TROIS MESURES CLÉS POUR TRANSFORMER LA SÉCURITÉ INFORMATIQUE

La sécurité, un enjeu prioritaire pour toutes les entreprises

Alors que les personnes, les terminaux et les objets sont de plus en plus connectés, la protection de l'ensemble de ces environnements et connexions est devenue plus essentielle que jamais. Dans le cadre d'une enquête récente portant sur les priorités informatiques, 69 % des personnes interrogées ont indiqué à Tech Pro Research que l'amélioration de la sécurité constituait leur principale initiative informatique pour 2017[1].

Les participants à cette enquête ont également indiqué que la sécurité serait leur plus gros enjeu informatique pour l'année à venir. En effet, les départements informatiques doivent sécuriser chaque interaction entre les utilisateurs, les applications et les données, quels que soient le mode et le lieu de connexion. Ils doivent en plus composer avec un environnement en constante évolution et de plus en plus dynamique.

Les risques de sécurité auxquels sont exposées les entreprises de tout secteur sont élevés et ils continuent d'augmenter. Selon une étude récente, le coût total moyen d'une violation de sécurité est passé de 3,52 millions de dollars à 3,79 millions de dollars en seulement un an[2]. Pour limiter ce risque, les entreprises qui adoptent des environnements de Cloud et virtualisés doivent impérativement bénéficier d'une visibilité et d'un contrôle maximum.

Des risques en perpétuelle évolution dans un environnement de menaces dynamique

Toutes les entreprises sont devenues numériques, transformation qui a entraîné des changements importants de l'environnement informatique, et par là même de nouveaux enjeux en matière de sécurité informatique.

Prenez pour commencer l'évolution des infrastructures d'applications, qui sont passées de Data Centers sur site exécutant une infrastructure physique à des environnements hautement dynamiques résidant sur des Clouds publics et privés. Et prenez en considération la manière dont les applications elles-mêmes changent. Les entreprises délaissent les piles d'applications monolithiques au profit d'applications multiniveaux distribuées basées sur des microservices. À mesure que les collaborateurs deviennent plus mobiles et se dispersent géographiquement, les environnements utilisateur évoluent. Ceux-ci ne se limitent plus aux postes de travail gérés par l'entreprise et sont maintenant axés sur les terminaux mobiles, les initiatives d'utilisation de terminaux personnels et l'Internet des objets (IdO).

Par conséquent, les modèles classiques de sécurité des périmètres réseau ne sont plus suffisants pour protéger le nombre croissant d'applications et d'utilisateurs ou pour répondre à des exigences de sécurité de plus en plus strictes. Les environnements et les utilisateurs ne sont pas confinés derrière des pare-feu de périmètre. Ils requièrent plutôt une protection plus flexible et agile contre des cybercriminels dont les attaques sont toujours plus sophistiquées. Le cyberespace est la source de plus en plus d'attaques. Même un hacker inexpérimenté, en s'appuyant sur des kits d'outils tels que Zeus et BlackPoS, peut cibler une entreprise avec des attaques avancées susceptibles d'avoir une incidence désastreuse sur sa productivité, ses ressources et sa réputation.

Alors que les entreprises s'adaptent pour faire face à ces nouvelles problématiques, les normes de conformité ne cessent de croître en complexité, obligeant une équipe informatique type à consacrer 20 % de son temps aux efforts de conformité.

LES ENJEUX LIÉS À LA SÉCURITÉ SONT CONSIDÉRABLES

- Passée de 2 % en 2010 à 22 % en 2016, la cybercriminalité constitue la cause des pannes de Data Center qui connaît la croissance la plus rapide[3].
- Le coût moyen d'une panne de Data Center a atteint 740 357 $ en 2016[4].

[1] Tech Pro Research, « IT Budget Research: Where CXOs are placing their bets for 2017 », juillet 2016.
[2] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/.
[3] Ponemon Institute, « Cost of Data Center Outages », janvier 2016.
[4] Ibid.

vmware®

Trois axes stratégiques pour une sécurité informatique efficace

Lorsque l'infrastructure et les utilisateurs évoluent rapidement, difficile de protéger une entreprise à l'aide d'une solution de sécurité robuste et conforme. Les règles traditionnelles en matière de sécurité des réseaux ne sont tout simplement plus adaptées, et les équipes informatiques doivent faire face aux changements suivants :

- Des infrastructures en pleine transformation : l'infrastructure utilisée pour exécuter les applications (serveurs de bases de données et Web, par exemple), qui reposait sur des environnements sur site, évolue pour prendre en charge les applications Cloud et distribuées.
- Une mobilité accrue : le département informatique doit étendre ses règles de sécurité pour pouvoir intégrer les nouveaux appareils et modèles.
- Des exigences de conformité toujours plus nombreuses : en matière de respect de la réglementation, l'environnement est devenu de plus en plus complexe compte tenu des nouvelles exigences imposées aux entreprises.

Assurer visibilité et contexte pour transformer la sécurité

Afin de garder une longueur d'avance sur vos besoins de sécurité changeants, vous devez bénéficier d'une excellente visibilité sur les interactions entre les utilisateurs et les applications. Il vous faut également une solution qui fournit un contexte suffisant pour comprendre la signification de ces interactions. Ensemble, cette visibilité et ce contexte accrus peuvent vous aider à adapter vos contrôles et règles de sécurité en fonction des applications que vous êtes censé protéger.

La base d'une telle solution ? Une couche logicielle omniprésente pour l'infrastructure d'applications et l'ensemble des terminaux indépendante de l'infrastructure physique sous-jacente ou de l'emplacement.

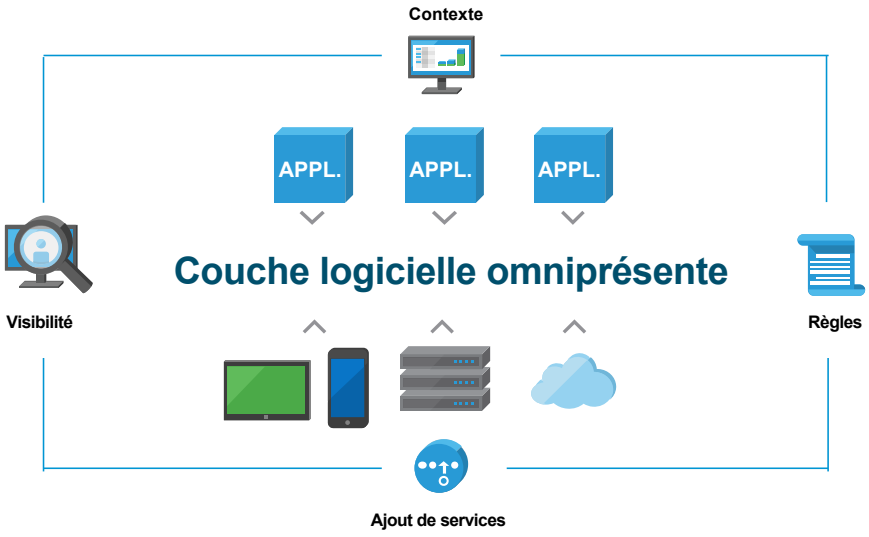


FIGURE 1. Une couche logicielle omniprésente pour une sécurité généralisée

En fait, une sécurité efficace nécessite plusieurs couches de protection. Et la solution logicielle appropriée au sein de l'infrastructure vous offre le meilleur point de contrôle possible pour accroître la visibilité, appliquer des règles et ajouter des services tiers afin de bénéficier d'une couche de protection intelligente supplémentaire.

Voyons plus en détail ces trois mesures clés qui vous permettront de transformer votre sécurité informatique :

- Sécuriser l'infrastructure d'applications : dissocier l'infrastructure des applications afin d'améliorer la visibilité et l'adéquation entre la sécurité et les applications.
- Sécuriser les identités et les terminaux : employer une couche logicielle omniprésente pour l'ensemble des utilisateurs et des terminaux afin d'optimiser la visibilité et le contrôle, sans le moindre impact sur l'expérience utilisateur.
- Rationaliser la conformité : mettre en place un logiciel pour l'infrastructure d'applications, les identités et les terminaux afin de simplifier la conformité.

« Comme de plus en plus d'entreprises cherchent à attirer les mêmes personnes sur un marché limité, le problème de déficit de compétences ne va faire que s'aggraver. Les entreprises seront peut-être obligées de repenser leurs stratégies et de rechercher des solutions [de sécurité] qui soient plus proactives et demandent moins de gestion pour leur permettre de tirer le meilleur parti de leurs ressources[5]. »

JAMES MAUDE
INGÉNIEUR SÉCURITÉ
AVECTO

1. Sécuriser l'infrastructure d'applications

Face à l'évolution des modèles d'infrastructure d'applications, l'approche de sécurité du réseau traditionnelle, axée sur les périmètres, ne peut pas fournir une visibilité et un contrôle suffisants à l'intérieur du Data Center. Dans le même temps, les données inactives stockées sont devenues une cible beaucoup plus intéressante pour les utilisateurs malveillants. Pour résoudre ces problèmes, vous devez transformer la manière dont vous sécurisez votre infrastructure d'applications.

La solution implique en premier lieu la virtualisation et la dissociation de l'infrastructure sous-jacente des applications qui s'exécutent dessus, que cette infrastructure réside sur site ou dans le Cloud public. Cette couche d'abstraction procure une visibilité complète sur le chemin de données, ainsi qu'un point d'application idéal pour compartimenter les applications à travers la micro-segmentation du réseau. En utilisant la micro-segmentation logicielle, les entreprises peuvent simplifier les règles de sécurité et les adapter plus précisément aux besoins applicatifs. Cela leur permet également de déplacer ces règles entre les Clouds privés et publics en même temps que les applications. Une couche d'abstraction offre également une plate-forme pour ajouter des services tiers afin de bénéficier d'une protection plus avancée.

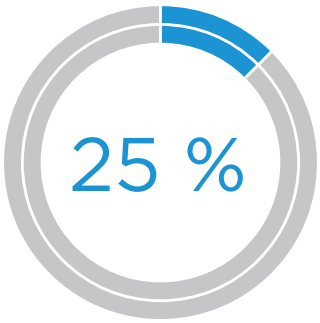
Par ailleurs, la micro-segmentation aide le département informatique à empêcher les menaces de sécurité de percer les défenses de l'entreprise en mettant en œuvre le principe de privilège minimum orienté applications, qui réduit la surface d'exposition aux attaques de l'infrastructure.

Une couche d'abstraction entre les applications et l'infrastructure sous-jacente permet au département informatique d'éviter les attaques, mais elle fournit aussi un point idéal pour chiffrer les données stockées. En chiffrant les données inactives, plus précisément au niveau de la charge de travail, les entreprises ont la garantie que les données de l'infrastructure d'applications sont en sécurité, même si elles tombent entre de mauvaises mains.

2. Sécuriser les identités et les terminaux

La transformation numérique des entreprises s'accompagne d'une prolifération des terminaux mobiles. Des terminaux Android, iOS, Windows, MacOS et autres sont utilisés par des entreprises comme la vôtre pour offrir davantage de moyens au personnel et repenser les processus métier traditionnels. Assurer la prise en charge de l'ensemble de ces terminaux et plates-formes est loin d'être simple, surtout avec la mise en œuvre d'initiatives en matière de mobilité d'entreprise, d'utilisation de terminaux personnels et d'IdO.

[5] http://www.information-management.com/gallery/6-top-it-security-trends-for-2017-10030567-1.html.



D'ici 2020, plus de 25 % de toutes les attaques identifiées dans l'entreprise impliqueront l'Internet des objets (IdO)[6].

En mettant en place une couche logicielle omniprésente pour l'ensemble des utilisateurs et des terminaux afin de vérifier l'identité des utilisateurs et la posture de sécurité des terminaux, vous serez armé pour relever ce défi. Cette approche assure une visibilité et un contrôle de bout en bout sur les utilisateurs et les terminaux, s'étendant jusqu'au Data Center ou au Cloud, où l'infrastructure d'applications réside. Avec une couche logicielle, le département informatique peut ajouter une couche de sécurité évolutive et conditionnelle à chaque niveau transactionnel, des utilisateurs aux ressources auxquelles ils accèdent. Cela contribue à sécuriser les données d'entreprise et à réduire la surface d'exposition aux cyberattaques, sans détériorer l'expérience utilisateur.

Recherchez une solution unique à même de protéger tous vos terminaux : smartphones, tablettes, ordinateurs portables, objets connectés, dispositifs IdO, etc. Votre département informatique pourra alors déployer en toute transparence n'importe quelle application, notamment les applications natives, Web, distantes, virtuelles et les postes de travail Windows, via un seul catalogue d'applications qui offre une authentification unique, une sécurité des données et une conformité des terminaux intégrées. Pour les espaces de travail dynamiques d'aujourd'hui, il vous faut une solution qui étend la sécurité au-delà de l'infrastructure de postes de travail virtuels (VDI) et des terminaux mobiles pour protéger également le Data Center, en s'appuyant sur la micro-segmentation.

Comme chaque entreprise a des besoins de sécurité bien spécifiques, votre solution doit également vous aider à personnaliser votre environnement en fonction de vos priorités. Vous disposerez d'une base pour collaborer avec des partenaires de sécurité, qui pourront tirer parti de la visibilité et des points de contrôle offerts afin de compléter la solution avec leurs propres offres de services.

« Les clients tournent le dos aux entreprises qui subissent des violations de sécurité, et le cadre réglementaire est tel que les entreprises vont avoir besoin d'une excellente protection, qu'elles l'intègrent à leur structure ou externalisent la responsabilité[7]. »

FADI ALBATAL
VICE-PRÉSIDENT SENIOR
ABOVE SECURITY

3. Rationaliser la conformité

La gestion des risques et le maintien permanent de la conformité sont toujours des problématiques majeures, en particulier pour des secteurs tels que les services financiers, l'administration publique et la santé, qui font face à des exigences strictes (PCI, HIPAA, ECPA, directive de l'Union européenne sur la protection des données personnelles, etc.). Les réglementations et les exigences se multiplient, alors que l'environnement numérique et les menaces persistantes avancées continuent d'évoluer. Par conséquent, il est plus difficile que jamais pour les entreprises d'assurer et de prouver leur conformité.

Pour ne rien arranger, avec la transition rapide des entreprises de Data Centers sur site au Cloud, il s'avère encore plus compliqué de respecter les impératifs en matière d'activité, de réglementation et de règles.

Avec une couche logicielle omniprésente pour l'infrastructure d'applications et l'ensemble des terminaux, vous adoptez une approche globale de la conformité. Cette approche unique vous offre un emplacement idéal pour mettre en œuvre des contrôles de conformité et bénéficier ainsi de la visibilité nécessaire pour prouver votre conformité. La solution appropriée fournit une plate-forme technologique à laquelle il est possible d'ajouter dynamiquement les outils et services validés de partenaires pour simplifier encore plus le processus de conformité.

En utilisant un cadre d'architecture de référence pour la conformité, vous pouvez lier les capacités logicielles et matérielles intégrées à des contrôles réglementaires spécifiques et une validation d'audit indépendante. De plus, vous pouvez exploiter un programme validé par un organisme indépendant pour exécuter des charges de travail hautement réglementées en toute sécurité. Que vous utilisiez un environnement de Cloud privé ou public, vous devez avoir l'assurance que votre entreprise peut maintenir une conformité permanente. Pour cela, vous avez besoin d'une solution qui vous offre la vitesse, l'efficacité et l'agilité requises, tout en simplifiant votre processus de conformité.

[6] Gartner Inc., « Selon Gartner, les dépenses mondiales liées à l'IdO atteindront 348 millions de dollars en 2016 », avril 2016.
[7] http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/.

Une sécurité qui s'adapte à l'évolution de l'environnement et des besoins

Une sécurité renforcée a toujours été essentielle pour les réseaux d'entreprise, et avec l'accélération des changements, elle est aujourd'hui plus nécessaire que jamais. À mesure que l'infrastructure, les applications et les profils de main-d'œuvre évoluent, votre équipe informatique doit s'échiner de plus en plus à protéger l'entreprise contre les nouvelles menaces émergentes.

La mise en place d'une couche logicielle omniprésente pour l'infrastructure d'applications et l'ensemble des terminaux peut vous aider à transformer votre sécurité. Cette couche vous permet d'optimiser la visibilité et le contexte des interactions entre les utilisateurs et les applications. Ainsi, vous êtes en mesure d'adapter les contrôles et règles de sécurité en fonction des applications à protéger. De plus, vous pouvez facilement ajouter des services de sécurité tiers à votre solution afin de bénéficier d'une protection intelligente supplémentaire.

COMMENCEZ DÈS AUJOURD'HUI !

Transformez votre sécurité informatique pour l'environnement actuel

EN SAVOIR PLUS >

Rejoignez-nous en ligne :

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.fr

Référence : 16-VMWA-4177_TS-0222_Solution_Overview_3_Key_Steps_Final
1/17