Livre blanc technique : **2023**

Traiter les principaux problèmes de sécurité liés à la modernisation de l'infrastructure de Data Center

vmware®

Table des matières

Traiter les principaux problèmes de sécurité liés à la modernisation de l'infrastructure de Data Center

Les entreprises modernes doivent impérativement se défendre contre l'impressionnant éventail des menaces de cybersécurité. Toute entreprise qui modernise son infrastructure Cloud y voit l'occasion de revoir ses stratégies de sécurité et d'apporter les ajustements nécessaires pour garantir l'alignement avec ses exigences de sécurité.

Les cyberattaques menacent les Data Centers en compromettant les informations sensibles stockées sur ces serveurs et en interrompant les opérations stratégiques. Les entreprises stockent souvent d'importants volumes de données financières, personnelles et stratégiques confidentielles, accessibles par des personnes non autorisées et exploitées dans un but crapuleux ou pour nuire à l'entreprise. Il existe pléthore de catégories d'attaques, des violations de données au vol de propriété intellectuelle en passant par l'extorsion et les rançongiciels. Ces derniers sont de loin les plus répandus. Lorsqu'un cybercriminel lance une attaque par déni de service ciblant des services de distribution de carburant, d'alimentation ou de santé au niveau national, il attire l'attention des gouvernements, des clients et des actionnaires.

De plus, les Data Centers constituant souvent un hub pour l'infrastructure informatique d'une entreprise, une attaque réussie contre eux peut entraîner une interruption opérationnelle généralisée. D'où une perte de productivité et de revenus, et un impact sur la réputation de l'entreprise.

Figure 1 : La protection des charges de travail est une question de processus, d'outils et de stratégie.

Les cyberattaques menacent aussi bien l'infrastructure d'une entreprise que la gestion de sa trésorerie. L'impact sur les dépenses d'investissement (CapEx) et les coûts d'exploitation (OpEx) peut être considérable lorsqu'il faut limiter les menaces potentielles, notamment en dehors de toute stratégie de sécurité globale.

Côté CapEx, une entreprise peut avoir besoin d'investir dans des technologies ou équipements de sécurité pour limiter le risque de futures attaques et satisfaire les obligations réglementaires. Il peut s'agir de pare-feu, de systèmes de détection/prévention des intrusions, de chiffrement et autres outils de sécurité. Ces efforts peuvent induire des dépenses supplémentaires imprévues lorsqu'ils n'entrent pas dans le cadre d'un exercice budgétisé et d'une posture proactive continue.

Côté OpEx, il peut être nécessaire de renforcer le personnel informatique et de sécurité pour gérer et administrer les nouvelles technologies de sécurité, ainsi que de former les autres collaborateurs à la détection et à la réponse aux violations. L'entreprise peut aussi avoir à allouer des fonds à la réponse aux incidents et à l'enquête approfondie en cas d'attaque, augmentant encore les dépenses d'exploitation globales.

La sensibilité aux cybermenaces est essentielle pour une stratégie de sécurité efficace

Les cybermenaces ne sont pas toutes conçues de la même manière ni avec le même objectif. Les responsables informatiques et architectes de la sécurité doivent connaître l'éventail des attaques, le modus operandi et le facteur de risque pour concevoir une stratégie de sécurité efficace. Il est important de noter qu'il ne s'agit pas d'une liste exhaustive de tous les types de cyberattaques, cette liste évoluant en permanence avec l'arrivée de nouvelles attaques. Par conséquent, les entreprises doivent mettre en place une stratégie de sécurité complète pour détecter les incidents de sécurité et y répondre rapidement.

Les types de cyberattaques les plus courants aujourd'hui

Attaques par déni de service distribué (DDoS)
Ces attaques envoient un volume important de trafic au réseau d'un Data Center, le submergeant et le rendant inaccessible aux utilisateurs légitimes.

Hameçonnage
Attaques qui utilisent l'e-mail ou d'autres formes de communication pour piéger les utilisateurs et les inciter à transmettre à un cybercriminel des informations sensibles comme des informations d'authentification.

Rançongiciel
Attaques qui chiffrent les données sur les serveurs d'un Data Center et fournissent la clé de chiffrement à l'entreprise contre le paiement d'une rançon.

Menace persistante avancée (APT)
Attaques ciblées conçues pour accéder au réseau d'un Data Center et voler des informations sensibles sur une longue période.

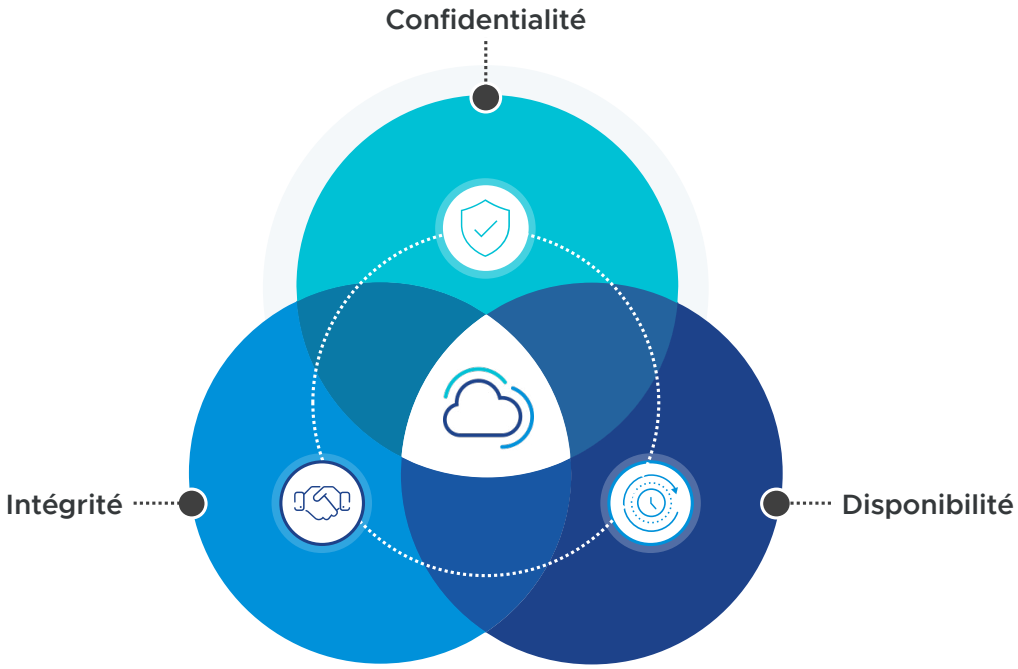
Logiciel malveillant
Logiciel malveillant qui accède au réseau d'un Data Center, vole des informations sensibles ou interrompt les opérations.

Attaques Cloud
Ces attaques ciblent les vulnérabilités de l'infrastructure Cloud pouvant conduire à un accès non autorisé, à des violations de données et autres activités malveillantes.

Attaques IoT
Ces attaques ciblent les vulnérabilités des terminaux Internet des objets (IoT), tels que les caméras de sécurité et les capteurs de température, connectés au réseau d'un Data Center.

Attaques internes
Ces attaques sont lancées par un collaborateur, un sous-traitant ou autre utilisateur de confiance qui a accès au réseau du Data Center.

Critères à prendre en compte lors de la conception d'une architecture de sécurité pérenne



Un bon moyen d'illustrer le niveau de sécurité requis au sein des plates-formes est de réfléchir à travers le prisme des trois principaux piliers de la sécurité des informations : confidentialité, disponibilité et intégrité.

1. La **confidentialité des données** fait référence à la protection des données sensibles contre l'accès ou la divulgation par des personnes ou des systèmes non autorisés. Elle est importante pour les entreprises car les informations sensibles peuvent être utilisées dans un but crapuleux ou pour nuire à l'entreprise si elles se retrouvent entre les mains des mauvaises personnes.

2. L'**intégrité des données** fait référence à l'exactitude et l'exhaustivité des données, ainsi qu'à la garantie que les données ne sont pas modifiées, altérées ou détruites de manière non autorisée. Elle est importante car elle garantit que les données utilisées par une entreprise sont exactes, fiables et de confiance. Des données inexactes ou altérées peuvent conduire à la prise de mauvaises décisions, à une perte financière et à un impact sur la réputation de l'entreprise.

3. La **disponibilité des données** fait référence à la capacité de personnes ou systèmes non autorisés à accéder à des données lorsqu'ils en ont besoin. Elle est importante pour les entreprises car sans accès aux données, les processus de gestion peuvent être interrompus entraînant une perte de productivité, une perte de revenus et un impact sur la réputation de l'entreprise. Elle est également essentielle à la continuité des opérations, à la conformité aux réglementations et à la satisfaction des clients.

Chaque fonctionnalité de sécurité d'une infrastructure peut être associée à un ou plusieurs de ces piliers. Par exemple, le chiffrement et le masquage des données sont des fonctionnalités du pilier Confidentialité des données, tandis que l'intégrité des données et le hachage sont associés au pilier Intégrité des données.

Chaque fonctionnalité de sécurité est ainsi conçue pour aider les entreprises à réduire et éliminer le risque. Atout très puissant, elles sont la raison pour laquelle les entreprises orientées sécurité choisissent les plates-formes VMware.

Traiter les principaux problèmes liés à la stratégie de sécurité

Lors de la planification d'un programme de modernisation de l'infrastructure Cloud, les responsables de l'infrastructure et des opérations doivent impérativement comprendre les principales exigences de sécurité liées à la protection de l'entreprise contre les attaques et déployer une architecture agile pour contrer les futures attaques.

Visibilité et observabilité

La sécurité commence par la visibilité. Les entreprises ne peuvent pas protéger ce qu'elles ne peuvent pas voir. Or, la visibilité seule ne suffit pas. L'observabilité offre une visibilité contextuelle intelligente. Les infrastructures et applications modernes complexes ne permettent pas de répondre facilement aux questions sur ce qui s'est passé, qui a été impacté et comment résoudre le problème. Les systèmes d'observabilité vous permettent d'inspecter et de comprendre la pile d'applications.

L'observabilité est un élément clé de la stratégie de protection de bout en bout. Elle dépasse le cadre de la visibilité et fournit des informations contextuelles à l'utilisateur sur la situation actuelle d'un système dynamique comme les Software-Defined Data Centers d'aujourd'hui.

La visibilité implique de comprendre quelles sont les ressources de processus utilisées, par qui et pour quelle raison, et avec quelle dimension d'intérêt. Les administrateurs système peuvent en apprendre beaucoup sur l'infrastructure en l'observant au travers de tous ses aspects. Alors qu'elle peut sembler évidente, cette exigence est souvent oubliée dans les politiques et processus obsolètes des différentes entreprises. Il est important de visualiser et de recevoir des informations détaillées sur les flux se déroulant sur l'ensemble du Data Center, avec inspection de couche 7 avec état et contexte intégral des charges de travail. Vous éliminez ainsi les angles morts et accélérez la résolution des incidents.

Implémentation d'une sécurité basée sur des règles

Dans les infrastructures software-defined, la gestion ou l'architecture de sécurité basée sur des règles est un bon moyen de définir et contrôler de manière dynamique l'interaction entre les services et les applications. La gestion de la sécurité basée sur des règles offre des fonctionnalités de sécurité intelligentes et renforce le contrôle granulaire sur le comportement des utilisateurs.

Or, l'évolution dynamique du réseau, la croissance rapide des attaques de sécurité, la répartition géographique des nœuds et les réseaux hétérogènes complexes peuvent énormément nuire à la performance des stratégies. Plus la définition d'une règle est intelligente, plus elle peut suivre le rythme de l'évolution des violations de sécurité. Par conséquent, dès lors que les responsables informatiques comprennent le flux des applications d'infrastructure, les ingénieurs peuvent définir un meilleur moyen pour protéger les applications et les ressources fondamentales. Introduire un système nécessitant une intervention humaine réduite signifie plus de flexibilité, plus de scalabilité et moins d'erreurs.

Garantir l'application des règles

Les politiques de sécurité jouent un rôle important dans le modèle de sécurité global de l'entreprise. Or, dans beaucoup d'entreprises, les défis sont de trois sortes :

1. Comprendre la portée de la politique (géré avec l'observabilité)
2. Définir une politique de sécurité complète qui prend en compte tous les aspects
3. Implémentation et exécution

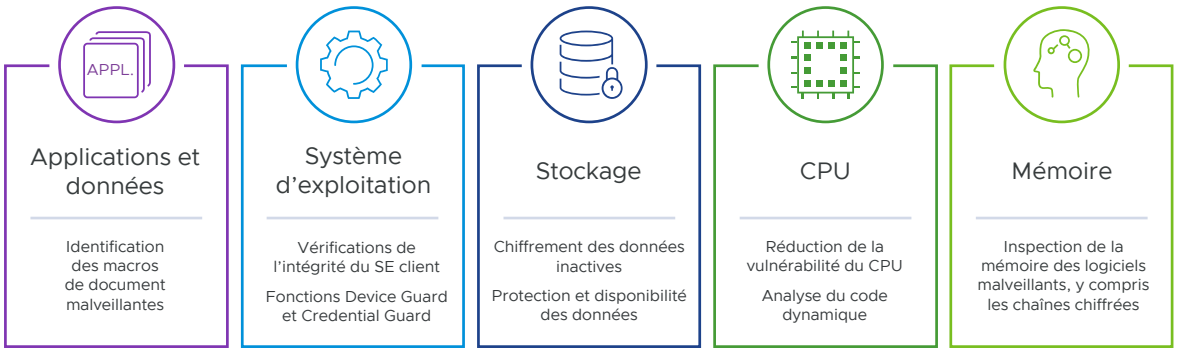
Les entreprises doivent mettre en place des processus solides pour satisfaire les exigences liées à la politique de sécurité. Les systèmes d'automatisation et intelligents, tels que ceux fournis par VMware NSX® ou le produit Advance Threat Analyzer, permettent d'exécuter ces processus de manière cohérente et plus fiable qu'avec une intervention humaine, source de défaut d'exécution.

Mettre en œuvre des architectures de sécurité modernes avec VMware Cloud Foundation

Dans VMware Cloud Foundation™ (VCF), la sécurité va au-delà des simples routeurs et commutateurs virtualisés. Les services de réseau et sécurité sont répartis par programmation entre les machines virtuelles, peu importe le matériel réseau sous-jacent ou la topologie. Les charges de travail sont ainsi ajoutées ou supprimées de manière dynamique et tous les services de réseau et sécurité associés à la machine virtuelle se déplacent avec elle, partout dans le Data Center.

Combiné à NSX, VCF reproduit la pile de réseau complète sous forme logicielle dans chaque réseau virtuel. Il offre une architecture logique distribuée pour les services des couches 2 à 7, y compris un commutateur logique, un routeur, un pare-feu, un équilibreur de charge et un VPN.

Sécurité dans VMware Cloud : au-delà du simple pare-feu



En plus des services de réseau classiques, les ingénieurs profitent de fonctionnalités de sécurité étendues :

Au niveau de la couche des applications :
Identification des macros de document malveillantes

Au niveau de la couche du système d'exploitation :
Les systèmes d'exploitation s'exécutant partout, vous voulez être certain qu'ils sont les plus sécurisés possible. Il s'agit donc de ne pas simplement compter sur un pare-feu au niveau de la machine, mais aussi sur votre infrastructure pour vous protéger des attaques.

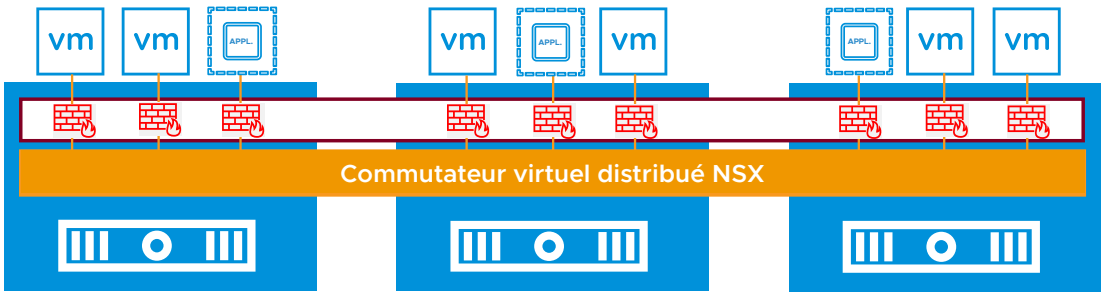
Au niveau de la couche du stockage :
VMware Cloud Foundation utilise VMware vSAN™ pour stocker les données des clients, et par la même, les sécuriser et les chiffrer, et ainsi garantir la mise à jour continue des règles de protection des données avancées contre les menaces modernes.

Au niveau de la couche du matériel :
VMware Cloud Foundation peut aussi aider à résoudre les problèmes matériels. Non seulement il inclut des options pour l'analyse de code dynamique dans les charges de travail, mais aussi pour la résolution des problèmes, comme les vulnérabilités du CPU, offrant la liberté à une organisation d'adapter sa réponse à ses besoins métier.

Mémoire :
VMware NSX Sandbox détecte les processus et éléments de logiciel malveillant qui tentent de se cacher dans la mémoire et agit immédiatement pour protéger les infrastructures.

Pare-feu nouvelle génération dans VMware Cloud Foundation

Le pare-feu de périmètre, aussi appelé pare-feu de réseau, est une mesure de sécurité traditionnelle utilisée pour contrôler le flux du trafic réseau entre les réseaux internes et externes. Si les pare-feu de périmètre peuvent fournir une couche de sécurité utile, ils ont aussi leurs limites : une visibilité limitée sur le trafic réseau interne, une protection limitée contre les menaces avancées et une protection limitée pour les utilisateurs mobiles et distants.



Le pare-feu distribué (DFW) est un pare-feu avec état, ce qui signifie qu'il surveille l'état des connexions actives et utilise ces informations pour déterminer les paquets réseau à autoriser à travers le pare-feu. DFW est mis en œuvre dans l'hyperviseur et appliqué aux machines virtuelles pour chaque vNIC. Autrement dit, les règles de pare-feu sont appliquées au niveau de la carte réseau virtuelle de chaque machine virtuelle. L'inspection du trafic se produit au niveau de la carte réseau virtuelle d'une VM lorsque le trafic est sur le point de quitter la VM et d'entrer dans le commutateur virtuel (sortie). L'inspection se produit également au niveau de la carte réseau virtuelle lorsque le trafic quitte le commutateur mais avant d'entrer dans la VM (entrée).

Chaque machine virtuelle dispose de règles de stratégie de pare-feu et d'un contexte propre. Dans vMotion, lorsque des VM passent d'un hôte ESXi à un autre, le contexte DFW (tableau de règles, tableau de suivi des connexions) se déplace avec la VM. En outre, toutes les connexions actives restent intactes dans vMotion. En d'autres termes, la stratégie de sécurité DFW est indépendante de l'emplacement de la VM.

Conclusions

Aspect important de la modernisation du Data Center, la sécurité permet de protéger les données précieuses d'une entreprise contre les cyberattaques. Pour protéger les données sensibles, il est important de mettre en œuvre des mesures de sécurité solides, telles que la segmentation du réseau, des pare-feu, des systèmes de détection et prévention des intrusions et le chiffrement. La modernisation de toute l'infrastructure de Data Center renforce la sécurité et permet une approche plus granulaire de la prévention des menaces.

- **Exploiter une architecture Software-Defined Data Center (SDDC)** telle que VMware Cloud Foundation permet d'automatiser et d'orchestrer l'infrastructure et la sécurité. L'application et la mise en œuvre cohérentes des règles de sécurité sont ainsi simplifiées sur l'ensemble du Data Center et la réponse aux incidents de sécurité accélérée.
- **Implémenter la virtualisation de réseau** telle que VMware NSX intégré à VMware Cloud Foundation, permet de créer plusieurs réseaux virtuels au sein d'un même réseau physique. Vous instaurez ainsi un contrôle granulaire du trafic réseau, ainsi que la micro-segmentation qui permet de réduire la surface d'attaque et d'isoler les différentes charges de travail et applications les unes des autres, rendant difficile le déplacement latéral des cybercriminels dans le réseau.
- **Déployer une analyse des menaces améliorée** en utilisant des outils comme Advanced Threat Protection peut fournir aux entreprises une visibilité et des informations supplémentaires sur les menaces de sécurité, ainsi que la possibilité d'y répondre de manière plus rapide et efficace.
- **L'automatisation et l'orchestration** permettent d'identifier rapidement les incidents de sécurité et d'y répondre, à l'aide d'outils de sécurité capables de détecter et de répondre automatiquement aux menaces de sécurité.
- **Améliorer la conformité :** la modernisation du Data Center et l'optimisation de la sécurité peuvent aider les entreprises à respecter les obligations réglementaires et de conformité, telles que HIPAA, PCI-DSS et SOC 2, en fournissant une infrastructure sécurisée et conforme.

Déployer VMware Cloud Foundation permet d'intégrer toutes ces technologies et fonctions de sécurité modernes à une plate-forme de modernisation du Data Center sécurisée, conforme et agile.