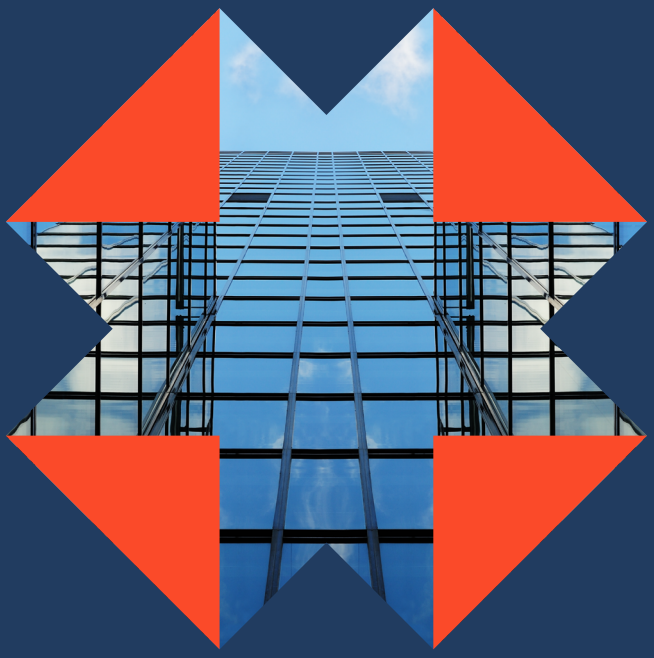

Plan de protection Symantec pour le cloud

Les quatre piliers de la confidentialité et de la sécurité

Équilibrez le rapport bénéfice/risque du cloud

La popularité du cloud est facile à comprendre. Pratique et flexible, il favorise la productivité et permet de réduire les dépenses d'investissement informatiques (CAPEX) puisque les départements IT paient seulement ce qu'ils utilisent. Il est également prisé des utilisateurs des différentes divisions de l'entreprise pour contourner les projets IT traditionnels. Si vous êtes responsable RH ou marketing, par exemple, pourquoi attendre des mois pour obtenir une nouvelle application quand vous pouvez simplement utiliser votre carte bancaire pour en profiter en quelques minutes, avec une tarification à l'usage. Tout est ainsi pour le mieux… jusqu'à ce que vous envisagiez les questions de confidentialité et de sécurité des données.

Évitez les pièges et les risques de sécurité dans le cloud

Pour profiter pleinement des avantages du cloud, les entreprises doivent veiller à se protéger contre une nouvelle génération de menaces et de risques de sécurité qui concernent exclusivement les environnements cloud. Maintenant que les données sensibles, confidentielles et soumises à conformité sont régulièrement consultées et stockées en dehors du réseau de l'entreprise, une approche traditionnelle axée sur la protection du périmètre réseau ne suffit plus.

Voici comment veiller à ce que vos services cloud de logiciels (SaaS), de plates-formes (PaaS) et d'infrastructure (IaaS) bénéficient d'une protection de pointe.

Confidentialité et sécurité des données

Les deux facettes d'une sécurité cloud robuste

S'il est préférable d'envisager la sécurité cloud d'un seul tenant, deux catégories de services cloud nécessitent d'être protégées de différentes manières et pour différentes raisons :

Enjeu nº 1 : Confidentialité des données dans le cloud

L'essor du « Shadow IT » (ces applications cloud non validées par l'IT) présente un risque grave pour la confidentialité des données. En moyenne, les DSI estiment entre 30 et 40 le nombre d'applications cloud utilisées dans leur entreprise. En réalité, il n'y en a pas moins de 1 232[1]. Si vous ne savez pas combien d'applications cloud sont en usage dans votre entreprise, ni quels types de données elles contiennent, comment veiller à la confidentialité et la conformité de ces informations ?

Enjeu nº 2 : Sécurité des données dans le cloud

Les fournisseurs IaaS et PaaS les plus réputés protègent leur datacenters avec des solutions de sécurité à la pointe de la technologie. Pour autant, ils ne sont pas totalement invulnérables, en particulier si des informations d'authentification sont dérobées ou si les systèmes accédant à ces services sont compromis. Vous devez évaluer la sécurité de vos charges de travail hébergées et être en mesure d'appliquer vos propres contrôles de sécurité avancée ainsi que des mesures d'urgence en cas d'attaque, même si vous n'exécutez pas ces charges dans votre infrastructure.

Découvrez les quatre piliers de la protection cloud qui permettent d'atteindre la confidentialité et la sécurité des données dont votre entreprise a besoin.

« ...en moyenne, les DSI estiment toujours entre 30 et 40 le nombre d'applications et services cloud utilisés dans l'entreprise, alors que le chiffre réel est 30 fois supérieur à leur estimation la plus juste. »[1]

[1] Symantec 1H 2017 Shadow Data Report

Les quatre piliers de la sécurité cloud

Nº 1 : Encadrez l'accès aux données, applications et systèmes dans le cloud

Les moyens d'accéder aux données, applications et services sont nombreux. Vous devez donc adopter une approche intégrée de la protection de vos données dans le cloud, que les utilisateurs y accèdent via le Web, le courrier électronique ou une application cloud.

Approche recommandée par Symantec

Chez Symantec, nous pensons que pour préserver la confidentialité des données dans le cloud, il est avant tout crucial de comprendre ce que vous devez protéger.

Symantec CloudSOC CASB Gateway vous apporte de la visibilité sur le Shadow IT, des moyens d'analyse et de gouvernance sur les données utilisées dans les applications cloud, et vous aide à vous protéger contre les menaces qui ciblent les comptes cloud. Une fois que vous avez identifié ce qu'il faut protéger, mettez en œuvre la gouvernance des données avec Symantec Web Security Service. Contrôlez rigoureusement les autorisations d'accès sur de multiples systèmes d'authentification, pour mettre vos utilisateurs à l'abri des menaces et sécuriser leurs données.

Pour aller plus loin dans la protection :

- **Symantec Email Security.cloud :** renforcez les outils de sécurité intégrés dans les plates-formes e-mail, notamment celles d'Office 365 et de Google Apps, afin de bloquer efficacement les malwares, les spams et les attaques ciblées.
- **Symantec Endpoint Protection :** contribuez à protéger vos utilisateurs sur tous les terminaux qu'ils utilisent (Windows, Mac, Android et iOS) pour contrer les menaces avancées et les attaques Zero Day.

Nº 2 : Sécurisez vos données, où qu'elles se trouvent

Chaque jour, vos informations d'entreprise s'échangent entre appareils mobiles et applications cloud. Pour sécuriser ces données, il vous faut plus que des outils périmétriques conventionnels.

Approche recommandée par Symantec

Pour Symantec, la sécurisation de votre entreprise passe par l'élimination de ces angles morts à haut risque afin de mettre les données à l'abri et de préserver votre conformité.

Symantec Data Loss Prevention (DLP) découvre, surveille et aide à protéger les données sensibles et confidentielles utilisées dans les applications cloud, comme Office 365, Box, Dropbox, Google Apps et Salesforce. Il est facile d'appliquer au cloud vos politiques DLP existantes. Vous n'avez donc pas à réécrire l'intégralité de vos règles de confidentialité.

Pour aller plus loin dans la protection :

- **Symantec Information Centric Security :** chiffrez les données sur l'ensemble des terminaux, disques durs, médias amovibles, fichiers, applications e-mail et cloud. Vos utilisateurs peuvent ainsi partager des informations et collaborer de manière productive, sans compromettre la sécurité ou la conformité.
- **Symantec VIP :** favorisez la protection contre les fuites de données en veillant à ce que seules les personnes habilitées puissent accéder aux informations. Vous avez le choix entre plusieurs méthodes d'authentification haut de gamme. Ces outils vous permettent d'appliquer des politiques d'authentification cohérentes sur vos environnements sur site comme dans le cloud.

Les quatre piliers de la sécurité cloud

Nº 3 :
Défendez-vous contre les menaces avancées

Vos applications, données et charges de travail dans le cloud vous sont précieuses. Veillez à ce qu'elles ne soient pas vulnérables aux nombreuses attaques des cyber criminels, dont les méthodes évoluent très vite.

Approche recommandée par Symantec

Symantec reconnaît que la sécurisation de votre entreprise signifie de mettre au jour chaque menace, quelle que soit sa cible, des terminaux aux applications en passant par les réseaux et les services cloud.

Symantec Content and Malware Analysis aide à détecter et bloquer les menaces avancées qui peuvent aisément déjouer les systèmes de détection traditionnels. Il reclasse automatiquement les nouveaux malwares ciblés et les menaces Zero Day, et sert d'intermédiaire pour le sandboxing et la validation bien avant que le contenu potentiellement malveillant atteigne vos utilisateurs. Pour ce faire, il exploite les renseignements collectés chaque jour par le Global Intelligence Network de Symantec auprès de 175 millions[2] de terminaux dans le monde.

Advanced Threat Protection For Email aide à protéger contre les menaces e-mail persistantes et furtives grâce à l'analytique heuristique (prédictive) avancée, à l'inspection globale des liens et au sandboxing dans le cloud, renforcé par le Machine Learning et l'analyse comportementale.

Pour aller plus loin dans la protection :

- **Symantec Endpoint Protection Cloud :** bénéficiez d'une protection des terminaux[3] optimale contre les menaces nouvelle génération sur tous vos terminaux informatiques. Désormais proposée sous forme de service SaaS, cette solution est très facile à prendre en main. Vous pouvez commencer à protéger vos utilisateurs en moins de cinq minutes[4].

Nº 4 :
Protégez les applications et charges de travail placées dans le cloud

Stimulez l'innovation en transférant applications et infrastructure vers le cloud en toute sécurité. Vous pouvez ainsi profiter de la flexibilité du cloud et de son moindre coût sans exposer votre activité aux menaces de sécurité.

Approche recommandée par Symantec

Symantec recommande de protéger chaque charge de travail afin qu'elle s'exécute sans risque.

Symantec Cloud Workload Protection vous apporte une sécurité cloud native et automatisée pour les charges de travail que vous exécutez sur des plates-formes de cloud public comme Amazon Web Services (AWS) et Microsoft Azure. Détectez et localisez les angles morts à haut risque de vos déploiements cloud, puis veillez à protéger et maîtriser chaque charge de travail hébergée.

Pour aller plus loin dans la protection :

- **Symantec Data Center Security :** surveillez et protégez vos serveurs et vos charges de travail en toute transparence, aussi bien sur vos clouds privés qu'au sein de vos datacenters sur site.
- **Symantec Web Application Firewall :** protégez vos applications et données web et bloquez les attaques grâce à une technologie basée sur la plate-forme ProxySG Secure Web Gateway, leader sur son segment[5].
- **Symantec Control Compliance Suite :** identifiez les relations entre sécurité, risque et conformité sur l'ensemble de vos applications et données cloud, et appliquez les politiques nécessaires pour préserver la conformité dans tout votre environnement cloud.

[2] Symantec.com/fr/fr/products/endpoint-protection
[3] AV-TEST Best Protection: Symantec Endpoint Protection and Norton Security, 2015 et 2016
[4] Symantec.com/fr/fr/products/endpoint-protection-cloud
[5] https://www.symantec.com/fr/fr/products/secure-web-gateway-proxy-sg-and-asg

Agissez sans tarder:

Commencez par déterminer votre exposition au risque.

Notre évaluation du risque Shadow IT vous apporte une vision complète du Shadow IT dans votre entreprise. Vous disposez ainsi des connaissances nécessaires pour reprendre le contrôle de la confidentialité et éliminer les risques.

Demandez votre évaluation »

Symantec