STORMSHIELD



Solutions de protection des données

Vers un déploiement sans contrainte ?

Juillet 2022

PROTECTION DES DONNÉES

Tous les jours, les Directions des Systèmes d'Information et leurs équipes doivent intégrer des mises à jour, des correctifs de sécurité, de nouvelles applications ou configurer un ordinateur pour l'arrivée d'un nouveau collaborateur. Des opérations qui ne sont pas sans risque.

Toutes ces opérations prennent en effet du temps et peuvent entrainer des erreurs ou des blocages avec un impact sur l'activité de l'entreprise. Pour être plus agiles, de plus en plus d'organisations ont décidé de délaisser les postes de travail « classiques » – avec leurs nombreux clients lourds – au profit de clients légers ou de postes virtuels.

Mais cette évolution ne doit pas se faire au détriment de la protection des données, qui doivent être chiffrées de bout en bout pour en garantir la confidentialité. L'expérience utilisateur, ou plutôt l'expérience collaborateur, ne doit pas être oubliée non plus, car ce chiffrement doit se réaliser de la façon la plus transparente pour les métiers. Ce recours de plus en plus courant aux applications en mode SaaS oblige alors les éditeurs de solutions de sécurité à innover en proposant notamment une solution de chiffrement des données sous forme de service.

C'est l'une des promesses de la solution Stormshield Data Security.

Stormshield
Leader européen de la cybersécurité et filiale à 100% d'Airbus Defense & Space Cyber Programmes, Stormshield propose des **solutions de confiance**, certifiées et qualifiées au plus haut niveau européen. Il est l'éditeur qui couvre le plus grand périmètre de protection parmi les détenteurs des Visas de Sécurité de l'ANSSI (Agence Nationale de la Sécurité des Systèmes

Sommaire

04 **La gestion des postes de travail et des logiciels : un casse-tête permanent**

05 **Les coûts des déploiements des logiciels**

06 **L'âge d'or des applications lourdes est-il fini ?**

07 **Retours d'expérience**

08 **Une sécurité des données renforcée, avec moins de contraintes**

09 **Stormshield Data Security : le service de chiffrement sans agent**

La gestion des postes de travail et des logiciels : **un casse-tête permanent**

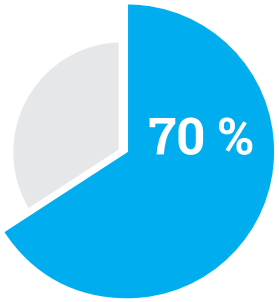
La mort de l'ordinateur de bureau est annoncée depuis des années. Mais force est de constater que ces postes de travail historiques – PC et Mac – restent incontournables dans les organisations, alors même qu'ils symbolisent pourtant les lourdeurs de la gestion IT. La faute à des déploiements et mises à jour de différents systèmes d'exploitation et de logiciels qui s'avèrent trop souvent contraignants, risqués, chronophages et onéreux.

OS plus supporté, nouveaux prérequis, incompatibilité avec une version d'un autre logiciel, conflits avec une application installée par un collaborateur… La gestion des postes de travail est jalonnée d'obstacles qui concernent tous les systèmes d'exploitation, de Windows à MacOS en passant par Linux. De nombreux facteurs peuvent en effet avoir un impact négatif sur le temps de déploiement des applications et de correctifs. Dans les faits, il faut parfois plusieurs mois pour mettre totalement à jour un parc informatique.

Mais le système d'exploitation n'est pas le seul à compliquer la tâche des Directions des Systèmes d'Information (DSI). Une simple évaluation de son parc de clients lourds peut révéler que des dizaines, et plus souvent des centaines, de postes de travail ne disposent pas des mises à jour et des correctifs disponibles pour des logiciels courants (tels que Java, Adobe Reader et les autres). Le déploiement des mises à jour et l'installation de nouvelles applications représentent pourtant des étapes indispensables pour à la fois renforcer la sécurité de son Système d'information (SI) et répondre aux besoins des métiers.

Déploiement logiciel et **transformation numérique**

Pour faire face à la complexité de gestion des postes de travail et des logiciels, les projets d'accélération numérique s'orientent de plus en plus vers les plateformes Cloud. D'après une étude menée par IDC en 2021, ce type de solution est vu comme un investissement stratégique dans les projets de modernisation, avec une croissance de 22% contre 5% pour les investissements IT au global.



70 % des applications seront cloud-natives d'ici 2024[1].

Lorsqu'il est appliqué à l'IT, le TCO (*Total Cost of Ownership*) est défini comme la somme des coûts d'acquisition, de mise en œuvre, de gestion, de soutien et d'utilisation de la technologie. Le prix d'achat d'un ordinateur n'est qu'une composante du coût d'un appareil tout au long de son cycle de vie.

Pour le service informatique, encore souvent considéré comme un simple centre de coûts, ces TCO d'achat et de suivi représentent une métrique financière très importante. L'optimisation de ces coûts conduit les entreprises à migrer rapidement vers le cloud. Selon la même étude IDC, la part des applications cloud-native va passer, d'ici 2024, de 10% à 70%, grâce à l'adoption de technologies comme les micro services, les containers, l'orchestration et le DevOps.

[1] Source : Article de IDC pour EasyVista – Mai 2021 : https://www.easyvista.com/fr/rapport-idc-service-client-et-support-it

L'âge d'or des **applications lourdes** est-il fini ?

Les postes de travail « classiques » offrent de multiples options. Mais leur administration reste lourde et compliquée. Et si la solution se situait du côté des clients légers, plus faciles à utiliser, moins chers à l'achat et gérables à distance ?



Le parc des entreprises n'est plus uniquement basé sur les systèmes d'exploitation de Microsoft. Les utilisateurs professionnels se connectent aussi aux réseaux d'entreprise et à leurs sources de données à partir d'appareils fonctionnant sous iOS et Android, voire MacOS ou Linux dans certains domaines, souvent pour des promesses de rapidité et d'agilité. Cette volonté d'être plus agile se traduit également par l'utilisation de clients légers au détriment des clients lourds.

Pratique originelle et désormais dépassée, le téléchargement et l'installation des logiciels depuis le site d'un éditeur ou un master ont pris un premier sérieux coup de vieux avec l'arrivée des stores d'applications comme Google, Apple ou Microsoft. Peu de temps après, les premières générations de clients légers ont accentué cette tendance – comme une application Web, ces clients légers permettent aux utilisateurs d'accéder à la plupart de leurs outils à partir d'un simple navigateur, y compris depuis des plateformes autres que Windows où les clients lourds ne sont souvent pas supportés.

Ainsi la donne a évolué avec le poids que prennent ces nouvelles générations de clients légers et leurs applications en version Cloud, comme Salesforce, Microsoft Office 365 ou Google Workspace. Toutes ces applications sont ainsi de plus en plus intégrées dans les entreprises en mode SaaS (*Software-as-a-Service*). Fin 2018, 78 % des éditeurs proposaient ce modèle, selon une étude Syntec Numérique/IDC[1] . Pour la DSI, la promesse est donc celle d'une administration simplfiée et centrale des terminaux et logiciels. Une réalité dans laquelle il est possible d'appliquer automatiquement des stratégies de profils à des groupes de clients légers configurés de la même façon. L'idée étant d'avoir un poste de travail « standard ».

En poussant cette idée, plus loin, naît le concept du *Desktop-as-a-Service* (DaaS). Ici, c'est le fournisseur du service qui assure directement la gestion de l'infrastructure technologique : provisionnement des ressources, équilibrage de charge, gestion des problèmes réseau, etc. Différents avantages qui n'exonèrent pas cependant la DSI de continuer à administrer les postes virtuels, à faire attention au protocole de déport de bureau et à contrôler les licences.

[1] Source : Communiqué de presse du Syntec Numérique – 6 décembre 2018 : https://syntec-numerique.fr/sites/default/files/Documents/2018_12_06_Communique_de_presse.pdf

Retours d'expérience

Le poste de travail reste encore au centre du SI de toutes les organisations.

Mais à chacune ses objectifs et ses défis, autour de l'expérience utilisateur.

Standardiser le poste de travail dans le monde de l'aviation

L'objectif de cette première entreprise est simple : atténuer l'impact de la gestion des logiciels (déploiement de correctifs de sécurité, migration vers une nouvelle version...) sur l'activité des collaborateurs. À terme, elle souhaiterait en effet que toutes les opérations effectuées sur les ordinateurs de bureau soient à la fois pratiques, rapides et transparentes.

Pour relever ce double défi (diminution des coûts de maintenance et des déploiements), cette organisation ambitionne de « standardiser » le poste de travail afin de ne plus gérer d'applications on demand, ni de couches supplémentaires. Quel que soit le profil métier, chaque utilisateur disposerait d'une machine à la configuration commune.

Simplifier les déploiements dans le monde du conseil et des services

Cette organisation mondiale a un turn-over très élevé et doit donc gérer des départs quasi quotidiens. Pour assurer une immobilisation minimale des postes, l'équipe informatique a donc besoin de réinstaller très rapidement un poste de travail. Cela implique d'avoir le minimum de complexité et de personnalisation à administrer.

Afin de ne pas pénaliser les nouveaux entrants, les applications et les données doivent être accessibles depuis un navigateur et à la demande, comme le propose l'environnement Google Workspace.

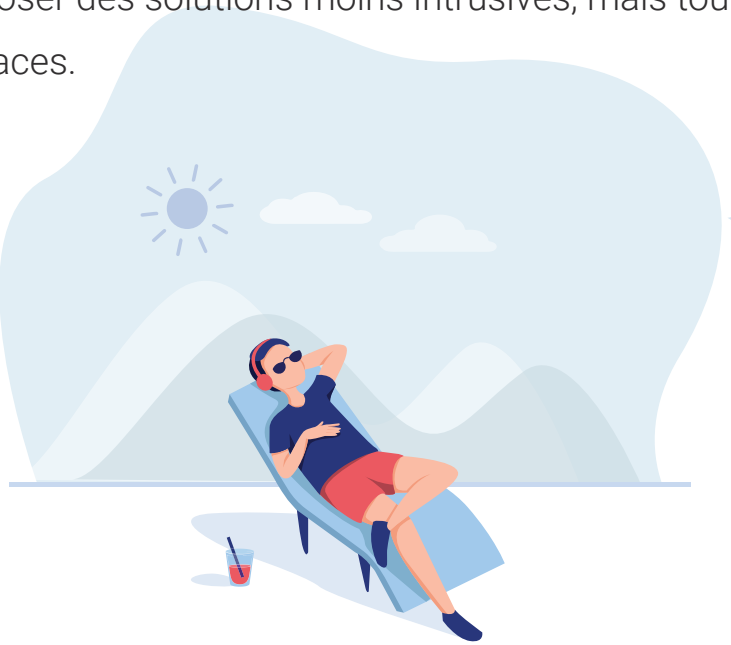
S'appuyer sur les stores d'applications dans le monde industriel

Pour ce groupe international, les applications comme Outlook ne sont plus adaptées à son mode d'organisation. Il préfère dorénavant Outlook Web Access afin de bénéficier de postes de travail moins lourds et de réduire les interactions avec d'autres applications sur le poste de travail. L'objectif est de permettre aux collaborateurs de pouvoir accéder à leurs données depuis n'importe où et quel que soit le terminal.

De façon générale, il souhaite limiter le déploiement de clients lourds sur chaque terminal au profit de solutions accessibles depuis un navigateur. Pour atténuer l'impact des déploiements de solutions « classiques », cette entreprise a décidé de s'appuyer sur des outils standards. Les équipes peuvent ainsi accéder à la boutique en ligne SharePoint Store, pour souscrire à des applications.

Une sécurité des données renforcée, **avec moins de contraintes**

La tendance de l'utilisation des applications SaaS sur les lieux de travail a donc permis de répondre – au moins dans un premier temps – aux attentes des utilisateurs et des équipes IT. Pour la protection de la donnée et les éditeurs des solutions de sécurité, le challenge consiste alors à proposer des solutions moins intrusives, mais tout aussi efficaces.



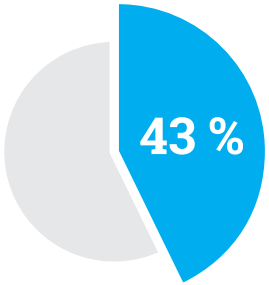
Quel que soit leur service, les collaborateurs ont aujourd'hui une approche data centric qui veut que la donnée soit au cœur de leur métier. Avec l'hyper connexion, le périmètre de l'entreprise a profondément changé : les échanges de données sont permanents entre les services internes et les partenaires externes. En parallèle, la mobilité des équipes implique de pouvoir accéder aux données, quel que soit l'endroit et à partir de différents terminaux fixes et mobiles. De quoi renforcer la nécessité de déporter la sécurité dans les outils qui permettent ces accès, en l'occurrence les navigateurs, et de généraliser le chiffrement.

Mais ces collaborateurs acceptent de moins en moins des contraintes qu'ils jugent non indispensables ou disproportionnées. Or, parmi ces contraintes, il y a celles liées à la cybersécurité. Et cette généralisation nécessaire du chiffrement des données se heurte encore à une idée reçue qui voudrait que chiffrer soit compliqué. Puisque toute nouvelle solution ou procédure ne vaut que si elle est comprise, adoptée et maîtrisée, il est impératif de sensibiliser les utilisateurs au caractère particulier des données et à la simplicité du chiffrement. La DSI doit ici jouer un rôle majeur, car elle représente un élément important de la stratégie en matière de protection des données.

Et cette (r)évolution concerne également les éditeurs de sécurité du domaine. Après les agents lourds des débuts de la cybersécurité, il convient aujourd'hui de proposer des solutions intuitives et simples à utiliser. L'objectif : satisfaire les utilisateurs finaux qui perçoivent encore le chiffrement comme une contrainte. **Et si la clé de la transformation numérique était la confiance des collaborateurs en interne – et des clients en externe – dans la capacité de l'organisation à protéger les données qui leur sont confiées ?**

Stormshield Data Security : **la solution de chiffrement SaaS**

La protection des données doit demeurer une priorité. Mais afin de répondre aux attentes des équipes IT, il devient capital de s'appuyer sur des solutions qui suivent la tendance des clients légers. Et pour les collaborateurs, il faut intégrer les attentes d'ergonomie et de facilité d'utilisation. Autant de promesses et de fonctionnalités intégrées dans la nouvelle solution de Stormshield Data Security, votre produit de chiffrement de données en mode SaaS.



43 % des organisations reconnaissent l'importance d'avoir une stratégie globale en matière de chiffrement[1].

La sécurité des données est plus que jamais vitale dans un contexte de forte concurrence et de multiplication des fuites de données. Cet objectif exige de généraliser le chiffrement pour renforcer la confidentialité de certains documents critiques et des dossiers partagés en ligne ou échangés via une messagerie.

La généralisation du chiffrement des documents et des e-mails est d'autant plus indispensable que les entreprises migrent une partie de leur SI ou de leurs applications vers le cloud. Le nouveau service de Stormshield Data Security répond à cette évolution en s'intégrant complètement à l'environnement de travail Google Workspace pour assurer la confidentialité des données échangées. Sans avoir besoin d'installer et de maintenir un agent à jour sur les postes de vos collaborateurs. Le chiffrement de confiance est effectué de bout en bout sous le contrôle unique de l'entreprise, avant que les données ne soient enregistrées sur les serveurs de la plateforme Cloud. Son administrateur n'aura donc aucun accès à ces données.

L'offre SaaS de Stormshield Data Security pour Google Workspace est un service de protection des données clé en main et souverain. Les processus de chiffrement et de déchiffrement ainsi que la gestion des clés utilisateurs sont entièrement assurés par Stormshield.

[1] Source : Étude « Global Encryption Trends », Ponemon – avril 2018

À retenir

Avec la multiplication des appareils mobiles et des nouvelles applications Web, les DSI ont pris conscience de la valeur **des interfaces utilisateur simples et intuitives**.

Car les collaborateurs ne s'intéressent pas tant à la technologie qu'à l'agilité offerte par celle-ci. Pour cela, de plus en plus de métiers s'appuieront sur des applications Web intuitives et des outils collaboratifs. **À la clé, une promesse d'un échange et d'un accès plus rapide aux données**.

Souvent considérée comme une contrainte, la question de la protection des données ne doit pas être sous-estimée – que ce soit pour les utilisateurs ou leurs équipes IT. Cette question de cybersécurité doit rester l'une des priorités des DSI, pour **protéger les données sans nuire à leur accessibilité**. L'intégration du chiffrement de bout en bout dans le navigateur et le caractère intuitif de l'application seront les premières réponses à cet objectif.

Le succès de cette évolution majeure dans l'approche de la cybersécurité dépendra de l'adhésion des employés. Pour cela, **changer les mentalités vis-à-vis du chiffrement** sera un défi majeur pour les DSI dans les années à venir.

L'informatique dans le cloud est déjà la nouvelle norme. Et c'est la culture de l'entreprise qui en retient la transition et non pas la technologie…



STORMSHIELD

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Notre mission : **cyber-séréniser nos clients** pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. **Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance.**

Pour en savoir plus : www.stormshield.com

www.stormshield.com



Copyright Stormshield - 2018-2022