NTT Security

Livre blanc

Complexité, coût et conformité : les trois « C » qui mettent un coup de projecteur sur la « Security as a Service »

La gestion de la sécurité se complique de jour en jour.

L'essor des charges de travail des mobiles, de l'IoT et du cloud accroît les volumes de données utilisateurs tout en intensifiant leur utilisation et en resserrant les exigences de conformité. Les dirigeants de la fonction sécurité doivent alors trouver le juste équilibre entre l'analyse proactive du champ des menaces et le traitement du nombre croissant de tâches immédiates qui leur incombent.

Mais la poursuite de cet objectif à l'aide de solutions sur site devient rapidement un véritable casse-tête pour les entreprises. Elle pèse sur leurs budgets et sur leurs effectifs IT qualifiés déjà trop sollicités.

Tout naturellement, les DSI et les RSSI partent en quête de solutions alternatives.

Pour les y aider, ce livre blanc explore la popularité grandissante des solutions « Security as a Service » (SECaaS). Nous y compilons également les recommandations de NTT Security aux entreprises qui chercheraient à migrer leurs solutions de sécurité dans le cloud.

C'était mieux avant

Sous l'influence d'une explosion du nombre de terminaux connectés à travers des réseaux hautement distribués, l'informatique d'aujourd'hui se veut mobile. Les salariés apportent leurs propres appareils et applications sur leur lieu de travail et transfèrent constamment des données de et vers le cloud. Le tout dans un contexte de vaste déploiement industriel de l'IoT, créateur de nouveaux vecteurs d'attaque à neutraliser.

Il va sans dire que la gestion de la sécurité gagne peu à peu en complexité, tandis que la fréquence et l'efficacité des attaques s'accroissent. Preuve en est : les violations de données de l'année 2017.

Revue de presse

- En janvier, aux États-Unis, un établissement d'enseignement supérieur a dû verser l'équivalent de 28 000 $ en bitcoin à des pirates afin de déverrouiller ses fichiers suite à une attaque par ransomware[1]. Survenu pendant les vacances d'hiver, l'incident a largement perturbé les systèmes de messageries vocale et électronique mais également le service en ligne des bourses, tout en bloquant l'accès de 1 800 étudiants et salariés à leurs ordinateurs. Cette attaque témoigne du besoin d'intégrer des services de sécurité sans matériels sur site, à l'aide d'une solution de protection dans le cloud. À la clé : une gestion centralisée de la sécurité, une détection managée des menaces et une meilleure visibilité sur les infrastructures IT.
- D'après le rapport NTT Security 2017 sur l'état des menaces dans le monde, les attaques de phishing étaient responsables de 73 % des infections par malware des entreprises[2]. Or, l'implémentation et l'exécution de solutions anti-phishing sur site peuvent s'avérer complexes et coûteuses. En février 2017, le fisc aux États-Unis alertait les experts-comptables contre les e-mails de phishing se faisant passer pour des communications légitimes d'éditeurs de logiciels de gestion fiscale en plein pic d'activité[3]. Aujourd'hui, il devient impératif d'adopter des solutions anti-phishing dans le cloud, déployables rapidement, évolutives en fonction des besoins et dotées de fonctionnalités intégrales comme la surveillance et la détection des attaques de phishing avancées, et la neutralisation et la remédiation de ces incidents.

À l'heure où les équipes IT reçoivent 578 alertes de sécurité par jour[4] en moyenne, les DSI et les RSSI peinent à conserver une vision plus globale du champ des menaces. De fait, le suivi des tendances en matière de cybercriminalité et le développement de stratégies pérennes de neutralisation des attaques ou de réduction de leur impact demandent du temps et des ressources.

1. LA Times 2. Rapport NTT Security 2017 sur l'état des menaces dans le monde 3. Communiqué de presse du fisc des États-Unis : « Security Summit Alert: Tax Professionals Warned of New Scam to "Unlock" Their Tax Software Accounts » 4. SC Magazine, Balabit CSI Report

Défis de gestion de la cybersécurité moderne à l'ère du cloud

La mise en conformité pose encore d'autres difficultés aux DSI et RSSI. Tant les entreprises publiques que privées se voient imposer des exigences règlementaires de plus en plus nombreuses – à l'international, au sein de zones de libre-échange comme l'UE et le NAFTA, et souvent en parallèle à des règles sectorielles et des variations d'implémentation nationales.

Rien que pour le RGPD, le Gartner prédit que plus de la moitié des entreprises concernées n'auront pas achevé leur mise en conformité, même au bout d'un an.[5]

Pourtant, les équipes dirigeantes des entreprises ont également pris conscience de l'impact de leur sécurité sur leurs activités et leur réputation, surtout à mesure que leur migration dans le cloud étend leur empreinte numérique. À la vue des violations de sécurité qui frappent d'autres entreprises, elles voudront savoir si elles aussi courent un risque.

Les DSI et les RSSI devront alors leur fournir des réponses claires et convaincantes (étayées par des données, par exemple) afin de créer un climat de confiance.

La complexité, vecteur d'inefficacité de votre sécurité

1. Baisse de la productivité IT
2. Vulnérabilités non détectées
3. Gouvernance et politiques hétérogènes
4. Définition floue des responsabilités
5. ROI seulement partiel des investissements technologiques
6. Problèmes potentiels de communication avec les équipes dirigeantes
7. Intégration technologique médiocre
8. Trop-plein de terminaux actifs à gérer et à surveiller

Sur fond de menaces mouvantes et de marchandisation de certains types d'attaques, l'essor des menaces persistantes avancées (APT) nécessite des investissements dans des technologies tout aussi sophistiquées. Toutefois, ces dernières reposent généralement sur des opérations de configuration et de maintenance complexes.

Dans la pratique, qu'elle soit basique ou avancée, la gestion de l'infrastructure de sécurité se concentre sur le traitement de toutes les alertes générées par les pare-feux, les systèmes de détection et autres. Or, les équipes de sécurité doivent désormais faire face à une avalanche de notifications, y compris de nombreux faux positifs et doublons en provenance de différentes machines et différents environnements (cloud, hybrides, sur site et virtuels). En plus d'être gourmand en temps et en ressources humaines, le traitement de ces notifications pourra détourner l'attention des analystes des alertes rouges qui pourraient indiquer une violation grave.

Dans ce contexte, beaucoup d'entreprises ont déjà demandé le soutien et les conseils d'intervenants externes de confiance afin d'évaluer leur niveau de protection et d'améliorer l'efficacité de leurs opérations de sécurité. Aujourd'hui, elles attendent encore davantage de ces fournisseurs de solutions de sécurité : une gestion de bout-en-bout du cycle de sécurité de leurs ressources critiques dans de multiples environnements cloud et sur site, le tout adossé à une réduction de la complexité, des coûts et des risques. Ce nouveau modèle, c'est la SECaaS, ou « Security as a Service ».

Gros plan sur la SECaaS

Parce qu'elle permet aux entreprises d'accéder à des services de sécurité dans le cloud, la SECaaS pourrait bien faciliter la vie des RSSI et renforcer le niveau de sécurité informatique de chaque entreprise.

Ce modèle consiste à confier le déploiement et la gestion des technologies clés habituellement exécutées sur site à un fournisseur de services de sécurité managés. Ainsi, les DSI et les RSSI ont rapidement accès à des fonctions de sécurité de pointe à la demande, le tout en maintenant leurs coûts d'investissement et d'exploitation au plus bas.

Pour cela, la SECaaS allie l'automatisation à une surveillance humaine continue. Des experts examinent et analysent les alertes 24h/7j. Ils les trient en fonction de leur niveau de risque avant de prendre les mesures de gestion adaptées. Résultats : une meilleure visibilité sur les menaces, avec à la clé la simplification de leur neutralisation et la réduction de leur impact.

Parce qu'elle repose sur l'expérience et les interventions d'analystes chevronnés, la SECaaS épargne aux RSSI le recrutement, l'embauche et le maintien d'un vaste pool de compétences internes. En arrière-plan, l'infrastructure elle-même bénéficie constamment des dernières versions et des derniers correctifs de logiciels, ce qui minimise les perturbations de vos opérations et les risques de non-conformité liés à l'humain.

Parmi les technologies disponibles en mode SECaaS :

- Continuité et reprise d'activité (PCA/PRA)
- Surveillance continue
- Prévention de la perte de données (DLP)
- Sécurité des e-mails
- Cryptage
- Gestion des accès et des identités (IAM)
- Gestion des intrusions
- Sécurité des réseaux
- Évaluation de sécurité
- Gestion des événements et des informations de sécurité (SIEM)
- Analyse de vulnérabilités
- Sécurité web

Une offre de service complète pourrait également intégrer à la fois la continuité et la reprise d'activité (PCA/PRA), la prévention des pertes de données (DLP), la sécurité web et des e-mails, le cryptage, la gestion des accès et des identités (IAM), les évaluations de sécurité et les analyses de vulnérabilités.

Répartition des responsabilités

Si la liste des services possibles est longue, toute entreprise qui envisage la SECaaS ne pourra jamais externaliser l'intégralité de sa mise en conformité. En vertu des lois sur les données et la confidentialité ou des règlementations comme le RGPD, elle devra toujours assumer la responsabilité de la protection de ses informations sensibles.

Bien que les fournisseurs externes puissent exécuter des fonctions de sécurité vitales, il revient au client SECaaS de configurer et d'implémenter correctement le service choisi. Il lui incombe également de revoir régulièrement et de maintenir à jour tous ses contrôles et politiques transférés vers un fournisseur de solutions SECaaS. Si vous envisagez de passer à ce modèle, mieux vaut donc demander aux fournisseurs s'ils vous accompagneront sur ces questions dans le cadre de leur service.

5. Communiqué de presse : « Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation »

Autres considérations : choisissez le bon modèle

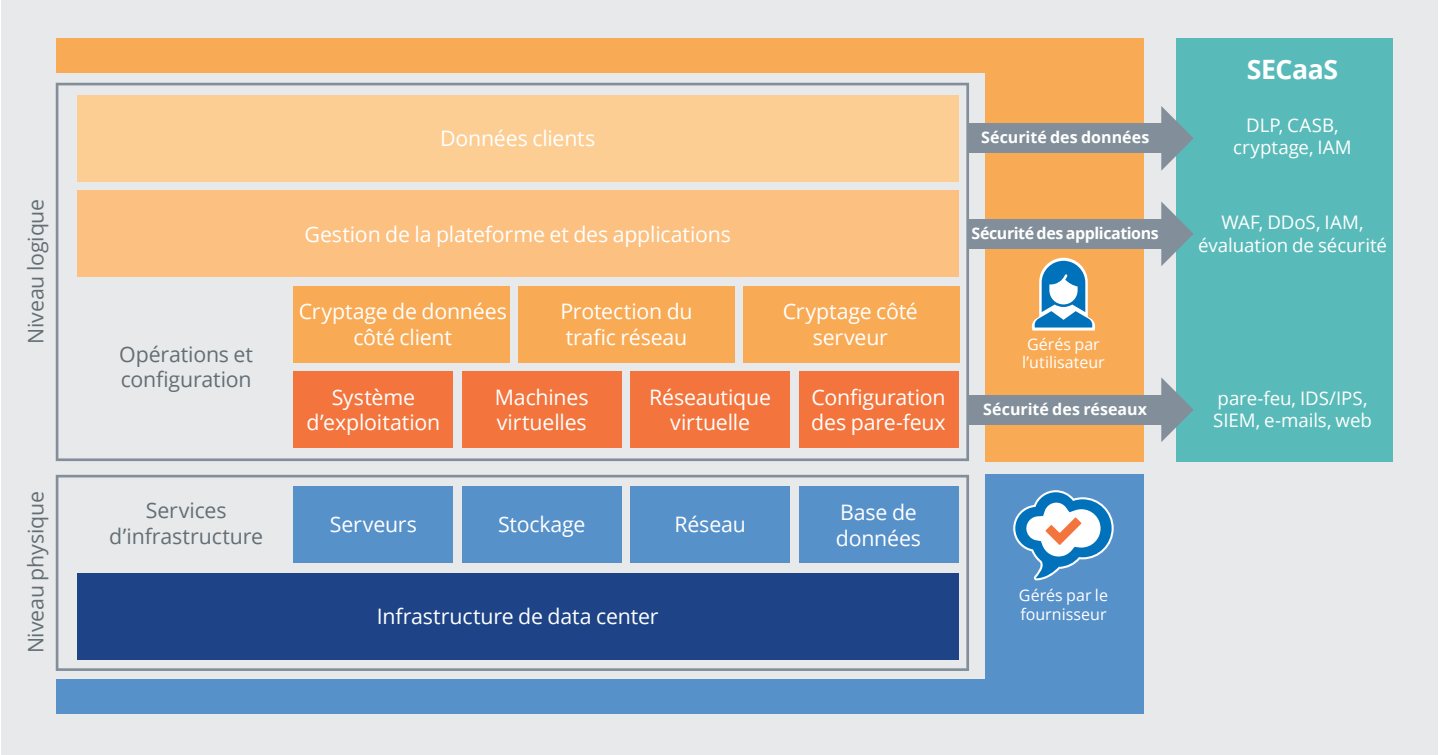
L'adoption de fonctionnalités cloud en entreprise s'accompagne également de risques, de responsabilités et de problématiques de sécurité. Il est donc essentiel de saisir les responsabilités assumées par les trois principaux modèles de cloud computing (IaaS, PaaS et SaaS), ainsi que leurs dépendances vis-à-vis de la SECaaS.

- **L'IaaS** accroît la flexibilité et le contrôle des ressources d'infrastructure des utilisateurs ou entreprises clientes. Toutefois, il leur revient de sécuriser leurs applications, runtime, middleware et infrastructure. À titre d'exemple, citons Amazon EC2 et l'IaaS Microsoft Azure.
- **La PaaS** fournit une plateforme pour le développement et le déploiement d'applications web. Les responsabilités peuvent être partagées entre l'utilisateur et le fournisseur. Les solutions SECaaS comprennent davantage de contrôles basés sur les applications, comme l'analyse de ces applications et des passerelles web sécurisées (SWG).
- **Le SaaS** propose quant à lui un service consommable aux fonctionnalités intégrées. Ce modèle offre le plus haut niveau de sécurité intégrée – les fournisseurs SaaS devant assumer une plus grande responsabilité dans ce domaine. Toutefois, l'utilisateur doit renoncer à la flexibilité et au contrôle sur ses services. À titre d'exemple, citons Office 365 et Salesforce.

Le niveau de responsabilité assumé par l'entreprise cliente dépend donc directement du modèle de service choisi. Des gains de flexibilité et de contrôle s'accompagnent de la nécessité de contracter des services de sécurité supplémentaires en mode SECaaS.

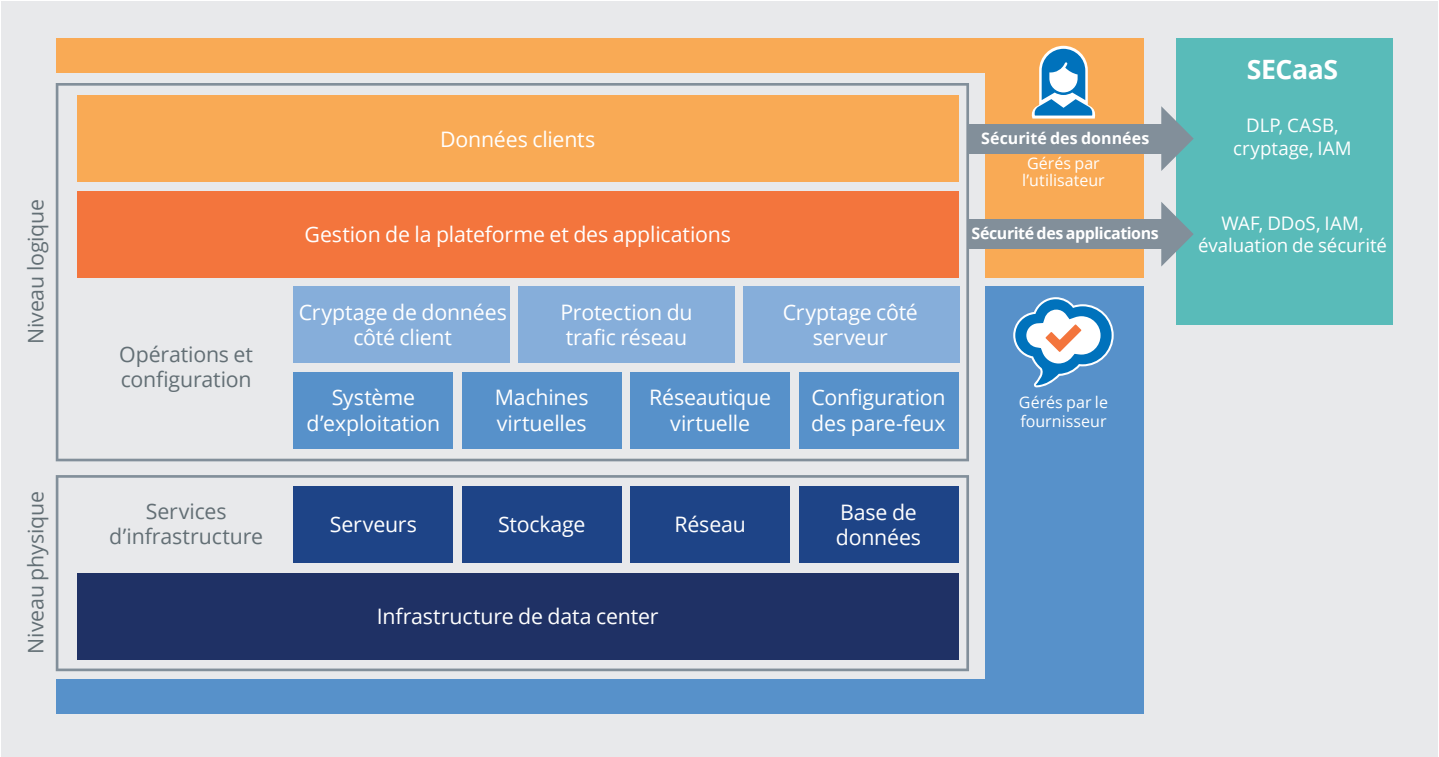
Par exemple, les entreprises qui adoptent un modèle de services d'infrastructure sont sans doute mieux placées pour exploiter tous les avantages de la SECaaS. Le schéma ci-dessous illustre les types d'offres SECaaS directement liées aux responsabilités d'infrastructure assumées par l'utilisateur.

Schéma 1 : Modèle de sécurité partagé – Infrastructure as a service (IaaS)



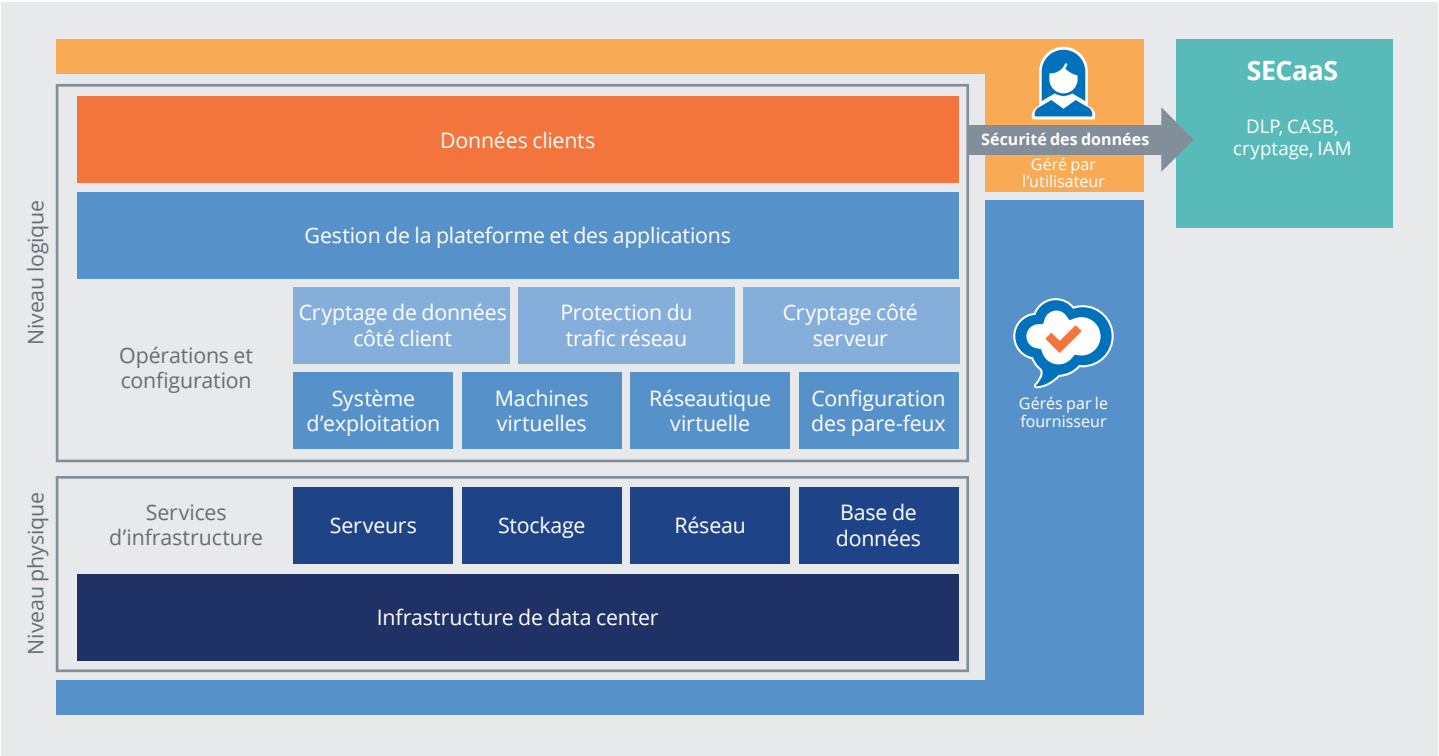
En revanche, les modèles SaaS ou d'abstraction des services reposent moins sur la SECaaS pour la sécurisation des ressources sous la responsabilité de l'utilisateur, puisque le fournisseur intègre déjà de nombreuses fonctions de sécurité à son service. Toutefois, ces fonctionnalités de protection intégrées se montrent souvent incapables de neutraliser les menaces persistantes avancées (APT), surtout celles à l'intérieur du réseau de l'utilisateur du service. En effet, ces fonctions se concentrent davantage sur la prévention que sur la détection et l'intervention.

Schéma 2 : Modèle de sécurité partagé – Platform as a service (PaaS)



Bien que les services abstraits ou containerisés intègrent parfois des technologies comme les pare-feux d'applications web (WAF) ou la protection contre les attaques DDoS, il est possible que leurs utilisateurs soient amenés à configurer et surveiller ces services afin d'optimiser leurs capacités de contrôle et de neutralisation.

Schéma 3 : Modèle de sécurité partagé – Software as a service (SaaS)



Fournisseur de solutions SECaaS : comment faire le bon choix ?

Toutes les entreprises qui envisagent de confier la gestion de leur sécurité à un fournisseur de services de sécurité managés (MSSP) ou SECaaS externe poursuivent des objectifs similaires : baisse des coûts, automatisation des processus, simplification de la mise en conformité, ou encore accès à des services et technologies de pointe. Toutefois, la sélection d'un tel fournisseur revient souvent à déterminer sur quelles fonctionnalités clés l'entreprise est prête à faire l'impasse.

Par exemple, le choix d'un MSSP qui ne propose pas de services en mode SECaaS pourra vous permettre de vous délester de tâches chronophages. Mais il vous en coûtera des investissements en matériels supplémentaires, en appui du service managé.

Un fournisseur de sécurité intégrale spécialisé, dont les experts pourront évaluer votre infrastructure existante afin de planifier, concevoir et déployer de façon stratégique des services managés sur site adaptés, représente sans aucun doute votre meilleure chance de libérer tout le potentiel des solutions SECaaS.

Vous pourrez ainsi bénéficier de services scalables à la demande, mais aussi exploiter des solutions de sécurité avancées comme des services managés de détection et d'intervention sur incident (analytique avancée, cyberveille appliquée, interventions rapides sur incidents, etc.). Le tout sans investir en capital et en externalisant l'intégralité de la gestion et de la surveillance de votre sécurité.

Autres questions à poser à votre fournisseur SECaaS potentiel :

1. Dans quelle mesure ses fonctionnalités d'automatisation accélèrent-elles les temps de réponse et avec quelle précision trient-elles les notifications en fonction du niveau de risque ?
2. Dans quels délais peut-il intervenir en cas de détection d'un problème ?
3. À quelle fréquence met-il à jour ses technologies pour tenir compte de la nature mouvante des attaques et exploiter les dernières innovations ?
4. Le fournisseur assure-t-il une surveillance 24h/7j et quelles garanties de sécurité offre-t-il ?
5. Quel niveau d'expérience, d'expertise technologique et d'ancienneté les conseillers du fournisseur affichent-ils ?
6. Le fournisseur propose-t-il une interface centralisée pour vous permettre de gérer de multiples solutions SECaaS ?

Cette dernière question s'avère cruciale. En effet, il n'est pas rare que les entreprises opèrent des technologies à la fois d'ancienne et de nouvelle générations, ce qui complique davantage leur gestion et la visualisation de leurs informations exploitables sur les risques et la sécurité.

Certes, le fournisseur SECaaS se charge de la gestion et de l'exploitation des matériels et logiciels utilisés pour la fourniture du service. Mais les clients ont tout de même besoin d'une console web pour afficher leur environnement de sécurité managée et réaliser toute tâche de contrôle de leur conformité qui leur incombe.

Conclusion

Comme l'a démontré le rapport NTT Security 2017 sur l'état des menaces dans le monde, la sécurité repose sur la synergie des technologies, des processus et des équipes. En clair, le simple ajout de technologies pour résoudre un problème, sans tenir compte des processus ni du type et du niveau de ressources humaines indispensables à leur gestion, pourra faire plus de mal que de bien. Par ailleurs, la plupart des entreprises sont tout bonnement incapables d'intégrer de nouvelles technologies de sécurité au rythme de l'évolution éclair des menaces – sans parler de maintenir leur efficacité optimale.

Il y a encore peu, la sécurité représentait l'un des principaux obstacles à l'adoption du cloud. Mais les avantages du modèle SaaS ont accéléré son adoption et imposé des innovations inexistantes quelques années auparavant. Les fournisseurs cloud leaders ont désormais intégré la sécurité à leur infrastructure, avec à la clé la création d'environnements au moins aussi bien protégés que ceux traditionnels sur site.

À l'heure où la règlementation et les attentes en matière de gouvernance insistent toujours plus sur les questions de sécurité, la SECaaS offre aux entreprises une excellente occasion de renforcer leur protection et leur conformité, tout en simplifiant leurs opérations et en maîtrisant leurs coûts.

Cas d'utilisation de la SECaaS

Un RSSI s'inquiète de la vitesse à laquelle son entreprise adopte des applications SaaS, sans aucune méthode ni politique pour évaluer le niveau de sécurité de chaque application.

L'entreprise utilise de nombreuses applications SaaS sans avoir analysé suffisamment les risques. Par conséquent, elle manque de visibilité sur ces applications et les données qui s'y trouvent.

Malgré tout, le RSSI hésite à bloquer l'accès aux services cloud. En effet, l'entreprise a enregistré une hausse importante de sa productivité depuis que ses départements peuvent choisir les outils les mieux adaptés à leurs besoins.

Toutefois, le prochain audit RGPD lui donne à réfléchir. Le RSSI s'inquiète du manque de ressources pour rassembler toutes les informations requises avant la date butoir.

Il décide alors de déployer des CASB (Cloud Access Security Broker) pour y remédier. Ces points de contrôle installés entre les utilisateurs de services cloud et leurs fournisseurs appliquent les politiques de sécurité de l'entreprise au moment de l'accès aux ressources cloud. À la clé :

- Visibilité sur l'utilisation du cloud
- Évaluation des risques des fournisseurs SaaS
- Reporting de conformité
- Prévention de la perte de données
- Définition de politiques granulaires par solution SaaS et accès rapide aux outils CASB dans le cloud pour le RSSI.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.