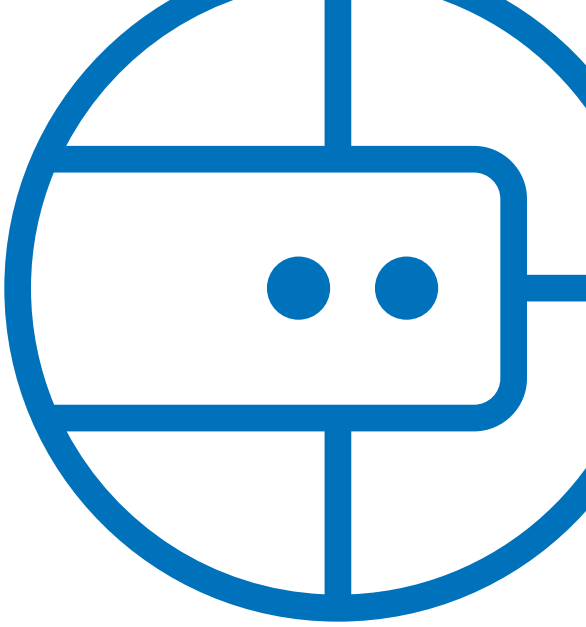
SOPHOS



Guide d'achat pour la protection des serveurs

Les cyber menaces ciblant les serveurs sont de plus en plus complexes et de plus en plus virulentes. Des épidémies dévastatrices de ransomware, comme WannaCry et NotPetya, ont révélé le besoin de mettre en place des capacités anti-ransomware fortes. Les failles exploitées par Spectre et Meltdown ont montré que les technologies anti-exploit, le contrôle des applications et les outils d'investigation comme l'EDR (Endpoint Detection et Response) sont des composants essentiels de toute stratégie de sécurité des serveurs.

Les serveurs étant généralement les ressources les plus précieuses des entreprises, la pression se fait de plus en plus forte sur les responsables informatiques pour choisir la protection la plus efficace. Il n'est pas suffisant d'utiliser pour vos serveurs une solution de sécurité conçue pour les postes de travail, vous avez besoin de solutions élaborées entièrement autour de la protection des serveurs.

Ce guide a pour objectif de vous offrir des conseils pratiques sur les fonctions et les capacités clés à rechercher au moment de choisir la solution de sécurité de vos serveurs, ainsi que les questions à poser aux éditeurs pour vous assurer de l'efficacité de ces fonctionnalités.

Environnements de serveur

Selon les besoins de votre entreprise, vous pouvez exploiter vos propres serveurs sur site, héberger vos données dans le Cloud public (dont Amazon Web Services [AWS], Microsoft Azure, Google Cloud) ou toute solution hybride mélangeant les deux. Vous avez donc besoin au minimum d'une solution de sécurité qui vous permette de gérer facilement ces différentes configurations de manière consolidée.

De préférence, cette solution doit offrir des bénéfices supplémentaires, tels que le déploiement de politiques de sécurité cohérentes sur l'ensemble de vos serveurs, que vous pouvez gérer de manière centralisée. Le déploiement automatisé de la protection serveur dans le Cloud (via un script par exemple) est essentiel pour que celle-ci puisse être activée (ou désactivée) en fonction des besoins et sans intervention de l'administrateur serveur.

Et comme les entreprises choisissent des environnements de déploiement mixtes, il est impératif que les options de licences soient les plus claires possible. Recherchez pour cela un éditeur qui propose un seul type de licence, que ce soit pour le Cloud, en local ou un mélange des deux, et épargnez-vous les tracas de la gestion d'une combinaison hétérogène de licences.

Capacités et fonctionnalités clés des produits

La sécurité serveur moderne a évolué pour conserver une longueur d'avance sur les menaces toujours plus avancées. Pour sécuriser vos serveurs, que ce soit en local ou dans le Cloud, recherchez un ensemble de fonctionnalités qui protège contre les menaces inconnues, les ransomwares, les exploits et les piratages :

- **Anti-ransomware** – Certaines solutions sont dotées de techniques spécifiquement conçues pour empêcher le chiffrement malveillant des données par un ransomware. Souvent, les techniques spécifiquement anti-ransomware pourront également nettoyer tous les fichiers touchés, par exemple en les restaurant vers un état sain non affecté. Les solutions anti-ransomware devraient non seulement stopper les ransomwares ciblant les fichiers, mais également ceux utilisés pour effacer les disques et pour falsifier l'enregistrement d'amorçage maître. Et plus spécifiquement pour les serveurs, il est nécessaire d'empêcher les systèmes endpoint distants ou indésirables de chiffrer les fichiers sur les partages réseau ou sur d'autres serveurs connectés.
- **Verrouillage des serveurs/Mise sur liste blanche/Refuser par défaut** – Créer une liste blanche d'applications autorisées vous permet de bloquer l'exécution d'applications non autorisées sur vos serveurs. Les acheteurs devraient rechercher une solution qui peut automatiquement identifier les applications fiables et qui offre également aux utilisateurs une certaine souplesse dans la personnalisation, afin de réduire le temps et l'énergie déployés pour la création d'un ensemble sécurisé de règles. De plus, le verrouillage ou le déverrouillage d'un serveur ne devrait pas nécessiter de temps d'arrêt.
- **Anti-exploit** – Une technologie anti-exploit est conçue pour stopper les attaquants en bloquant les outils et les techniques mis en œuvre lors d'une attaque. Par exemple, les exploits EternalBlue ou DoublePulsar ont été utilisés pour exécuter les ransomwares NotPetya et WannaCry. Les technologies anti-exploit bloquent la poignée de techniques utilisées pour propager les malwares et lancer des attaques, repoussant ainsi de nombreuses attaques Zero-Day inédites (sans utiliser de signature). La prévention complète contre les exploits protège également les serveurs qui ne peuvent pas être corrigés rapidement, ou pour lesquels des correctifs ne sont pas disponibles.

[1] Gartner Top 10 Security Projects for 2018

- **EDR (Endpoint Detection and Response)** – L'EDR permet aux responsables informatiques de rechercher de manière proactive les menaces évasives et d'analyser en profondeur les incidents de sécurité pour les aider à comprendre leur ampleur et leur impact. Idéalement, la solution choisie devrait être dotée de fonctionnalités EDR qui vous aident à affiner vos analyses en réduisant la quantité d'informations que vous devez passer au crible et en fournissant des informations sur les fichiers suspects pour vous aider à prendre une décision éclairée.
- **Anti-piratage** – Les serveurs sont la cible privilégiée des pirates, car ils contiennent les données les plus sensibles des entreprises. Recherchez une solution qui propose des capacités spécifiques pour bloquer en temps réel les attaques répétées des pirates. Quelques exemples d'outils bloquant le piratage des serveurs incluent la prévention de la collecte d'identifiants, la prévention des mouvements latéraux, la prévention du Code Cave, la protection contre l'élévation des privilèges et la protection contre la migration de processus.
- **Machine Learning** – Il existe plusieurs types de Machine Learning, dont le Deep Learning et ses réseaux neuronaux, les forêts d'arbres décisionnels, les analyses bayésiennes et le clustering. Indépendamment de la méthodologie utilisée, les moteurs de détection des malwares par Machine Learning devraient être conçus pour détecter les malwares connus et inconnus, sans avoir recours aux signatures. L'avantage du Machine Learning est qu'il peut détecter les malwares inédits, augmentant ainsi le taux global de détection des malwares. Au moment d'évaluer une solution basée sur le Machine Learning, les entreprises devraient prendre en considération le taux de détection, le taux de faux positifs et les effets sur les performances.
- **Réponse aux incidents/Sécurité synchronisée** – Les solutions de protection des serveurs devraient fournir des outils capables, au minimum, d'offrir un aperçu des événements antérieurs en vue d'éviter de futurs incidents. De manière idéale, ces solutions devraient pouvoir répondre automatiquement aux incidents, sans avoir besoin de l'intervention d'un analyste, afin d'empêcher les menaces de se propager ou de provoquer plus de dégâts. Il est important que les outils de protection des serveurs communiquent avec ceux des réseaux, comme le pare-feu, afin de détecter les serveurs compromis et de fournir une visibilité sur toutes les applications présentes sur le serveur.
- **Surveillance de l'intégrité des fichiers** – Cette fonction protège les données et les fichiers système critiques contre toute modification involontaire, et, en option, surveille les emplacements des applications clés. Sophos Central Server Protection surveille et traque en continu les modifications imprévues et inattendues pour identifier les potentielles violations des normes de sécurité PCI DSS.
- **Contrôle des applications** – Cette fonction permet de contrôler quelles applications sont autorisées à s'exécuter sur le serveur, afin de réduire la surface d'attaque. Pour simplifier et accélérer la configuration, il est préférable de filtrer les applications par catégories.
- **Gestion centralisée** – La console devrait permettre la visibilité et la gestion des environnements mixtes de serveur en toute simplicité. Les alertes, les événements et les rapports devraient notamment tous être disponibles depuis un seul écran facile d'accès et simple à comprendre.
- **Découverte et protection des ressources** – La protection dans le Cloud consiste à protéger chaque instance ou VM (machine virtuelle) et chaque compartiment de stockage. Il est vital de découvrir toutes les ressources et tous les compartiments de stockage présents dans les environnements de Cloud public, comme Amazon Web Services (AWS) et Microsoft Azure, car les attaquants sont connus pour exploiter et réaffecter les régions de Cloud non utilisées, par exemple pour le cryptomining. Les produits s'intégrant nativement grâce à une API avec les plateformes de Cloud public affichent les nouvelles ressources et stockages, y compris dans des régions qui ne sont pas activement utilisées.

Administration et édition de rapports

En général, vous ne vous connectez à vos serveurs que lorsqu'il y a un problème. Ce qui signifie qu'à des fins de gestion, il y a deux exigences principales :

1. Simplicité du déploiement et du contrôle de tous les serveurs
2. Facilité d'utilisation de l'interface pour prendre rapidement les mesures nécessaires en cas de problème

Dans de nombreux cas, déployer des solutions individuelles de plusieurs éditeurs pour différents serveurs dans différents environnements peut engendrer des problèmes de gestion considérables en raison de la multiplicité des consoles. La situation peut rapidement devenir incontrôlable s'il s'agit de gérer un parc de serveurs de plus grande envergure. Répondre à une attaque sérieuse exige une action rapide et décisive, qui n'est pas entravée par le temps perdu à essayer de localiser l'information critique nécessaire à la prise de décision. Il vous faut donc rechercher une solution qui consolide l'information sur un seul écran, afin de trouver ce qui est important en un minimum de temps et d'efforts.

Certaines solutions sont également capables d'associer votre serveur avec votre pare-feu, ce qui permet à ces derniers de partager leurs données sur les menaces. Par exemple, si un serveur est identifié comme compromis, il peut être isolé du reste du réseau pour empêcher tout dommage supplémentaire pour l'entreprise. Le trafic et les applications sur le serveur peuvent également être identifiés avec précision, permettant ainsi de donner la priorité aux applications importantes ou au contraire interdire l'accès aux applications indésirables.

Permettre l'utilisation d'un script pour faciliter le déploiement (en particulier pour les déploiements Cloud) réduit la quantité de travail que l'administrateur serveur devra investir, lui permettant de se concentrer sur d'autres missions. La mise sur liste blanche d'applications ou le contrôle des applications en fonction de catégories permettent une configuration plus rapide de ce qui est autorisé ou non à s'exécuter sur un serveur, par rapport à une installation purement manuelle.

Comparaison des produits sur le marché

Après avoir lu les sections précédentes pour déterminer vos besoins stratégiques, utilisez maintenant ce tableau pour comparer les solutions de différents éditeurs et évaluer leur pertinence pour votre entreprise.

Comparaison des fonctionnalités			Intercept X Advanced for Server with EDR	Trend Micro Deep Security	Symantec Cloud Workload Protection	Microsoft Enterprise Mobility + Security	CrowdStrike Falcon Prevent/ Falcon Spotlight
GESTION		Une console pour protéger serveurs, endpoint, mobiles, email et Wi-Fi	✓	✗	✗	✗	✗
		AWS/Azure Workload Discovery	✓	✓	✓	✓	✓
		Exclusions automatiques des contrôles (par exemple Exchange, SQL Server)	✓	✗	✓	✓	✗
		Virtualisation : Agent léger avec contrôle centralisé	✓	✓	✗	✗	✗
PRÉVENTION	RÉDUCTION DE LA SURFACE D'ATTAQUE	Filtrage Web (bloque les sites Web malveillants)	✓	✓	✓	✓	✗
		Contrôle du Web (contrôle l'accès aux sites potentiellement inappropriés)	✓	✗	✗	✗	✗
		Mise sur liste blanche des applications (verrouillage du serveur)	✓	✓	✗	✓	✗
		Contrôle des applications basé sur les catégories	✓	✗	✗	✗	✗
		Contrôle des périphériques/appareils	✓	✗	✗	✗	✗
		Évaluation des correctifs	✗	✓	✓	✓	✓
	AVANT EXÉCUTION	Protection anti-malware par Machine Learning	✓	✓	✓	✓	✓
		Prévention contre les exploits	✓	✓	✓	✓	✓
		Protection contre la perte de données (DLP)	✓	✗	✗	✓	✗
DÉTECTION		Anti-piratage (par exemple protection contre le vol d'identifiants et le Code Cave)	✓	✗	✗	✓	✗
		Protection anti-ransomware (détection du comportement et restauration)	✓	✓	✗	Détection sans restauration	Détection sans restauration
		Protection du secteur de boot et contre la réinitialisation du disque	✓	✗	✗	✗	✗
		Surveillance de l'intégrité des fichiers/Surveillance des modifications	✓	✓	✓	✓	✗
RÉPONSE		Sécurité synchronisée (intégration immédiate avec le pare-feu)	✓	✗	✗	✗	✗
		Visualisation de la chaîne de la menace	✓	✗	✗	Requiert Defender ATP	✓
		Recherche des menaces	✓	✗	✗	Requiert Defender ATP	✓

Sécurité centralisée

Protéger vos serveurs fait partie intégrante de la stratégie de sécurité de votre entreprise. Mais si l'on prend en compte les autres systèmes endpoint, les téléphones mobiles, la sécurité du réseau, le chiffrement et plus encore, la gestion de cet ensemble peut se révéler très complexe. En effet, pour de nombreux éditeurs, chaque domaine supplémentaire de sécurité exige une console et un cadre de politiques de sécurité supplémentaires. Les interfaces seront différentes d'une console à l'autre et ces dernières n'offriront aucune intégration de la sécurité entre les divers appareils et composants de l'infrastructure.

Sophos Central vous permet de gérer toutes vos solutions de sécurité Sophos depuis une seule console. Celle-ci est conçue pour offrir une vue unifiée, avec une interface intuitive qui reste cohérente lorsque vous passez d'une solution à l'autre. Et cerise sur le gâteau, les produits Sophos sont élaborés pour fonctionner ensemble, vous offrant ainsi une meilleure sécurité. Par exemple, vos serveurs fonctionnent avec vos pare-feu pour identifier automatiquement les serveurs compromis, les isoler et les nettoyer, le tout en seulement quelques secondes.

Évaluer la sécurité des serveurs : Les 10 questions à poser

Pour évaluer une solution de protection des serveurs, vous pouvez commencer par poser à l'éditeur les questions suivantes :

1. Le produit prend-il en charge différents déploiements de serveurs, par exemple en local, dans le Cloud ou hybride ?
2. La mise sur liste blanche automatique des applications/« Refuser par défaut » est-elle incluse dans le produit, sans frais supplémentaires ?
3. Le produit est-il doté d'une technologie spécifiquement conçue pour stopper les ransomwares puis restaurer les fichiers affectés ?
4. Existe-t-il une technologie pour prévenir les attaques basées sur les exploits et les attaques sans fichiers ? Quelles techniques anti-exploit sont utilisées, et quels types d'attaques peuvent-elles détecter ?
5. Comment le produit protège-t-il contre les attaques persistantes des pirates ?
6. Quelles techniques sont utilisées par le produit pour détecter les malwares inconnus ? Utilise-t-il le Machine Learning pour rechercher en continu les attributs et comportements malveillants ?
7. Pour les produits affirmant exploiter le Machine Learning, peuvent-ils fournir une confirmation des performances de la détection par des organismes indépendants ? Qu'en est-il du taux de faux positifs ?
8. Quel niveau de visibilité sur une attaque l'éditeur fournit-il, tel que l'analyse détaillée des attaques (RCA) ?
9. Le produit répond-il automatiquement aux menaces ? Peut-il automatiquement nettoyer une menace en réponse à un incident ?
10. Le produit s'intègre-t-il de manière native avec le Cloud public (par exemple AWS/Azure/Google), avec la capacité de découvrir automatiquement les ressources Cloud ?

Conclusion

Avec les cyber menaces évoluant toujours plus en complexité et en malignité, il est vital d'avoir en place une protection efficace pour vos serveurs. Comprendre les menaces et les technologies clés nécessaires pour les combattre vous permettra de choisir la meilleure protection des serveurs possible pour votre entreprise. Et cette protection doit être conçue en tenant compte des ressources des serveurs, car il n'est pas suffisant de simplement exécuter une protection Endpoint non adaptée aux environnements de serveurs.

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

19-05-09 FR (PS)

SOPHOS