Livre blanc

McAfee Security Connected — Une sécurité complète et rentable

intel Security

Sommaire

Avant même que les effets du séquestre ne se manifestent, il était prévu que le budget informatique global du gouvernement fédéral des États-Unis soit réduit de 121,7 milliards de dollars en 2012 à 115,5 milliards en 2013, selon le Professional Services Council[1]. Ces coupes s'inscrivent, entre autres mesures, dans l'initiative que Steven VanRoekel, directeur des systèmes d'information (DSI) du gouvernement des États-Unis, nomme « doing more with less » (faire plus avec moins) et qui vise à améliorer l'efficacité et la rentabilité des systèmes informatiques de l'administration publique tout en favorisant l'innovation, en éliminant le gaspillage, et en rationalisant et en consolidant les opérations des organismes publics[2]. Parallèlement, Steven VanRoekel et d'autres hauts dirigeants s'accordent à dire qu'elles ne doivent pas entraver les projets fédéraux de sécurité. Cela étant, les exigences en matière de cybersécurité imposées aux organismes publics se sont accrues, comme l'a indiqué le NIST (National Institute of Standards and Technology) dans sa publication *Security and Privacy Controls for Federal Information Systems and Organizations* (Contrôles de sécurité et de confidentialité pour les organismes et les systèmes d'information fédéraux), un catalogue de technologies de sécurité qui aident les administrations à se conformer à la loi FISMA et à d'autres réglementations[3].

Face à la tendance à la baisse de l'enveloppe fédérale, à des cybermenaces toujours plus nombreuses et dangereuses et à des obligations sans cesse plus strictes, une question se pose : « Est-il possible de se doter d'une solution de cybersécurité complète offrant une visibilité en temps réel sur les menaces et une protection à un coût raisonnable ? ». La réponse est oui. Non seulement vous pouvez mettre en place une sécurité à la fois totale et rentable, mais avec le cadre d'implémentation Security Connected de McAfee (filiale d'Intel® Security), cette sécurité est plus efficace car elle allie intégration, informations en temps réel sur les menaces, corrélation et rapidité, pour une protection renforcée à un coût moindre par rapport à d'autres solutions et aux produits individuels. Ce même cadre qui offre une sécurité plus performante améliore en outre l'efficacité opérationnelle pour atteindre l'objectif de rationalisation et de consolidation de l'informatique poursuivi par M. VanRoekel.

Nous avons conçu le cadre d'implémentation Security Connected pour aider nos clients à intégrer plusieurs produits, services et partenariats dans le but d'assurer une réduction des risques de sécurité de manière efficace, rentable et centralisée. Dans un discours prononcé à la Maison Blanche en 2012, Mike DeCesare, Président de McAfee, a décrit en ces termes la nécessité d'un tel cadre — et le défi qu'est aujourd'hui amené à relever le secteur de la sécurité : « Il nous faut unifier, simplifier et consolider la manière dont nous fournissons la sécurité au moyen d'un cadre qui vise à intégrer des technologies potentiellement disparates, en créant des ponts pour relier des "îlots" de sécurité et combler les failles technologiques. Chez McAfee, nous avons baptisé cette approche "Security Connected", ou la sécurité connectée. »

Fondée sur plus de vingt ans de pratiques éprouvées en matière de sécurité, l'approche Security Connected apporte une assistance précieuse à tous les organismes et programmes publics, indépendamment de leur envergure et de leur situation géographique. Elle leur permet de renforcer et d'optimiser la sécurité pour une meilleure rentabilité de l'investissement et d'aligner les stratégies de sécurité avec les initiatives gouvernementales.

Les ressources et outils du cadre Security Connected montrent clairement la voie à suivre pour passer du concept de sécurité initial à son implémentation et peuvent être adaptés aux risques, à l'infrastructure et aux objectifs spécifiques de l'administration. Par ailleurs, les systèmes sont évolutifs, de sorte qu'ils peuvent être déployés aussi bien dans le cadre d'un programme à petite échelle que dans tout l'environnement d'un organisme de très grande taille.

Architecture de référence Security Connected

Le cadre d'implémentation Security Connected offre une plate-forme et une architecture de meilleures pratiques qui assurent la résilience aux infrastructures des administrations publiques :

- Systèmes de commande et de contrôle militaires de terrain
- Surveillance continue
- Services numériques critiques pour le secteur public
- Cyberpréparation
- Réponse axée sur les renseignements
- Partage sécurisé d'informations pour les opérations conjointes
- Mobilité sécurisée
- Centres d'opérations de sécurité (SOC)
- Centres de données de services partagés
- Infrastructures virtualisées sécurisées
- Environnements réseau tactiques

Plus important encore, Security Connected assure une résilience aux infrastructures, c'est-à-dire un fonctionnement sans interruption lors d'une cyberattaque. La résilience exige :

- une action rapide pour garantir la protection ou la réponse en cas d'attaque ;
- l'agilité nécessaire pour soit adopter de nouvelles technologies facilitatrices, soit ajouter rapidement des fonctionnalités capables de refouler une nouvelle menace ;
- de stimuler la collaboration avec une communauté d'intérêts à mesure que les dépendances augmentent.

La plate-forme Security Connected assure une résistance et une résilience aux menaces avancées, permet une réaction ultrarapide et offre un cadre d'implémentation pour l'ajout de nouvelles fonctionnalités. Couplé à notre programme Partenaires McAfee® Security Innovation Alliance, ce cadre concorde de façon incomparable avec les exigences en matière de cyberdéfense des administrations et offre des niveaux d'évolutivité, de capacité de survie et d'intégration sans précédent pour protéger les environnements complexes des organismes publics.

Qu'est-ce qui explique la rentabilité de notre cadre d'implémentation ? La réponse est simple : les économies réalisées grâce à l'emploi de logiciels commerciaux standard.

Des logiciels commerciaux plus avantageux que les logiciels conçus pour les administrations publiques

Nous concevons des logiciels prêts à l'emploi pour la grande distribution : les coûts de la recherche, du développement, de la maintenance et des mises à jour continues sont absorbés par McAfee et répartis sur un grand nombre d'utilisateurs commerciaux. La raison pour laquelle ces logiciels ont été imposés dans de nombreux programmes d'entreprise et gouvernementaux est qu'ils procurent des économies considérables en coûts d'achat, de développement et de maintenance. Ces solutions coûtent moins cher qu'un logiciel personnalisé et offrent souvent plus d'avantages.

Comparons-les avec les solutions personnalisées destinées aux administrations publiques. Dans le domaine de la cybersécurité, le gouvernement américain a soumis des appels d'offres pour des outils de sécurité spécialisés qui nécessitent un développement personnalisé, ne sont pas testés en environnement réel et dont les coûts de fonctionnement et de maintenance sont élevés. Parfois, ces outils ne sont même pas déployés, alors que les fonds sont bel et bien alloués et les montants par conséquent dépensés. Ainsi, signalons un exemple édifiant qui doit tirer la sonnette d'alarme : le programme RAMP (Risk Assessment and Management Program) du ministère américain de la Sécurité intérieure a bénéficié d'un financement de 57 millions de dollars qui, en dépit des bonnes intentions du projet, ont finalement été dilapidés[4].

Si les propositions semblent être des réponses à des problèmes réels, il se peut en réalité que les systèmes ne soient pas compatibles avec d'autres systèmes de l'environnement réseau ou ne fonctionnent pas à grande échelle, comme l'exige l'administration. Une solution peut très bien fonctionner de façon optimale dans le laboratoire où elle a été développée, mais une fois déployée dans l'environnement réel et confrontée à de véritables menaces, des problèmes imprévus risquent d'apparaître. Aussi performante soit-elle en laboratoire, une solution inefficace « sur le terrain » n'a aucun intérêt. Quant à cet outil prodigieux dans un réseau composé de cinquante-mille terminaux, comment s'en tirera-t-il lorsqu'ils seront cinq-cent-mille voire un million ?

En 2012, un lanceur d'alertes a révélé que l'Office of Information and Technology (OIT) du ministère américain des Anciens combattants a déployé seulement 16 % des 400 000 licences de la technologie de chiffrement des terminaux qu'il avait achetée, en dépit des compromissions de données répétées subies. L'enquête qui a suivi a déterminé que : « L'OIT n'a pas installé ni activé l'ensemble des licences en raison d'une planification et d'une gestion inappropriées du projet. En particulier, l'OIT n'a pas alloué le temps nécessaire pour tester le logiciel et s'assurer de sa compatibilité avec les ordinateurs du ministère des Anciens combattants, vérifier si des ressources humaines suffisantes étaient disponibles pour installer le logiciel de chiffrement sur ces ordinateurs et surveiller de façon adéquate le projet pour garantir le chiffrement de tous les postes de travail et ordinateurs portables du ministère[5] ».

Le rapport coût-bénéfice des outils spécialement conçus pour les administrations publiques ne joue pas non plus en leur faveur. Prenez en compte les éléments suivants :

- Les solutions ponctuelles nécessitent des contrôles de gestion individuels et des personnes pour les faire fonctionner.
- Cela engendre un cloisonnement qui les isole les unes des autres, et le partage d'informations se limite à échanger des feuilles de calcul, chacune contenant une multitude de données. Résultat : une sécurité fracturée, nécessitant des interventions continues, tout sauf performante.
- Cette approche d'intégration par feuilles de calcul est très fastidieuse et peu rentable, en particulier lorsque l'on sait que dans de nombreuses organisations, entre 70 % et 80 % du budget informatique peut être absorbé par les charges d'exploitation.

Pour réduire les coûts informatiques dans un environnement soumis à des contraintes budgétaires, il faut envisager des solutions qui réduisent ces 70 % à 80 % de charges d'exploitation. Le cadre d'implémentation Security Connected de McAfee remplit cet objectif.

Une autre raison pour laquelle les logiciels commerciaux standard sont supérieurs aux logiciels spécifiquement conçus pour les administrations est que le secteur privé est généralement mieux équipé pour développer les solutions informatiques les plus à jour dans un environnement en mutation rapide. C'est tout particulièrement vrai dans le domaine de la cybersécurité, où les menaces affluent avec une telle rapidité et en si grand nombre que les éditeurs de solutions de sécurité innovent constamment pour pouvoir les contrer. Avant que les exigences des administrations puissent être traduites en solutions personnalisées, les menaces se sont déjà transformées et les exigences risquent d'être dépassées face à la nouvelle génération de menaces. Le rôle du gouvernement doit consister à favoriser la recherche de base en cybersécurité, pas la recherche appliquée qui aboutit au développement de produits.

Simplicité ou complexité : l'approche de type plate-forme

Même si cela peut sembler paradoxal, en matière de sécurité, une approche simple est plus efficace qu'une approche complexe. De fait, comme l'a si bien dit Howard Schmidt alors qu'il regagnait le secteur privé après avoir conseillé le gouvernement des États-Unis sur les questions de cybersécurité, la complexité est l'ennemi de la sécurité — et coûte certainement plus cher. Opter pour un seul cadre d'implémentation ou une suite de produits unique capable de répondre à tous vos besoins constitue un choix on ne peut plus judicieux. Outre le fait d'être simple, cette approche est plus efficace que la mise en place d'une série d'outils peut-être incapables de se connecter les uns aux autres et qui compliquent la génération de rapports. De plus, elle vous évite de devoir faire appel à plusieurs fournisseurs de solutions de sécurité pour bénéficier d'une protection contre toutes les menaces — à partir du moment où un éditeur de confiance vous offre une approche complète. La plate-forme Security Connected propose les fonctionnalités de base ainsi qu'un environnement ouvert qui répond à tout l'éventail des besoins actuels et émergents en matière de sécurité avec une efficacité optimale.

Avec la gamme de produits McAfee disponibles via Security Connected, vos dispositifs de défense du réseau étoffent leurs connaissances à mesure qu'ils protègent, et deviennent des producteurs et des consommateurs de renseignements sur les menaces issus de votre propre réseau. Ils créent un écosystème propice à la résilience, éliminant la majorité des éléments parasites et se concentrant sur les menaces les plus complexes de façon à garantir une utilisation optimale des ressources, aussi limitées soient-elles. Étant donné que les solutions automatisent les tâches de protection tout en gérant les stratégies, les alertes, événements et informations de nature administrative susceptibles de distraire les administrateurs sont moins nombreux. Seuls demeurent les éléments qui ont le plus d'importance et pour lesquels une intervention humaine aura réellement de l'intérêt.

L'écosystème est informé par le service McAfee Global Threat Intelligence (McAfee GTI), qui est intégré dans nos solutions et les alimente en informations en temps réel sur les menaces concrètes, permettant ainsi une connaissance en continu de la situation. Tel un système immunitaire, McAfee GTI protège des attaques. Pour ce faire, il détecte et corrèle électroniquement, de façon ultrarapide, les données sur les comportements identifiés comme dangereux fournies par des sources du monde entier. En quelques millisecondes, McAfee GTI évalue les modifications, attribue des niveaux de risque et distribue des recommandations en matière de protection aux produits, assurant une couverture multiniveau sur tous les vecteurs de menaces.

Alliée à McAfee GTI, la plate-forme Security Connected facilite la gestion de la sécurité pour les organismes publics de toute taille et, partant, ces tâches compliquées que sont l'intégration de protections et de contrôles pertinents de même que l'établissement d'une ligne de base et d'un processus d'escalade pour les principaux risques. Grâce à l'approche Security Connected, vous disposez d'une plate-forme intégrée de solutions intelligentes qui exploitent des informations sur les menaces. Ces solutions améliorent la fiabilité et instaurent une confiance dans les systèmes informatiques, tels que les ordinateurs portables et les postes de travail ainsi que les tablettes, smartphones et systèmes embarqués qui utilisent des clouds, sont hébergés dans ceux-ci ou créent leurs propres clouds, et se connectent d'un réseau à l'autre. Avec McAfee, vous bénéficiez d'une couverture étendue avec des contrats beaucoup moins nombreux et une complexité réduite. Vous pouvez donc véritablement « faire plus avec moins ». Une seule plate-forme suffit pour obtenir 35 à 40 contrôles certifiés par le NIST : vous n'avez pas à souscrire 35 à 40 contrats.

De plus, Security Connected vous offre des options supplémentaires. Grâce au programme Partenaires McAfee Security Innovation Alliance, vous pouvez bénéficier des technologies de sécurité les plus innovantes, non seulement celles proposées par McAfee mais également celles de milliers de développeurs qui peuvent intégrer leurs applications dans notre plate-forme de gestion extensible. À l'heure actuelle, plus de 150 partenaires technologiques participent à notre programme. Ces petites et grandes entreprises partagent le même engagement envers l'innovation continue dans le domaine de la sécurité. Leurs outils peuvent également s'intégrer dans le cadre d'implémentation Security Connected. Le programme Security Innovation Alliance vous permet de tirer parti de vos investissements existants, en unifiant des outils stratégiques et en les optimisant si nécessaire.

Une valeur ajoutée constatée par les clients

De notre point de vue, la valeur ne se mesure pas uniquement en termes d'amélioration de la sécurité et de réduction du risque. La valeur ajoutée que nous apportons est double : une amélioration de la sécurité *associée* à une diminution des coûts opérationnels. Nous mettons un point d'honneur à réaliser des études auprès des clients qui ont mis en œuvre nos plates-formes intégrées et, selon leurs dires, les effets en aval tangibles induits par le cadre Security Connected sont bien plus vastes. Voici quelques exemples de nos conclusions :

- Une grande municipalité située dans le nord-est des États-Unis a économisé 18 millions de dollars en cinq ans grâce à la normalisation avec McAfee.
- Un grand fabricant de produits de grande consommation a réduit le nombre de ses fournisseurs de solutions de sécurité de trois à un seul. Il a également diminué le nombre de serveurs et de consoles de gestion de la sécurité de 75 %, et constaté des économies de plus de 1 million de dollars en coûts de centre d'assistance, de gestion des incidents et d'application des patchs sur une période de trois ans.
- Un grand établissement de soins de santé a vu ses dépenses en sécurité informatique baisser de moitié après avoir opté pour McAfee. Il a également réduit la complexité de ses processus de gestion des fournisseurs (matériel, licences logicielles, etc.), et ses coûts d'audit et de conformité ont chuté de 3 millions de dollars.
- Une administration locale américaine a choisi McAfee pour standardiser son cadre de sécurité et déterminé qu'elle économiserait entre 5 et 8 millions de dollars sur une période de trois ans.

La consolidation : une proposition gagnante

Dans un article du *Federal Times* consacré aux coupes dans les budgets, M. VanRoekel remarquait : « Je pense que la pression fiscale aura pour effet une vague d'innovations et de gains d'efficacité à laquelle nous n'aurions pas assisté en période de rehaussement budgétaire. » C'est précisément ce que fait le cadre Security Connected : il fournit une approche novatrice de la sécurité qui procure une amélioration considérable de l'efficacité.

Avantages de la plate-forme Security Connected :

- Sécurité optimale à un coût raisonnable
- Approche intégrée de la réduction des risques posés par les menaces qui permet d'interconnecter les produits, les services et les partenariats
- Solutions commerciales standard à la rentabilité garantie et performantes dans votre environnement (quelle que soit sa taille), bien plus que les solutions spécifiquement conçues pour les administrations publiques
- Fournisseur leader du secteur possédant une gamme complète d'outils de sécurité de premier ordre
- Simplicité d'une plate-forme unique de solutions qui fonctionnent de concert et se complètent l'une l'autre
- McAfee GTI, qui ajoute cet élément crucial que sont les renseignements sur les menaces à l'ensemble du cadre d'implémentation
- D'autres possibilités de produits intégrés à la plate-forme Security Connected grâce à notre programme Security Innovation Alliance, qui assure interopérabilité et ouverture, de même qu'une amélioration de l'efficacité opérationnelle
- Économies de coûts avérées

Tirer parti d'un cadre intégré tel que Security Connected et utiliser des logiciels commerciaux standard plutôt que des technologies spécifiquement développées pour les administrations génèrent des gains d'efficacité majeurs. Il est possible de se doter d'une cybersécurité complète offrant une visibilité en temps réel sur les menaces et une protection performante à un coût raisonnable. La bonne approche en matière de sécurité, fondée sur l'intégration de logiciels commerciaux, peut répondre à toutes les exigences d'un organisme public : optimiser son état de protection, réduire ses dépenses, simplifier ses opérations et respecter les obligations officielles en matière de cybersécurité. C'est ce que nous appelons une proposition de valeur digne de ce nom.

Informations supplémentaires

Pour plus d'informations sur Security Connected, consultez la page **www.mcafee.com/fr/enterprise/security-connected/index.aspx**. Pour plus d'informations sur les solutions McAfee pour le secteur public, consultez la page **www.mcafee.com/fr/industry/public-sector/index.aspx**.

À propos de McAfee

McAfee fait désormais partie d'Intel Security. Avec sa stratégie Security Connected, une approche innovante de la sécurité optimisée par le matériel, et son réseau mondial de renseignements sur les menaces Global Threat Intelligence, Intel Security consacre tous ses efforts à développer des solutions et des services de sécurité proactifs et éprouvés, qui assurent la protection des systèmes, des réseaux et des équipements mobiles des entreprises et des particuliers du monde entier. Intel Security associe le savoir-faire et l'expérience de McAfee aux innovations et aux performances éprouvées d'Intel pour faire de la sécurité un élément essentiel de chaque architecture et plate-forme informatique. La mission d'Intel Security est de permettre à chacun de vivre et de travailler en toute confiance et en toute sécurité dans le monde numérique. **www.intelsecurity.com**.

1. **http://fedconnects.com/index.php/2013/01/part-one-federal-it-budgets-and-infrastructures-face-challenges-and-a-new-era/**
2. **http://cio.gov/wp-content/uploads/2012/09/FY2013-IT1.pdf**
3. **http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800_53_r4_draft_fpd.pdf**
4. **http://dailycaller.com/2012/07/24/beleaguered-homeland-security-agency-wastes-57-million-on-failed-computer-contract/**
5. **http://www.va.gov/oig/pubs/VAOIG-12-01903-04.pdf**

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com