DÉCOUVRIR LA DURE RÉALITÉ DE LA GESTION DES TERMINAUX

Combler les fossés en matière de sécurité à l'échelle d'une multitude d'appareils

Central by LogMeIn

TABLE DES MATIÈRES

INTRODUCTION

L'une des plus grandes tendances en matière de sécurité, et qui n'a fait que croître en 2018, est la gestion des terminaux. Les outils de gestion des terminaux simplifient le processus de gestion informatique en permettant à une entreprise de centraliser la gestion, les mises à jour et le dépannage de l'ensemble de ses appareils, dont les ordinateurs fixes et portables, les routeurs, les téléphones mobiles, etc.

Pour mieux comprendre les tendances actuelles du marché, les menaces commerciales et la manière dont les entreprises tentent de contrer ces menaces, nous avons mené une étude auprès de 1000 professionnels de l'informatique. Ces professionnels de l'informatique représentaient des petites et moyennes entreprises d'Amérique du Nord et d'Europe.

Le résultat de notre étude montre qu'une nette majorité des professionnels de l'informatique considèrent que la gestion des terminaux est une priorité de leurs équipes en raison de la prolifération d'un large éventail d'appareils au sein de leurs organisations. Ces professionnels ont suivi les failles de sécurité très publiques et coûteuses de l'année écoulée (Equifax, le piratage de la NSA du gouvernement américain, pour ne citer que quelques exemples) entraînées par des systèmes non patchés, et ils comprennent que ne pas se préparer à contrer ces menaces peut avoir un impact considérable sur les résultats commerciaux et la réputation d'une entreprise.

Cependant, contrer les cybermenaces n'est pas la seule raison pour laquelle la communauté informatique considère que l'adoption de la gestion des terminaux est une priorité. Les évolutions sur le lieu de travail l'exigent également :

1. Les politiques d'utilisation des appareils personnels (BYOD ou bring your own device) et de télétravail, qui concernent notamment les ordinateurs portables et les appareils mobiles, sont de plus en plus courantes au sein des entreprises petites et grandes, et cette tendance a peu de chances de s'inverser durant l'année à venir.
2. Qui dit une pléiade d'appareils dit une multitude d'apps et de logiciels disparates sur ces appareils, qui doivent être gérés de façon centralisée et protégés contre les risques potentiels.
3. Les entreprises poursuivent la migration de leur activité vers le nuage, ce qui accroît les risques d'accès illicite aux données sensibles.

les comportements sur le lieu de travail évoluent dans le sens d'une simplification pour l'utilisateur final, au prix d'un risque accru de failles de sécurité. Lorsqu'on ajoute les cybermenaces auxquelles les entreprises sont confrontées au quotidien, on comprend que les professionnels de l'informatique du monde entier cherchent des solutions globales et exhaustives pour gérer de manière centralisée l'ensemble des terminaux.

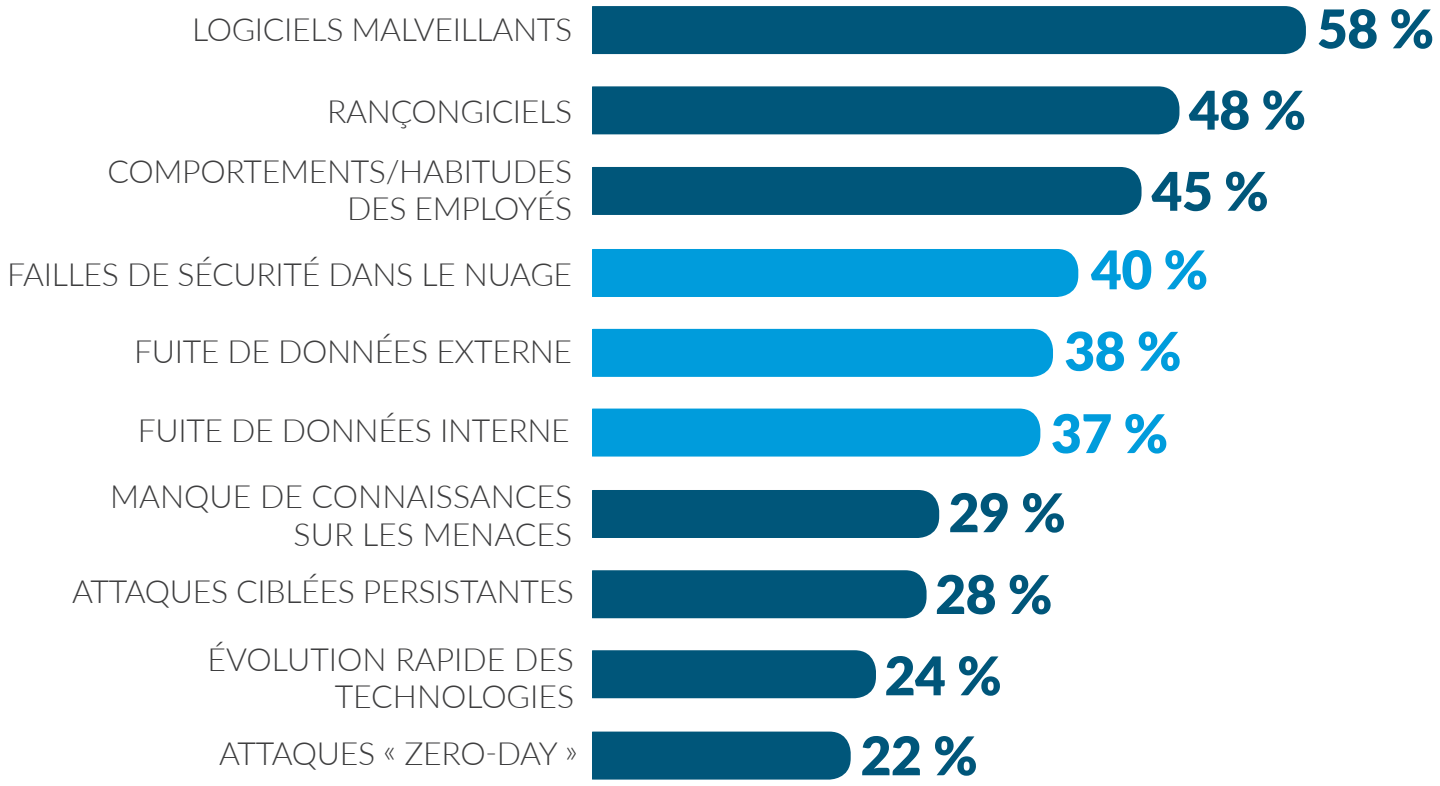
Si les professionnels de l'informatique considèrent que la gestion des terminaux est une priorité, et si les évolutions sur le lieu de travail l'exigent, **SEULEMENT LA MOITIÉ D'ENTRE EUX AGISSENT DE MANIÈRE PROACTIVE POUR RÉPONDRE AUX PROBLÈMES DE SÉCURITÉ** en amont d'une fuite.

TENDANCES DU MARCHÉ :
LES RISQUES DE SÉCURITÉ SONT RÉELS ET DE PLUS EN PLUS OMNIPRÉSENTS

Les professionnels de l'informatique ont abordé 2018 habités par diverses préoccupations en matière de sécurité, et leurs inquiétudes étaient justifiées : selon McAfee, les « rançongiciels » ont augmenté de 56 %[5] et étaient impliqués dans 39 % des attaques liées aux logiciels malveillants en 2017[5]. En effet, les rançongiciels ne se contentent plus de cibler les ordinateurs, mais s'attaquent également à d'autres terminaux, dont les serveurs et les réseaux[5].

Notre étude suggère que les professionnels de l'informatique ne sont pas au bout de leurs peines : en moyenne, ils doivent affronter 4 problèmes de sécurité, provenant de sources internes et externes. Les logiciels malveillants constituent leur principale préoccupation en matière de sécurité, suivi par les rançongiciels et les comportements et habitudes des employés. Vient ensuite le triptyque failles de sécurité dans le nuage, fuites de données externes et fuites de données internes. Ces problèmes bien réels ne font que renforcer la nécessité de mettre en place une gestion exhaustive des terminaux dans toute l'organisation. La capacité à placer ces menaces de sécurité informatique en quarantaine constitue la première étape pour éviter que l'intégralité du réseau soit contaminée.

LES ÉQUIPES INFORMATIQUES SONT CONFRONTÉES À PLUSIEURS RISQUES DE SÉCURITÉ, ET SONT PARTICULIÈREMENT PRÉOCCUPÉES PAR LES LOGICIELS MALVEILLANTS ET LES RANÇONGICIELS.



TENDANCES COMMERCIALES :
NOTRE APPROCHE EN MATIÈRE DE SÉCURITÉ DOIT SUIVRE L'ÉVOLUTION DES PRATIQUES SUR LE LIEU DE TRAVAIL

LE BYOD ENTRAÎNE UNE PROLIFÉRATION DES TERMINAUX. LES ÉQUIPES INFORMATIQUES DOIVENT DONC FAIRE ÉVOLUER LEUR FAÇON D'ABORDER LA SÉCURITÉ, SANS QUOI ELLES RISQUENT D'ÊTRE EXPOSÉES À DES CYBERMENACES POTENTIELLES.

Il n'y a pas si longtemps, les professionnels de l'informatique avaient un nombre limité de terminaux à gérer et à sécuriser, et ces terminaux étaient sous leur contrôle direct. Ils pouvaient protéger leur entreprise contre les menaces et les cyberattaques en sécurisant le périmètre et leurs systèmes sur site. Mais au cours des dernières années, le BYOD et le télétravail ont transformé la façon dont les gens travaillent, ce qui a poussé les équipes informatiques à repenser la façon dont elles gèrent et sécurisent les terminaux et le réseau de leur entreprise.

Tant que les entreprises chercheront à offrir plus de souplesse à leurs employés et à tirer profit d'une augmentation de la productivité et d'une diminution des coûts, les politiques BYOD et de travail à distance continueront à s'enraciner. De fait, une étude de MarketsandMarkets sur la tendance du BYOD révèle que le taux d'adoption en Amérique du Nord était de 36 % début 2017 et devrait atteindre 50 % au cours de l'année 2018[1].

Notre enquête montre qu'en dépit des préoccupations concernant les menaces sur les terminaux, 30 % des professionnels de l'informatique n'ont pas une idée précise du nombre de terminaux utilisés dans leur entreprise.

QUEL EST LE NOMBRE DE TERMINAUX UTILISÉS DANS VOTRE ENTREPRISE ?

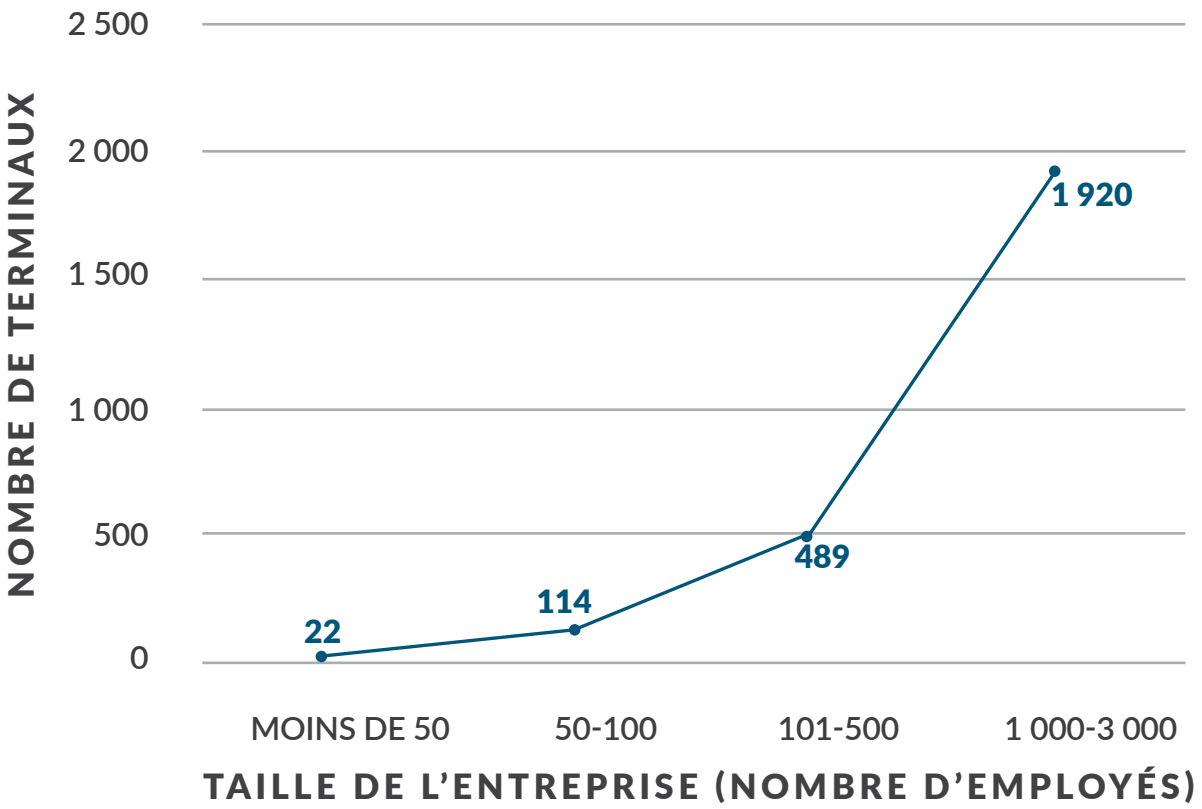
CONNAISSENT LE NOMBRE DE TERMINAUX

NE SONT PAS SÛRS

Pour ces entreprises, trouver un moyen de s'adapter à la tendance BYOD à l'aide d'une solution exhaustive qui gère de manière sécurisée un large éventail d'appareils s'imposera pour contrer efficacement les cyberattaques.

Les professionnels de l'informatique capables d'estimer le nombre de terminaux dans leur entreprise font état d'une moyenne de 750 extrémités (serveurs, ordinateurs des employés, appareils mobiles). Ce nombre conséquent de terminaux ajoute un niveau de complexité supplémentaire à l'effort nécessaire pour les gérer efficacement tout en protégeant les entreprises des menaces de sécurité tant internes qu'externes.

NOMBRE MOYEN DE TERMINAUX / NOMBRE D'EMPLOYÉS



LES PROBLÈMES DE L'APPROCHE ACTUELLE : LES ORGANISATIONS DOIVENT SE PRÉPARER À GAGNER LA GUERRE, PAS SEULEMENT LA BATAILLE

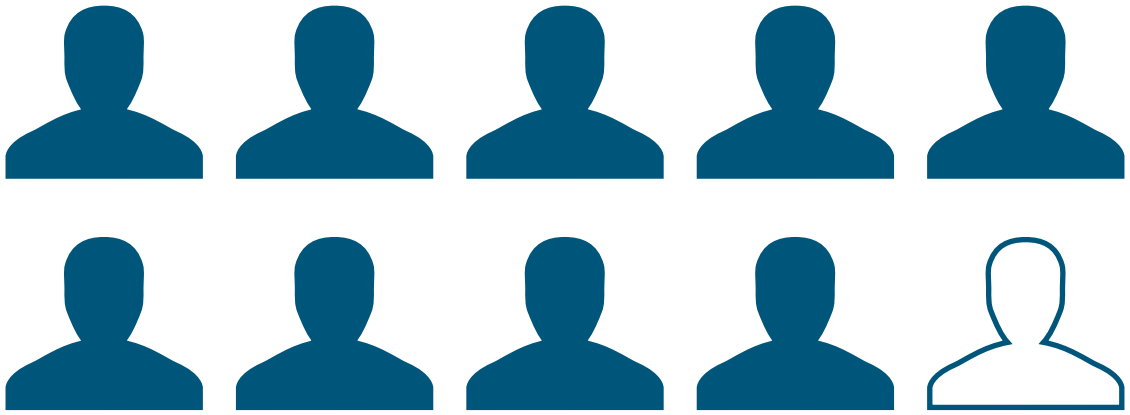
Étant donné la pléthore de terminaux ainsi que les préoccupations en matière de sécurité interne et externe, il n'est pas étonnant que près de 9 professionnels de l'informatique sur 10 (88 %) considèrent que la gestion des terminaux est une priorité pour leurs équipes.

À ce titre, les solutions anti-logiciels malveillants sur les terminaux constituent la deuxième mesure de sécurité la plus courante mise en œuvre par les professionnels de l'informatique pour répondre aux problèmes de sécurité.

Les pare-feu, l'authentification et le chiffrement sont d'autres mesures de sécurité couramment utilisées pour lutter contre les problèmes de sécurité.

Grâce à ces mesures de sécurité, la plupart des professionnels de l'informatique (82 %) s'estiment prêts à faire face aux problèmes de sécurité, mais seulement 26 % sont convaincus que ces mesures de sécurité sont efficaces pour leurs utilisateurs finaux.

LA GESTION DES TERMINAUX EST DÉJÀ UNE PRIORITÉ, MAIS IL FAUT ALLER PLUS LOIN POUR PROTÉGER LES ORGANISATIONS À LONG TERME.



PRÈS DE

9 sur 10

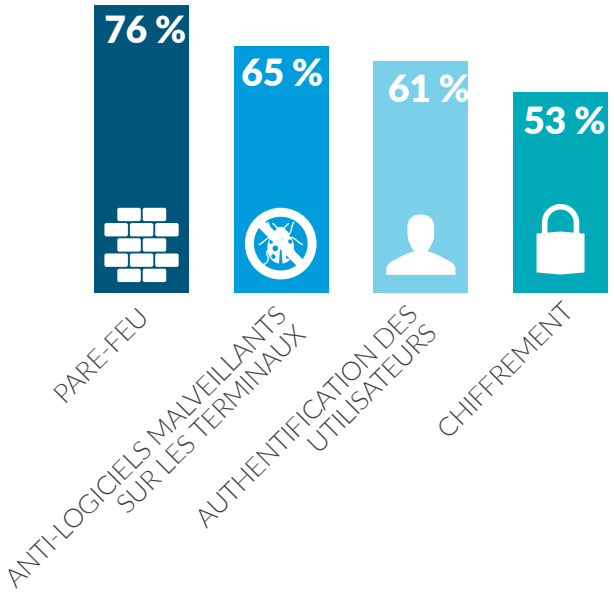
professionnels de l'informatique considèrent que la gestion des terminaux est une priorité

CES DONNÉES PROUVENT QU'IL RESTE BEAUCOUP DE PROGRÈS À FAIRE POUR ASSURER LA SÉCURITÉ DES TERMINAUX À LONG TERME DE MANIÈRE GLOBALE ET EXHAUSTIVE :

1. Bien que 71 % des professionnels de l'informatique affirment qu'ils s'occupent activement de la sécurité du matériel, ils ne sont que 56 % à s'occuper activement de la sécurité des logiciels, et seulement 48 % à s'occuper de celle des appareils mobiles. Ce manque de couverture laisse des trous béants dans leur stratégie de sécurité. Alors qu'un nombre croissant d'employés utilisent leurs smartphones ou tablettes personnels à des fins professionnelles (téléchargement de documents de travail, édition, envoi d'e-mails, etc.), il est de plus en plus important de s'assurer que ces appareils sont aussi sécurisés que les PC et les autres terminaux.

2. En outre, de nombreuses mesures de sécurité ne sont pas actuellement mises en œuvre par un pourcentage important des équipes informatiques, comme la gestion des correctifs tiers et les contrôles d'accès sur les appareils mobiles, exposant ainsi leur organisation aux cyberattaques.

MESURES PRISES POUR RÉPONDRE AUX PROBLÈMES DE SÉCURITÉ



POURCENTAGE DES PROS DE L'INFORMATIQUE QUI NE PRENNENT PAS LES PRÉCAUTIONS SUIVANTES

IMPACT QUANTITATIF :
EN NE VOUS PRÉPARANT PAS, VOUS VOUS PRÉPAREZ À ÉCHOUER

Malgré les nouvelles récentes concernant les piratages et les problèmes liés à la sécurité, à peine plus de la moitié des professionnels de l'informatique (52 %) consacrent du temps à traiter de manière proactive les problèmes de sécurité en amont d'une attaque ou d'une fuite.

Les risques que ces menaces de sécurité font peser sur les entreprises ne sont pas seulement d'ordre opérationnel, mais ils peuvent également avoir un impact concret sur les résultats financiers, endommager la réputation de l'entreprise à long terme, et même entraîner la faillite de l'entreprise.

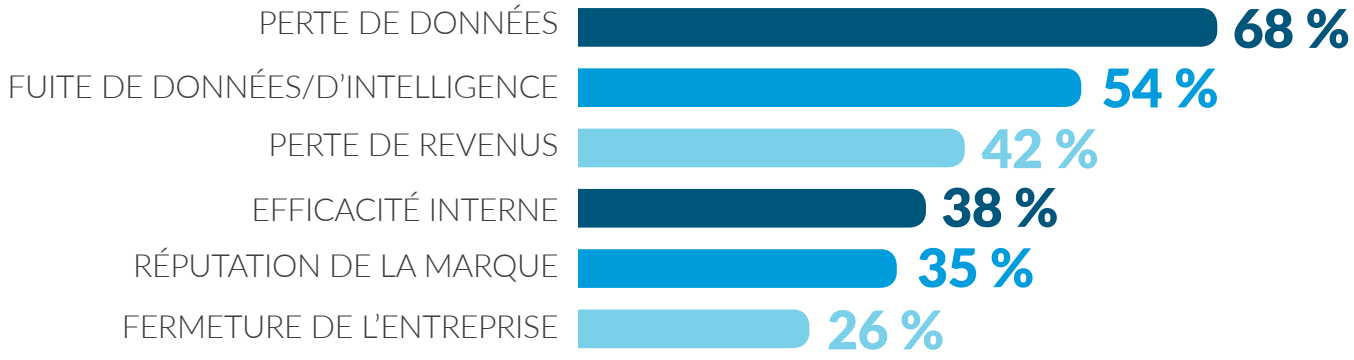
LES CHIFFRES SONT MIROBOLANTS

Selon certaines estimations, WannaCry à lui seul aurait entraîné des dommages allant de centaines de millions à des milliards de dollars à l'échelle mondiale. L'attaque du rançongiciel ExPetr a entraîné environ $300 millions de pertes pour FedEx/TNT[5].

En outre, selon une étude mondiale menée par Osterman Research pour Malwarebytes, environ 16 % des organisations touchées par une attaque de rançongiciel ont connu une indisponibilité d'au moins 25 heures, sachant que certaines organisations ont rapporté une indisponibilité de leurs systèmes de plus de 100 heures !

Notre étude montre que les professionnels de l'informatique estiment que les risques les plus graves associés à une faille de sécurité sont la perte de données, la fuite de données et la perte de revenus.

RISQUES LIÉS AUX FAILLES DE SÉCURITÉ



LES AVANTAGES DE L'INVESTISSEMENT : ALORS QUE LA NATURE DES RISQUES ÉVOLUE, LES INVESTISSEMENTS DOIVENT SUIVRE

LA SÉCURITÉ INFORMATIQUE DOIT DÉPASSER LES MÉTHODES CONVENTIONNELLES DE PROTECTION POUR GÉRER DE MANIÈRE EXHAUSTIVE LES MENACES ÉMERGENTES

Notre étude montre que se prémunir contre les logiciels malveillants sur les terminaux est l'une des 3 principales priorités en matière de sécurité, qui consomme la majorité du budget consacré à la sécurité informatique. Les pare-feu et la formation informatique complètent le podium des priorités les mieux dotées.

Toutefois, d'autres mesures de sécurité capables de prévenir les risques, comme la surveillance et les alertes automatiques (26 %), la protection contre les logiciels malveillants sur les appareils mobiles (17 %) et la gestion des correctifs tiers (14 %), ne sont pas aussi bien dotées.

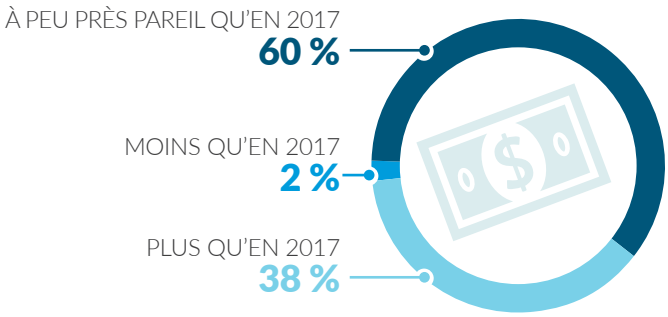
D'ailleurs, les professionnels de l'informatique affirment que les domaines dans lesquels ils investissent le moins sont :

La gestion des correctifs tiers et l'accès des utilisateurs aux appareils mobiles et au matériel.

Ces mesures, qui reçoivent peu d'investissements, ont pourtant de grands avantages lorsqu'elles sont mises en œuvre :

- Gagnez du temps et de l'argent et améliorez la productivité en surveillant les menaces, et en distinguant les menaces réelles des fausses menaces
- Améliorez la sécurité en vous concentrant sur les vrais incidents de sécurité
- Assurez la conformité avec les meilleures pratiques en matière de sécurité
- Vérifiez que la sécurité de votre entreprise est à jour et que toutes les dernières fonctionnalités sont installées
- Faites en sorte que les appareils mobiles des employés n'offrent pas une passerelle vers les données et informations privées de votre entreprise

BUDGET INFORMATIQUE 2018 VS 2017



La **vaste majorité (70 %) des professionnels de l'informatique** alloue **moins de 25 %** de leur budget à la sécurité informatique

CE QUE VOUS POUVEZ FAIRE

Alors que les cyberattaques deviennent de plus en plus fréquentes et sophistiquées et que l'on constate une prolifération des terminaux sur les lieux de travail, les équipes informatiques se préparent en mettant en place diverses mesures de sécurité et en accordant la priorité à la gestion des terminaux. Toutefois, il faudrait en faire plus pour éviter de subir les cyberattaques :

ÊTRE PROACTIF

N'attendez pas une attaque ou une faille pour gérer la sécurité. Les mesures de sécurité préventives, comme la surveillance et les alertes automatiques ou la gestion des correctifs, peuvent protéger votre organisation contre de nombreuses attaques.

PATCHER VOS SYSTÈMES

La gestion des correctifs est un élément essentiel de la sécurisation de votre infrastructure informatique. Que vous consacriez un jour de la semaine au déploiement des correctifs sur vos systèmes ou que vous mettiez en place des alertes proactives pour vous informer lorsqu'ils sont nécessaires, la gestion des correctifs est essentielle.

METTRE EN ŒUVRE UNE APPROCHE PLUS GLOBALE DE LA SÉCURITÉ

Les attaques ne concernent plus que les PC. Les appareils mobiles, les serveurs et autres terminaux sont de plus en plus vulnérables aux cyberattaques.

ÉDUQUER VOS EMPLOYÉS

Aider les employés à adopter et conserver de bons comportements et de bonnes habitudes en matière de cybersécurité est essentiel pour sécuriser vos infrastructures informatiques.

Sources

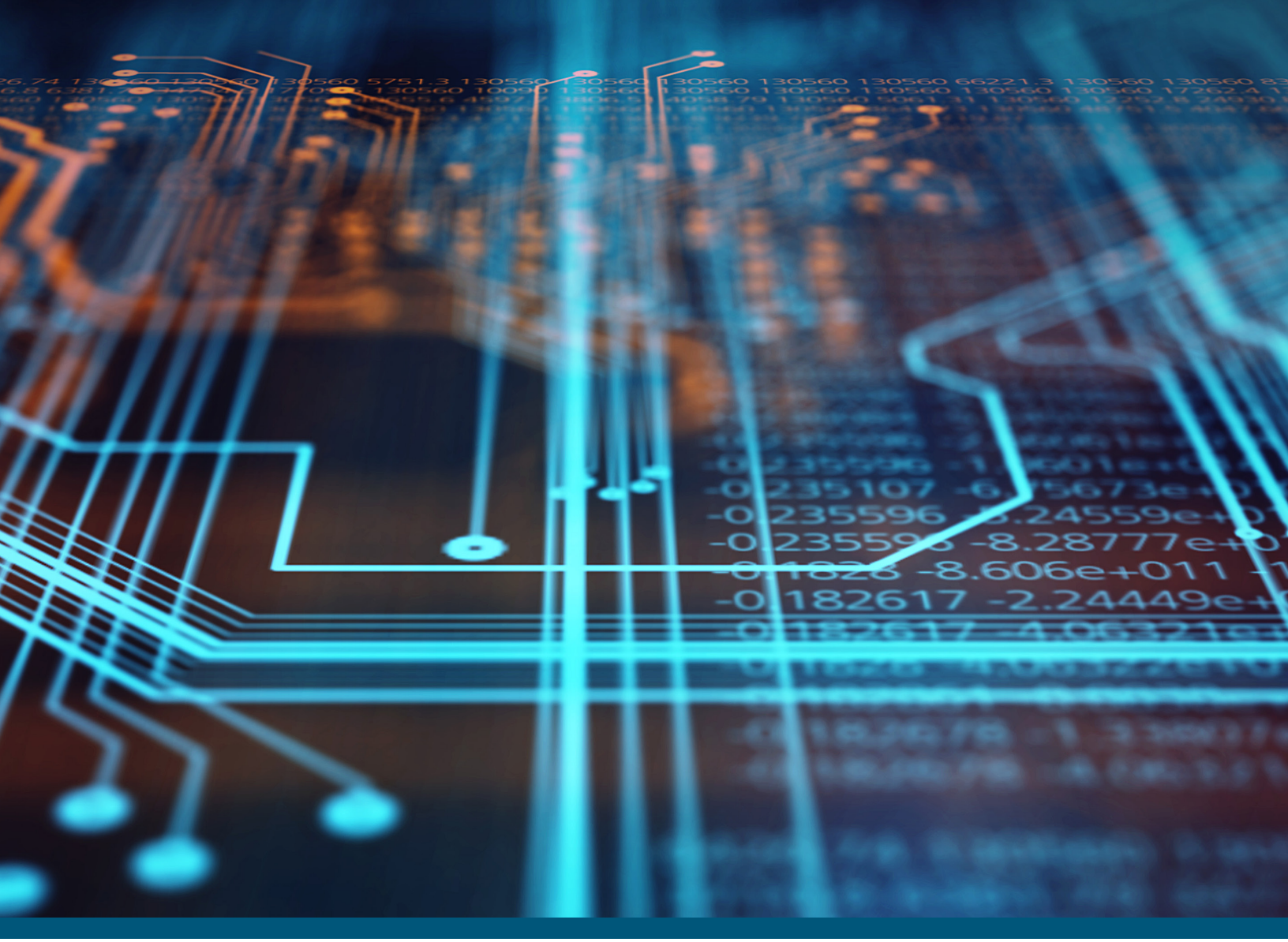
[1] Mobile Business Insights: The latest BYOD trends and predictions, from mobile focus to endpoint management par Jonathan Crowl, 14 août 2017

[2] Entrepreneur: Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware par Jorge Rey, 30 novembre 2016

[3] Infographie ZDNet.com : 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud par Amy Talbott, 2 octobre 2017

[4] 2016-2017 Ransomware statistics and facts Published par Sam Cook, 17 janvier 2018 dans Antivirus

[5] Verizon 2018 Data Breach Investigations Report par Maria Korolov, CSO, 10 avril 2018



Central by LogMeIn

AUTOMATISATION ET GESTION DES TERMINAUX SIMPLE ET SÉCURISÉE

LogMeIn Central, qui fait partie des solutions de gestion des identités et des accès de LogMeIn Inc., est une solution dédiée à la gestion des terminaux via le nuage qui permet aux professionnels informatiques de surveiller, de gérer et de sécuriser efficacement leur infrastructure informatique. Que vous ayez des employés distants ou des terminaux disséminés dans le monde entier, LogMeIn Central fournit aux services informatiques la vitesse, la souplesse et la visibilité nécessaires pour augmenter la productivité, diminuer les coûts et atténuer les risques. Classé numéro 1 des outils d'accès à distance pour la gestion des parcs d'ordinateurs des PME, LogMeIn Central équipe chaque terminal sur votre réseau de fonctions d'accès à distance haut de gamme, afin que vous puissiez les dépanner à toute heure et en tout lieu.

https://www.logmein.com/central