot d'ordre des années 2000 et n'a fait que s'accélérer dans les années 2020, les organisations se démenant pour s'adapter à des environnements nouveaux et en pleine mutation. Avec l'adoption croissante du datacenter software-defined (SDDC), les organisations sont devenues plus dépendantes des serveurs comme la base des fonctions métiers. Cela signifie que la sécurité des serveurs doit être essentielle à votre stratégie globale de défense d'entreprise, en protégeant contre les menaces jusqu'à la couche du firmware.

Les attaques par ransomware devraient coûter

265 milliards de dollars à l'échelle mondiale d'ici 2031. [3]

Défis en matière de cybersécurité

Les cybermenaces arrivent de partout. Si les acteurs traditionnels incluent les hacktivistes, les groupes terroristes, les États-nations hostiles, les organisations criminelles, les hackers solitaires et les espions d'entreprise, vous devez également vous méfier des menaces venant de l'intérieur.

Les reportages d'aujourd'hui se concentrent sur la rapidité, la sophistication, l'efficacité et l'impact financier accrus des cyberattaques. En 2021, par exemple, on enregistre 50 % de cyberattaques en plus perpétrées par semaine dans les réseaux d'entreprise par rapport à 2020.[2] Et bien que les ransomware aient coûté 20 milliards de dollars à l'échelle mondiale en 2021, ce chiffre devrait atteindre 265 milliards de dollars d'ici 2031.[3]

[1] CyberCrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 13 novembre 2020

[2] DARKReading, Businesses Suffered 50% More Cyberattack Attempts per Week in 2021, 11 janvier 2022.

[3] Cloudwards, Ransomware Statistics, Trends, and Facts for 2022 and Beyond, 22 mars 2022.

Attaques courantes :

Programmes malveillants : ils englobent tous les types de logiciels malveillants, tels que les logiciels espions, les logiciels publicitaires ou les virus, qui nuisent aux performances ou à la sécurité de votre serveur.

Ransomware : les ransomware sont une forme de logiciels malveillants qui, lorsqu'ils sont téléchargés sur un serveur, peuvent bloquer l'accès aux données et aux fichiers sur l'appareil jusqu'à ce qu'une rançon soit payée.

Attaques par hameçonnage : l'hameçonnage consiste à contacter frauduleusement plusieurs personnes ou sociétés pour tenter d'obtenir un accès non autorisé à des informations sensibles et/ou personnelles.

Chaîne logistique : les pirates cherchent de plus en plus à exploiter les faiblesses de la chaîne logistique ou des fournisseurs tiers à mesure que des organisations comme la vôtre améliorent la sécurité. En 2020, la cyberattaque de SolarWinds, une grande société de gestion IT, est passée inaperçue pendant des mois, et a donc infecté ses clients avec un code malveillant. Selon Accenture, « 40 % des cyberattaques visent la chaîne logistique ».[4]

40%
des cyberattaques visent la chaîne logistique.[4]

[4] Accenture, Securing the Supply Chain, 2020

Conformité et pression réglementaire

Devant l'augmentation des menaces mondiales, la pression réglementaire continue de s'accentuer pour définir des recommandations de bonnes pratiques visant à sécuriser les infrastructures gouvernementales et stratégiques, mais aussi le secteur privé. C'est important, car aux États-Unis, près de 90 % des infrastructures stratégiques, telles que les services de santé, l'énergie, les finances, les transports, les télécommunications et les services publics, sont détenus par le secteur privé.[5]

En mai 2021 et en janvier 2022, les États-Unis ont publié des décrets qui définissent un cadre de protection de l'infrastructure du pays et fournissent des directives détaillées sur l'architecture Zero-Trust. Les États-Unis ne sont pas les seuls à avoir la volonté d'agir. Les gouvernements internationaux élaborent des directives réglementaires en réponse aux cybermenaces, et les institutions privées créent des politiques et des mandats pour limiter les menaces persistantes avancées. Ces exigences ne se limitent pas aux agences fédérales, mais s'étendent également aux infrastructures stratégiques et à d'autres marchés verticaux.

Si les gouvernements cherchent à juguler ou limiter les cyberattaques, les organisations doivent également se préparer à davantage de directives et de mandats, tels que :

- **Authentification à plusieurs facteurs (MFA) :** l'authentification à plusieurs facteurs, également appelée authentification à deux facteurs (2FA)[6], protège les données contre l'accès par un tiers non autorisé. Cette technologie de sécurité exige qu'un utilisateur soit vérifié pour obtenir l'accès en utilisant au moins deux informations d'identification indépendantes. Les secteurs d'activité comme « la finance, la santé, la défense, les forces de l'ordre et le gouvernement fédéral demandent déjà une authentification à deux facteurs pour accéder aux systèmes, réseaux, sites Web et emplacements physiques. »[7]
- **Chiffrement des données au repos** : il s'agit de disques à autochiffrement avec une gestion des clés de niveau entreprise.

[5] The White House, Press Briefing: Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure, 28 juillet 2021.
[6] NIST, Back to Basics: What's multi-factor authentication - and why should I care?, 16 juin 2016.
[7] Okta, Which Industries Require Two-Factor Authentication?, consulté en juin 2022.

Quels sont les enjeux ?

Les cyberattaques peuvent être catastrophiques pour une organisation. En fonction de l'ampleur de l'attaque et des dommages causés, le délai de reprise peut être considérable. La reprise après une attaque par ransomware prend en moyenne 22 jours.[8] Voici certains défis que les organisations peuvent rencontrer :

- Interruption de service pour tenter de découvrir ce qui s'est passé, puis pour récupérer toutes les données perdues
- Perte permanente de données internes et client, ce qui compromet les prospects à long terme
- Paiement d'amendes et de réaménagements pour s'assurer de respecter toutes les règles et réglementations
- Mauvaise publicité et perte d'activité immédiatement après une cyberattaque
- Perte de réputation à long terme, car les clients hésitent à poursuivre leurs relations avec des entreprises qui ont été attaquées

La reprise après une attaque par ransomware prend en moyenne

22 jours [8]

Certaines organisations se concentrent tellement sur leur croissance qu'elles en arrivent à négliger les dispositions de sécurité appropriées pour protéger et soutenir leur activité. Pourtant, une faille peut rapidement altérer la capacité de votre organisation à bien fonctionner. Si l'on ajoute à cela le fait que l'infrastructure, les charges applicatives et l'utilisation des données deviennent de plus en plus complexes, le maintien d'une infrastructure et d'opérations IT sécurisées gagne considérablement en complexité.

Bien que la transformation numérique crée des opportunités illimitées, cela reste difficile de créer un environnement IT agile et moderne tout en préservant la confiance de vos clients et parties prenantes. Si vous ne parvenez pas à anticiper la hausse des menaces de sécurité, les dommages pourraient être catastrophiques. Il faut savoir que 64 % des Américains reprocheraient à une entreprise, plutôt qu'au pirate, la perte de leurs données personnelles à la suite d'une attaque.[9] En outre, 84 % des consommateurs ont confirmé qu'ils sont plus fidèles aux entreprises qu'ils perçoivent comme ayant des contrôles de sécurité solides.[10]

84 %

des consommateurs ont confirmé qu'ils sont plus fidèles aux entreprises qu'ils perçoivent comme ayant des contrôles de sécurité solides.[9]

[8] Statista, Length of impact after a ransomware attack Q1 2020- Q3 2021, novembre 2021.

[9] Forbes, 50 Stats Showing Why Companies Need To Prioritize Consumer Privacy, 22 juin 2020.

[10] SalesForce Research Report, State of the Connected Customer: Third Edition, juin 2019.

Ressources

Infographie sur l'architecture cyber-résiliente

Vidéo sur l'architecture cyber-résiliente

Document technique sur la sécurité cyber-résiliente dans les serveurs Dell PowerEdge

Partie 2 : Pratiques d'excellence du secteur

Zero-Trust

est une approche architecturale composée d'un cadre de principes de sécurité et de pratiques d'excellence.

Zero-Trust est une réponse à la complexité des environnements IT modernes, comptant notamment le Cloud et le Cloud hybride, des ressources basées sur le Cloud qui ne se trouvent pas dans les limites du réseau de votre organisation. Au problème de la complexité viennent également s'ajouter l'augmentation récente du nombre d'utilisateurs distants, les millions d'appareils BYOD et d'autres réglementations gouvernementales.

Zero-Trust n'est pas une architecture unique, mais un ensemble de principes directeurs pour le workflow, la conception du système et les opérations. Les approches de sécurité efficaces sont passées d'un ensemble de périmètres statique et à granularité large à quelque chose de beaucoup plus fluide, où aucune confiance n'est accordée aux ressources ou aux comptes utilisateur sur la seule base de leur emplacement physique ou réseau ou de leur propriété.

En d'autres termes, une approche Zero-Trust évalue et valide de nombreux points dans l'environnement IT avant d'accorder des autorisations. L'élément essentiel de Zero-Trust est la vérification des ressources au sein de l'entreprise avant de fournir l'accès, ainsi que la vérification continue avant l'exécution du processus ou le déplacement latéral au sein du réseau.

La pression réglementaire a pris une ampleur considérable depuis que les attaques par ransomware ont frappé des entités fédérales, l'infrastructure stratégique et le secteur privé. Le décret de la Maison-Blanche publié le 12 mai 2021 en témoigne. Depuis, une documentation fournie a été créée pour définir les détails de l'implémentation de la sécurité et des nouvelles réglementations. Face à l'évolution des directives réglementaires, les organisations réalisent que les solutions de sécurité sont devenues impératives, et non plus facultatives. Les exigences Zero-Trust, qui ont commencé avec la publication spéciale SP800-207 avec le ministère de la Défense américain, ont continué d'être définies conjointement avec le décret de la Maison-Blanche et en coopération avec la CISA et l'OMB (Bureau de la gestion et du budget). Nous constatons que les gouvernements internationaux suivent le mouvement avec des exigences plus strictes.[11]

Ressources

Infographie sur l'architecture Zero-Trust

[11] NIST, Zero Trust Architecture, 10 août 2020.

Partie 3 : Commencer par un socle sécurisé

La philosophie de Dell en matière de sécurité repose sur notre cyber-résilience.

Pour développer une cyber-résilience efficace, vous devez commencer par protéger votre organisation contre les acteurs malveillants tout au long du cycle de vie de l'équipement. Conformément au cadre de cybersécurité NIST, Dell utilise une approche du cycle de vie de développement de la sécurité (SDL) (NIST SP800-160) pour créer des produits et des solutions qui englobent les besoins de sécurité de la conception, la fabrication, la chaîne logistique et la gestion jusqu'à la mise hors service.

- Le firmware du serveur est conçu pour bloquer, empêcher et contrer l'injection de code malveillant pendant toutes les phases du cycle de vie de développement du produit.
- Des pratiques de codage sécurisées sont appliquées à chaque étape du développement du firmware.
- Une modélisation des menaces et des tests d'intrusion ont lieu pendant le processus de conception.

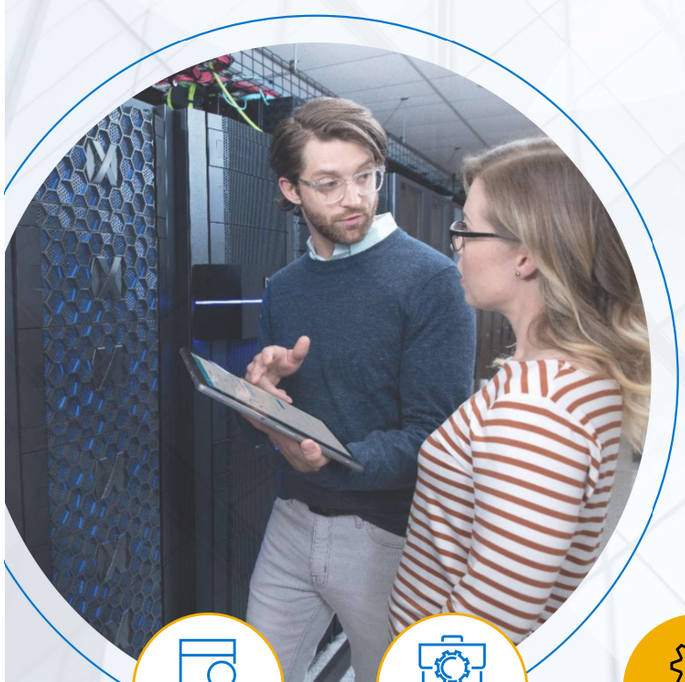
La protection de vos données et de votre propriété intellectuelle nécessite une approche en couches. Dans les serveurs Dell PowerEdge, les fonctions de sécurité sont conçues avec des couches qui se chevauchent de manière intentionnelle. Ainsi, si un mécanisme est compromis, une autre couche est présente pour déjouer l'attaque. Cette approche de « défense en profondeur » améliore la résilience et constitue le cœur de notre architecture cyber-résiliente.

Les serveurs PowerEdge sont dotés de processeurs Intel Xeon Scalable qui offrent des fonctionnalités de sécurité avancées, notamment Intel SGX, qui permet de protéger les données et le code d'application en temps réel, de la périphérie au datacenter et au Cloud public multiclient. Cela permet une collaboration améliorée (par exemple, pour l'apprentissage fédéré dans l'IA) à l'aide de données partagées, sans compromettre la confidentialité. Intel Crypto Acceleration augmente les performances des charges applicatives très exigeantes en chiffrement, notamment les services Web SSL, l'infrastructure 5G et les VPN/pare-feu, et réduit l'impact du chiffrement omniprésent sur les performances.

Cette architecture s'appuie sur un héritage de sécurité PowerEdge avec des fonctionnalités améliorées qui protègent efficacement votre infrastructure en détectant les menaces de manière fiable et en procédant à une récupération rapide en cas de cyberattaque. Il s'agit d'une approche qui s'aligne sur les composants clés du cadre NIST (NIST SP 800-193).

Silicon Root of Trust

Les serveurs PowerEdge utilisent une racine de confiance immuable en silicium pour attester de manière cryptographique de l'intégrité du BIOS et du firmware iDRAC (Integrated Dell Remote Access Controller). Cette racine de confiance est fondée sur des clés publiques programmables, en lecture seule et à usage unique, qui protègent contre le piratage par logiciel malveillant. L'un des aspects les plus critiques de la sécurité des serveurs consiste à garantir que le processus de démarrage puisse être vérifié comme étant sécurisé. Elle fournit un ancrage de confiance pour les opérations de démarrage. En complément de cela, le processus de démarrage du BIOS s'appuie sur la technologie Intel Boot Guard, qui vérifie que la signature numérique du hachage cryptographique de l'image de démarrage correspond à la signature stockée dans le silicium par Dell Technologies en usine.



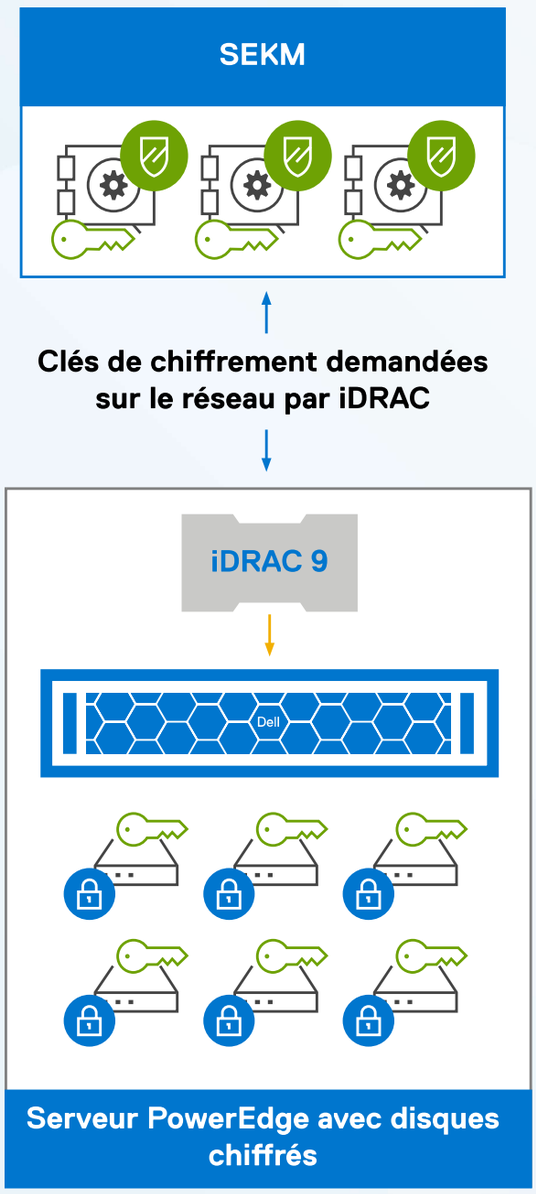
Gestion des accès et des identités

La gestion des accès et des identités (IAM) est un domaine critique, en particulier pour la protection contre les attaques par ransomware, avec des contrôles tels que l'authentification à plusieurs facteurs pour activer le moindre privilège et une approche de la sécurité Zero-Trust. Elle est conçue pour s'assurer que seules les personnes autorisées peuvent accéder aux ressources et données IT appropriées et contrôler le périmètre d'accès.

Protection avancée des données

La protection des données consiste à protéger vos données d'entreprise, qu'elles soient utilisées, en transit ou au repos, généralement via le chiffrement. Les serveurs PowerEdge offrent un large éventail d'options de stockage sécurisé pour vos données.

La gestion des clés externe est une bonne pratique qui consiste à stocker les clés ailleurs que sur les disques et le serveur d'hébergement. Le gestionnaire des clés d'entreprise sécurisées (SEKM) permet aux clients PowerEdge de gérer les clés de manière centralisée pour les disques SED dans les serveurs PowerEdge et évolue au rythme de l'extension de la capacité de stockage. La gestion des clés locale (LKM) est également disponible pour les environnements où l'accès central peut être difficile ou lorsque les exigences de sécurité sont moins strictes.



Exemple d'implémentation SEKM

Ressources

Infographie sur la protection des données

Page Web de SEKM

Vidéo sur SEKM

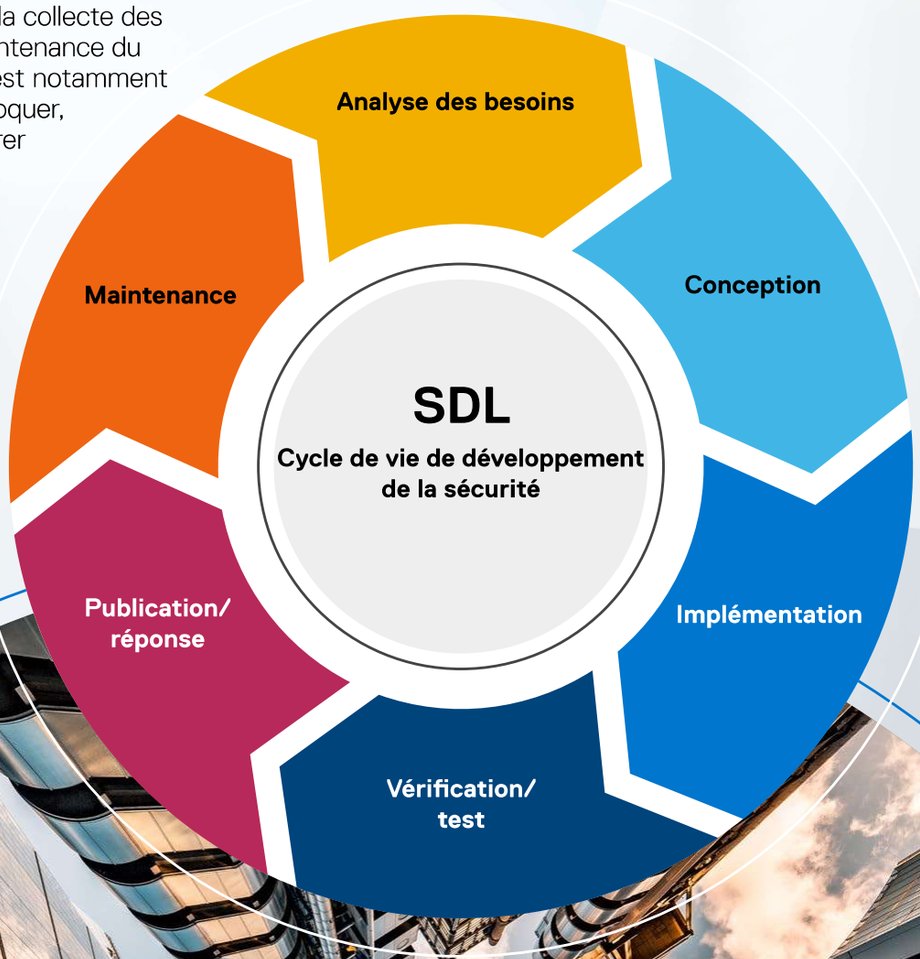
Document technique Enable OpenManage Secure Enterprise Key Manager (SEKM) on Dell PowerEdge Servers

Infographie sur SEKM

Vidéo sur l'architecture cyber-résiliente

Cycle de vie de développement de la sécurité Dell

Dell Technologies crée délibérément un code de contrôle de sécurité pour chaque phase du cycle de vie du serveur, de la collecte des exigences à la maintenance du serveur. Ce code est notamment développé pour bloquer, empêcher et contrer l'injection.



Assurance de la chaîne logistique vérifiée

L'approche complète par Dell Technologies de l'assurance de la chaîne logistique inclut des dispositions fondamentales, comme un personnel physique et des contrôles de cybersécurité. Dell Technologies améliore également l'assurance de l'intégrité des composants avec son offre Secured Component Verification (SCV). SCV permet aux clients de vérifier de manière cryptographique que les composants définis en usine correspondent à ce qui leur a été fourni.

Sécurité fournit la confidentialité, l'intégrité et la disponibilité des informations qui décrivent la chaîne logistique IT, ou traversent la chaîne logistique IT, ainsi que des informations sur les parties impliquées dans la chaîne logistique IT.

Intégrité s'assure que les produits ou services IT de la chaîne logistique IT sont authentiques et inchangés et qu'ils fonctionneront conformément aux spécifications de l'acquéreur et sans fonctionnalités supplémentaires indésirables.

Qualité réduit les vulnérabilités susceptibles de limiter la fonction prévue d'un composant, d'entraîner un échec de composant ou de fournir des opportunités d'exploitation.

Résilience s'assure que la chaîne logistique IT fournira les produits et services IT requis malgré les interruptions.

Ressources

Vidéo sur Secured Component Verification

Note technique de Secured Component Verification

Tech Talk Secured Component Verification

Document technique de la chaîne logistique sur l'évaluation de la sécurité de Secured Component Verification (NCC Group)

Avantages des produits cyber-résilients

- Temps d'activité maximal pour la productivité du personnel
- Préservation de la réputation de l'entreprise
- Confiance des clients
- Conformité pour éviter les amendes et les réaménagements coûteux
- Liberté d'innover sans distraction

Partie 4 : Utiliser la cyber-résilience pour répondre aux exigences Zero-Trust

L'approche Zero-Trust de Dell Technologies a été affinée pour s'aligner sur les normes du ministère américain de la Défense (DoD). Nous mettons en place une architecture Zero-Trust grâce à des fonctionnalités cyber-résilientes étendues et une approche à sept piliers qui permet aux utilisateurs d'effectuer des vérifications à chaque point de l'environnement IT avant que les autorisations ne soient accordées.

Pilier 1 : Confiance dans l'appareil

Notre racine de confiance matérielle en silicium offre un niveau de sécurité tout au long du cycle de vie du serveur, de la conception à la mise hors service. Notre chaîne logistique sécurisée comprend plusieurs couches de contrôle, telles que la vérification des composants, afin de garantir que nos serveurs et logiciels n'ont pas été altérés ou modifiés de manière malveillante. SCV contient des certificats d'inventaire signés de manière chiffrée sur l'ensemble de la gamme de serveurs PowerEdge, y compris l'auto-vérification sécurisée, pour vous assurer une tranquillité d'esprit quant à l'intégrité de votre matériel lors du transfert vers votre datacenter.

Pilier 2 : Confiance dans l'utilisateur

Avec iDRAC, les administrateurs IT peuvent déployer, mettre à jour et surveiller en toute sécurité les serveurs PowerEdge en local ou à distance. Pour renforcer la sécurité, iDRAC permet l'authentification à plusieurs facteurs à l'aide de RSA SecureID, ainsi que des intégrations via Active Directory, l'intégration LDAP avec authentification unique (SSO) et un contrôle d'accès et un audit basés sur les rôles.

Pilier 3 : Confiance dans le transport et la session

Le BMC de PowerEdge (iDRAC) dispose d'un module réseau dédié, et les options Secure Shell (SSH) / TLS (Transport Layer Security) permettent de chiffrer et d'authentifier les données qui transitent entre vos serveurs et le navigateur exécutant votre interface utilisateur Web iDRAC. L'iDRAC permet la gestion à distance et surveille le système pour détecter les événements critiques à l'aide de capteurs situés sur la carte système. Des alertes et des événements de log sont envoyés lorsque les paramètres dépassent leurs seuils actuels.

Pilier 4 : Confiance dans les logiciels

Nous effectuons des tests proactifs de vérification, de validation et de sécurité tout au long du cycle de vie des logiciels pour protéger nos logiciels et réduire le risque d'insertion de failles de sécurité liées aux logiciels malveillants ou au codage. Le démarrage vérifié de bout en bout inclut des images signées du BIOS et du firmware, qui garantissent qu'aucun code non autorisé ne s'exécute sur un serveur PowerEdge. D'autres fonctionnalités cyber-résilientes incluent la détection automatisée des dérives, les fonctionnalités de démarrage UEFI sécurisées et la récupération pour le BIOS et les systèmes d'exploitation.

Pilier 5 : Confiance dans les données

SEKM fonctionne conjointement avec des disques à autochiffrement pour le chiffrement matériel, ainsi qu'une gestion des clés centralisée et évolutive pour vous aider à déployer et surveiller les clés de chiffrement, y compris les sites distants et même dans le Cloud. Cela assure une protection contre tout accès non autorisé à des disques ou systèmes perdus ou volés. Ce chiffrement matériel peut être associé au chiffrement logiciel tel que le chiffrement VMware® vSAN™ sur VxRail.

Le calcul confidentiel assure la protection des données en cours d'utilisation au niveau du processeur et de la mémoire, et inclut les technologies Intel (SGX, TME). Intel SGX offre une isolation au niveau des applications ou des fonctions afin de minimiser le périmètre de confiance.

Le fait de combiner le chiffrement des données au repos, la gestion évolutive des clés et le calcul confidentiel peut fournir les niveaux de protection nécessaires pour faire face aux menaces en constante évolution d'aujourd'hui.

Pilier 6 : Visibilité et analytique

La capacité à observer ce qui se passe dans votre environnement est essentielle. La détection des dérives du firmware, par exemple, fournit des informations en temps réel sur l'état d'intégrité du firmware, notamment sur les modifications non autorisées. Si des modifications sont détectées, le système peut être restauré à un état sécurisé connu. En outre, les événements de modification peuvent être suivis via la journalisation automatisée et les alertes, ce qui facilitera l'audit et l'analyse pour évaluer l'intégrité globale du système.

Pilier 7 : Automatisation et orchestration

OpenManage Enterprise est une application de gestion et de surveillance des systèmes qui fournit une vue complète des serveurs PowerEdge, du stockage interne et d'autres composants. Elle inclut la détection des dérives pour rechercher les modifications d'un modèle de configuration défini par l'utilisateur, crée des alertes et des logs pour suivre l'état du système et permet de corriger les erreurs de configuration en fonction des règles de préconfiguration. OpenManage englobe la restauration du firmware, des mises à jour centralisées, le renouvellement automatique des certificats SSL (Secure Sockets Layer) et des déploiements automatisés pour une configuration de sécurité cohérente.

Ressources

Présentation du gestionnaire de clés d'entreprise OpenManage Secure

Modèles de base Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing

Infographie sur l'architecture Zero-Trust

Vidéo sur Zero-Trust

Partie 5 : Assurer la réussite de votre société avec Dell Technologies et Intel

La hausse de la sophistication des menaces et l'extension de la surface d'attaque exigent une approche modernisée de la cyber-résilience. Notre réponse consiste à vous accompagner dans la création d'une architecture Zero-Trust avec une gamme d'outils et de technologies. Notre approche de la sécurité permet des contrôles plus granulaires, en commençant par l'accès et l'autorisation, jusqu'à la résilience des données et des systèmes, tout en offrant une expérience utilisateur supérieure.

En choisissant Dell Technologies et Intel comme partenaires, vous bénéficierez des avantages suivants :

- Une cyber-résilience éprouvée où la sécurité est intégrée dès la conception
- Une simplicité accrue pour concilier vos objectifs métiers et votre productivité avec la sécurité et la confidentialité
- Une suite matérielle et logicielle conçue pour protéger votre infrastructure IT tout en vous offrant la confiance, le contrôle et l'évolutivité nécessaires à votre posture de sécurité
- Une vigilance continue pour maintenir une posture de sécurité rigoureuse à l'aide d'une réponse rapide aux failles de sécurité et attaques courantes

Ressources

Page Web Solutions de sécurité

Services de résilience métier

Détection et réponse managées

Pour en savoir plus sur les serveurs PowerEdge cyber-résilients, rendez-vous sur Dell.com/Servers.

Abonnez-vous à notre podcast Power2Protect de Dell Technologies pour écouter les derniers épisodes sur la sécurité et la cyber-résilience.

DELL Technologies

intel