SOPHOS
Cybersecurity made simple.

Les vilains secrets des pare-feu réseau

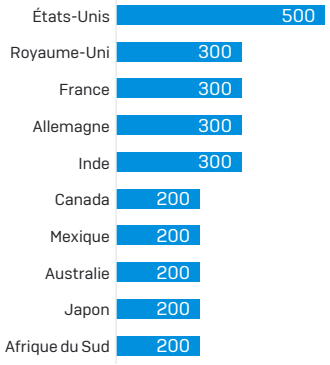
Résultats d'une enquête indépendante menée par Sophos auprès de 2 700 responsables informatiques de PME.

Introduction

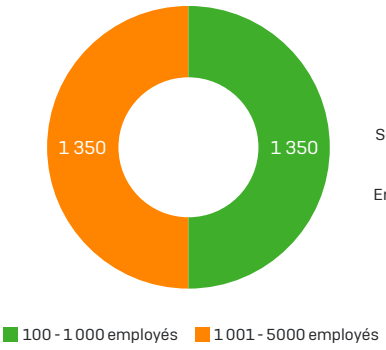
À la fin de l'année 2017, Sophos a parrainé une enquête indépendante portant sur l'état de la sécurité des réseaux auprès de PME du monde entier. Ce programme de recherche a mis en lumière les expériences, les inquiétudes et les besoins futurs des responsables informatiques, avec un intérêt particulier porté sur les pare-feu et la protection des réseaux.

Menée par le cabinet d'analystes britannique Vanson Bourne, l'étude a permis d'interroger 2 700 responsables informatiques travaillant dans des entreprises de 100 à 5 000 utilisateurs, situées dans une dizaine de pays différents et réparties sur l'ensemble des continents.

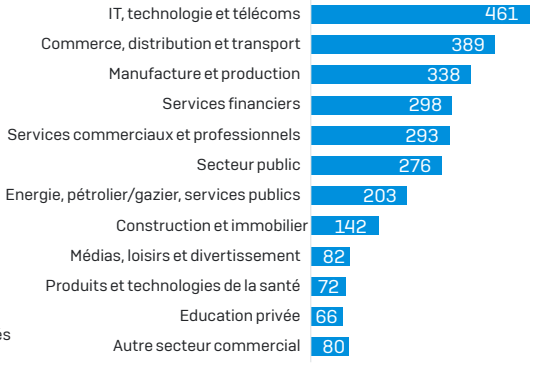
Pays du répondant



Taille de l'entreprise



Secteur de l'entreprise



Le présent rapport révèle les vilains secrets des pare-feu d'aujourd'hui, en exposant pourquoi ces derniers ne répondent pas aux attentes des entreprises dans des domaines clés de la protection, de la visibilité et de la réponse aux menaces et l'impact que ces insuffisances ont sur les responsables informatiques du monde entier.

VILAIN SECRET 1

LES PARE-FEU N'OFFRENT PAS LA PROTECTION DONT LES ENTREPRISES ONT BESOIN

Résumé

- Les entreprises ont en moyenne 16 ordinateurs infectés par mois.
  - 13 par mois en moyenne pour les entreprises de 100 à 1 000 utilisateurs.
  - 20 par mois en moyenne pour les entreprises de 1 001 à 5 000 utilisateurs.
- 79% des responsables informatiques souhaitent que leur pare-feu offre une meilleure visibilité.
- Une « meilleure protection » est l'amélioration n°1 des pare-feu souhaitée par près de la moitié des responsables informatiques (48%).

La norme est désormais de plusieurs infections par mois

Votre pare-feu est la passerelle entre votre réseau et Internet. Souvent, il fait également office de passerelle entre les différentes parties de votre environnement informatique ; Par exemple entre votre DMZ et vos serveurs, divers segments LAN, les réseaux Wi-Fi et les zones fiables et non fiables. Avec votre protection Endpoint, c'est un véritable pilier de votre infrastructure de sécurité.

En raison de cette position charnière, c'est également une indispensable première ligne de défense contre les malwares, les stoppant avant qu'ils ne puissent entrer dans votre réseau et les empêchant de se déplacer latéralement ou de se propager sur l'ensemble de votre environnement.

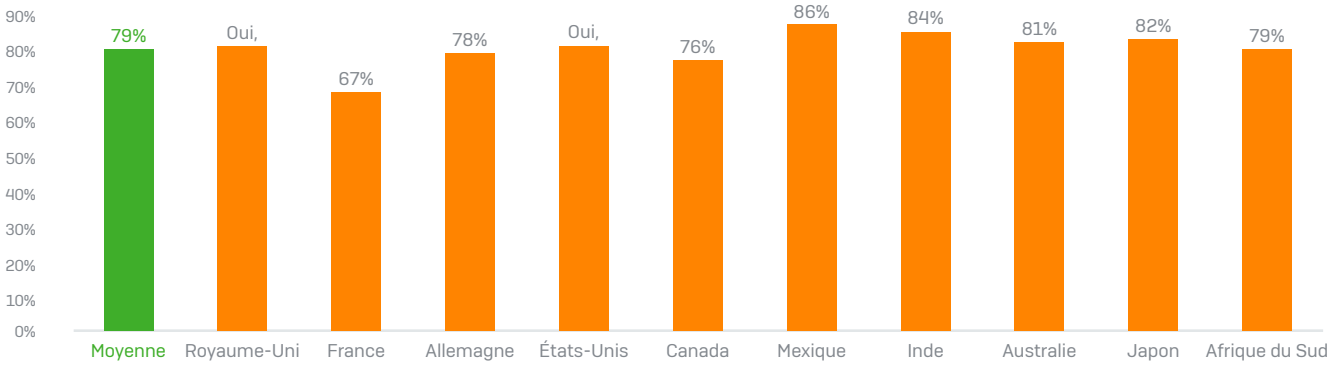
Malgré l'importance ce son rôle dans votre stratégie de sécurité informatique, l'enquête révèle que les pare-feu n'offrent pas la protection dont les entreprises ont besoin. Les entreprises subissent, en moyenne, 16 ordinateurs infectés chaque mois. Les plus petites entreprises (100 à 1 000 utilisateurs) recensent 13 ordinateurs infectés chaque mois, tandis que les plus grandes entreprises (1 001 à 5 000 utilisateurs) en recensent 20.

> **16** ordinateurs infectés par mois

Compte tenu de ces infections répétées, il n'est pas surprenant que 4 responsables informatiques sur 5 (79 %) souhaitent que leurs pare-feu les protègent mieux. En effet, près de la moitié des responsables informatiques (48%) souhaitent en premier que leurs pare-feu fournissent une meilleure protection. Ce besoin d'une meilleure sécurité englobe les deux périmètres informatiques : protection externe pour empêcher les menaces d'entrer et protection interne pour empêcher toute propagation si elles parviennent à entrer.

L'insuffisance de la protection est, malheureusement, un problème mondial, avec au moins deux tiers des responsables informatiques de tous pays confondus souhaitant une meilleure protection.

% DE RÉPONDANTS SOUHAITANT QUE LEUR PARE-FEU OFFRE UNE MEILLEURE PROTECTION



VILAIN SECRET 2

LES RESPONSABLES INFORMATIQUES NE SAVENT PAS COMMENT 45% DE LA BANDE PASSANTE EST CONSOMMÉE

Résumé

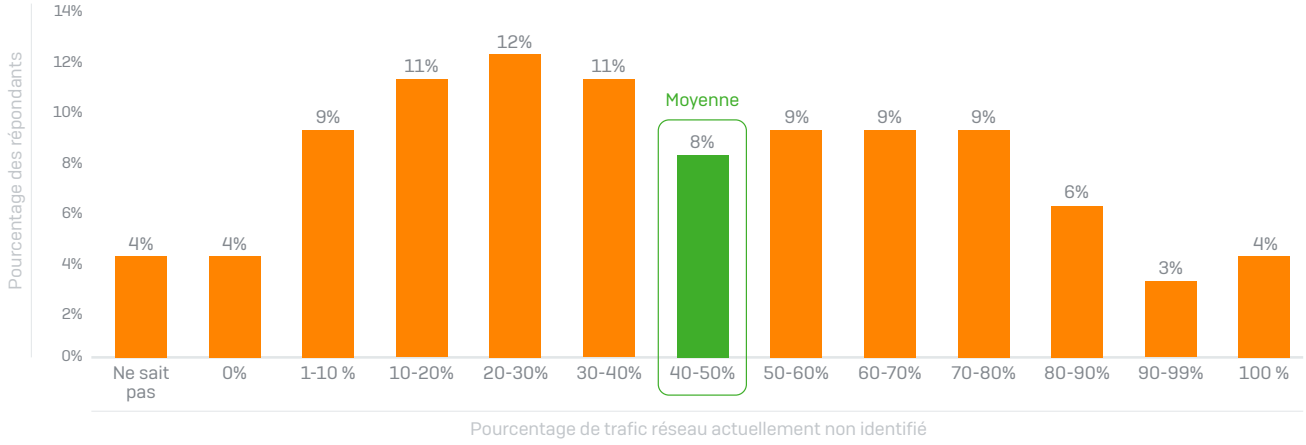
- En moyenne, 45% du trafic réseau est non identifié. Par conséquent, celui-ci ne peut pas être contrôlé.
- Près d'un responsable informatique sur quatre (23 %) ne peut pas identifier 70% du trafic réseau.
- Le manque de visibilité sur le trafic réseau laisse percer plusieurs sujets de préoccupation :
  - 84 % sont préoccupés par la sécurité.
  - 52 % sont préoccupés par la productivité.
  - 4 sur 10 sont préoccupés par le fait qu'ils ne savent pas comment est utilisée leur bande passante.
  - 42 % sont préoccupés par leur responsabilité légale ou leur conformité liées aux contenus potentiellement illégaux ou inappropriés.
  - 50 % ont investi dans des applications personnalisées qu'ils ne peuvent pas faire passer en priorité.
- Le secteur de la santé a le plus de difficultés avec les applications personnalisées, car deux tiers (67 %) ne peuvent pas identifier leurs applications personnalisées.
- 85 % des responsables informatiques veulent que leur pare-feu offre une meilleure visibilité.

Vous ne pouvez pas contrôler ce que vous ne voyez pas

Contrôler le trafic réseau est le rôle essentiel de tout pare-feu. Nous devrions pouvoir privilégier les applications essentielles, limiter les applications non-professionnelles et bloquer les applications malveillantes, telles que les clients BitTorrent. Le problème réside dans le fait que si vous ne pouvez pas voir ce qui passe sur votre réseau, vous ne pouvez pas le contrôler.

L'enquête a révélé que 45 % du trafic réseau ne peut actuellement pas être identifié. Ce qui signifie que le « contrôle des applications » n'est simplement pas possible pour près de la moitié du trafic. Et pour près d'un responsable informatique sur quatre (23 %) la situation est pire, car ils ne peuvent pas identifier 70 % ou plus de leur trafic réseau.

QUEL POURCENTAGE DE VOTRE TRAFIC RÉSEAU N'EST ACTUELLEMENT PAS IDENTIFIÉ ?



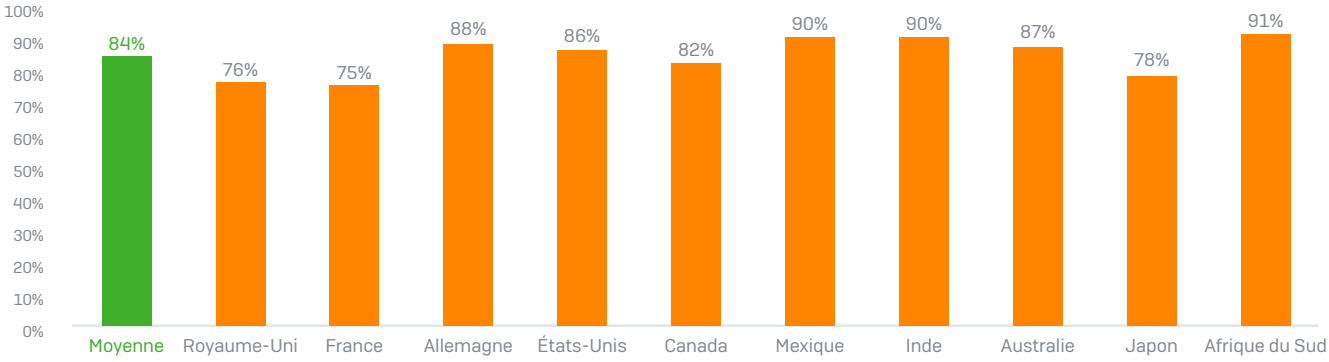
Cela est dû au fait que la grande majorité des pare-feu conventionnels identifient les applications en se basant sur les signatures, comme c'est d'ailleurs le cas pour les antivirus classiques. On retrouve ainsi les mêmes problèmes rencontrés avec ces derniers : les applications inconnues ne sont pas catégorisées et ne sont donc pas identifiées, et même si elles ont une signature, de nombreuses applications parviennent à modifier leurs modèles de trafic sur le réseau afin de contourner la détection. De plus, de nombreuses applications se « déguisent » en navigateurs Web pour éviter tout contrôle, car la quasi-totalité des pare-feu autorisent l'accès à Internet pour surfer sur le net.

Le manque de protection et de visibilité est également un problème partagé mondialement, et l'Inde semble en souffrir le plus avec 57 % de son trafic réseau qui est non identifié. Inversement, le Japon est le pays le moins impacté avec un tiers du trafic non identifié. Cela est probablement dû à des contrôles de politique plus stricts, une plus faible propension à utiliser des applications SaaS/Cloud souvent chiffrées et une plus faible propension à utiliser des applications non autorisées.

Le manque de visibilité laisse percer plusieurs sujets de préoccupation :

Sécurité. Si vous ne pouvez pas voir ce qu'il se passe sur votre réseau, comment pouvez-vous identifier ce qui est malveillant, suspect ou à haut risque ? Et comment pouvez-vous déterminer si le comportement de certains utilisateurs n'augmente pas le risque que votre entreprise soit infectée par un malware ou subisse une violation ? C'est pour cela que la sécurité est un sujet de préoccupation pour 84 % des répondants.

% DE RÉPONDANTS ESTIMANT QUE LE MANQUE DE VISIBILITÉ SUR LES APPLICATIONS EST UN SÉRIEUX PROBLÈME DE SÉCURITÉ



Productivité. Si vous ne pouvez voir comment est consommée votre bande passante, vous ne pouvez pas établir de priorités entre vos applications critiques et les applications non-professionnelles. Vous n'obtenez pas non plus d'informations sur les personnes qui en font usage. La perte de productivité liée aux applications non désirées ou inutiles est un sujet de préoccupation pour un peu plus de la moitié (52 %) des entreprises interrogées.

Opacité. À l'heure du 'tout Internet' et de la prévalence des applications Cloud, la bande passante est devenue une ressource professionnelle critique en plus d'une charge financière importante. Les entreprises se tournent vers leurs équipes informatiques pour leur expliquer comment cette ressource précieuse est utilisée, mais le manque de visibilité sur le trafic réseau rend cette tâche impossible. Par conséquent, en moyenne 4 responsables informatiques sur 10 sont inquiets du fait qu'ils sont dans l'incapacité d'expliquer comment la bande passante est consommée.

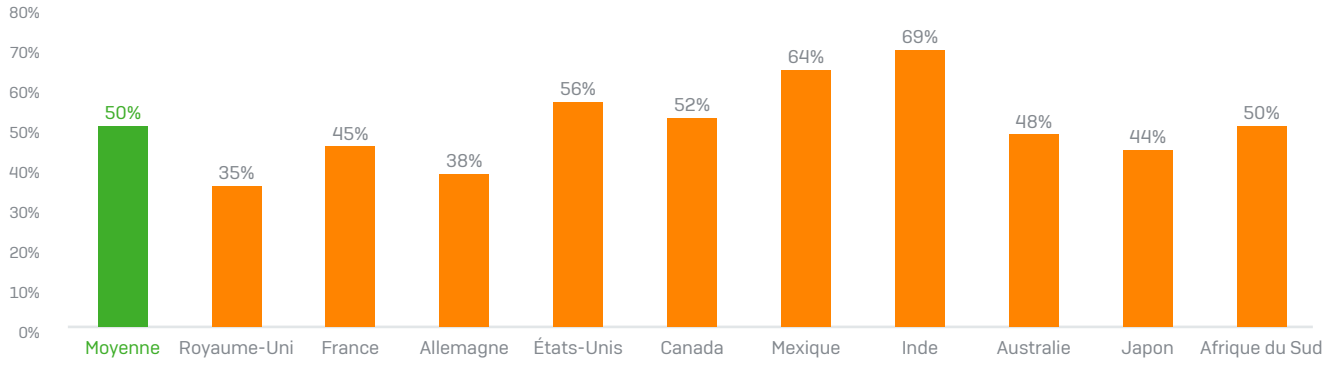
L'enquête a révélé des variations significatives entre les pays sur ce sujet. Les responsables informatiques en Inde (61 %) et en Afrique du Sud (55 %) sont les plus inquiets, tandis que ceux au Japon (28 %) et en Allemagne (30 %) sont les moins inquiets. Cela reflète vraisemblablement des pratiques commerciales différentes à travers le monde et des attentes différentes quant au respect des politiques de l'entreprise.

Responsabilité légale et conformité. Bien que les responsables informatiques des pays interrogés soient soumis à différentes obligations légales ou de conformité, ils sont tous préoccupés par la possibilité que des contenus illégaux ou inappropriés soient téléchargés, hébergés ou distribués sur leur réseau. En moyenne, 42 % partagent cette inquiétude, avec l'Inde (52 %) et le Royaume-Uni (47%) en tête de liste. Sans la capacité de voir ce qui est présent sur le réseau, les responsables informatiques ne peuvent pas garantir une transparence totale, mettant potentiellement leur entreprise dans une position de non-conformité.

Investissement (RoI). Les applications professionnelles ou verticales personnalisées sont de plus en plus fréquentes et elles représentent un investissement certain pour toutes les entreprises. Celles-ci vont des programmes modifiés pour répondre à des besoins professionnels particuliers aux applications entièrement conçues sur mesure destinée à une seule entreprise. L'enquête a révélé que 50 % des entreprises ont des applications réseau personnalisées que leur pare-feu ne peut pas identifier. Par conséquent, les informaticiens sont incapables de leur donner la priorité sur le réseau, limitant ainsi leur capacité à maximiser le retour sur investissement de l'application et à assurer le rendement de travail des utilisateurs.

Le retour sur investissement est également un sujet de préoccupation plus ou moins grand selon les pays. L'Inde, le Mexique et les États-Unis ont plus d'applications personnalisées non identifiées que la moyenne, tandis que le Royaume-Uni se situe en bas du classement avec 35 %. Cette différence semble refléter des disparités d'investissement dans des applications personnalisées par rapport à des applications en vente libre, mais également des problèmes de visibilité.

% DE RÉPONDANTS DISPOSANT D'APPLICATIONS PERSONNALISÉES QUE LE PARE-FEU NE PEUT PAS IDENTIFIER



Tous les secteurs industriels rencontrent des difficultés à identifier leurs applications professionnelles personnalisées, et il semble que le secteur de la santé soit celui qui en souffre le plus. Deux tiers des organismes de santé disposent d'applications personnalisées que leur pare-feu ne peut pas identifier, et qui donc ne peuvent pas être contrôlées. Cela s'explique probablement par le fait que les organismes de santé sont plus enclins à utiliser des applications personnalisées pour répondre à leurs besoins spécifiques et que leurs infrastructures sont généralement vieillissantes.

Pour 85% : La visibilité est la priorité n°1

Nous l'avons déjà vu, vous ne pouvez pas contrôler ce que vous ne pouvez voir. C'est pourquoi 85% des responsables informatiques souhaitent que leurs pare-feu offrent une meilleure visibilité. Cela leur permettrait de :

- **Réduire les risques liés à la sécurité** en identifiant les utilisateurs et les applications à risque.
- **Augmenter la productivité** en contrôlant le trafic relatif aux applications non-professionnelles.
- **Optimiser la bande passante** pour une utilisation professionnelle.
- **Réduire les inquiétudes liées à la responsabilité légale et à la conformité** en bloquant les contenus illégaux ou inappropriés.
- **Maximiser le retour sur investissement** des applications professionnelles personnalisées.
- **Identifier** l'intégralité du trafic réseau.

> **85%** souhaitent que leur pare-feu offre une meilleure visibilité

VILAIN SECRET 3

LES PARE-FEU INEFFICACES VOUS COÛTENT DU TEMPS ET DE L'ARGENT

Résumé

- Il faut en moyenne 3,3 heures pour identifier, isoler et nettoyer les ordinateurs infectés.
- En moyenne, les entreprises perdent 7 jours ouvrés par mois à nettoyer les ordinateurs infectés.
  - Les petites entreprises (100-1 000 utilisateurs) y consacrent en moyenne 5 jours ouvrés par mois.
  - Les plus grandes entreprises (1 001-5 000 utilisateurs) y consacrent en moyenne 10 jours ouvrés par mois.
- 99 % s'accordent sur le fait qu'il serait pratique si le pare-feu pouvait isoler automatiquement les machines infectées.
- 97 % pourraient choisir une protection Endpoint et pare-feu du même éditeur, s'il en résulte un meilleur taux de détection et permet une réponse automatisée.

Plus d'une semaine est perdue chaque mois pour réparer les ordinateurs infectés

Comme nous l'avons déjà vu, les pare-feu n'offrent pas la protection dont les entreprises ont besoin. Par conséquent, les équipes informatiques consacrent beaucoup de temps et d'énergie à réparer les ordinateurs infectés.

Pour déterminer l'étendue de ce problème, deux questions clés étaient posées dans le cadre de l'enquête :

1. **Combien de temps** cela prend-il, en moyenne, pour identifier, isoler et nettoyer les machines infectées ?
2. En moyenne, **combien d'ordinateurs infectés** votre entreprise doit-elle gérer chaque mois ?

Les réponses sont très surprenantes.

En moyenne, il faut 3,3 heures, ou près d'une demi-journée de travail pour identifier, isoler et nettoyer les ordinateurs infectés. Curieusement, les plus petites entreprises y parviennent en moins de temps que les plus grandes. Les entreprises de 100 à 1 000 utilisateurs y consacrent en moyenne 2,9 heures, tandis que les entreprises de 1 001 à 5 000 utilisateurs peuvent y consacrer jusqu'à 3,9 heures.

Les entreprises déplorent, en moyenne, 16 ordinateurs infectés par mois. En estimant une journée de travail à

> **7 jours** consacrés au nettoyage des ordinateurs infectés chaque mois (sur une base de 7,5 h/jr)

7,5 heures, cela signifie qu'elles consacrent 7 jours entiers de travail chaque mois à nettoyer les infections.

Lorsque nous considérons les implications de ce temps de nettoyage, nous devons prendre en compte la

Taille de l'entreprise	Nb d'ordinateurs infectés /mois	Heures pour nettoyer un ordinateur	Heures totales de nettoyage /mois	Nb jours/mois (7,5h = 1 jour)
100 – 1 000	13	2,8	36,4	4,9
1 001 – 5 000	20	3,9	78	10,4
Moyenne	16	3,3	52,8	7,04

durée immédiate et le coût en ressources, mais également les coûts d'opportunités, c'est à dire ce que l'équipe informatique aurait pu réaliser à la place. Les équipes informatiques sont soumises à une pression grandissante, qui résulte du fait qu'on leur demande de faire toujours plus sur leur temps imparti, doublé du fait qu'il existe une réelle pénurie de compétences en sécurité informatique. 70 % des professionnels de la cybersécurité déclarent que leur entreprise a été affectée par une pénurie d'experts en cybersécurité[i]. Et la plupart peut difficilement se permettre de perdre 7 jours de travail par mois pour réparer les ordinateurs infectés.

Étant donné les conséquences en termes de coût et de temps passé à réparer manuellement les ordinateurs infectés, il n'est pas surprenant que 99 % des responsables informatiques veulent que leur pare-feu isole automatiquement les systèmes compromis, et 90 % s'accordent sur le fait que cette fonction serait 'extrêmement' ou 'très' utile. Près de la totalité des répondants (97%) pourraient choisir leur protection Endpoint et pare-feu avec le même éditeur afin de bénéficier d'un meilleur taux de détection et d'une meilleure réponse automatisée.

Conclusion

Les vilains secrets des pare-feu réseau d'aujourd'hui éclatent au grand jour : ils n'offrent pas les capacités clés dont ont besoin les entreprises. De la protection réseau à la visibilité et la réponse aux menaces, l'expérience vécue aujourd'hui par les responsables informatiques est bien en deçà de leurs attentes et de leurs besoins pour protéger leurs entreprises. À la lumière de ce constat, il est temps pour les entreprises de jeter un nouveau regard sur leur sécurité réseau et de mettre en place des solutions qui répondent mieux à leurs besoins.

Lectures complémentaires

[i] *The Life and Times of Cybersecurity Professionals. The Enterprise Strategy Group, 2017*

- Livre blanc « Firewall : Les meilleures pratiques pour bloquer tout ransomware » – Comment les attaques récentes de ransomwares, comme WannaCry et Petya, se sont déroulées et les fonctions indispensables des pare-feu pour stopper ces types d'attaque.
- Livre blanc « Pourquoi les administrateurs réseau ont besoin d'une visibilité complète sur les applications » – Une analyse détaillée des difficultés inhérentes à la visibilité du trafic réseau et comment les résoudre.
- Guide d'achat Pare-feu – Technologies et fonctions clés à considérer au moment de l'achat d'un pare-feu, ainsi que les questions à poser aux éditeurs.

Sophos XG Firewall : Résoudre les problèmes des pare-feu réseau

Sophos XG Firewall est conçu pour répondre à l'évolution des besoins des responsables informatiques, et pour remédier aux principaux problèmes rencontrés avec les pare-feu actuels.

- **Protection.** XG Firewall stoppe les menaces inconnues avec une suite complète de protections avancées, dont les technologies de Deep Learning, IPS, ATP, Sandboxing et double moteur antivirus.
- **Visibilité.** XG Firewall expose les risques cachés avec une visibilité sur toutes les applications, les utilisateurs les plus à risque, les menaces avancées, les charges suspectes, et bien plus.
- **Réponse.** XG Firewall répond automatiquement aux incidents en identifiant et en isolant immédiatement les systèmes infectés jusqu'à leur nettoyage.

Découvrez la reconnaissance des experts du marché pour XG Firewall :

- NSS Labs – « Le mieux classé »
- SC Media – « Une convergence très créative d'un grand nombre de fonctionnalités puissantes. »
- PC Pro – « Une appliance UTM extrêmement souple qui allie une performance optimale avec un prix raisonnable. »

En savoir plus et commencer un essai gratuit de 30 jours : www.sophos.fr/interceptx.

Équipe commerciale France :
Tél. : 01 34 34 80 00
Email : info@sophos.fr

04/04/18 FR (TN)

SOPHOS