LIVRE BLANC :
PROTÉGER LES INFORMATIONS
D'ENTREPRISE DANS LE CLOUD

Protéger les informations d'entreprise dans le cloud

À qui s'adresse ce document ?

Alors que de plus en plus d'entreprises adoptent le cloud, les responsables IT doivent se préparer à protéger les informations dans le cloud

Symantec™

Sommaire

Introduction

La technologie évolue par vagues en permanence. Et les RSSI doivent suivre ses changements, sous peine de se laisser dépasser.

Il suffit d'examiner l'histoire récente pour constater cette nature oscillante de la technologie. Dans les années 80, les mainframes IBM étaient prédominants. Dans les années 90, l'informatique client-serveur entrait en scène avec les données distribuées sur les PC. Puis le web devint le modèle prédominant et le balancier est reparti en direction de la centralisation des serveurs. Mais, presque aussitôt, les mobiles se sont imposés avec les applications téléchargées sur les appareils des employés, le nouveau client-serveur en quelque sorte.

À présent, avec la prolifération des appareils mobiles au sein de l'entreprise, l'on assiste à une nouvelle mutation du modèle IT. On passe à un provisionnement des informations nécessaires au moment voulu, à partir de serveurs centralisés consolidés dans le cloud. Le balancier continue d'osciller et les charges de travail IT migrent en masse vers le cloud.

Les responsables IT doivent embrasser le cloud

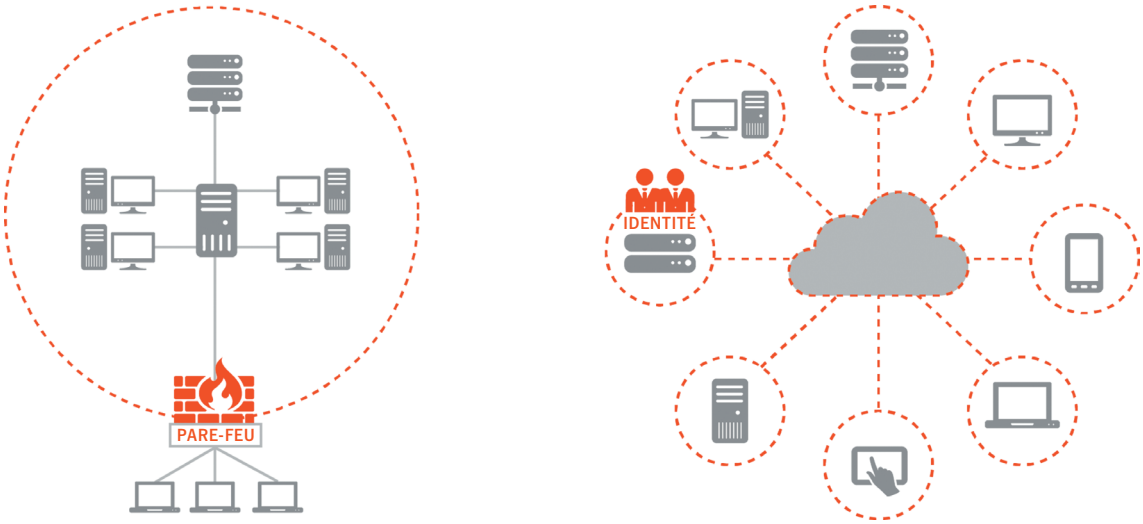
Les responsables IT, et notamment les RSSI, se doivent d'évoluer rapidement pour tirer parti de l'adoption accélérée du cloud par leur entreprise, et pour cela, ils doivent adapter leur approche.

Certes, le nouveau modèle peut présenter des ressemblances avec l'ancien environnement client-serveur. Mais, sous bien des aspects, il s'agit d'un univers très différent, impliquant des technologies liées au cloud, sans parler du cloud lui-même. Le Gartner parle de « centre névralgique des forces » : le cloud, la mobilité, les réseaux sociaux et l'information. IDC parle, quant à lui, de « troisième plate-forme ». Mais peu importe comment on la qualifie, aux yeux de la plupart des analystes, cette convergence de l'informatique mobile, des réseaux sociaux, des services cloud et de l'analyse du big data a radicalement transformé notre activité et nos existences.

Ce n'est d'ailleurs pas un concept totalement nouveau. Ce qui est nouveau, c'est le rythme auquel les entreprises adoptent le cloud comme plate-forme de choix, et, par le fait, acceptent de nouvelles réalités. Elles sont obligées d'admettre qu'elles ne possèdent ou ne gèrent plus la plupart de leurs applications car les applications comme Salesforce, Box et Office 365 sont à présent dans le cloud. Les organisations IT commencent également à externaliser la gestion de leurs infrastructures car, pour pouvoir rester compétitives, elles ont besoin de profiter des avantages apportés par des fournisseurs cloud comme Amazon et Rackspace. Et même, les sociétés se trouvent dépossédées de leurs terminaux mobiles puisque les employés utilisent au travail leurs propres appareils.

Ce qui est le plus important, du point de vue de la sécurité, c'est que l'organisation ne peut plus se contenter d'une défense périmétrique puisque le travail n'est plus confiné en un lieu précis entre ses quatre murs. Les bureaux sont virtuels et Internet est le lieu où s'effectue la collaboration.

Dans ce contexte, quelles sont les priorités des chefs d'entreprise avisés ? En l'absence de tout périmètre, la vulnérabilité des données est extrême. C'est pourquoi ces dirigeants se préoccupent de sécuriser les aspects du cloud qu'ils peuvent contrôler afin de protéger leur propriété intellectuelle. Ces aspects sont l'identité et l'information.



Les responsables IT peuvent protéger leurs entreprises en sécurisant et authentifiant l'identité des personnes qui accèdent aux applications et aux informations de leur entreprise. Ils peuvent également mettre en place des solutions et des politiques régissant les mouvements des informations sensibles afin d'empêcher leur déplacement vers des endroits non sécurisés où elles peuvent être volées.

Oui, le cloud transforme à grande vitesse la manière dont s'exerce l'activité de l'entreprise. Et, non, les contrôles de sécurité pour ce nouvel univers ne sont pas encore suffisants. Mais les chefs d'entreprise disposent de solutions pour protéger leurs informations dans le cloud. Voici un cadre de travail qui sera utile aux responsables IT pour préserver la sécurité de leur informations.

La sécurité du cloud repose sur trois facteurs essentiels

Pour qu'une stratégie de sécurité des données soit efficace, son concept de base est sensiblement identique, qu'il s'agisse de sécuriser l'entreprise ou de sécuriser le cloud. Dans les deux cas, la stratégie doit combiner harmonieusement trois composants clés : la protection des identités, la protection des informations et un moteur de corrélation déclenchant des réponses automatiques pratiques. Cela dit, le cloud présente quand même des défis spécifiques lorsqu'il est nécessaire de mettre en place une politique de sécurisation des employés qui utilisent leurs appareils personnels en dehors du réseau de l'entreprise. Examinons chacun de ces composants.

1. Protection des identités

La protection des identités est la serrure sur la porte d'entrée du cloud. Elle empêche les attaquants d'entrer et s'assure que les employés ont accès aux applications cloud dont ils ont besoin. Lorsqu'elle est correctement paramétrée, elle améliore également l'expérience utilisateur en permettant la transparence des ouvertures de session. L'idéal est de disposer d'identifiant unique sans mot de passe, utilisable quel que soit l'appareil, le lieu et le moment, permettant d'accéder aux données et aux apps nécessaires.

L'expérience utilisateur est vitale ici car l'utilisateur est le maillon faible de la chaîne de sécurité. Si le processus sous-jacent à la sécurité est facile d'utilisation et efficace, vous pouvez limiter les risques créés par les utilisateurs. Vous pouvez implémenter une sécurité qui, tout en étant robuste, reste simple et n'incite pas certains utilisateurs à la contourner.

Prenons le cas d'une violation de données pour voir comment fonctionne la protection des identités lorsqu'une solution de protection des informations est en place. La protection des identités vous permet d'identifier la personne ou l'appareil responsable de l'action suspecte ou risquée, et d'évaluer quelles données sont touchées à partir de quel appareil. Il est important d'identifier qui (utilisateur/appareil) est l'auteur de l'attaque, quelle est la cible visée et comment réagir avec une précision chirurgicale.

Grâce à la protection des identités, vous êtes également en mesure d'établir des corrélations entre différents incidents et de les associer à un utilisateur ou un appareil particuliers. C'est capital car, fréquemment, les attaques ne se réduisent pas à une seule activité, mais à un grand nombre de petites actions, apparemment inoffensives, mais qui, combinées, constituent une menace à prendre au sérieux.

2. Protection des données

La protection des identités ne suffit pas à elle seule. Les données sont ce qui doit être protégé, et cela, en tout lieu. Il en résulte que, pour être complète, une solution de protection des informations doit découvrir, surveiller et protéger les données dans les divers environnements où elles résident : cloud, mobiles et dans les locaux de l'entreprise. Vous avez sans doute étudié des solutions qui traitent de la protection des données dans l'enceinte physique de votre entreprise. Il est intéressant d'étendre cette notion à une protection des informations dans le cloud.

La protection des données veille à la sécurisation du stockage ou des transferts de données critiques au sein de l'entreprise, ou dans le cloud, en des endroits qui seraient potentiellement accessibles à des cybercriminels. Une solution flexible de protection des informations intègre des politiques granulaires qui prennent en compte le contenu et vous permettent de choisir comment traiter les données en fonction de leur type. Est-il possible de déplacer en toute sécurité des informations vers le cloud avec un simple rappel que ce déplacement rend les données plus vulnérables ou est-ce que le déplacement est trop risqué pour pouvoir être autorisé ?

3. Moteur de corrélation

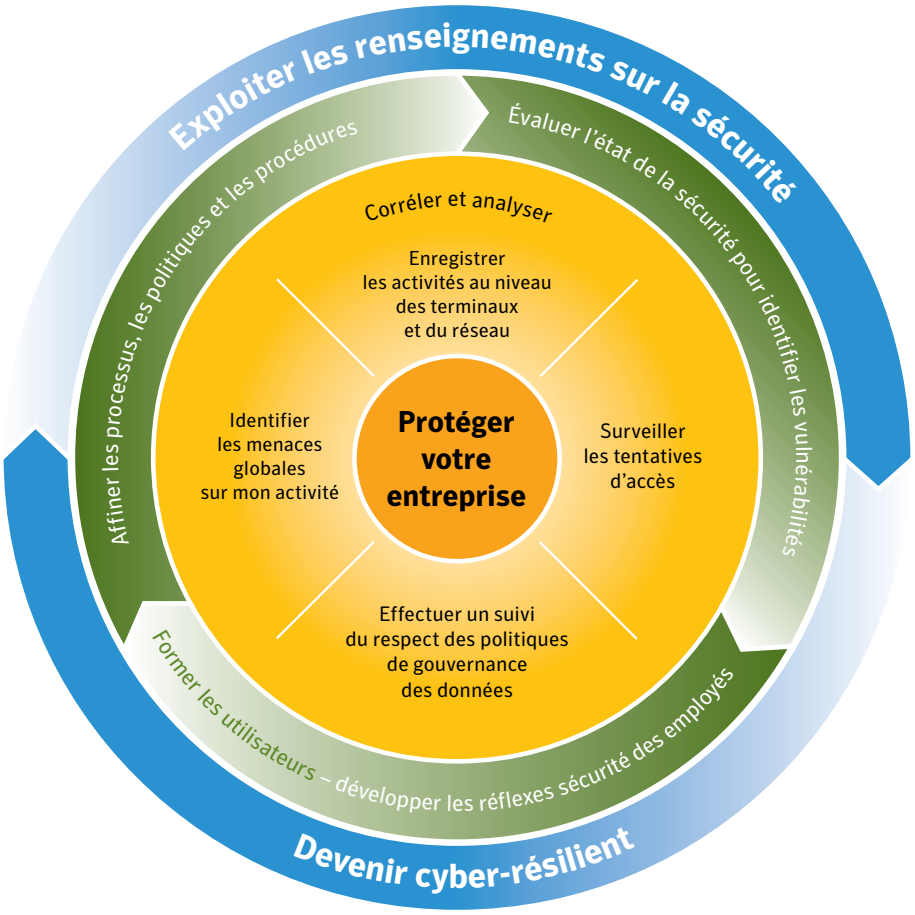
Un moteur de corrélation permet de suivre des activités de manière détaillée et d'établir entre elles des corrélations par utilisateur. Le moteur de corrélation ne doit pas se contenter de consolider des alertes centrées sur les identités et sur les données, mais il doit également ajouter du contexte ou de l'intelligence.

Une corrélation en temps quasi-réel nécessite un éclairage contextuel de ce qui est en train de se passer. Combiner intelligence des identités et des données au contexte permet de détecter les menaces plus rapidement, et donc de prendre plus rapidement les mesures pour les prévenir. En effet, seule la rapidité de la détection et des mesures de défense permet d'endiguer les dégâts infligés à votre entreprise. Reconstituer le puzzle sur plusieurs systèmes, même une heure après l'attaque, est trop risqué.

La sécurité du cloud ne se développera pas en vase clos

Dans l'idéal, votre solution de protection des informations n'aura pas à fonctionner en vase clos. Pour être authentiquement résiliente, surtout si elle a adopté un modèle de cloud hybride, une entreprise devra disposer d'une solution qui détecte rapidement les menaces ciblées de sorte que, même si un utilisateur ou un appareil a été compromis, l'entreprise pourra identifier à quel moment la menace a pénétré le réseau.

Une protection optimale des informations (surveillance des tentatives d'accès et suivi de l'utilisation qui est faite des données) s'inscrit dans une stratégie plus large identifiant les menaces externes et observant l'activité sur les terminaux, une stratégie qui évalue régulièrement les processus à des fins d'amélioration et de formation continue des employés pour qu'ils améliorent leurs réflexes de sécurité.



Un cas concret sur comment fonctionne la sécurité du cloud

Imaginons que votre solution de protection des informations ait remarqué qu'un ingénieur – appelons-le Jacques – a essuyé toute une série d'échecs d'identification avant d'arriver à accéder au réseau. Cela sort de l'ordinaire, sans être nécessairement alarmant. Mais voici que Jacques essaie d'ouvrir un fichier auquel il n'a pas le droit d'accéder. L'accès lui est refusé et sa tentative est consignée dans un journal.

Peu après, Jacques accède à un fichier contenant des informations sur le développement commercial d'un nouveau produit. Bien que l'accès à ce fichier ne lui soit pas bloqué, il sort quand même du cadre normal de son travail. Du coup, Jacques est marqué comme utilisateur à haut risque par le moteur de corrélation. Voilà que Jacques émet une commande qui copie le fichier du nouveau produit vers une app cloud non autorisée par l'entreprise. Cela déclenche automatiquement une action.

Le fichier est retiré de l'app cloud et mis en quarantaine, et une demande d'authentification est soumise à Jacques. Si ce dernier n'arrive pas à s'authentifier, il sera bloqué jusqu'à ce que le service IT arrive à déterminer s'il s'agit d'un infiltré malveillant ou si ses données d'identification ont été compromises. À ce stade, il apparaît qu'un incident a été consigné plus tôt dans la semaine concernant un e-mail suspect, qui, alors, ne semblait pas faire partie d'une attaque ciblée. Mais, lorsque l'identité de Jacques est corrélée à tous les destinataires dudit message, le service IT commence à soupçonner Jacques de n'être qu'une victime. À l'aide des données collectées concernant l'e-mail suspect, les membres de l'équipe sont en mesure d'identifier d'autres victimes possibles de ce qui pourrait bien être une menace persistante avancée (APT).

Les solutions Symantec™ sont un choix tout indiqué pour la sécurité du cloud

L'activité des entreprises connaît un enrichissement indéniable grâce au cloud qui leur ouvre de nouveaux modes de développement et accroît la productivité des employés. Ceux-ci adoptent ces nouvelles opportunités, ne craignant pas de les exploiter même en dehors du contrôle du service IT, ce qui les amène à utiliser leurs appareils personnels pour accéder aux données dans des applications cloud non autorisées par l'entreprise. C'est à la direction de celle-ci qu'il incombe en dernier recours de protéger l'entreprise et ses données, et cela signifie de trouver une solution de sécurité du cloud qui limite les risques, sans nuire à la productivité dans un environnement cloud de plus en plus complexe.

Symantec™ Identity: Access Manager, combiné avec Symantec Data Loss Prevention, constitue le socle de la protection de vos informations dans le cloud. Access Manager, plate-forme leader du contrôle des accès, offre une protection des identités pour les applications cloud. Access Manager s'intègre étroitement à deux solutions Symantec d'authentification : Symantec Validation and ID Protection Service et Symantec Managed PKI Service, pour ajouter une authentification à deux facteurs à toutes vos apps cloud.

Symantec Data Loss Prevention, solution leader de prévention des pertes de données, aide à protéger les données sensibles en découvrant, surveillant et protégeant les informations, que celles-ci soient dans l'entreprise ou en transit. La synergie des offres Symantec de protection des identités et de protection des informations crée une couche de sécurité inégalée qui protège vos données sensibles, aussi bien dans l'enceinte de l'entreprise que dans le cloud.

Et qui vous protège vous, le chef d'entreprise, lorsque le balancier repart soudainement en arrière.

Pour en savoir plus sur l'aide que Symantec peut apporter à votre entreprise, consultez go.symantec.com/sam et go.symantec.com/dlp.

À propos de Symantec

Symantec Corporation (NASDAQ: SYMC) est le leader mondial en cybersécurité. Exploitant l'un des plus importants réseaux mondiaux de cyber-renseignements, nous sommes à même de déceler davantage de menaces et de protéger davantage les clients contre la nouvelle génération d'attaques. Nous aidons les entreprises, les administrations et les particuliers à sécuriser leurs données les plus importantes quel que soit l'endroit où elles se trouvent.

Pour obtenir les adresses et numéros de téléphone de nos agences locales, visitez notre site web.

Tour Égée
17 avenue de l'Arche
La Défense 6
92671 Courbevoie Cedex,
France
+33 (0)1 41 38 57 00
www.symantec.com/fr

21354920FR 01/16