Rapport Shadow IT France 2017

En collaboration avec le CESIN

Powered by Symantec

Édito

Depuis le développement de services en mode SaaS dans les Clouds publics, les problématiques de fuite de données sont devenues de vrais challenges pour les entreprises et les RSSI en particulier. Il s'est d'abord agi de reprendre le contrôle des achats de ces services opérés directement par les utilisateurs qui, pour la plupart, utilisaient des circuits d'achats non informatiques (achats de fournitures par exemple) et passaient donc au travers des préconisations du RSSI en matière de protection des données. Avec la complicité des services achats, la plupart des entreprises ont désormais repris le contrôle et ont pu faire rentrer ces services dans le patrimoine informationnel officiel de l'entreprise avec les avantages que cela représente en matière de sécurité (gestion des habilitations, protection des données, contractualisation avec les bonnes clauses, etc.) sans pour autant brider la créativité des métiers.

Restait à traiter un pan qui s'est avéré encore plus problématique : il s'agit du Shadow IT, phénomène qui s'est développé avec la gratuité de nombreux services en ligne et auxquels les utilisateurs se sont inscrits sans toujours se rendre compte du danger que cela pouvait représenter pour le patrimoine informationnel de l'entreprise. Cela peut aller de la création d'un Réseau Social d'Entreprise hors contrôle de cette dernière avec des offres gratuites comme LinkedIn ou Facebook, à la constitution de services collaboratifs pour des besoins ponctuels en recourant à la gratuité avec à la clé une protection des données réduite à sa plus simple expression. La principale calamité en la matière restant les sites de partage de fichiers qui pullulent sur le WEB et dont la protection laisse le plus souvent à désirer.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique. Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique, et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels. Le CESIN compte plus de 400 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

Or, jusqu'à une période récente, le RSSI était aveugle sur ces usages de services gratuits. Tout au plus disposait-il de statistiques de consommation Internet obtenues à partir des outils de filtrage WEB mais la foisonnance des sites consultés ne pouvait pas lui donner beaucoup d'indications sur l'utilisation réelle de ces services et sur l'ampleur du phénomène.

Depuis quelques années de nouveaux outils sont apparus qui devraient redonner au RSSI davantage de visibilité sur ces usages : il s'agit de produits dit CASB (Cloud Access Security Broker) qui sont des points de concentration, déployés dans l'entreprise ou dans le Cloud, placés entre les utilisateurs et les services du Cloud, utilisés pour appliquer les politiques de sécurité de l'entreprise. Ces CASB adressent des sujets très divers comme l'authentification, l'autorisation d'accès, le SSO mais aussi la visibilité des applications utilisées dans le Cloud. L'idée est de montrer par « qui » et « comment » sont utilisées ces applications tout en proposant une vision globale de l'utilisation de celles-ci ainsi que certains conseils pour se prémunir des risques principaux.

Le CESIN, en coopération avec l'un de ses partenaires, Symantec, a donc décidé de mener une étude sur l'utilisation du Shadow IT en France avec le concours de ses membres. Après une collecte des logs sur plusieurs mois, deux rapports ont été produits : un à destination de l'entreprise participante avec ses propres données, et un autre anonymisé et consolidé qui a permis de produire cette étude. Ces rapports permettent aux décideurs d'observer les tendances des usages internes et peuvent les aider à détecter des comportements déviants, voire des menaces. Ce besoin de visibilité s'inscrit typiquement dans la lutte contre le Shadow IT.

Alain Bouillé
Président du CESIN

Symantec

La Génération Cloud

Les projets de transformation numérique, engagés par toutes les organisations, publiques ou privées, petites à grandes, multinationales ou locales, ont un facteur en commun : l'utilisation croissante du Cloud Computing. Si, il y a encore quelques années, la question de l'opportunité stratégique pouvait se poser, force est de constater que nous sommes aujourd'hui de facto entrés dans la Génération Cloud. La flexibilité, la décentralisation et l'optimisation des coûts sont parmi les avantages qui font le succès du Cloud. Le Gartner Group estime la croissance du chiffre d'affaires des services de Cloud public entre 2017 et 2020 à + 58% (de 220 à 411 milliards de dollars). Les entreprises ainsi que les individus ont très rapidement su tirer parti du Cloud, ou plutôt des Clouds : Symantec recense plus de 22 000 applications Cloud, ayant un aspect business et permettant le partage d'informations !

Autant d'opportunités de gains de productivité pour les entreprises et les employés, mais menant vers une organisation sans frontières. En effet, les collaborateurs, les terminaux, les données, les serveurs, les applications sont dorénavant à l'extérieur de l'entreprise, posant un problème global de visibilité, de contrôle et donc de sécurité du système d'information, impliquant des risques pouvant impacter la confidentialité, l'intégrité et la disponibilité.

Ces applications sont souvent disponibles en version gratuite, avec des fonctionnalités de base qui peuvent suffire à l'utilisateur (mais qui n'aura généralement pas consulté les conditions d'utilisations), ou proposées via des circuits commerciaux qui, logiquement, s'adressent directement à leurs clients potentiels : les métiers.

Dans tous les cas, l'accès aux applications ou services peut échapper à la vigilance des équipes informatiques ou de sécurité. La prolifération des usages va conduire à l'émergence d'un système d'information parallèle, directement ou indirectement connecté au SI de l'organisation, ou « Shadow IT » et de son corollaire « Shadow Data » qui présente le vrai danger pour les informations.

Le rapport Symantec Shadow Data Report* démontre un écart saisissant entre la perception des responsables informatiques du nombre d'applications utilisées dans leurs entreprises et la réalité du terrain.

Il est plus que jamais fondamental de conserver le contrôle de la protection des informations les plus sensibles des organisations publiques ou privées, pour des raisons évidentes de confidentialité, mais aussi pour répondre aux évolutions règlementaires.

Le « Shadow IT » n'est pas une fatalité. La première étape est de l'admettre et de l'identifier pour pouvoir mettre en place les mesures de sécurité humaines, procédurales et technologiques permettant de continuer à tirer parti des avantages apportés par le Cloud, en limitant au maximum les risques induits.

Laurent Heslault
Directeur des Stratégies Sécurité, Symantec France

Shadow IT : perception vs. réalité

Le rapport Symantec Shadow Data Report*, réalisé lors du 1er semestre 2017, auprès d'entreprises au niveau mondial, montre un écart très important entre la perception des DSI du nombre d'applications cloud utilisées par rapport à la réalité :

- Perception : 30 à 40 apps
- Réalité : + de 1 200
- + 30% depuis 2016

Méthodologie

En partenariat avec le CESIN, Symantec a proposé aux membres de participer à une étude sur le Shadow IT en France en bénéficiant d'un audit gratuit, sur le modèle du Cloud Services Risk Assessment Report via sa plateforme CloudSoC.

Les membres participants à l'étude ont capturé pendant plusieurs semaines des logs de pare-feu ou de proxy, qui, après anonymisation, ont été analysées par une instance privée et chiffrée de l'outil CloudSOC. Chaque participant a reçu un rapport d'audit personnalisé très détaillé. Les données, également anonymisées, ont été regroupées par le CESIN avant d'être éditées par Symantec pour produire ce rapport.

*1H 2017 Shadow Data Report

Shadow IT Perception vs. Réalité

Les DSI estiment en moyenne à 30-40 le nombre d'applications et services Cloud utilisés dans leur entreprise. Qu'avons-nous observé lors de cette étude auprès des membres du CESIN sur l'utilisation du Shadow IT en France ?

Min. **287**

Max. **5 945**

Moyenne de CloudApps par entreprise

1 697

Quels sont les apps et services Cloud les plus utilisés ?

	Par utilisateur	Par trafic web
1	Google	Google
2	Facebook	Facebook
3	MSN	YouTube
4	Bing	OneDrive
5	Twitter	Google Drive

Les sites de transfert de fichiers Hightail et WeTransfer apparaissent respectivement en 8ème et 10ème position du classement par trafic.

Quels types d'apps et services Cloud sont le plus utilisés ?

	Par utilisateur	Par trafic web
1	Réseaux Sociaux	Moteurs de recherche
2	Moteurs de recherche	Réseaux Sociaux
3	Partage de fichiers	Partage de fichiers
4	Messagerie	Vidéos
5	Vidéos	Messagerie

Les 4 premiers (moteurs de recherche, réseaux sociaux, partage de fichiers et vidéos) représentent 88% du trafic total.

Symantec

Par catégorie, quels sont les apps et services Cloud les plus utilisés ?

Réseaux sociaux	Par utilisateur	Par trafic web
1	Facebook	Facebook
2	Twitter	Yammer
3	LinkedIn	Workplace by Facebook
4	Google+	Twitter
5	Yammer	LinkedIn

- Apparition de Workplace by Facebook dans le Top 10 par utilisateur.
- Facebook représente 90% du trafic web du Top 10.

Partage de fichiers	Par utilisateur	Par trafic web
1	Google Drive	OneDrive
2	Google Cloud Storage	Google Drive
3	OneDrive	Hightail
4	Evernote	WeTransfer
5	Dropbox	Google Cloud Storage

Présence significative des sites Mega et Uptobox dans le Top 10 par trafic.

Vidéos	Par utilisateur	Par trafic web
1	Dailymotion	YouTube
2	YouTube	Dailymotion
3	Vimeo	Vimeo

Si Dailymotion est 1er (de peu) en termes d'usage, YouTube représente 8 fois plus de volume.

Messagerie	Par utilisateur	Par trafic web
1	Outlook.com	Outlook Web App
2	Outlook Web App	Google Mail
3	Google Mail	Yahoo Mail

Présence dans le Top 10 d'outils de messagerie spécifiquement utilisés dans certains pays et d'applications d'automatisation d'emailing.

Remarques additionnelles :

- Utilisation largement majoritaire de Tumblr comme plateforme de blogging
- Utilisation notable de Pinterest et d'Instagram en termes d'usage et de trafic
- Services en ligne : Deezer et Giphy arrivent en tête, devant des outils de traduction ou de conversion de format

ATTENTION à la longue traine des « CloudApps »

Même si les résultats pour le top des classements semblent prévisibles, il convient d'évaluer la totalité des applications et services détectés, à la fois en terme de légitimité et de risque potentiel au sein de chaque entreprise. L'utilisation même très sporadique d'un service Cloud « exotique » peut suffire à compromettre un système d'information, notamment par exemple lorsque les attaques via la « Supply Chain » se multiplient.

Les 7 Commandements du Shadow IT

Michel Juvin, Expert en Cyber Sécurité, membre du CESIN

01 Instaurer la confiance

Le dialogue doit être le plus ouvert possible avec les utilisateurs afin de montrer que les services IT sont à leur disposition pour étudier ensemble leurs attentes fonctionnelles. Les utilisateurs doivent avoir confiance dans le fonctionnement de leur informatique et les relations avec leurs partenaires pour être efficaces. La confiance s'appuie sur l'écoute et la compréhension des cas d'utilisation.

02 Analyser les flux

Il est nécessaire que le DSI utilise les indicateurs qu'il a à sa disposition, notamment ceux relatifs aux logs des firewalls et autres switchs qui permettent de filtrer les échanges vers l'extérieur. Un tableau avec la description du flux va permettre de faire une analyse de risques sur les flux et prendre les décisions pour contrôler les échanges d'information sortants de l'entreprise.

03 Réduire le risque

Compte tenu des échanges d'une entreprise avec d'autres fournisseurs de services ou de partenaires, il est nécessaire de faire une analyse de risque des flux les plus critiques. Le RSSI doit classer les flux entre ceux déjà enregistrés pour lesquels le risque est connu et accepté, ou les transférer vers des nouveaux acteurs de la sécurité.

04 Piloter l'infrastructure

L'architecture et le paramétrage de l'infrastructure, clef de voûte de tous les accès au SI d'entreprise, permettent l'existence du Shadow IT ou l'interdire. Le recours à un outil de monitoring de la sécurité des « Apps » telles que les solutions de type CASB (Cloud Access Security Broker) est devenu une nécessité. La DSI doit, au même titre que tous les autres accès, les filtrer et les classer dans le tableau de suivi, pour en surveiller l'activité et être en mesure de réagir en cas de problème de sécurité avec un des fournisseurs.

05 Coopérer avec les départements juridique, achat et finance

La définition d'une procédure d'acquisition des solutions informatiques est une étape clef dans le contrôle du Shadow IT. Le RSSI doit être informé par l'un des acteurs de la demande pour effectuer une analyse des risques sur l'information échangée. Il proposera un plan d'actions pour les réduire s'il estime qu'il y a un risque sur le capital informationnel de l'entreprise. Il est nécessaire que cette procédure d'acquisition soit simple d'utilisation pour faciliter la mise en œuvre de solutions innovantes. A l'opposé, un processus lourd et peu agile entraînera les employés vers le Shadow IT.

06 Eduquer les utilisateurs

En parallèle, l'éveil des utilisateurs aux risques relatifs à la gestion des données de l'entreprise est une des actions nécessaires pour réduire le risque de Shadow IT. Il est illusoire de penser qu'on pourrait avoir un officier de sécurité surveillant toutes les actions des utilisateurs, de fait, il est nécessaire de leur donner les moyens de rester vigilant lorsqu'une action peut exposer les données de l'entreprise au monde externe.

07 Positionner le curseur (on-prem vs. off-prem) pour délimiter « l'aire de jeu* »

L'idée est de définir pour chaque domaine si l'entreprise est capable de gérer le risque de perte d'information ou de déni de service relatif à l'outsourcing de son information, ses services, son organisation ... A titre d'exemple, voici des domaines qui doivent être documentés pour positionner le curseur entre « géré en interne » ou en « externe » : les terminaux, la gestion et le maintien opérationnel des serveurs, les données, les applications, la gestion des identités, la supervision des solutions de sécurité... Le RSSI doit définir en fonction de l'activité de l'entreprise et avec l'aide des utilisateurs si les informations, les services ou la gestion de l'information est mieux gérée en interne ou avec l'aide d'un service hébergé dans un Cloud externe.

* Abrégé de l'environnement de travail des utilisateurs qui s'est étendu vers les solutions de type Cloud-as-a-Service

Nous ne pouvons plus avoir une vision binaire du monde, blanc ou noir, blacklist or whitelist, ... il faut mesurer le risque pour donner un indice de confiance. Globalement, une bonne discussion entre un demandeur, son management et le Business Analyst de l'équipe IT permettra d'officialiser le choix de la solution finale tout en estimant les risques au-delà du coût immédiat de la solution.

Shadow IT & Shadow Data : (re)prenez le contrôle !

Pour adresser les nouveaux enjeux sécurité liés à l'adoption des apps et services Cloud, le Gartner prévoit que 85% des grandes entreprises utiliseront une plateforme CASB (Cloud Access Security Brokers) en 2020*. Au-delà de sa solution CloudSOC, Symantec vous propose également une approche CASB 2.0 afin de parfaitement intégrer la protection cloud dans votre infrastructure et vos politiques de sécurité.

Identifier et contrôler le Shadow IT

CloudSOC Audit permet de gagner en visibilité sur les services cloud utilisés dans l'entreprise en :

- Recensant et surveillant l'utilisation des apps cloud, les utilisateurs et usages à risque,
- Analysant les attributs de risque des apps cloud,
- Participant à l'éducation des utilisateurs sur les politiques d'entreprise d'usage du cloud,
- Fournissant des rapports de sécurité et de conformité de l'activité cloud.

L'intégration avec Secure Web Gateway et Endpoint Protection permet de renforcer la visibilité au niveau des activités web et d'automatiser la mise en place de politiques d'accès dynamiques, basées sur les attributs de risque, tout en permettant de mieux contrôler les usages même en dehors du périmètre de l'entreprise.

Protéger les données

CloudSOC aide à prévenir les pertes et vols de données en :

- Classant les données sensibles et traçant leur utilisation, en conformité avec les politiques de protection de l'information de l'entreprise et réglementations,
- Identifiant les utilisateurs de données à risque,
- Contrôlant et remédiant aux risques d'exposition des données sensibles dans les apps cloud.

L'intégration des solutions de protection de l'information permet de déployer les mêmes politiques DLP on-premise et dans le cloud, d'automatiser les mécanismes de chiffrement des données en transit, de contrôler les accès, et d'adapter les méthodes d'authentification au contexte, le tout sans contraindre l'expérience utilisateurs.

Détecter les menaces et y remédier

Grâce à l'analyse contextuelle UBA (User Behavior Analytics), CloudSOC aide à se prémunir des menaces en :

- Détectant les activités malveillantes en fonction du contexte d'utilisation d'une ou plusieurs apps,
- Identifiant et renforçant les politiques selon le niveau de risques et la criticité des activités,
- Alertant, bloquant ou mettant en quarantaine les comptes compromis.

L'intégration avec les solutions Advanced Threat Protection et de sandboxing permet de mieux détecter les menaces zero-day et d'analyser tout comportement suspicieux. Grâce au GIN (Global Intelligence Network), l'intelligence sur les toutes dernières menaces est étendue aux apps et services cloud.

Répondre aux incidents

CloudSOC offre des fonctionnalités d'investigation et de réponse à incidents en :

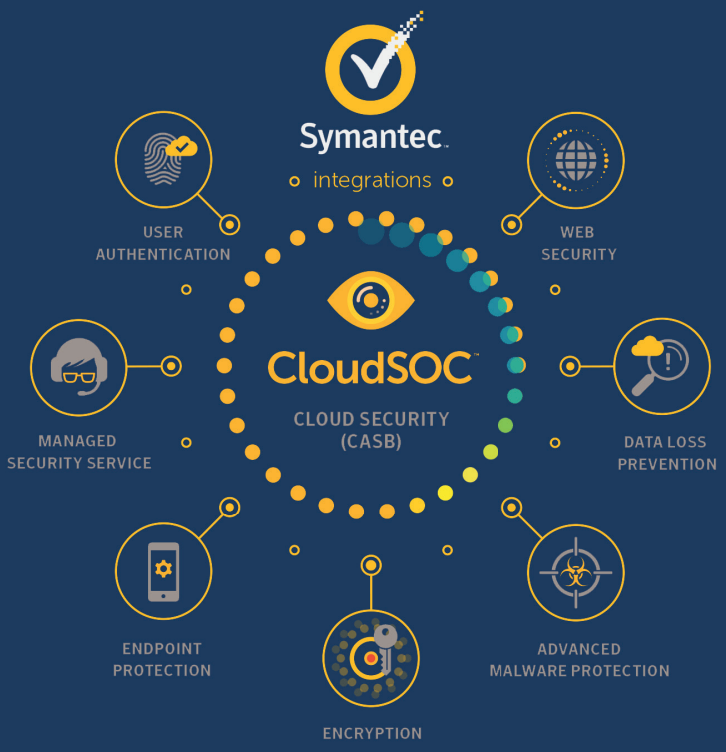
- Traduisant en logs les données fournies par les API, en temps réel pour une action rapide,
- Fournissant la granularité et la consolidation des données, nécessaires à l'investigation sur les activités,
- Contrôlant l'activité grâce aux dashboards et rapports personnalisables,

L'intégration avec une solution de SIEM permet un enrichissement des données et une analyse forensique plus poussée.

*Gartner, 'Market Guide for Cloud Access Security Brokers', 10/24/2016

Plus de sécurité, moins de complexité

Déployez une solution de sécurité cloud s'intégrant avec votre infrastructure existante. Symantec CloudSOC vous aide à améliorer votre posture de sécurité, à réduire la complexité opérationnelle, et à proposer une expérience utilisateur optimale.



Pour plus d'information sur Symantec CloudSOC et les autres solutions Symantec intégrées, rendez-vous sur : **go.symantec.com/casb**

A propos de Symantec

Symantec Corporation (NASDAQ: SYMC), leader mondial de la cyber sécurité, aide les entreprises, les gouvernements et les particuliers à sécuriser leurs données les plus importantes, quelle que soit leur localisation. Les organisations du monde entier se tournent vers Symantec pour des solutions stratégiques et intégrées afin de se défendre contre des attaques sophistiquées au niveau des terminaux, du cloud et des infrastructures. De plus, une communauté mondiale de plus de 50 millions de personnes et familles comptent sur les solutions Norton et LifeLock pour leur protection digitale sur l'ensemble de leurs terminaux. Symantec opère l'un des réseaux civils de cyber intelligence les plus étendus au monde, qui lui permet de détecter et de protéger contre les menaces les plus avancées.

Pour plus d'informations, retrouvez-nous sur www.symantec.com/fr ou sur les réseaux sociaux Facebook, Twitter et LinkedIn.

Symantec

Symantec France S.A.S
17 avenue de l'Arche, La Défense 6, 92671 Courbevoie Cedex, France
+33 (0)1 41 38 57 00 | www.symantec.fr