DELL Technologies

Microsoft

Livre blanc

Bénéficiez d'une protection de sécurité avancée avec les fonctionnalités combinées de Windows Server 2022 et des serveurs Dell EMC™ PowerEdge™ de nouvelle génération

Renforcez les charges applicatives stratégiques avec un environnement de matériel, de firmware et de système d'exploitation plus sécurisé

Selon Cybersecurity Ventures, la cybercriminalité mondiale devrait coûter un total de 6 000 milliards de dollars en 2021 et atteindre 10 500 milliards de dollars en 2025[1]. À elles seules, les attaques par rançongiciel ont été multipliées par 61 en six ans pour atteindre 20 milliards de dollars en 2021, une attaque se produisant actuellement toutes les 11 secondes[1]. Une enquête IDC de 2021 a révélé que plus d'un tiers des organisations interrogées dans le monde avaient subi une attaque ou une violation par rançongiciel au cours des 12 derniers mois (et souvent plusieurs attaques)[2]. Et bien qu'IBM estime que le coût d'une seule violation de données s'élève désormais à 4,24 millions de dollars[3], le coût réel des violations peut être beaucoup plus élevé : dans certains cas, des hôpitaux américains ont dû rediriger des patients d'urgence vers d'autres hôpitaux et refuser des ambulances en raison d'attaques par rançongiciel.[4]

Les attaques de firmware peuvent constituer une menace particulièrement pernicieuse pour les organisations. Cela est dû au fait qu'une attaque de firmware peut entraîner l'infection par des logiciels malveillants avant que le système d'exploitation (SE), et donc la sécurité logicielle exécutée sur ce dernier, n'aient même démarré. Pourtant, moins de la moitié des organisations ont pris des mesures pour renforcer leurs systèmes par rapport aux attaques de firmware, même si ces attaques sont devenues cinq fois plus fréquentes au cours des cinq dernières années[5]. En fin de compte, le niveau de sécurité des charges applicatives correspond à celui de l'ensemble des piles sur lesquelles elles s'exécutent.

Pour faire face à cette fréquence à la croissance exponentielle, à la variété et au coût des menaces liées aux logiciels malveillants, la sécurité moderne doit être multicouche. En effet, les logiciels malveillants peuvent compromettre les systèmes au niveau du matériel et du firmware, ou lors du démarrage. Dans ces domaines, une sécurité uniquement software-defined est inefficace. Pour contrer cette vulnérabilité, la sécurité des serveurs modernes ne peut pas dépendre d'une stratégie reposant sur une approche unique. Elle doit être intégrée à l'ensemble de la pile d'infrastructure. La combinaison de serveurs Dell EMC™ PowerEdge™ de nouvelle génération et de Windows Server 2022 simplifie la tâche importante des administrateurs qui consiste à aligner le matériel, le firmware et le système d'exploitation afin de sécuriser correctement les charges applicatives stratégiques.

Avantages combinés du serveur Secured-core Windows Server 2022 et des serveurs PowerEdge de nouvelle génération

Le serveur Secured-core est une nouvelle fonctionnalité de Windows Server 2022 qui utilise le matériel, le firmware et les fonctionnalités du système d'exploitation pour assurer la protection contre les menaces actuelles et futures. La combinaison du logiciel de serveur Secured-core Windows Server 2022 s'exécutant sur du matériel de serveur PowerEdge de nouvelle génération offre trois avantages considérables aux organisations comme la vôtre :

- Protection avancée
- Défense préventive
- Sécurité simplifiée

Protection avancée

D'après les données de renseignements sur les menaces de Microsoft, les PC Secured-core offrent plus de deux fois plus de protection contre les infections que les PC standard. Microsoft intègre désormais cette même technologie dans l'espace serveur avec les serveurs Secured-core Windows Server 2022[5]. Les protections activées par un serveur Secured-core sont conçues pour créer une plate-forme sécurisée pour les charges applicatives et les données stratégiques sur ce serveur. Plus précisément, les serveurs Secured-core utilisent la prise en charge du processeur pour la technologie DRTM (Dynamic Root of Trust for Measurement) afin de placer le firmware dans un sandbox matériel. Cet isolement permet de limiter l'impact des failles de sécurité dans des millions de lignes de code de firmware avec un niveau de privilège élevé.

Outre l'isolement du firmware dans Windows Server 2022, la sécurité basée sur la virtualisation (VBS) isole les parties critiques du système d'exploitation, telles que le noyau, du reste du système. Cela permet de s'assurer que les serveurs restent dédiés à l'exécution des charges applicatives stratégiques, et de protéger les applications et les données connexes contre les attaques et l'exfiltration.

Pour protéger davantage le firmware des serveurs PowerEdge contre les attaques, Dell Technologies aide à sécuriser la chaîne logistique des serveurs PowerEdge afin de s'assurer que personne n'a altéré le serveur lors de son transfert de l'usine vers le site du client (pour plus de détails, voir la section Sécurité supplémentaire grâce à l'intégrité de la chaîne logistique Dell Technologies ci-dessous).

Défense préventive

La fonctionnalité Secured-core permet de se défendre de manière proactive et de perturber la plupart des voies que les pirates peuvent utiliser pour exploiter vos systèmes. L'intégrité du code protégée par l'hyperviseur (HVCI) dans VBS isole la fonction de prise de décision d'intégrité du code (CI) du reste du système d'exploitation Windows, ce qui permet de s'assurer que la seule façon dont la mémoire du noyau peut devenir exécutable consiste à effectuer une vérification de l'intégrité du code. VBS permet également d'utiliser Windows Defender Credential Guard, dans lequel les informations d'identification et les secrets de l'utilisateur sont stockés dans un conteneur virtuel auquel le système d'exploitation ne peut pas accéder directement.

Trusted Platform Module 2.0 (TPM 2.0) est fourni par défaut avec les serveurs Secured-core. Il fournit un magasin protégé pour les clés et les données confidentielles, telles que les mesures des composants chargés lors du démarrage. La possibilité de vérifier que le firmware qui s'exécute pendant le démarrage est signé de façon valide par l'auteur prévu et qu'il n'a pas été altéré contribue à améliorer la sécurité. Cette racine de confiance matérielle augmente également la protection fournie par des fonctionnalités telles que le chiffrement de lecteur BitLocker, qui utilise le module TPM 2.0 et facilite la création de workflows basés sur des attestations qui peuvent être intégrés dans des stratégies de sécurité zero-trust. Ensemble, ces défenses permettent à vos équipes IT et SecOps de mieux utiliser leur temps dans les nombreux domaines de sécurité qui nécessitent leur attention.

Les serveurs PowerEdge de nouvelle génération prennent en charge la technologie Unified Extensible Firmware Interface (UEFI) Secure Boot conforme aux normes de l'industrie. UEFI Secure Boot vérifie les signatures cryptographiques des pilotes UEFI et d'autres codes chargés avant l'exécution du système d'exploitation afin de s'assurer que des logiciels malveillants n'ont pas altéré le firmware. En outre, les serveurs PowerEdge prennent en charge le module TPM 2.0 afin d'améliorer la sécurité du firmware et du système d'exploitation.

Sécurité simplifiée

Lorsque vous achetez un serveur Secured-core PowerEdge, vous avez l'assurance que Dell Technologies a fourni un ensemble de matériel, de firmware et de pilotes qui répondent à la promesse Secured-core. Microsoft collabore étroitement avec Dell Technologies pour simplifier la mise en œuvre de la sécurité sur les serveurs PowerEdge.

Les nouvelles fonctionnalités du Centre d'administration Windows permettent aux administrateurs de configurer facilement les fonctions de sécurité du système d'exploitation des serveurs Secured-core Windows Server 2022. La nouvelle fonctionnalité de sécurité du Centre d'administration Windows permet aux administrateurs de mettre en œuvre la sécurité avancée d'un simple clic. Le Centre d'administration Windows présente l'état de toutes les fonctions de sécurité requises pour les serveurs Secured-core Windows Server 2022 et permet aux administrateurs d'activer les fonctionnalités selon les besoins à partir d'un seul emplacement.

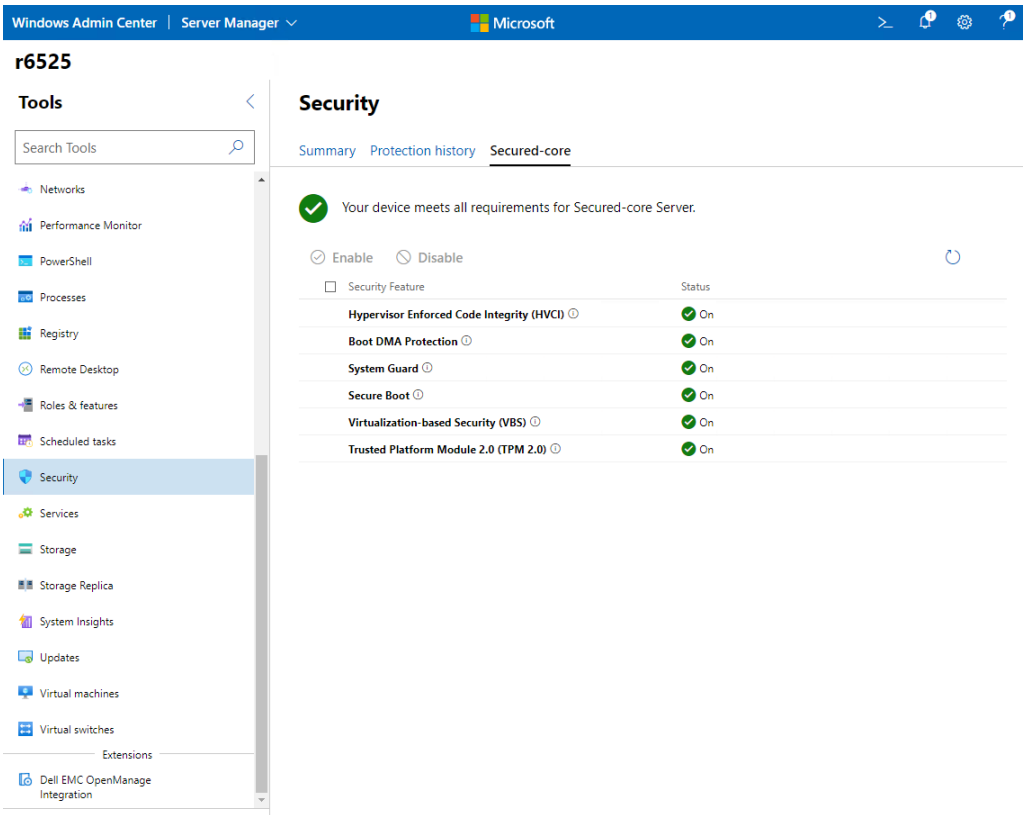


Figure 1. Écran de confirmation Secured-core dans le Centre d'administration Windows

Dell EMC™ OpenManage™ Integration with Windows Admin Center est une extension du Centre d'administration Windows qui simplifie davantage la gestion des serveurs Secured-core. Cette extension du Centre d'administration Windows simplifie les tâches de sécurité (entre autres) des administrateurs IT en gérant à distance les serveurs PowerEdge. Dans le contexte des serveurs Secured-core Windows Server 2022, l'extension OpenManage Integration with Windows Admin Center vous permet d'afficher votre inventaire des serveurs PowerEdge à partir du Centre d'administration Windows et fournit une vue unifiée de l'intégrité, du matériel et des informations d'inventaire des firmware des composants des serveurs PowerEdge.

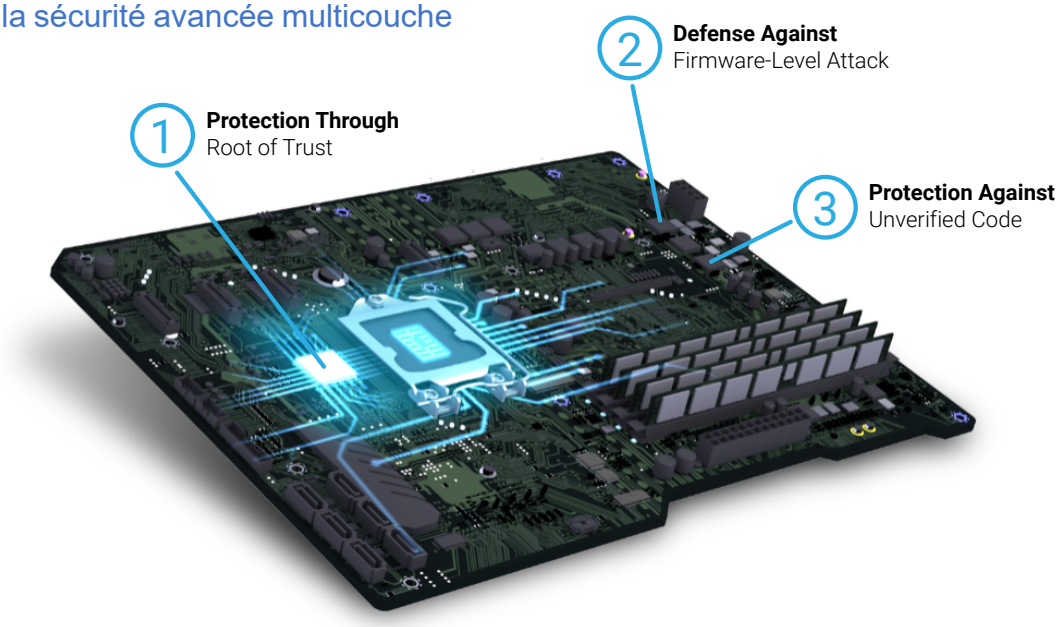
Prise en charge des serveurs PowerEdge pour les serveurs Secured-core Windows Server 2022

En raison de la nature multicouche des défenses des serveurs Secured-core, le support de votre OEM constructeur de matériel est crucial. Les serveurs PowerEdge sont testés et certifiés par Dell Technologies pour s'assurer que le matériel et le firmware répondent aux exigences des fonctions de sécurité de Windows Server 2022. En outre, le matériel et le firmware des serveurs PowerEdge sont configurés pour prendre en charge le serveur Secured-core Windows Server 2022. Le Tableau 1 décrit comment le matériel des serveurs PowerEdge soutient les fonctionnalités de Windows Server 2022.

Tableau 1. Mise en correspondance des fonctions de sécurité de Windows Server 2022 et des principales fonctionnalités de prise en charge des serveurs Dell EMC™ PowerEdge™ de nouvelle génération

	Windows Server 2022	Serveurs Dell EMC™ PowerEdge™ de nouvelle génération
Protection avancée	Les systèmes Secured-core placent le firmware dans un sandbox matériel, ce qui contribue à limiter l'impact des failles de sécurité basées sur le firmware. VBS isole les composants critiques du système d'exploitation des logiciels malveillants avancés.	Dell Technologies aide à sécuriser la chaîne logistique des serveurs PowerEdge afin de s'assurer que personne n'a altéré le serveur ou compromis le firmware lors du transfert de l'usine vers le site du client.
Défense préventive	Les fonctionnalités VBS telles que HVCI et Windows Defender Credential Guard empêchent des classes entières de failles de sécurité et protègent mieux les ressources confidentielles telles que les informations d'identification. Le module TPM 2.0 fournit une racine de confiance matérielle utilisée comme base sécurisée.	Les serveurs PowerEdge prennent en charge la technologie Secure Boot UEFI standard pour vérifier les signatures cryptographiques des pilotes UEFI et d'autres codes chargés avant l'exécution du système d'exploitation. Les serveurs PowerEdge prennent en charge le module TPM 2.0.
Sécurité simplifiée	Le Centre d'administration Windows facilite l'accès pour configurer les serveurs Secured-Core.	Microsoft collabore avec Dell Technologies pour simplifier l'activation de la sécurité sur les serveurs PowerEdge. L'intégration du Centre d'administration Windows avec Dell EMC™ OpenManage™ simplifie davantage la gestion des serveurs Secured-core.

Description de la sécurité avancée multicouche



1

Protection par le biais de la racine de confiance

En partenariat avec des OEM leaders sur le marché tels que Dell Technologies et des fournisseurs de silicium tels qu'Intel et AMD, les serveurs Secured-core utilisent une racine de confiance matérielle standard associée à des fonctions de sécurité intégrées aux processeurs modernes.

Les serveurs Secured-core utilisent le module TPM 2.0 et un processeur moderne avec DRTM pour démarrer les serveurs de manière plus sécurisée et minimiser les failles de sécurité du firmware.

2

Défense contre les attaques au niveau du firmware

Les serveurs Secured-core utilisent la sécurité matérielle du processeur moderne pour lancer le système dans un état fiable, empêchant ainsi les logiciels malveillants avancés d'altérer l'intégrité du système et d'effectuer une attaque au niveau du firmware.

System Guard Secure Launch utilise le processeur pour valider l'appareil afin de démarrer de façon plus sécurisée, ce qui permet d'éviter les attaques de firmware avancées.

3

Protection contre le code non vérifié

Le code s'exécutant dans la base informatique de confiance s'exécute avec intégrité et n'est pas soumis à des attaques.

Doté de HVCI, un serveur Secured-core démarre uniquement les fichiers exécutables signés par des autorités connues et approuvées. L'hyperviseur définit et applique des autorisations pour empêcher les logiciels malveillants de tenter de modifier la mémoire et de la rendre exécutable.

Prise en charge des serveurs PowerEdge de nouvelle génération pour la connectivité sécurisée dans Windows Server 2022

Les serveurs PowerEdge de nouvelle génération prennent en charge le chiffrement AES-256 SMB (Server Message Block) pour les charges applicatives axées sur la sécurité. Cette prise en charge signifie que les serveurs PowerEdge qui exécutent Windows Server 2022 peuvent fournir un chiffrement de bout en bout pour les données de charge applicative afin de renforcer la sécurité. Le chiffrement AES 256 bits utilisé pour SMB dans Windows Server 2022 est également suffisamment robuste pour résister aux attaques de type « force brute » par les ordinateurs quantiques si des mots de passe suffisamment forts sont utilisés.

Les serveurs PowerEdge et Windows Server 2022 étendent le chiffrement SMB de bout en bout des serveurs individuels aux communications internes des clusters avec le chiffrement AES-256 pour le trafic de données SMB est-ouest. Ces contrôles de chiffrement SMB supplémentaires permettent de renforcer davantage les charges applicatives et de fermer les voies d'attaque.

Enfin, Windows Server 2022 utilise Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) inclus dans les processeurs Intel® Xeon® Scalable de 3e génération et le chiffrement AES vectorisé pour 256 bits (vAES256) inclus dans les processeurs AMD EPYC™ Zen 3. Les ensembles d'instructions de ces processeurs avancés optimisent les performances du chiffrement AES-256 dans les serveurs PowerEdge. Grâce à ces technologies de sécurité avancées, Dell Technologies et Microsoft vous évitent d'avoir à choisir entre une sécurité robuste et une réactivité optimale pour les charges applicatives stratégiques.

Sécurité supplémentaire grâce à l'intégrité de la chaîne logistique Dell Technologies

L'intégrité de la chaîne logistique Dell Technologies protège les composants de matériel et de firmware contre toute compromission lors de la fabrication et de l'expédition. Dans le domaine de l'intégrité matérielle, Dell Technologies s'assure qu'aucune altération des produits ou insertion de composants contrefaits n'a lieu avant d'expédier les produits aux clients. Les contrôles mis en place par Dell Technologies couvrent la sélection des fournisseurs, l'approvisionnement, les processus de production et la gouvernance par le biais d'audits et de tests. Les inspections des ressources au cours de la production permettent d'identifier les composants marqués de manière inadéquate, s'écartant des paramètres de performances normaux ou contenant un identifiant électronique incorrect.

En ce qui concerne l'intégrité des logiciels, Dell Technologies cherche à s'assurer qu'aucun logiciel malveillant n'est inséré dans les firmwares ou les pilotes de périphérique avant d'expédier un produit aux clients, ainsi qu'à empêcher toute faille de sécurité du codage. Dell EMC applique la certification ISO 9001 pour tous les sites de fabrication mondiaux. Le strict respect de ces processus et contrôles permet de minimiser le risque d'intégration de composants contrefaits au sein des produits Dell Technologies™, et d'infiltration de logiciels malveillants dans les firmwares ou les pilotes de périphérique. En outre, Dell Technologies met en œuvre ces mesures dans le cadre du processus de cycle de développement logiciel (SDLC).

Dell Technologies s'efforce également de garantir la sécurité physique des sites de fabrication et des chaînes de transport. Dell Technologies demande à certaines usines dans lesquelles les produits Dell Technologies sont fabriqués de répondre aux exigences de sécurité des installations de l'Association pour la protection des marchandises transportée (« Transported Asset Protection Association » ou TAPA), notamment de recourir à des caméras contrôlées en circuit fermé dans les zones clés, à des contrôles d'accès et à la surveillance continue des entrées et sorties. Dell Technologies a également mis en place des mesures visant à protéger les produits contre le vol et l'altération lors du transport dans le cadre d'un programme logistique leader sur le marché. Enfin, la solution Secured Component Verification (SCV) de Dell Technologies pour les serveurs PowerEdge permet aux clients Dell Technologies de vérifier que le serveur PowerEdge qu'ils ont reçu correspond à ce qui a été fabriqué en usine.

Protégez vos charges applicatives vitales avec une meilleure base de sécurité de Windows Server 2022 et des serveurs Dell EMC PowerEdge de nouvelle génération

Les charges applicatives sont aussi sécurisées que la base sur laquelle elles s'exécutent. La menace des logiciels malveillants et des violations de données ne fera qu'augmenter à l'avenir, principalement parce que les acteurs malveillants continuent de rechercher des méthodes d'attaque qui contournent la sécurité logicielle traditionnelle. Les attaques de firmware ciblent spécifiquement les serveurs pendant le processus de démarrage, avant même que la sécurité logicielle n'ait commencé à protéger les systèmes. La protection moderne des serveurs nécessite une sécurité multi-approche qui couvre le matériel, le firmware et le système d'exploitation.

La mise à niveau vers Windows Server 2022 est plus logique que jamais. La fonctionnalité de serveur Secured-core de Windows Server 2022 aide les organisations à contrer les menaces qui visent le firmware et le système d'exploitation. Lorsqu'ils sont associés aux protections d'intégrité matérielle et logicielle de Dell Technologies, les serveurs Dell EMC PowerEdge de nouvelle génération qui exécutent Windows Server 2022 peuvent fournir une sécurité moderne à l'ensemble de la pile pour le matériel, le firmware et le système d'exploitation. De plus, les fonctionnalités de connectivité sécurisée de Windows Server 2022 prises en charge dans les serveurs PowerEdge de nouvelle génération étendent cette sécurité au-delà des serveurs individuels à des clusters entiers au sein de votre datacenter. En outre, la prise en charge de Windows Server 2012 prend fin en octobre 2023, ce qui signifie qu'il est temps de commencer à définir des plans de mise à niveau[6].

Pour en savoir plus sur la façon dont Windows Server 2022 et les serveurs Dell EMC PowerEdge de nouvelle génération peuvent vous aider à sécuriser vos charges applicatives et vos données stratégiques, rendez-vous sur www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. « Cybercrime To Cost The World $10.5 Trillion Annually By 2025. » Novembre 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[2] IDC. « IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach. » Août 2021.
[3] IBM. « How much does a data breach cost? » 2021. www.ibm.com/security/data-breach.
[4] Dan Goodin. « Hospitals hamstrung by ransomware are turning away patients. » *Ars Technica.* Août 2021. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. « New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats. » Mars 2021. www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/.
[6] Au moment de la rédaction de ce document. Pour obtenir les dernières informations sur la fin de la prise en charge de Windows Server 2012, rendez-vous sur la page du cycle de vie de Windows Server 2012 : https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Modernisez-vous avec Windows Server 2022.
Le système d'exploitation prêt pour le Cloud qui optimise les investissements sur site avec des fonctionnalités hybrides.