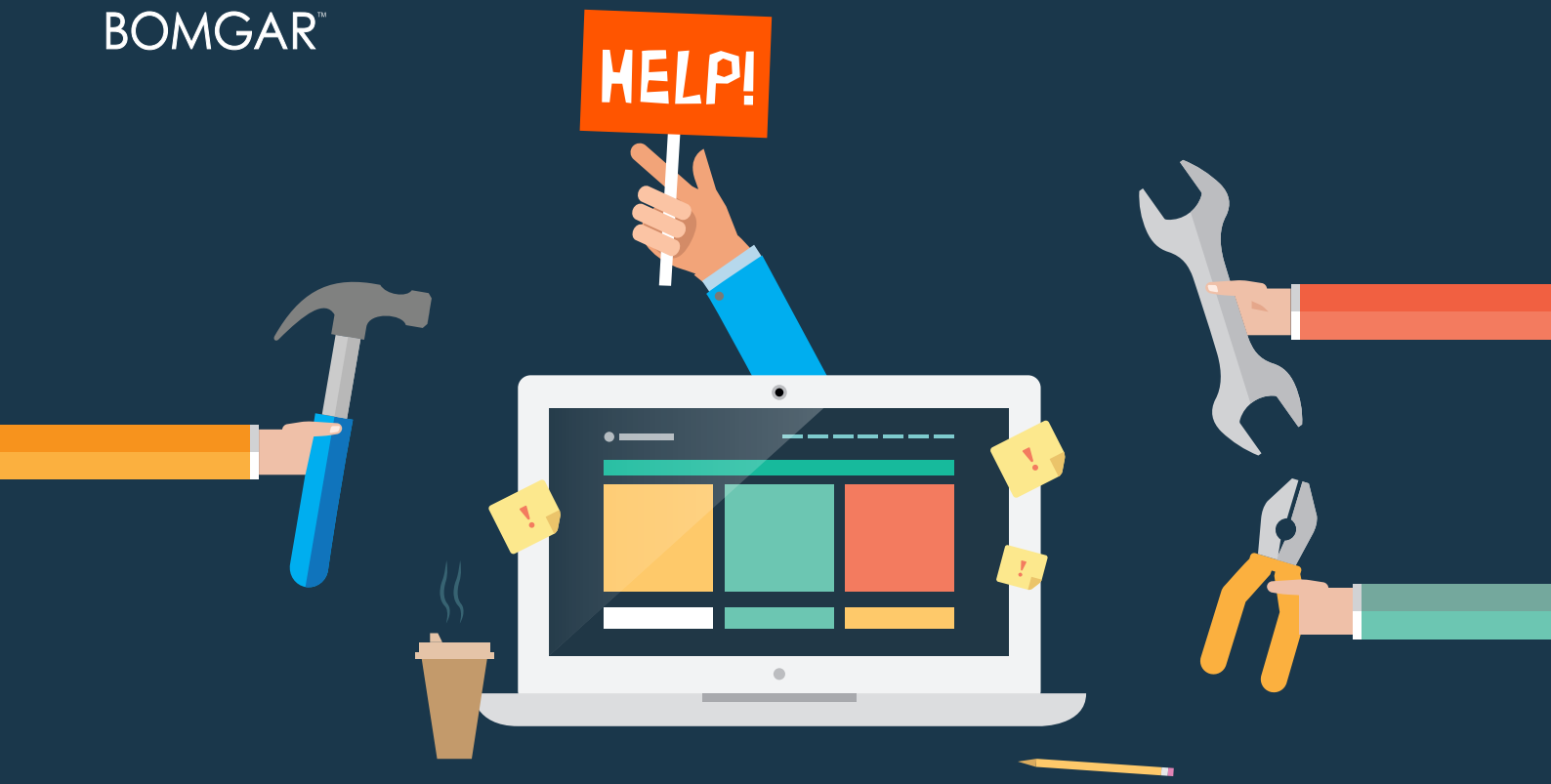
BOMGAR™



SOLUTIONS DE PRISE EN MAIN À DISTANCE : N'EN CHOISISSEZ-EN QU'UNE, MAIS CHOISISSEZ-LA BIEN

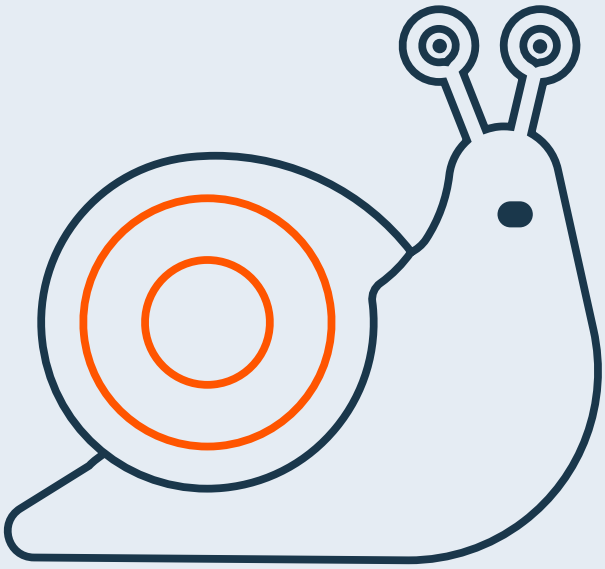
Les bénéfices de la consolidation pour votre entreprise

Trop d'équipes support technique utilisent encore plusieurs outils de prise en main à distance (PMAD) pour accompagner leurs utilisateurs. Faites le bilan au sein de votre propre organisation. Il est très probable que différentes solutions soient utilisées pour couvrir les différents cas d'utilisation tels que :

- Dépanner les utilisateurs au sein et en dehors du périmètre réseau traditionnel
- Accéder à distance aux serveurs, postes de travail et autres systèmes fonctionnant sans opérateur
- Assurer la maintenance des dispositifs réseau (switches, routeurs, etc.)
- Assurer une maintenance multi-plateforme (Windows, Linux et Mac)
- Assurer le support d'un large panel de terminaux mobiles sous iOS et Android
- Faciliter l'accès à distance des fournisseurs et tiers
- Dépanner des dispositifs hors réseau tels que des robots industriels ou autres dispositifs non connectés à Internet

Toutefois, lorsqu'il s'agit d'outils de PMAD, moins il y en a, mieux c'est. Le fait d'utiliser plusieurs outils ralentit la productivité, alourdit les tâches administratives, coûte bien plus cher qu'on ne le pense et met en danger la sécurité informatique.

"En l'absence d'une stratégie à long terme, un patchwork de plusieurs produits et outils est non seulement difficile à gérer mais aussi source d'inefficacité, de frais supplémentaires et d'insécurité."



Inefficacité et gestion complexe

Des processus manuels ou hétérogènes impactent la productivité. Quand votre équipe de support informatique utilise différents outils de contrôle à distance, les tâches que réalisent au quotidien les techniciens sont souvent ralenties par le temps nécessaire pour passer d'une solution à une autre, selon les opérations à effectuer. Ce manque d'efficacité sera encore plus important s'il n'y a pas d'intégration avec les systèmes CRM, solutions ITSM, portails de support en ligne et support par chat. Pour gérer un incident, vos techniciens devront sans doute ouvrir plusieurs programmes, ce qui créera une expérience incohérente pour l'utilisateur.

De nombreux outils basiques d'accès à distance comme VNC, RDP et certaines versions de TeamViewer et LogMeIn n'offrent pas la flexibilité et la modularité que recherchent les organisations. Certains ne supportent même pas tous les systèmes d'exploitation utilisés ou ne peuvent pas s'intégrer avec les solutions CRM ou ITSM en place.

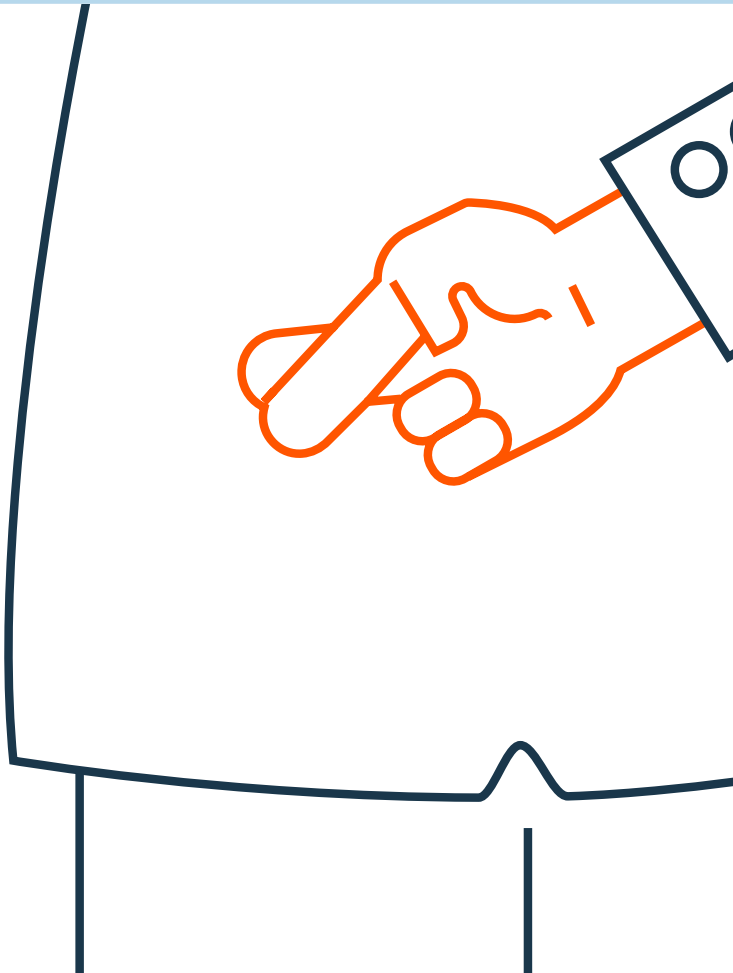
Les solutions les plus basiques sont souvent très chronophages et lourdes à gérer. Avec la solution Bomgar, l'administration et la gestion des utilisateurs, des groupes et des permissions se font de façon centralisée. Le provisioning rapide s'intégrant avec les annuaires existants comme LDAP/Active Directory permet aux administrateurs d'automatiser l'administration de la solution Bomgar et de supprimer tous les processus manuels.

Quelle réelle valeur ?

Les outils basiques et gratuits de prise en main à distance ont souvent des cas d'utilisation très limités qui ne satisfont pas les besoins des entreprises désormais très connectées et équipées en termes de technologies. Si vous souhaitez avoir accès à distance à votre PC fixe personnel ou exécuter des tâches de support basiques pour une petite entreprise, un outil de support gratuit pourra faire l'affaire.

Mais pour des besoins plus complexes ou pour des opérations de support dans de plus grandes entreprises, étendre les fonctionnalités de ces outils devient vite très coûteux. Le manque d'efficacité des outils rallonge les délais de résolution des incidents et impacte la profitabilité des opérations.

Peut-être avez-vous même déjà été victime de la technique d'appât classique qui vous contraint à acheter des compléments (add-ons) et des mises à niveau non inclus dans les frais de licence, pour obtenir de la solution en question qu'elle fasse ce dont vous avez besoin.



Et la sécurité dans tout ça ?

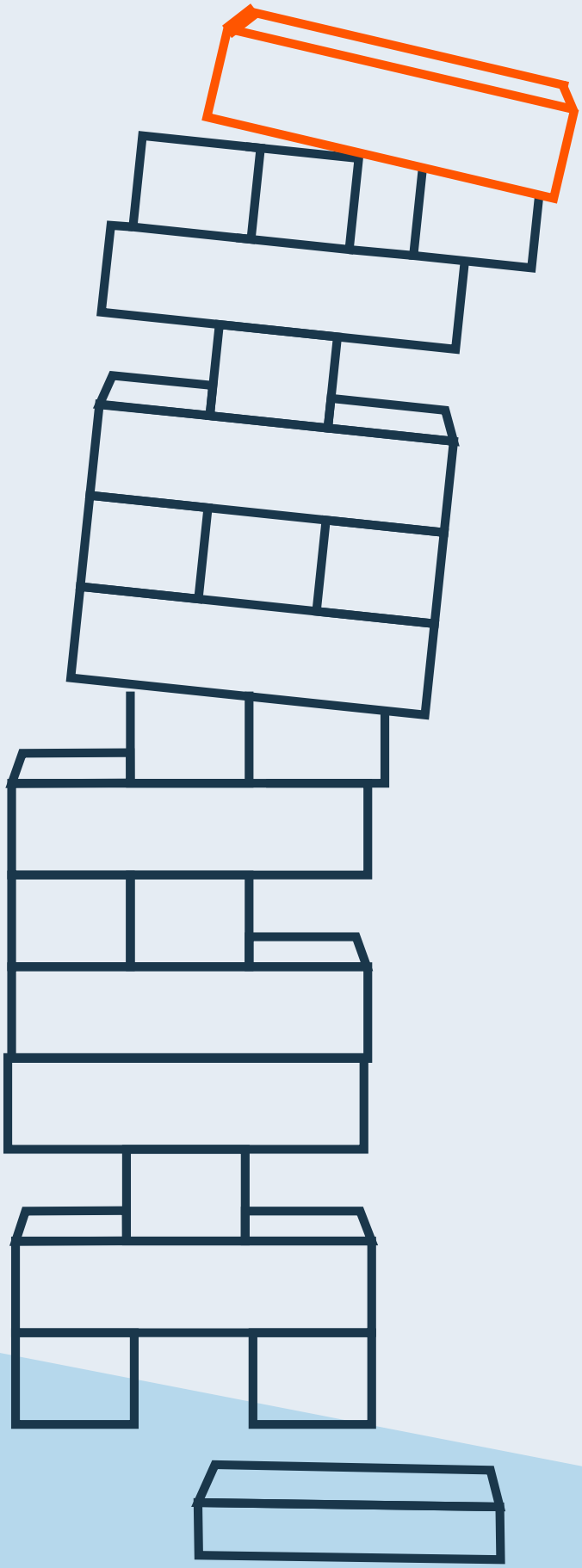
L'accès à distance est le vecteur d'attaque préféré des cybercriminels[1]. Ces derniers trouvent facilement des chemins d'accès à distance mal sécurisés à votre réseau, et la plupart des entreprises et équipes sécurité n'ont pas connaissance de l'ensemble des chemins d'accès à distance qu'utilisent les employés et les fournisseurs. Souvent, les entreprises ne sont pas en mesure de savoir combien de connexions de prise en main à distance ont eu lieu pendant une période donnée, alors imaginez pour savoir ce qui s'est passé durant ces sessions !

De nombreux outils traditionnels de prise en main à distance n'offrent pas de contrôle sur les connexions, de reporting ou d'enregistrement, ou n'offrent que des fonctionnalités très limitées. Il en résulte des enregistrements incomplets - voire inexistants - avec différents niveaux d'informations ou sous différents formats, et donc le besoin d'agréger et de synchroniser les logs à partir de multiples silos de données.

L'utilisation de plusieurs outils de prise en main à distance crée des problèmes de sécurité avant même qu'un incident ne se produise. Peu de solutions de prise en main à distance peuvent s'intégrer avec des solutions de gestion d'identités ou de répertoires tels qu'Active Directory, LDAP ou RADIUS. Gérer manuellement qui a accès aux outils expose donc l'entreprise à des risques conséquents.

Des outils comme les VPN représentent un risque énorme pour les fournisseurs et tierces parties. Les cybercriminels ciblent ces utilisateurs pour avoir accès au VPN et s'infiltrer sur le réseau. Il ne leur reste alors plus qu'à s'y déplacer latéralement pour accéder, sans aucune autorisation requise, aux systèmes sensibles, sans même pouvoir être détectés avant bien longtemps.

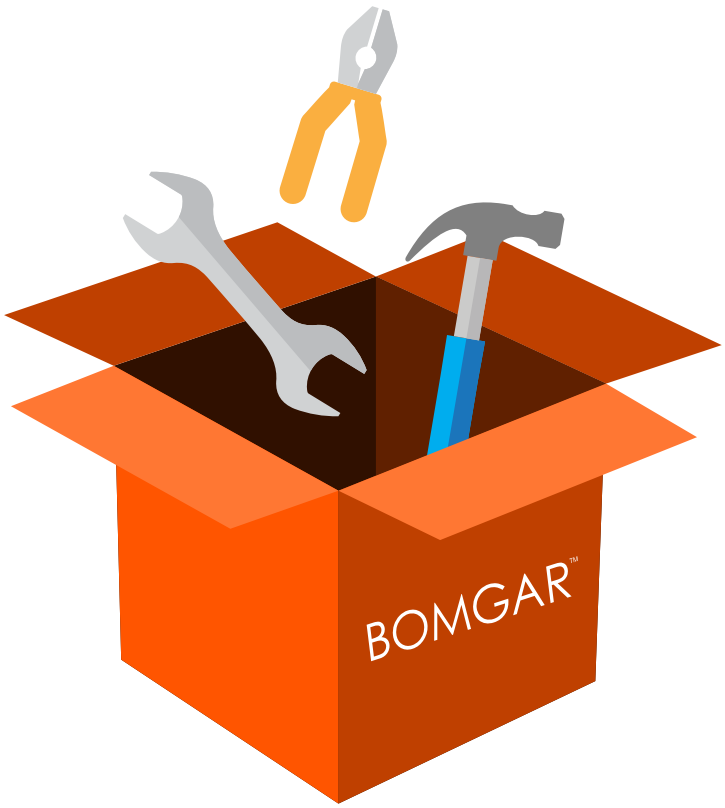
Enfin, quand une entreprise ne centralise pas ses technologies de prise en main à distance, la coexistence de plusieurs outils crée toujours plus de brèches de sécurité. Et quand une entreprise manque de visibilité sur l'activité de support, le risque qu'un cybercriminel utilise des identifiants volés au service technique pour compromettre des données augmente.



[1] 2017 Trustwave Global Security Report

Consolidez votre support à distance avec Bomgar

Bomgar vous permet d'accéder à distance à tout système, rapidement et via une solution unique, pour le dépanner quelle que soit la plate-forme et où qu'il se trouve dans le monde. Bomgar offre les fonctionnalités de sécurité, d'intégration et d'administration dont vos équipes IT et support client ont besoin pour gagner en productivité, accroître la performance et délivrer une expérience client supérieure.



"Bomgar nous permet de prendre la main sur Windows, Mac, Android, Linux etc., et d'opérer sur tous les systèmes : stations de travail, portables, PC et bien plus."

UNIVERSITE TOULOUSE 1 CAPITOLE

Performance et efficacité. Analysez vos processus de support : il y a de fortes chances pour que de nombreux cas se trouvent être des exceptions et cas particuliers. Avec Bomgar, vous constaterez que tous les scénarios de support sont standards et peuvent être gérés à partir d'un seul et même outil. Les techniciens se connectent aux utilisateurs, où qu'ils soient et quelle que soit la plateforme utilisée. Les intégrations proposées par Bomgar avec différentes solutions ITSM, les API et les kits SDK (Software Development Kit) permettent à votre organisation de maximiser l'investissement de l'infrastructure existante.

Pas de frais cachés. Utiliser une solution unique supprime les achats en doublon. Aussi, mettez à profit le temps nécessaire pour l'installation, la maintenance, le dépannage ou la gestion de plusieurs outils au service de la résolution d'incidents. Contrairement à certains autres fournisseurs, Bomgar ne facture pas plus pour des fonctionnalités clés telles que le partage de caméra à distance ou le support sur terminaux mobiles : tout est compris dans la licence.

Sécurité renforcée. En amont de la prise en main à distance, Bomgar contrôle l'authentification du technicien en s'intégrant avec les protocoles de gestion d'identités et de fournisseurs de sécurité externe (Active Directory, LDAP, Kerberos et RADIUS). Les clients ont des obligations règlementaires et des approches à la conformité différentes : Bomgar permet aux administrateurs de fixer leurs propres règles par technicien ou par équipe.

Traçabilité. Chaque session Bomgar est enregistrée et tracée dans un répertoire centralisé. L'administrateur peut visualiser tout ce qui a été fait lors de la session et ainsi faciliter la préparation des audits ou identifier la source d'une faille potentielle. De plus, l'intégration avec les outils SIEM favorise les alertes et le monitoring.

Pour savoir comment Bomgar Remote Support peut aider votre organisation, visitez www.bomgar.com/fr/controle-a-distance

A PROPOS DE BOMGAR

Bomgar est le leader des solutions d'accès sécurisés pour les entreprises. Les solutions Bomgar pour le support et la prise en main à distance, et pour la gestion des accès privilégiés et des identifiants aident les professionnels du support et de la sécurité informatiques à améliorer leur productivité et la sécurité de leurs systèmes en proposant des connexions fiables et contrôlées à tout type de système ou périphérique, partout dans le monde. Plus de 13 000 entreprises dans 80 pays utilisent Bomgar pour fournir des services d'assistance de qualité et réduire les risques de menaces sur les données et les systèmes critiques. Bomgar est une entreprise privée et possède des bureaux à Atlanta, Jackson, Washington D.C., Francfort, Londres, Paris et Singapour. Connectez-vous à Bomgar : visitez www.bomgar.fr.

CONTACT | INFO@BOMGAR.COM | +33 (0)1 44 75 75 80 | BOMGAR.COM/FR