LIVRE BLANC

Cloud: Isoler pour mieux protéger

La Covid-19 offre aux RSSI une occasion unique d'isoler leur environnement web.

Un vent nouveau souffle sur la cybersécurité. Même avant la pandémie, la mécanique du changement semblait s'accélérer. Aujourd'hui, les entreprises, la tech et, plus généralement, la société dans son ensemble semblent évoluer à un rythme effréné.

Force est de constater que la crise sanitaire et son effet catalyseur sur la transformation digitale ont grandement compliqué le travail des RSSI. Mais ils ont aussi ouvert la voie à de nouvelles approches de la cybersécurité.

Les vulnérabilités actuelles se nourrissent de l'explosion du nombre de télétravailleurs, de l'évolution des comportements des clients et de la complexité des environnements cloud. Mais plutôt que de revenir aux vieux réflexes ou bricoler des solutions de fortune, le moment est venu de remettre à plat tout le modèle traditionnel axé sur les technologies de détection et de prévention.

À l'heure où 81 % des entreprises déclarent avoir subi une intrusion de quelque nature que ce soit, la cybersécurité se situe clairement à un tournant. Les organisations tiennent ainsi une opportunité de sortir renforcées de la pandémie, à condition toutefois de revoir leur mode de pensée et de porter un nouveau regard sur l'isolation.

Une sensation de déjà-vu?

Le concept d'isolation n'est pas nouveau. Par contre, les technologies qui sous-tendent les solutions actuelles le sont. Dans les départements informatiques, ces innovations promettent de mettre un terme au fatalisme ambiant du genre : « nous serons compromis tôt ou tard ». Postes de travail virtuels (VDI), virtualisation des applications, virtualisation des clients... les technologies d'isolation traditionnelles ont pour fonction première d'empêcher du contenu actif d'atteindre les terminaux. Si le principe est bon, l'expérience utilisateur (UX), elle, en pâtit. Avec la VDI et les applications virtuelles, le contenu en question est exécuté sur une infrastructure séparée avant d'être restitué sur l'écran de l'utilisateur pixel par pixel. Résultat : des temps de chargement à rallonge des pages web et un décalage notable entre l'action de l'utilisateur (saisie clavier, clic sur un lien, etc.) et son affichage à l'écran. En outre, les utilisateurs perdent souvent des fonctions standards comme l'impression ou le copier-coller de contenu.

81%

des entreprises déclarent avoir subi une intrusion d'une nature ou d'une autre.[1]

[1] The Future of IT Network Security Report 2020, Menlo Security

La virtualisation des clients nécessite l'installation de logiciels spéciaux sur les terminaux, la modification du système d'exploitation et une reconfiguration des PC, ce qui rend souvent ces clients instables. Même lorsque tout se passe comme prévu, la virtualisation consomme une quantité importante de ressources des machines des utilisateurs. C'est précisément pour lutter contre ce phénomène que la plateforme cloud de Menlo Security isole le contenu web à l'aide de notre technologie Isolation Core™. Ainsi, elle offre aux entreprises un affichage 100 % sécurisé du contenu des e-mails et des pages web, sans nuire à la productivité et à l'expérience utilisateur.

Phishing, ransomware, malvertising... la plateforme Menlo s'attaque aux principales menaces tout en sécurisant les messageries personnelles et professionnelles et en facilitant la mise en conformité des entreprises – le tout sans perte de fonctionnalités ni dégradation de l'UX.

Étudions désormais ses avantages concrets pour une entreprise comme la vôtre.

70%

des salariés utilisent des solutions SaaS et un accès à distance pour connecter leur appareil au réseau de leur entreprise..

Protection renforcée des télétravailleurs

Le basculement en télétravail vous a certes permis de maintenir la continuité de votre activité en cette période de grande incertitude. Mais le revers de la médaille, c'est que le travail à distance complique aussi votre cybersécurité. Aujourd'hui, au moins 70 % des salariés utilisent des solutions SaaS et un accès à distance pour connecter leur appareil au réseau de leur entreprise. Quant aux exploits de navigateur, ils exposent vos utilisateurs à tous les dangers. D'où l'importance capitale d'une maintenance régulière (correctifs, mises à jour, etc.). Toutefois, il est difficile de s'y tenir lorsque les utilisateurs, les terminaux et les équipes IT sont géographiquement dispersés.
Dans une certaine mesure, les RSSI comptent sur la discipline et la vigilance inflexibles de leurs utilisateurs. Dans les grandes entreprises, ce sont des dizaines de milliers de terminaux qui dépendent de leur assiduité. Autant dire que le défi est de taille, sachant que le moindre de ces appareils peut causer la paralysie de tout un réseau.

C'est là que Menlo Security Isolation Core™ entre en jeu pour veiller à ce que vos politiques de cybersécurité s'appliquent à tous vos utilisateurs où qu'ils se connectent – chez eux, au bureau, sur un site client ou à partir d'un réseau Wi-Fi public. Ainsi, votre entreprise et vos télétravailleurs sont protégés en permanence. Menlo Security a étendu sa technologie Isolation Core™ à sa Cloud Security Platform afin de vous fournir une couche de protection séparée et universelle dans le cloud. Tout le trafic web et e-mail passe par cette plateforme qui bloque les menaces, tout en laissant le reste du trafic circuler à l'écart des terminaux des utilisateurs. De leur côté, les équipes de sécurité peuvent protéger les données et contrôler ces flux à partir d'une seule et même console. En clair, même si l'appareil d'un utilisateur comporte une vulnérabilité connue ou inconnue, les malwares ne l'atteindront pas. Aucun contenu – malveillant ou non – ne s'exécutera sur le navigateur des utilisateurs.

La passerelle web sécurisée (SWG) de notre plateforme intègre un CASB (Cloud Access Security Broker), des fonctions de prévention des pertes de données (DLP), un pare-feu « as a Service » (FWaaS) et Menlo Private Access. Notre ambition : offrir un accès Internet sécurisé et transparent aux entreprises et à leurs utilisateurs. Aujourd'hui, nous protégeons huit des dix plus grandes banques de la planète, quatre des cinq principaux émetteurs de carte de paiement et plusieurs administrations fédérales américaines..

Environnement sécurisé pour le cloud et la transformation digitale

Tout projet de transformation digitale passe par la migration des services et de l'infrastructure IT dans le cloud, rompant ainsi avec le modèle traditionnel de réseau en étoile (hub-and-spoke) selon lequel tout le trafic Internet doit passer par un point de contrôle central. Si cette architecture permet aux utilisateurs de se connecter aux plateformes SaaS et aux applications web depuis n'importe où dans le monde, le passage systématique par un point de contrôle central peut créer un goulet d'étranglement et allonger les temps de latence..

Les applications SaaS utilisées par les salariés pourront changer au fil du temps, ce qui modifiera les schémas de trafic. À elle seule, l'application Office 365 peut créer plus de 20 connexions persistantes par utilisateur, avec pour conséquence une saturation des équipements réseau. Quant aux fluctuations du volume de trafic, elles créent des schémas imprévisibles qui risquent de surcharger certains composants clés de l'environnement de sécurité réseau. Qu'ils soient pris séparément ou collectivement, ces problèmes nuisent aux performances des applications et par là même à l'expérience utilisateur. En proposant une tout autre approche de la protection des utilisateurs, l'isolation permet de sortir de l'impasse. Au lieu de créer un effet d'entonnoir, cette technologie exécute les sessions web à l'écart des terminaux des salariés et en restitue le contenu sur leur écran.

Quels que soient les documents téléchargés ou les liens consultés, les cybercriminels ne peuvent entrer en contact direct avec les terminaux utilisateurs, ce qui bloque les malwares et prévient les autres menaces de type mouvements latéraux.Les salariés peuvent alors utiliser Internet en toute sérénité et bénéficier de tous les avantages du cloud sans devenir une menace en puissance pour leur entreprise.

ThatEn d'autres termes, l'isolation est un passage obligé de votre migration cloud et de votre transformation digitale. Elle vous permet de gagner en visibilité sur le trafic et d'appliquer scrupuleusement tous les contrôles de sécurité pour libérer le potentiel des applications SaaS. Vos salariés n'ont alors rien à craindre puisque tout le trafic web passe par la plateforme

Études de cas

Plus de 350 des plus grandes entreprises au monde utilisent déjà la plateforme d'isolation de Menlo Security pour protéger leurs utilisateurs et bloquer les malwares au quotidien.

Quels que soient les documents téléchargés ou les liens consultés, les cybercriminels ne peuvent entrer en contact direct avec les terminaux utilisateurs, ce qui bloque les malwares et prévient les autres menaces de type mouvements latéraux.Les salariés peuvent alors utiliser Internet en toute sérénité et bénéficier de tous les avantages du cloud sans devenir une menace en puissance pour leur entreprise.

ThatEn d'autres termes, l'isolation est un passage obligé de votre migration cloud et de votre transformation digitale. Elle vous permet de gagner en visibilité sur le trafic et d'appliquer scrupuleusement tous les contrôles de sécurité pour libérer le potentiel des applications SaaS. Vos salariés n'ont alors rien à craindre puisque tout le trafic web passe par la plateforme d'isolation de Menlo Security.

Un établissement financier mondial a déployé la technologie Menlo Security Isolation Core™ pour plus de 100 000 utilisateurs. En l'espace de 180 jours, ces derniers ont cliqué sur près de 2 000 liens de phishing et accédé à pas moins de 8 500 sites web malveillants. Seuls 30 % des clics sur ces sites étaient considérés comme sûrs..

Nombre d'infections par malware et autres compromissions réseau : zéro..

Aux États-Unis, une banque régionale comptant 2 000 salariés et un chiffre d'affaires annuel avoisinant le milliard de dollars a isolé son réseau pour se prémunir contre 100 % des menaces web et de messagerie. En trois ans, elle est parvenue à décommissionner tous ses équipements physiques et à migrer sa sécurité dans le cloud. En réduisant la consommation VPN de bande passante, elle a pu améliorer ses performances réseau..

Retour sur investissement : 261 %.

Une administration fédérale américaine et ses 80 000 utilisateurs ont obtenu d'excellents résultats au bout de 30 jours d'utilisation de la Cloud Security Platform de Menlo Security.

Plus de 8 000 sites web malveillants consultés : zéro infection par malware ou autre compromission..

L'isolation et son effet libérateur

Dans tous les secteurs, les bouleversements provoqués par la Covid-19 (nouveaux comportements, parcours clients 100 % numériques et explosion du télétravail) ont accéléré la transformation digitale.

l'heure où la pandémie change nos modes de vie et de travail, les équipes de cybersécurité ont du mal à tenir le rythme. En cause : l'inadéquation des méthodes traditionnelles de détection et de réponse face à la migration en masse des applications et systèmes critiques vers le cloud..

C'est donc le moment de repenser la sécurité des réseaux, des ressources propriété intellectuelle et des utilisateurs contre un champ de cybermenaces toujours plus vaste. Dès lors qu'elles feront les bons choix, les entreprises pourront atteindre un niveau de protection sans précédent..

En somme, les RSSI tiennent une occasion unique de s'affranchir des concepts réducteurs du passé.

Alors que la transformation digitale poursuit son inexorable marche, l'isolation selon Menlo Security s'impose comme la garante de la sécurité de l'Internet et de la messagerie des utilisateurs. Ainsi, les salariés peuvent accéder à leurs applications web et leurs services SaaS depuis n'importe où et n'importe quel terminal, sans risquer d'infecter le réseau de leur entreprise.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The company's Cloud Security Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 695-0695
ask@menlosecurity.com