DELL Technologies

AMD
together we advance_

Livre blanc

Sécurisation de la frontière numérique : découvrez l'approche Zero-Trust de Dell et AMD

Protégez votre organisation à l'aide de la sécurité de bout en bout de Dell et AMD

Sommaire

Introduction

Les appareils nous servant à nous connecter offrent de nombreuses possibilités, mais ces connexions constituent également des points de vulnérabilité supplémentaires susceptibles d'être exploités par des acteurs malveillants. D'après certaines estimations, les cyberattaques coûteront aux organisations jusqu'à 10 500 milliards de dollars d'ici 2025[1]. En outre, selon une estimation, la reprise de l'activité après une cyberattaque prend environ 277 jours[2].

Si les nouvelles technologies, telles que l'intelligence artificielle (IA), améliorent la productivité et les opérations métier pour de nombreuses organisations, elles rendent également les données vulnérables aux cyberattaques plus sophistiquées. À chaque avancée technologique, les leaders du secteur des technologies doivent modifier leurs stratégies pour lutter efficacement contre les nouveaux moyens utilisés par les cybercriminels pour accéder aux données et les exploiter. Pour contrer ces menaces et assurer la sécurité des données, vous avez besoin d'une protection intégrée pour chaque composant du datacenter, depuis les serveurs et le stockage jusqu'aux réseaux, en passant par les logiciels et les firmwares. La protection commence par la réduction des attaques au niveau de la chaîne logistique sur le site de fabrication, et se poursuit tout au long du processus de transport, jusqu'à l'utilisation par le client. Mais les attaques ne se limitent pas au datacenter. Les organisations présentes dans le Cloud sont confrontées à des défis supplémentaires en matière de sécurité des données.

Ensemble, Dell et AMD fournissent une architecture cyberrésiliente spécialement conçue pour aider les organisations à adopter une stratégie Zero-Trust, qui repose sur l'idée que les composants système sont vulnérables tout au long de la chaîne et qu'une protection est nécessaire à chaque étape. Une stratégie Zero-Trust utilise des règles solides basées sur l'identité pour chaque ressource IT, ainsi que des principes de « moindres privilèges » pour l'accès. L'architecture cyberrésiliente Dell inclut des fonctionnalités avancées axées sur l'intégrité du démarrage et la protection des données, ainsi que les fonctions de sécurité de l'iDRAC (Integrated Dell Remote Access Controller). Les serveurs Dell PowerEdge intègrent une fonctionnalité Root-of-Trust basée sur le silicium qui établit une chaîne de confiance pour la vérification cryptographique des composants matériels et logiciels du serveur. AMD Infinity Guard fournit une couche de sécurité supplémentaire qui réduit la surface d'attaque potentielle lors du démarrage et de l'exécution des logiciels. AMD Infinity Guard englobe plusieurs fonctions de sécurité supplémentaires, notamment Platform Secure Boot et Platform Secure Processor, qui garantissent la protection des serveurs PowerEdge à chaque étape de leur cycle de vie.

Architecture cyber-résiliente Dell

L'architecture cyberrésiliente Dell utilise les fonctions de sécurité PowerEdge qui se combinent pour assurer la résilience nécessaire et la prise en charge d'une stratégie Zero-Trust. Les fonctions de sécurité doivent protéger contre les menaces, détecter les activités suspectes et permettre une restauration rapide en cas de violation. Dans le même temps, elles doivent maintenir une posture de confiance basée sur la vérification pour une approche Zero-Trust de moindre privilège, qui consiste à limiter l'accès des utilisateurs et des appareils aux données dont ils ont besoin pour effectuer leurs tâches. Les contrôles de sécurité PowerEdge fonctionnent de façon conjointe pour offrir une solution de sécurité complète qui garantit la résilience tout en appliquant une posture Zero-Trust. Pour plus d'informations sur l'ensemble des fonctionnalités et services de l'architecture cyberrésiliente Dell, voir le livre blanc.

Garantir l'intégrité du démarrage

Souvent négligé, l'environnement de prédémarrage peut faire l'objet d'attaques si aucune mesure de protection n'est prise. Si l'intégrité du BIOS, du firmware ou d'un pilote est compromise lors du démarrage, l'acteur malveillant peut obtenir l'accès à l'ensemble du système. Faute de contrôles appropriés, il peut infiltrer le système à tout moment et atteindre sa cible : vos données.

Pour limiter les failles de sécurité, le fournisseur du serveur doit protéger le BIOS, mais également vérifier et valider des composants et des firmwares spécifiques du serveur, tels que la mémoire et les processeurs. Les fabricants de matériel de serveur doivent s'assurer que leurs composants s'intègrent entièrement à l'architecture du serveur afin que les contrôles de sécurité et de validation fonctionnent de manière transparente. Chaque serveur Dell PowerEdge offre plusieurs couches de sécurité pour protéger le cycle de démarrage : fonctionnalité Root-of-Trust basée sur le silicium, UEFI Secure Boot et fonctions de sécurité de l'iDRAC, y compris la restauration du firmware et la récupération rapide du système d'exploitation.

En plus de ces couches de sécurité basées sur le serveur Dell PowerEdge, les processeurs AMD sont dotés des technologies PSB (Platform Secure Boot) et PSP (Platform Security Processor) pour protéger les données en cours d'utilisation. Ensemble, Dell et AMD couvrent tous les aspects du cycle de démarrage afin d'offrir un socle sécurisé à vos données et vos charges applicatives.

1 Chuck Brooks, « Cybersecurity Trends & Statistics For 2023; What You Need to Know », consulté le 4 décembre 2023, https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=9885ce219dba.

2 Ken Kizzee, « Cyber Attack Statistics to Know », consulté le 19 décembre 2023. https://parachute.cloud/cyber-attack-statistics-data-and-trends/.

Dell iDRAC et Root-of-Trust

Le concept RoT (Root-of-Trust) part du principe que, si un système détermine qu'une base est sûre, l'ensemble des validations et des vérifications de sécurité ultérieures s'inscrivent dans une chaîne de confiance continue. Prenez l'exemple d'une maison : si les fondations sont instables et deviennent fragiles, l'intégrité des murs importe peu. De même, si le BIOS de votre serveur est compromis, il peut être vain de vouloir protéger le système d'exploitation du serveur.

La chaîne de confiance des serveurs PowerEdge assure la vérification cryptographique transparente de tous les composants du serveur, depuis le socle jusqu'aux données. De cette manière, les composants de la pile de logiciels du système (hyperviseur, système d'exploitation, applications) savent que le serveur sous-jacent est digne de confiance lorsque le serveur est opérationnel. Cette couche pose les bases d'une chaîne de confiance dans un serveur et crée une plateforme de serveur à la fois fiable et sécurisée. Les serveurs Dell utilisent une fonctionnalité RoT basée sur le silicium qui est unique et intégrée à chaque serveur pour fournir une vérification cryptographique qui garantit un démarrage sécurisé à chaque cycle de démarrage à froid ou cycle marche/arrêt. À partir de la version 4.10.10.10, l'iDRAC fournit un mécanisme RoT conçu pour vérifier l'image du BIOS. Tant que l'opération de vérification n'est pas terminée, il ne permet pas au serveur de démarrer. Pour les serveurs PowerEdge équipés de processeurs AMD, l'iDRAC (Integrated Dell Remote Access Controller) tire parti de la technologie AMD PSB pour vérifier le code du BIOS avant le chargement du système d'exploitation. La technologie AMD PSB examine l'intégrité du BIOS en interagissant avec la mémoire ROM du BIOS principal et AMD FCH (Fusion Controller Hub) pour un traitement RoT approfondi. Cette validation minutieuse s'étend jusqu'au chargeur de démarrage du système d'exploitation, garantissant ainsi une chaîne de confiance continue.

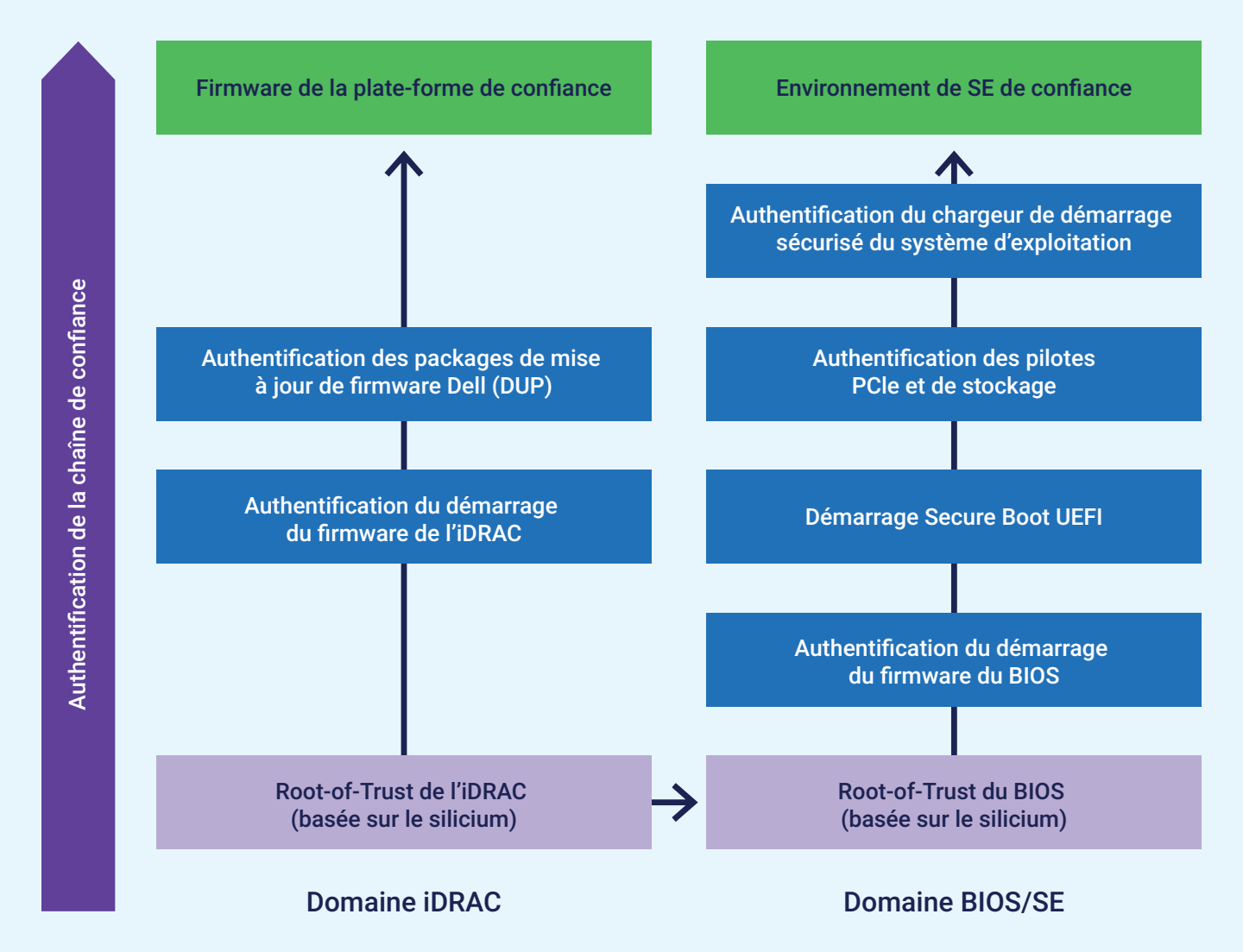

Figure 1 : Domaines de Root-of-Trust basée sur le silicium des serveurs PowerEdge avec iDRAC9.

En cas d'échec de la validation du BIOS, l'iDRAC arrête immédiatement le serveur et avertit l'utilisateur. Cela empêche le démarrage de firmwares non autorisés. L'iDRAC inclut également un système de sauvegarde et de restauration pour les firmwares du BIOS et de l'iDRAC, qui renforce la fiabilité du serveur et protège les opérations du serveur contre une éventuelle corruption des firmwares. Pour fournir une protection supplémentaire, l'iDRAC propose également une analyse du BIOS en direct que les utilisateurs peuvent exécuter à la demande ou planifier pour une exécution régulière. Cette analyse nécessite la licence iDRAC Datacenter et permet aux utilisateurs de détecter les problèmes potentiels avant le redémarrage afin d'assurer une atténuation proactive[3].

UEFI Secure Boot

Les serveurs Dell PowerEdge utilisent la technologie UEFI Secure Boot standard pour valider les chargeurs de démarrage spécifiques du système d'exploitation, ce qui garantit l'intégrité du noyau du système d'exploitation et d'autres composants essentiels. UEFI joue un rôle de bouclier contre les logiciels malveillants et les ransomwares dans les environnements de prédémarrage. Pour garantir l'interopérabilité, les fabricants de serveurs et les fabricants de composants doivent collaborer pour s'assurer que le BIOS compatible UEFI reconnaît les signatures de pilote et de firmware des composants. En validant les signatures cryptographiques des pilotes UEFI et d'autres codes pré-système d'exploitation, UEFI Secure Boot tente de s'assurer que tout code chargé lors du démarrage est exempt de contenu malveillant.

Pour personnaliser encore davantage la sécurité, les administrateurs peuvent configurer des certificats personnalisés de signature du chargeur de démarrage du système d'exploitation pour UEFI Secure Boot. (Pour en savoir plus sur les options de personnalisation d'UEFI Secure Boot, rendez-vous sur https://infohub.delltechnologies.com/section-assets/direct-from-development-uefi-boot-enhanced-security-to-combat-threats.) Cette approche limite l'exécution aux chargeurs de démarrage sécurisés et fiables du système d'exploitation, qui protègent la chaîne Secure Boot en authentifiant le noyau et le système de fichiers du système d'exploitation. Cette fonctionnalité optimise la flexibilité, en particulier pour les administrateurs Linux qui préfèrent signer leurs propres chargeurs de démarrage de système d'exploitation plutôt que de dépendre des autorités de certification UEFI tierces par défaut. Les administrateurs peuvent télécharger des certificats personnalisés via l'API de l'iDRAC, améliorant ainsi l'authentification de leurs chargeurs de démarrage de système d'exploitation. À la différence des autres serveurs, les serveurs Dell PowerEdge prennent en charge la personnalisation complète de Secure Boot. Ils offrent notamment la possibilité de supprimer tous les certificats standard de l'autorité de certification Microsoft, VMware ou UEFI[4].

Validation du CPLD

Chaque serveur Dell PowerEdge valide le circuit logique programmable complexe (CPLD) à chaque démarrage marche/arrêt. Ce circuit logique programmable polyvalent[5] est composé de plusieurs circuits logiques programmables simples reliés par une matrice de commutation programmable. Son firmware, généralement stocké dans la mémoire EEPROM, Flash ou SRAM, permet de modifier les fonctions de la carte système au-delà des capacités du BIOS. Il est notamment possible de mettre en œuvre une logique spécifique pour les interactions entre les dispositifs de la carte système. La validation du CPLD garantit que les modifications apportées à la carte système n'endommageront ni vos serveurs, ni vos données.

Sécurité matérielle de l'iDRAC

En étendant la chaîne de confiance à d'autres composants matériels, l'iDRAC utilise le protocole SPDM (Security Protocol and Data Model), qui standardise la façon dont les serveurs collectent des informations sur leurs composants. Les informations relatives à l'identité, au firmware et à la configuration de chaque composant sont chiffrées. La sécurité matérielle de l'iDRAC utilise des échanges de clés authentifiés pour sécuriser les communications entre les composants et l'iDRAC. Avec SPDM, l'iDRAC peut authentifier la validité des composants, tels que les contrôleurs RAID PowerEdge (PERC) 12 et les cartes d'interface réseau (NIC), ce qui améliore non seulement la sécurité du serveur grâce à l'authentification des certificats d'identité d'appareil des composants, mais alerte également les utilisateurs en cas d'échec de l'authentification.

[3] Dell, « Improved security with iDRAC9 using Root of Trust and BIOS Live Scanning », consulté le 19 décembre 2023, https://dl.dell.com/manuals/common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf.

[4] Dell, « Sécurité cyber-résiliente dans les serveurs Dell EMC PowerEdge », consulté le 4 décembre 2023, https://www.delltechnologies.com/asset/en-us/products/servers/industry-market/cyber-resilient-security-with-poweredge-servers.pdf.

[5] Technopedia, « Complex Programmable Logic Device », consulté le 4 décembre 2023, https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld.

AMD Platform Secure Boot

Les processeurs AMD sont dotés de la technologie AMD PSB (Platform Secure Boot) pour répondre à une autre préoccupation croissante dans le paysage numérique actuel : les menaces au niveau du firmware. PSB utilise la fonctionnalité RoT basée sur le silicium AMD et vérifie le processus de démarrage, depuis le code du BIOS jusqu'au chargeur de démarrage du système d'exploitation via UEFI Secure Boot[6]. Dell utilise des cartes mères compatibles AMD PSB pour permettre uniquement l'exécution de leur code BIOS signé de manière cryptographique. En outre, Dell lie chaque processeur AMD à une carte mère spécifique à l'aide de fusibles programmables à usage unique qui associent le processeur aux clés de signature de code du firmware Dell[7]. Pour assurer la protection contre les attaques visant à intégrer des logiciels malveillants dans le firmware, les démarrages PSB autorisent uniquement les firmwares authentifiés par AMD Secure Processor[8].

En vérifiant de manière cryptographique la pile de logiciels, AMD Platform Secure Boot ajoute une importante couche de défense contre les intrusions non autorisées sur diverses plateformes, en particulier dans les environnements virtualisés ou dans le Cloud.

AMD Platform Secure Processor

Combiné à PSB, AMD Platform Secure Processor (PSP) renforce le processus de démarrage des serveurs Dell PowerEdge. Lorsqu'un processeur est mis sous tension pour la première fois dans l'usine Dell, AMD Platform Secure Processor intègre dans le processeur un ID Dell unique et permanent. Cet identifiant lie efficacement le processeur au serveur PowerEdge, créant ainsi une liaison sécurisée[9].

Grâce à cette intégration, PSP pourra empêcher un serveur PowerEdge de démarrer s'il détecte un processeur d'un autre serveur. Toutefois, la portabilité du processeur reste possible en cas de défaillance matérielle. Le processeur AMD est verrouillé sur la clé de signature du fournisseur plutôt que sur la carte mère afin d'offrir le juste équilibre entre sécurité et mobilité des composants[10].

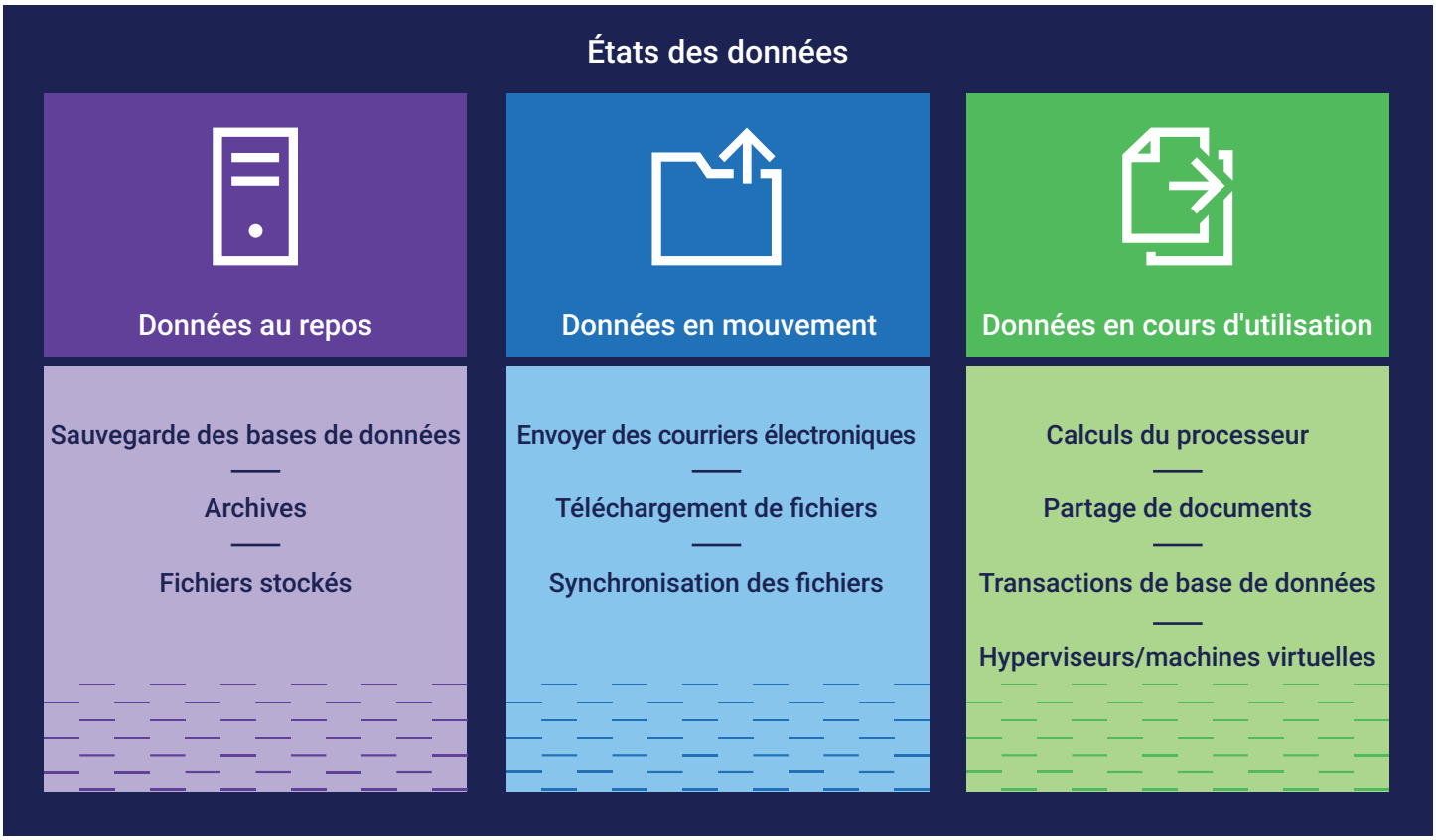

Figure 2 : États des données

[6] AMD, « Sécurité AMD Pro », consulté le 4 décembre 2023, https://www.amd.com/en/technologies/pro-security.
[7] AMD, « AMD Infinity Guard », consulté le 4 décembre 2023, https://www.amd.com/en/technologies/infinity-guard.
[8] AMD, « 4 Ways AMD Infinity Guard Helps Protect Your Data », consulté le 4 décembre 2023. https://www.amd.com/system/files/documents/content-security-infographic.pdf.
[9] AMD, « AMD Infinity Guard ».
[10] Dell, « Defense in-depth: Comprehensive Security on PowerEdge AMD EPYC Generation 2 (Rome) Servers », consulté le 4 décembre 2023 https://infohub.delltechnologies.com/p/defense-in-depth-comprehensive-security-on-poweredge-amd-epyc-generation-2-rome-servers/.

Protection de vos données

Lorsque les auteurs d'attaque accèdent aux systèmes, l'objectif final est toujours le même : mettre la main sur vos données, puis les voler, les manipuler, les vendre ou les détruire. Le serveur physique ne constitue pas le seul point de vulnérabilité. Des acteurs malveillants peuvent attaquer le réseau, les stratégies IT peuvent contenir des erreurs, les utilisateurs finaux peuvent utiliser des mots de passe faibles et les équipes IT peuvent définir des autorisations d'accès trop étendues. Les auteurs d'attaque sont susceptibles de diffuser des logiciels malveillants en ciblant les utilisateurs à l'aide d'e-mails d'hameçonnage.

Dell permet aux clients d'utiliser une approche Zero-Trust qui s'appuie sur plusieurs couches de sécurité pour assurer la protection contre tous ces types de failles de sécurité. Pour éviter qu'elles ne soient volées ou compromises, vous devez sécuriser les données au repos, en cours de traitement et en cours de transfert, jusqu'à leur mise hors service[11]. Avec des fonctionnalités telles que le chiffrement au repos, la gestion robuste de clés de chiffrement et le renouvellement automatisé des certificats, les serveurs Dell PowerEdge bloquent, dissuadent et atténuent les attaques malveillantes après le premier démarrage. Les serveurs Dell PowerEdge équipés de processeurs AMD offrent des fonctionnalités supplémentaires pour renforcer la sécurité, notamment les technologies AMD Secure Memory Encryption (SME) et Secure Encrypted Virtualization (SEV).

Données au repos

Pour protéger les données au repos, Dell fournit trois fonctions de sécurité principales : le chiffrement logiciel, la gestion de clés d'entreprise et le chiffrement de disque matériel. Les disques prennent en charge l'effacement sécurisé instantané (ISE), ce qui permet aux clients Dell d'effacer de manière cryptographique toutes les données stockées sur les disques à autochiffrement (SED), les disques ISE et les appareils NVM tels que les NVDIMM. Les disques SED protègent les données contre les attaques, par exemple lorsqu'un collaborateur mécontent ou un autre acteur malveillant retire physiquement des disques d'un serveur. Étant donné que le mot de passe de la clé de verrouillage du disque chiffré les lie à leur serveur et à leur contrôleur RAID spécifiques d'origine, un autre serveur ne peut pas accéder aux données. Pour une protection renforcée, l'iDRAC peut utiliser Dell OpenManage Secure Enterprise Key Manager avec Local Key Management (iLKM, LKM) qui fonctionne conjointement avec un gestionnaire de clés tiers externe pour verrouiller et déverrouiller le contrôleur de stockage au démarrage. Si un utilisateur démarre le serveur sans utiliser le gestionnaire de clés, l'iDRAC maintient le verrouillage du contrôleur de stockage afin que les données stockées sur l'appareil restent chiffrées. Pour en savoir plus sur les autres options en matière de clés de chiffrement, rendez-vous sur https://infohub.delltechnologies.com/section-assets/openmanage-sekm-storage-performance-infographic.

Données en cours de transfert

En ce qui concerne les données en cours de transfert, les vulnérabilités au niveau du réseau et du contrôle de l'accès aux données pourraient permettre aux auteurs d'attaque d'intercepter ou de modifier les données qui transitent sur le réseau. La connexion Web de l'iDRAC est un point de vulnérabilité possible. Dell propose donc plusieurs options pour sécuriser la connexion à l'aide d'un certificat TLS/SSL et réduire ainsi les risques d'attaque. Bien que ce certificat soit autosigné par défaut, les administrateurs peuvent créer un certificat personnalisé ou signé par une autorité de certification (AC) de confiance. Ce certificat est un gage de connexions chiffrées et sécurisées. Ainsi, les navigateurs Web et les outils tels que les utilitaires de ligne de commande peuvent interagir en toute sécurité avec le serveur via la connexion iDRAC.

L'iDRAC fournit également plusieurs contrôles afin de permettre aux utilisateurs de modifier les règles d'accès strictes qui autorisent l'accès SSH au serveur. Pour les utilisateurs de l'iDRAC disposant d'une licence de niveau datacenter, l'iDRAC propose le protocole SCEP (Simple Certificate Enrollment Protocol), qui assure le renouvellement automatique des certificats de serveur Web afin d'éviter les interruptions accidentelles de protection. Selon une étude réalisée en 2020 par l'entreprise tierce Principled Technologies, cette fonctionnalité de renouvellement automatique renforce la sécurité des serveurs tout en faisant gagner un temps précieux au personnel IT, en particulier lorsqu'il gère un parc de certificats de serveur[12].

Données en cours d'utilisation

Pour protéger les données en cours d'utilisation, les serveurs Dell PowerEdge offrent des fonctionnalités de calcul confidentiel AMD, notamment AMD Secure Memory Encryption (SME) et Secure Encrypted Virtualization (SEV), qui protègent les données lorsqu'elles transitent par la mémoire et les composants de traitement.

[11] Dell, « Reduce Your Risk of Unauthorized Server Data Access », consulté le 24 janvier 2024. https://infohub.delltechnologies.com/section-assets/data-protection-infographic.

[12] Principled Technologies, « Reduce hands-on deployment times to near zero with iDRAC9 automation », consulté le 4 décembre 2023, https://www.principledtechnologies.com/Dell/iDRAC9-v6.10-provisioning-infographic-0323.pdf.

Secure Memory Encryption

AMD SME chiffre toutes les données à mesure qu'elles entrent dans la mémoire afin de renforcer leur sécurité. Sans chiffrement de la mémoire, les données sont vulnérables aux logiciels malveillants et autres intrusions. C'est particulièrement vrai pour les technologies de mémoire les plus récentes, telles que les modules NVDIMM qui ne perdent pas de données lorsqu'ils sont hors tension. Cette protection s'étend à la mémoire via des moteurs de chiffrement hautes performances intégrés dans les canaux de mémoire, garantissant à la fois sécurité et vitesse. Dans la mesure où elle est totalement transparente pour le système d'exploitation hôte et les couches applicatives, la fonctionnalité AMD SME ne nécessite pas de modifications du logiciel applicatif. Elle permet ainsi d'améliorer la sécurité de la mémoire dans le cadre de manière aisée[13].

Le chiffrement des données en mémoire AMD SME change la donne par rapport aux anciennes méthodes de chiffrement de la mémoire qui étaient adaptées à des cas d'utilisation spécifiques. L'un des principaux avantages d'AMD SME est sa flexibilité, car les logiciels peuvent l'utiliser de différentes manières : soit en chiffrant l'ensemble de la mémoire DRAM pour une protection complète, soit en chiffrant uniquement des régions spécifiques, telles que celles utilisées par les machines virtuelles invitées[14].

AMD Secure Encrypted Virtualization

La technologie AMD SEV améliore le chiffrement de la mémoire et des machines virtuelles en mettant en œuvre un environnement TEE (Trusted Execution Environment) basé sur les machines virtuelles. Intégrée à l'architecture AMD-V, elle chiffre la mémoire de chaque machine virtuelle séparément, protégeant ainsi les machines virtuelles de l'hyperviseur et les unes des autres. Cette approche utilise le chiffrement pour protéger le code d'une machine virtuelle contre le code exécuté avec des privilèges supérieurs et potentiellement vulnérable (hyperviseur, par exemple). La couche de sécurité supplémentaire est particulièrement cruciale dans les environnements Cloud. Cette méthode garantit une protection renforcée des machines virtuelles face aux failles de sécurité externes. Le chiffrement se produit directement au niveau du contrôleur de mémoire. Les données sont chiffrées et déchiffrées sans ralentir la vitesse de traitement grâce à AMD Secure Processor qui gère tous les détails du chiffrement de manière invisible[15].

Dans certains cas, les données d'une machine virtuelle doivent communiquer avec d'autres machines virtuelles ou avec l'hyperviseur. AMD SEV permet alors à la machine virtuelle de choisir la clé de chiffrement à appliquer à des pages de mémoire spécifiques : une clé d'invité qui s'assure que la page reste privée pour la machine virtuelle ou une clé d'hyperviseur qui permet à l'hyperviseur et aux autres machines virtuelles de déchiffrer la page. Cette flexibilité assure la sécurité et la communication en fonction des besoins de chaque machine virtuelle[16].

AMD SEV offre des fonctionnalités supplémentaires qui étendent l'isolement cryptographique des machines virtuelles : SEV-Encrypted State (SEV-ES) et SEV-Secure Nested Paging (SEV-SNP). SEV-ES isole davantage les machines virtuelles de l'hyperviseur et les unes des autres en chiffrant le contenu du registre du processeur lors de la mise hors tension d'une machine virtuelle, ce qui le protège contre tout accès non autorisé via une machine virtuelle voisine ou l'hyperviseur. SEV-SNP s'appuie sur SEV et SEV-ES afin de renforcer la protection de l'intégrité de la mémoire et d'offrir des fonctions de sécurité supplémentaires en option pour les machines virtuelles. L'amélioration de l'intégrité de la mémoire permet à une machine virtuelle d'accéder aux données en mémoire uniquement si elle peut lire la dernière valeur qu'elle a écrite. Si une autre entité a modifié les données dans la mémoire, la machine virtuelle ne peut pas accéder aux données. Cette approche protège la machine virtuelle contre l'exécution de données ou de codes compromis.

Chiffrement et clés de chiffrement

AMD SEV utilise une clé de chiffrement unique pour chaque machine virtuelle de sorte que les machines virtuelles et l'hyperviseur sont isolés de façon cryptographique. Ce moteur de chiffrement sécurise les données lors de l'écriture et les déchiffre lors de la lecture. Lors de sa création, chaque machine virtuelle se voit attribuer une clé unique afin que les données soient incompréhensibles en cas de tentative d'accès non autorisée à sa mémoire. Chaque processeur AMD EPYC™ de 4e génération offre jusqu'à un millier de clés de chiffrement. Cette architecture ne modifie pas les applications au sein de la machine virtuelle. Elle agit au niveau du système d'exploitation et améliore la sécurité des données. Conçu pour protéger les données en cours d'utilisation, y compris le contenu de la mémoire, le matériel de chiffrement intégré au contrôleur de mémoire gère le chiffrement et le déchiffrement du trafic de la mémoire VRAM, renforçant ainsi la protection des données en cours d'utilisation[17].

[13] AMD, « AMD Infinity Guard ».
[14] AMD, « AMD Memory Encryption », consulté le 4 décembre 2023, https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf.
[15] AMD, « AMD Secure Encrypted Virtualization », consulté le 4 décembre 2023. https://www.amd.com/en/developer/sev.html
[16] AMD, « AMD Memory Encryption ». https://www.amd.com/content/dam/amd/en/documents/epyc-business-docs/white-papers/memory-encryption-white-paper.pdf
[17] AMD, « AMD Secure Encrypted Virtualization ».

Conclusion

De la commande de serveurs Dell PowerEdge équipés de processeurs AMD jusqu'à leur mise hors service et à chaque étape intermédiaire, Dell et AMD protègent vos données en mettant en œuvre de nombreuses couches de sécurité. Grâce aux couches étroitement intégrées de la fonctionnalité RoT basée sur le silicium et aux multiples couches de protection du démarrage, les pilotes, firmwares et versions du BIOS suspects sont éliminés de sorte que les composants du serveur sont sécurisés dès la fabrication. En outre, le chiffrement des disques SED et ISE garantit la sécurité de vos données, même si des acteurs malveillants retirent physiquement des disques ou des serveurs de votre datacenter. Grâce à d'autres fonctions de sécurité telles que les technologies AMD SME et SEV basées sur un processeur, qui protègent les données en cours de traitement, et aux contrôles logiciels de pointe via l'iDRAC, les serveurs Dell PowerEdge équipés de processeurs AMD garantissent la continuité de l'activité, quelles que soient les nouvelles méthodes d'attaque utilisées par les cybercriminels. Pour en savoir plus sur les serveurs Dell PowerEdge équipés de processeurs AMD EPYC de 4e génération, rendez-vous sur www.dell.com/servers/amd.

En savoir plus sur les solutions Dell et AMD

Contacter un expert Dell Technologies

Consulter d'autres ressources

Prenez part à la discussion avec #PowerEdge

DELL Technologies

AMD together we advance_