FROST & SULLIVAN

La sécurité des entreprises :

L'approche optimale pour un service haut de gamme

Un Livre Blanc de Frost & Sullivan

Auteur : Jean-Noël Georges

SOMMAIRE

LA PROTECTION FORTE : UNE NECESSITE POUR LES ACCES LOGIQUES ET PHYSIQUES

Depuis plus de dix ans, le nombre de violations graves de données augmente à l'échelle mondiale. Cette grande tendance en matière de sécurité n'a pas épargné l'année 2015. Les données sensibles sont désormais numériques, donc accessibles à travers les ordinateurs, les téléphones, les tablettes, les réseaux, les serveurs et, plus récemment, les applications et les services Cloud. En 2015 aux Etats-Unis, 781 violations des données ont été enregistrées, avec un impact potentiel sur 169 millions de dossiers personnels. Des études récentes de Frost & Sullivan ont évalué à près de 250 millions le nombre de données volées ou compromises sur le premier semestre 2015. 2016 suit la même tendance, avec des institutions mondiales directement attaquées ou ciblées. L'annonce récente du groupe hôtelier Hyatt concernant le vol de paiements dans 250 de ses établissements est un signal d'alarme pour toutes les entreprises. Les différents experts en sécurité l'affirment : la question n'est pas de savoir si votre système a été l'objet d'une attaque, mais plutôt quand elle aura lieu.

L'heure est venue de revenir à l'essentiel en matière de sécurité. Le contrôle des accès logiques et physiques est une nécessité primordiale. Un simple identifiant et mot de passe ne suffisent plus pour se protéger contre les intrusions et les attaques nuisibles. L'authentification forte au moyen d'une Infrastructure à Clés Publiques (ICP) protégera activement l'accès aux zones et aux données sensibles. Seules les personnes autorisées pourront accéder aux applications et aux services sélectionnés. Par ailleurs, le recours au chiffrement s'impose pour l'archivage ou l'échange de données sensibles. Pour assurer la haute sécurité de l'ensemble d'une infrastructure critique, il faut disposer d'un système qui facilite la gestion des clés de chiffrement.

LA REGLEMENTATION AU SERVICE DE LA MISE EN ŒUVRE DE L'AUTHENTIFICATION FORTE

De nouvelles réglementations telles que la loi Sarbanes-Oxley (SOX), la loi HIPAA et le Personal Data Notification & Protection Act aux Etats-Unis ainsi que la Directive sur la protection des données personnelles au niveau européen, ont obligé les entreprises à respecter les normes afin de réduire le nombre de violations de données. Toutes ces recommandations, ou normes, s'alignent pour protéger les données sensibles et personnelles générées par des individus. Naturellement, la solution la plus appropriée semble être une convergence entre les solutions d'identification et d'authentification sécurisées pour les accès logiques ou physiques.

Cette approche optimise la stratégie d'authentification d'une société tout en assurant aux utilisateurs futurs un système simple pour accéder aux zones sensibles grâce aux « credentials » sécurisés, numérisées et faciles d'emploi. En Europe, au sein de l'écosystème des paiements, l'Autorité Bancaire Européenne (ABE) a publié en décembre 2014 une directive stipulant qu'au 1er aout 2015, les entreprises de l'Union Européenne devaient commencer à rechercher et à déployer des solutions d'authentification à deux facteurs.

L'EXPLOSION DE NOUVEAUX USAGES MODIFIE LA FAÇON DONT LES ENTREPRISES DOIVENT SECURISER LEURS CONNEXIONS

L'explosion des appareils électroniques et les nouveaux usages associés ont obligé les entreprises à repenser leur politique de sécurité pour mieux s'adapter aux exigences. En effet, les employés sont de plus en plus nomades, et la mobilité représente une tendance du marché qui doit être prise en compte par les entreprises, car créatrice de nouvelles menaces envers les systèmes d'authentification existants. La vague « BYOD » (Bring Your Own Device) est une stratégie gagnant-gagnant pour les salariés et les employeurs. Elle augmente clairement la flexibilité et la satisfaction au travail tout en réduisant le coût de la gestion des appareils mobiles. Mais encore une fois, les nombreux appareil
ayant accès au réseau de l'entreprise augmenteront le risque de violations de données en créant de nouvelles portes d'entrée aux différents services. Pour une entreprise, il est difficile, voire impossible, de gérer la variété d'appareils mobiles, de systèmes d'exploitation et de versions de logiciels existant. Une enquête menée par Frost & Sullivan a révélé que les obstacles et les défis auxquels les entreprises sont confrontées pour mettre en œuvre la BYOD à grande échelle sont liés à la sécurité. La Mobile Device Management (MDM) ou « Gestion de Terminaux Mobiles » ainsi que la Mobile Application Management (MAM) ou « Gestion des Application Mobiles » sont des services que les grandes entreprises doivent prendre en compte afin de définir un ensemble de règles de sécurité communes fondées sur une stratégie de sécurité de l'entreprise.

De surcroît, des millions de téléphones portables sont volés ou perdus chaque année. Ces appareils peuvent contenir des données sensibles facilement accessibles s'ils ne sont protégés que par une simple combinaison d'identifiant et de mot de passe. Une stratégie d'authentification forte associée à des règles de contrôle d'accès strictes réduira le risque de menaces sécuritaires.

LES SERVICES CLOUD REVOLUTIONNENT LA GESTION DU RISQUE SECURITAIRE

Les entreprises ont vite compris les avantages d'une transition vers le Cloud et, plus précisément, vers le Cloud Computing et le SaaS, ou Software As A Service (logiciel comme un service). Chez Frost & Sullivan, nous avons identifié une tendance majeure baptisée la « logiciellisation » qui impacte déjà fortement la majorité des marchés verticaux.

Il existe aujourd'hui un logiciel pour pratiquement chaque industrie, chaque besoin et chaque activité spécifique. Cette tendance va se renforcer et influencera la façon dont les entreprises sécurisent l'accès et les privilèges associés à ces applications pour satisfaire le besoin de services à la demande.

L'authentification forte des employés accédant aux services Cloud est une obligation pour les entreprises souhaitant imposer le contrôle d'accès tout en facilitant les activités d'audit, de surveillance et de gestion des credentials. En outre, la mise en œuvre de systèmes de chiffrement robustes est indispensable pour mieux protéger les données conservées dans un environnement partagé.

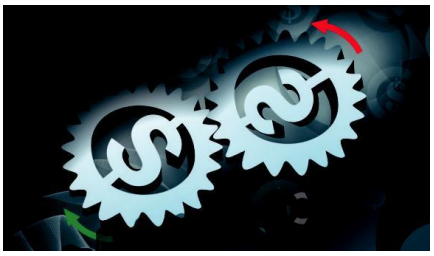
Par ailleurs, le nombre d'applications utilisées en mode SaaS augmentent massivement. Les entreprises font face à une transition majeure de l'approbation classique des accès sensibles vers les nouvelles exigences. Aujourd'hui, les sociétés gèrent au quotidien des demandes de création ou de gestion de profile d'authentification forte. Par conséquent, le contrôle d'accès devient une gageure sans le support d'une plateforme conviviale dédiée aux credentials et à l'administration des profils. Les identités des utilisateurs doivent être gérées afin de garantir une gestion de risques efficace et pour éviter les menaces et les risques perturbateurs.

Les services Cloud, le BYOD et le SaaS sont des solutions mises en œuvre pour augmenter la productivité et l'efficacité des effectifs, mais aussi pour réduire les coûts de façon significative. La solution de sécurité idéale pour une entreprise doit avoir un impact positif sur le coût total de possession (ou TCO de l'anglais « Total Cost of Ownership ») tout en offrant des fonctions de sécurité haut de gamme.

UNE SOLUTION DE SECURITE POUR OPTIMISER LE COÛT TOTAL D'ACQUISITION

Il existe aujourd'hui de nombreuses solutions de sécurité qui pourraient servir à contrôler les accès physiques et logiques, à sécuriser les accès aux services Cloud ou à assurer la gestion des identités des salariés, mais peu sont conçus pour optimiser le coût total de possession.

En raison de l'émergence de nouveaux appareils électroniques, de nouveaux usages et l'explosion des violations de sécurité, des solutions de sécurité flexibles et évolutives sont nécessaires. Face à l'évolution continue et rapide des menaces de sécurité, les entreprises sont contraintes de créer un système d'Identity Access Management (IAM) mettant en œuvre les dernières recommandations et évolutions en matière de sécurité. L'amélioration et la modification des plateformes doivent aussi être compatibles avec les systèmes existants.



Pour mieux maîtriser les coûts liés à la gestion des identités et au système de sécurité, les fournisseurs de solutions repensent leurs stratégies. Certains mettent à profit des solutions alternatives en mode Cloud afin de réduire les coûts d'infrastructure et de proposer un déploiement rapide avec un impact minime sur les fonctions existantes. L'expérience acquise par ces entreprises et leur gestion d'une diversité d'études de cas ont montré qu'il est possible d'automatiser de nombreux process pour réduire les coûts d'administration.

LES DISPOSITIFS MALINS POUR OPTIMISER LES COÛTS ET LES INVESTISSEMENTS

Cependant, il est probable que cela ne suffise pas à apporter un fort retour sur investissement. Heureusement, deux solutions existent pour répondre à certains des enjeux récents.

Comme nous l'avons déjà mentionné, la « logiciellisation » gagne du terrain et les logiciels pourraient, sur la base de la gestion des risques, devenir une solution alternative de protection du système. Les cartes à puce classiques (en plastique) sont conçues pour protéger les credentials, mais les coûts supplémentaires liés aux lecteurs de cartes externes et à la gestion des cartes pourraient s'avérer rédhibitoires. Tous les nouveaux ordinateurs portables sont dotés d'une puce cryptée intégrée. A l'aide du Trusted Platform Module (TPM), Microsoft a introduit le concept des **cartes à puce virtuelles** lors du lancement de Windows 8. Tout comme les cartes à puce physiques, les cartes virtuelles conservent les credentials dans un environnement chiffré et sécurisé. Les cartes virtuelles sont générées par le TPM et s'utilisent comme une carte en plastique classique. C'est actuellement l'alternative la plus pertinente. Les offres des éditeurs de Cart Management System (CMS), comme IDnomic (anciennement OpenTrust) sont désormais 100% compatibles avec les cartes à puce virtuelles.

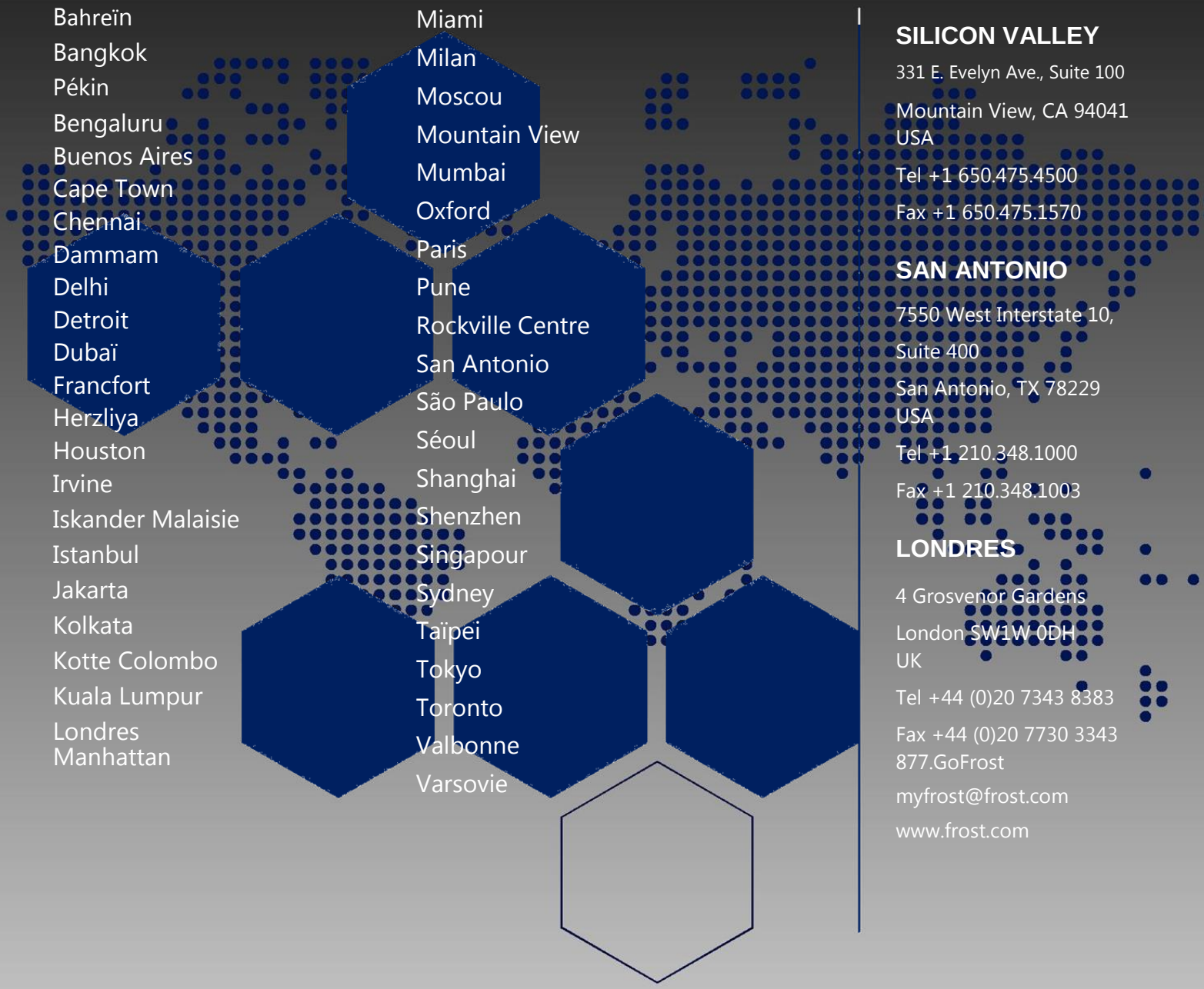
La stratégie de sécurité doit être adaptée au contexte d'évolution continue, non seulement en termes de normes de sécurité, mais également au regard du nombre croissant d'attaques potentielles et de violations de données. Par ailleurs, les technologies évoluent rapidement et, sans l'expertise requise, une entreprise aura du mal à respecter les exigences des normes sécuritaires. **L'externalisation** est un choix à prendre en compte par les entreprises. Rien n'oblige à avoir en interne un CMS, un IAM ou une Infrastructure à Clés Publiques. Par exemple, IDnomic propose déjà une interface utilisateur conviviale en mode Web pour faciliter l'administration des ICP et l'intégration du système existant dans le Cloud.

En plus de ces alternatives, il est important d'intégrer une stratégie mobile spécifique pour optimiser la gestion des credentials. Cette stratégie doit être construite autour d'une plateforme pour assurer la flexibilité et son intégration dans de nouveaux appareils, dans les systèmes d'exploitation et dans les services existants à valeur ajoutée, tels que la MDM.

La sécurité des entreprises est un concept complexe, mais il faut que les sociétés comprennent qu'il s'agit d'un aspect fondamental de la protection de leur image et de leur performance. Les entreprises doivent mettre en œuvre une stratégie de sécurité face à un contexte économique compétitif.

FROST & SULLIVAN

Auckland
Bahreïn
Bangkok
Pékin
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubaï
Francfort
Herzliya
Houston
Irvine
Iskander Malaisie
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
Londres
Manhattan
Miami
Milan
Moscou
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Séoul
Shanghai
Shenzhen
Singapour
Sydney
Taïpei
Tokyo
Toronto
Valbonne
Varsovie



SILICON VALLEY

331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
USA
Tel +1 650.475.4500
Fax +1 650.475.1570

SAN ANTONIO

7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
USA
Tel +1 210.348.1000
Fax +1 210.348.1003

LONDRES

4 Grosvenor Gardens
London SW1W 0DH
UK
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343
877.GoFrost
myfrost@frost.com
www.frost.com