SOPHOS

Démystifier le Zero Trust

L'ère du réseau d'entreprise et du périmètre de sécurité unique touche à sa fin. Les utilisateurs travaillent de plus en plus à distance, se connectant à Internet pour effectuer leur travail. L'essor des applications SaaS (Software-as-a-Service), des plateformes Cloud et d'autres services Cloud a petit à petit érodé le modèle consistant à protéger les ressources derrière un seul réseau. Nous ne pouvons plus nous reposer uniquement sur un réseau d'entreprise hermétique et nous ne devons plus accorder notre confiance à tous les systèmes situés à l'intérieur de ce réseau, car les frontières entre les réseaux s'effacent petit à petit.

Découvrez le « Zero Trust » ou la Confiance zéro, une philosophie de la cybersécurité qui touche à la manière de penser et de mettre en œuvre la sécurité. Le principe de Zero Trust se base sur la formule : « Ne faites confiance à rien, vérifiez tout » et se focalise sur la protection des ressources, où qu'elles soient physiquement ou numériquement, et sur le fait de ne jamais faire confiance à rien.

Aucun fournisseur, produit ou technologie ne vous permettra d'atteindre un niveau de confiance zéro. Pour y parvenir, il faut profondément revoir la manière dont nous protégeons nos ressources en modifiant notre approche de la cybersécurité et en installant une diversité de solutions de sécurité.

Ce livre blanc présente le concept de Zero Trust et les bénéfices de la mise en place d'un modèle Zero Trust, et il offre aux entreprises des conseils pour l'implémenter.

Les temps ont changé

Dans le domaine des technologies de l'information, la confiance peut être dangereuse, surtout lorsqu'elle est implicite, non qualifiée ou qu'on la donne sans condition.

Nous savons que créer un grand périmètre de sécurité hermétique à l'échelle de l'entreprise et faire confiance à tout ce qui se trouve à l'intérieur est une conception imparfaite. Ce type de réseau est très prisé des hackers : une fois à l'intérieur, ils échappent à la vue de tous. C'est alors pour eux un jeu d'enfant de se propager à travers le réseau et d'accéder aux systèmes importants, car les contrôles de sécurité les plus rigoureux se situent au niveau du périmètre.

Que vous le vouliez ou non, le périmètre s'érode.

Les utilisateurs travaillent de plus en plus à distance, sur des réseaux non fiables, comme les réseaux Wi-Fi publics des cafés par exemple. Ils veulent stocker leurs données dans le Cloud pour pouvoir y accéder à tout moment. Ils veulent utiliser leurs ordinateurs personnels pour accéder aux données et aux ressources de l'entreprise. Ils veulent un accès simplifié afin de travailler là où ils le souhaitent, quand ils le souhaitent et comme ils le souhaitent.

L'utilisation d'applications SaaS (Software-as-a-Service), de plateformes Cloud ou d'autres services Cloud sort les données du périmètre de l'entreprise, et les plateformes de Cloud public permettent désormais d'utiliser de nombreux appareils ou services en dehors de ce périmètre. Nos charges de travail se déplacent là où il est le plus rentable de les traiter, loin des réseaux que nous possédons, contrôlons et auxquels nous faisons confiance.

Tout est partout. L'ancien modèle de « réseau d'entreprise » doté de défenses statiques ne permet pas à aux entreprises d'adopter des éléments modernes comme le Cloud tout en protégeant simultanément les données, les utilisateurs et les clients. Nous devons profondément modifier notre approche.

Entrez dans le monde du Zero Trust

Le Zero Trust est une approche globale de la sécurité qui prend en compte ces menaces et les nouvelles méthodes de travail des entreprises. Il s'agit d'un modèle et d'une philosophie qui recouvrent la manière de penser et de mettre en œuvre la sécurité.

Il ne faut faire confiance à personne ni à rien de façon automatique, que ce soit à l'intérieur ou à l'extérieur du réseau de l'entreprise, même pas au réseau lui-même. Il ne faut pas faire confiance de manière implicite à l'emplacement sur un réseau si les défenses sont statiques, comme avec un pare-feu traditionnel.

Bien sûr, il faut pouvoir finir par faire confiance à quelque chose, mais avec le Zero Trust, cette confiance est temporaire et s'établit dynamiquement à partir de sources de données multiples, plus que nous n'en avons jamais utilisé par le passé, et elle est constamment réévaluée. Les sources de données incluent les informations sur la demande d'accès elle-même, sur l'utilisateur, le système, les conditions d'accès et sur les données d'intelligence sur les menaces. En outre, l'accès aux données ou aux ressources n'est accordé qu'en fonction des besoins, sur la base de chaque connexion.

Notre utilisation d'Internet au quotidien nous met sans cesse au contact de réseaux non fiables. Les ordinateurs qui ont accès à des réseaux Internet publics sont sécurisés de manière très différente de ceux qui se trouvent à l'intérieur d'un périmètre traditionnel, ce qui nécessite une surveillance supplémentaire et des couches de défense pour les protéger contre les menaces extérieures.

Le modèle Zero Trust vous encourage à traiter tous les appareils comme s'ils étaient connectés à Internet et, au lieu d'avoir un seul périmètre, vous devez créer des micropérimètres (ou microsegments), en appliquant des vérifications et des contrôles autour de chaque élément et entre chaque élément.

Les bénéfices du Zero Trust

Adopter un modèle Zero Trust apporte d'innombrables avantages, et nous avons dressé la liste des principaux.

Contrôlez l'ensemble du parc IT

Contrôlez tout, de l'intérieur de vos bureaux jusqu'à vos plateformes Cloud. Finis le manque de contrôle en dehors du périmètre de l'entreprise ou les difficultés avec les utilisateurs à distance.

Administrez et protégez tous les utilisateurs de la même manière

Ne plus considérer les choses comme étant à l'intérieur ou à l'extérieur du périmètre de l'entreprise permet de traiter tous les utilisateurs de la même manière. Cela simplifie la cybersécurité tout en garantissant que tous les systèmes et les utilisateurs sont traités de la même manière.

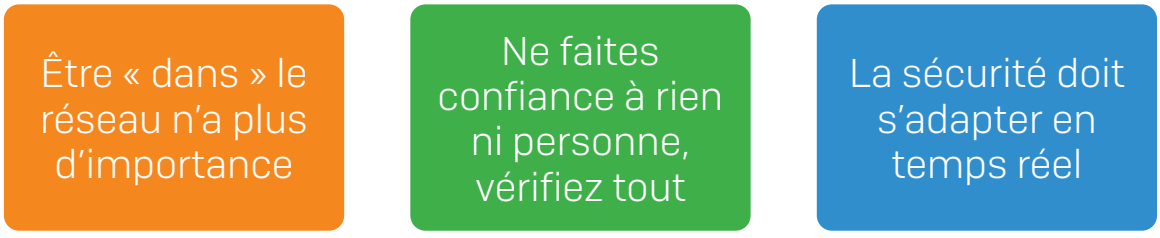
Maintenez la protection même lorsque vous n'avez pas la main/le contrôle total sur l'infrastructure utilisée

En utilisant l'identité, la localisation, l'état de santé de l'appareil, l'authentification multifacteur et la superposition de la supervision et de l'analyse, vous êtes en mesure d'avoir toujours en place une protection robuste quels que soient l'environnement, la plateforme ou le service.

Réduisez considérablement la mobilité des malwares ou des attaquants

Une fois à l'intérieur du périmètre, les attaquants ne pourront accéder qu'aux seuls systèmes auxquels l'utilisateur compromis a accès, ce qui les empêchera d'avoir le champ libre sur l'ensemble du réseau. En continuant à ne pas faire confiance à l'utilisateur authentifié, des contrôles mis en place entre ces systèmes limiteront encore la capacité de propagation.

Le Zero Trust en bref



Le Zero Trust est une notion importante qui fait l'objet de nombreuses discussions. Nous pouvons résumer les principaux concepts du Zero Trust en plusieurs préceptes faciles à garder en mémoire.

Être « dans » le réseau n'a plus d'importance

Imaginez que vous gérez votre entreprise depuis un endroit peu fiable, comme le Wi-Fi public d'un café, et que tous vos systèmes sont directement connectés au plus dangereux de tous les réseaux : l'Internet public. En imaginant cela comme votre réalité, vous êtes obligé de revoir entièrement votre sécurité et ne pas compter sur votre périmètre d'entreprise traditionnel.

Il y aura toujours des réseaux d'entreprise « de confiance » pour l'administration et les systèmes internes, mais l'objectif est de maintenir les utilisateurs ordinaires hors de ces réseaux, en utilisant des serveurs proxy d'applications et d'autres technologies, réduisant ainsi considérablement la surface d'attaque.

Ne faites confiance à rien ni personne, vérifiez tout

Partez du principe qu'il y a des attaquants à l'intérieur et à l'extérieur de vos réseaux et qu'ils sont là en permanence, attaquant constamment. Aucun utilisateur ou système ne doit être automatiquement considéré comme fiable et doit s'authentifier avant même d'envisager une connexion. En imaginant que vous êtes constamment attaqué de toutes parts, vous êtes poussé à mettre en place une authentification et une autorisation à toute épreuve pour vos ressources, à renforcer vos défenses et à surveiller et analyser en permanence tout ce qui se passe dans votre parc.

La sécurité doit s'adapter en temps réel

Les politiques de sécurité que vous mettez en place pour atteindre une confiance zéro doivent être dynamiques et changer automatiquement en fonction des informations provenant d'autant de sources de données et de technologies différentes que possible. Une politique statique comme « CET UTILISATEUR » sur « CE SYSTÈME » peut accéder à « CET ÉLÉMENT » ne vous protégera pas si ce système a été compromis alors que l'utilisateur l'utilise. Si votre politique prenait également en compte l'intégrité de l'appareil, comme l'identification des comportements malveillants, elle pourrait s'en servir pour s'adapter dynamiquement à la situation sans nécessiter l'intervention d'un administrateur.

Sophos a intégré depuis longtemps ce concept dans sa stratégie et sa philosophie de cybersécurité. Il s'agit de la Sécurité synchronisée, notre système de cybersécurité où nos produits partagent entre eux des informations. Cela nous permet d'avoir des politiques adaptatives et dynamiques, en tirant parti de toutes ces connaissances, de sorte qu'une politique de sécurité n'est jamais statique ni facilement contournable.

Tout cela n'est que la base d'une bonne posture et de bonnes pratiques de sécurité que vous avez peut-être déjà mises en place, notamment si vous vous êtes préparé pour le RGPD.

Les principes du Zero Trust

Ne faites confiance à rien. Jamais. Car lorsqu'on ne fait confiance à rien, on est obligé de recourir à des mesures de sécurité pertinentes partout où il y a un risque.

Vérifiez tout. Ne supposez pas que le fait de passer un contrôle donne naturellement confiance. Avoir des identifiants de connexion ne veut pas dire que vous êtes fiable. Cela veut seulement dire que vous avez des identifiants de connexion. Et ceux-ci peuvent être volés.

Nous pouvons décomposer cette approche en quatre principes simples à se rappeler.

Identifiez toujours

Vous avez besoin d'une source d'identité unique qui fasse autorité et vous devez l'utiliser partout grâce au Single Sign On (SSO). Tout doit être authentifié, avec une authentification multifacteur (MFA). Peu importe où se situe l'utilisateur, peu importe ce qu'il essaie d'accéder, validez ses identifiants, validez son 2e (ou 3e) facteur, et exigez régulièrement une réauthentification.

Si les identifiants sont volés ou si un système est piraté, la mise en place de l'authentification multifacteur et de la réauthentification régulière arrêteront rapidement l'attaquant.

Contrôlez toujours

Mettez en place des contrôles et des vérifications partout où cela est nécessaire, et adoptez et appliquez le principe de moindre privilège : les utilisateurs ne devraient avoir accès qu'au strict minimum nécessaire pour effectuer leur travail. Si un système est utilisé uniquement par les ressources humaines en Allemagne, alors seul le personnel en Allemagne devrait y avoir accès. Personne d'autre ne devrait pouvoir y accéder, même si le risque que cela se produise est très faible.

Analysez toujours

Ce n'est pas parce qu'une authentification a réussi, ou que l'accès est accordé à cet utilisateur ou à cet appareil, qu'il est fiable. Les menaces internes et les acteurs malveillants peuvent avoir accès à des identifiants valides. Enregistrez toute l'activité du réseau et du système pour pouvoir l'analyser et l'inspecter régulièrement, afin de vérifier ce qui se passe après l'authentification. Les outils SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response) et MDR (Managed Detection and Response) ont été conçus pour répondre exactement à ce besoin.

Protégez toujours

Utilisez une approche « Inside Out » de la cybersécurité. Vous devez penser la protection en vous focalisant d'abord sur les données avant de partir vers l'extérieur, en comprenant leurs possibles failles tout au long de leur cycle de vie au sein du réseau, depuis leur création jusqu'à leur destruction.

Prenez toujours en considération le risque avant tout, ne vous limitez pas à la conformité ou à la règlementation. Il est dangereux de n'appliquer la sécurité que pour répondre à un contrôle de conformité ou à une exigence règlementaire. Les exigences de conformité ne connaissent pas le contenu de votre réseau, les flux et les charges de travail, les systèmes et les technologies. Elles ne connaissent pas les risques liés à chaque élément possible de votre réseau. L'examen des risques et la modélisation des menaces auxquelles votre entreprise est confrontée vous permettront de savoir où la sécurité doit être renforcée, assouplie et où des micro-segmentations doivent être créées.

Progressez vers le Zero Trust

Comment pouvez-vous évoluer vers le Zero Trust et profiter de tous les avantages qu'il offre ?

Définissez votre surface et identifiez vos ressources

Cartographiez les chemins standards et les accès privilégiés

Mettez en place une architecture Zero Trust pour votre réseau

Créez des politiques Zero Trust

Supervisez et maintenez la posture de vos périmètres

Définissez votre surface et identifiez vos ressources

Tout d'abord, définissez quelle surface vous souhaitez protéger, contrôler et surveiller. Quelles sont les ressources, services, applications et systèmes utilisés par votre société ? Avoir une vision complète et bien définie de tout ce qui est utilisé sur l'ensemble du réseau vous aide ensuite à appliquer cette approche Zero Trust.

Cartographiez les chemins standards et les accès privilégiés

Une fois que vous avez tout pris en considération, vous devez ensuite cartographier les chemins standards : quels sont les flux, les comportements et les relations entre ces flux standards ? Ce groupe d'utilisateurs accède à cette application, ce système se connecte à ce réseau, ce service utilise ces données, etc. Mais aussi, quels sont les chemins privilégiés ? Cet administrateur voudra se connecter à cette console d'administration et utiliser le protocole RDP (Remote Desktop Protocol) pour accéder à ce serveur qui héberge des données sensibles, etc. Il faudra très certainement appliquer une sécurité ou des contrôles supplémentaires pour les chemins privilégiés.

Mettez en place une architecture Zero Trust pour votre réseau

Maintenant que vous savez ce qui est en jeu et qu'elles sont les relations entre tous les éléments, vous pouvez commencer à appliquer le concept de Zero Trust. Identifiez les mesures de sécurité et les contrôles d'accès que vous souhaitez appliquer, où vous souhaitez les appliquer, quelle technologie permettra de limiter au mieux quel risque, etc.

Créez des politiques Zero Trust

Ensuite, vous devez mettre en œuvre des politiques de sécurité Zero Trust qui utiliseront autant de sources de données différentes que possible pour ajouter du contexte à toute connexion ou demande.

Supervisez et maintenez la posture de vos périmètres

Enfin, et c'est peut-être le plus important, vous devez tout superviser finement afin de pouvoir maintenir vos périmètres nouvellement créés.

C'est l'un des plus grands changements auxquels les administrateurs doivent faire face. Alors qu'autrefois vous pouviez installer et configurer un antivirus sans jamais avoir à surveiller la console, avec le Zero Trust, vous devez changer vos habitudes.

Vous devez surveiller les événements qui se produisent, en exploitant des outils comme l'EDR (Endpoint Detection and Response) pour comprendre par où et comment une menace est entrée dans l'environnement et quels événements se sont produits avant une détection ou après une violation.

Des services managés ou MDR (Managed Detection and Response) peuvent réellement vous aider dans ce domaine, en permettant à des experts en cybersécurité de vous aider à surveiller votre réseau et à éliminer les menaces à votre place.

La pile de technologies Zero Trust

Il faut beaucoup de technologies pour sécuriser toutes les ressources et tous les assets sur votre réseau. Vous ne pourrez pas résoudre tous vos problèmes avec un seul éditeur, produit ou technologie.

Une pile de technologies Zero Trust doit couvrir deux aspects principaux : l'administration du Zero Trust et la sécurité et le contrôle de vos diverses ressources et assets.

L'administration est composée de 3 sous-domaines :

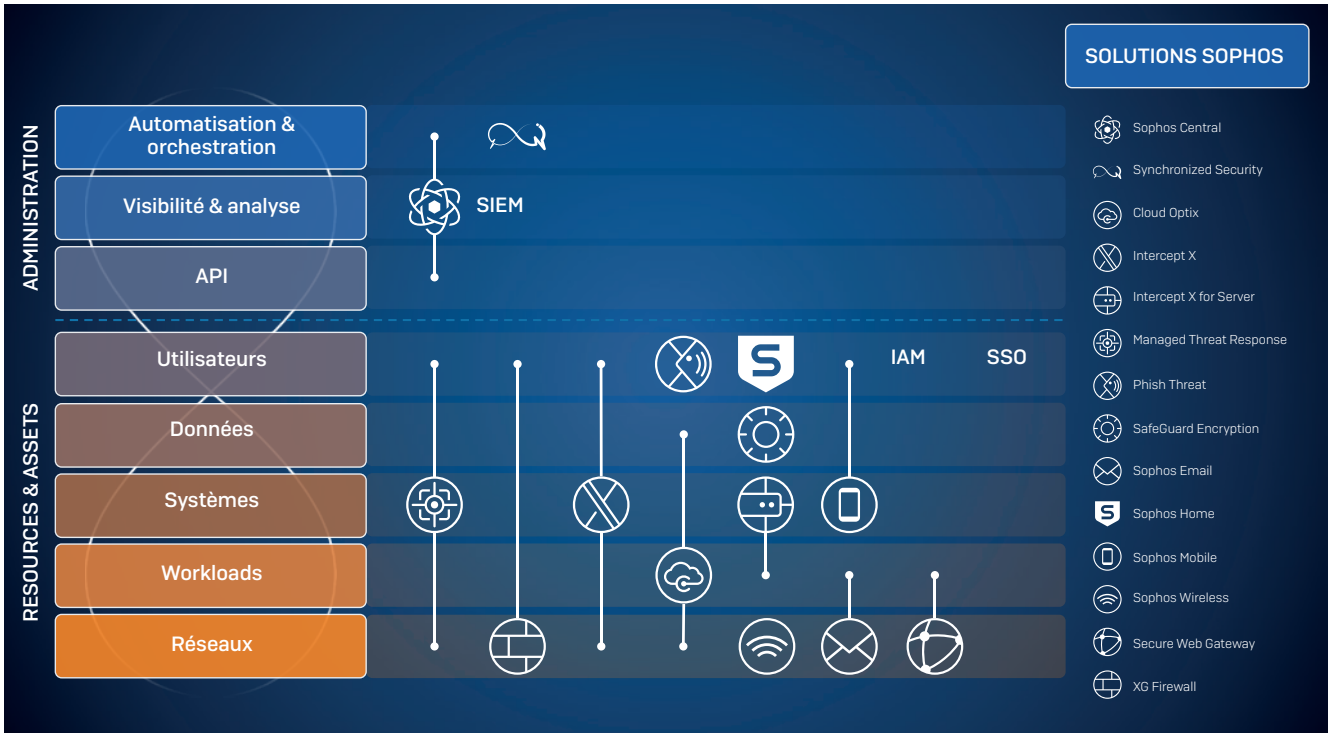
1. Automatisation et orchestration : pour définir des politiques dynamiques, coordonner les différentes technologies et tout mettre en place.
2. Visibilité et analyse : pour maintenir la surveillance du réseau et s'assurer que tout fonctionne, et pour identifier les menaces et les violations si elles se produisent.
3. API : pour intégrer vos différentes technologies entre elles, extraire des données d'un système pour les utiliser dans un autre.

Les ressources et assets sont composées de 5 sous-domaines :

1. Utilisateurs : les utilisateurs, admins, etc. qui travaillent pour ou avec l'entreprise.
2. Données : les éléments vitaux de toutes les entreprises et peut-être les ressources les plus importantes à protéger.
3. Systèmes : les serveurs, ordinateurs portables, machines virtuelles, etc. que vous utilisez au travail.
4. Workloads : les services et applications que vous utilisez pour traiter les données, effectuer des calculs, produire des rapports, etc.
5. Réseaux : les canaux de communication par lesquels les données cheminent — Web, email, Wi-Fi, Internet, etc.

Comment Sophos peut vous aider

Bien qu'un éditeur seul ne peut pas faire évoluer votre entreprise vers un modèle Zero Trust, Sophos dispose d'une vaste gamme de technologies pour vous en rapprocher le plus possible.



L'administration du Zero Trust

Sophos Central, notre plateforme de cybersécurité Cloud native, vous permet d'administrer un environnement Zero Trust. Elle orchestre toutes nos technologies dans une console unique, vous permettant de superviser toutes les technologies en un seul endroit et d'utiliser des API pour relier entre elles toutes les autres technologies tierces que vous utilisez.

Vous pouvez également utiliser un outil SIEM pour regrouper les journaux de vos produits Sophos et ceux des autres éditeurs, afin d'obtenir un aperçu complet de tout ce qui se passe dans votre entreprise. Nos API permettent d'extraire facilement des informations de notre plateforme Sophos Central pour les utiliser dans n'importe quel SIEM.

La Sécurité synchronisée de Sophos (contrôlée depuis Sophos Central) joue également un rôle majeur ici. En activant la sécurité synchronisée, les solutions Sophos partagent des informations entre elles et répondent automatiquement aux incidents. Dans un cadre Zero Trust, les solutions sont capables de s'adapter à tous les scénarios à l'aide de politiques de sécurité dynamiques et de réaliser automatiquement des tâches complexes comme l'isolement des machines.

Protection et contrôle des ressources et assets

Nombre de nos produits vous aident à sécuriser plusieurs ressources et assets en même temps, mais cela ne signifie en aucun cas que vous pouvez utiliser une seule technologie et vous reposer entièrement dessus. La sécurisation des utilisateurs, par exemple, nécessite un grand nombre de technologies différentes dans le cadre d'un réseau Zero Trust résilient.

Cloud Optix offre aux entreprises l'analyse en continu et la visibilité dont elles ont besoin pour détecter, corriger et prévenir les failles de sécurité et de conformité du Cloud qui pourraient les mettre en danger. Au sein d'un environnement Zero Trust, Cloud Optix aide à protéger les données, les systèmes, les workloads et les réseaux situés dans le Cloud public.

Intercept X offre une protection Endpoint incomparable. Il bloque la plus vaste gamme d'attaques avec une combinaison unique de technologies de détection des malwares par Deep Learning, de prévention des exploits, de détections comportementales et de protection anti-ransomware. Au sein d'un environnement Zero Trust, Intercept X aide à protéger toutes les ressources et assets.

Intercept X for Server est conçu pour protéger les environnements de serveur Cloud, locaux ou hybrides. Au sein d'un environnement Zero Trust, Intercept X for Server aide à protéger à la fois vos systèmes et vos workloads.

Le service MTR (Managed Threat Response) est notre solution de réponse aux menaces dirigée par des experts. Il fusionne Machine Learning et intelligence humaine et fournit des capacités de recherche, d'identification et de réponse aux menaces 24 h/24 et 7 j/7. Au sein d'un environnement Zero Trust, le service MTR aide à protéger toutes vos ressources et assets.

Phish Threat est notre solution anti-phishing dédiée. Vos employés bénéficient de formations de sensibilisation à la sécurité et vous obtenez des rapports conçus pour évaluer le niveau de préparation de votre entreprise face au phishing. Au sein d'un environnement Zero Trust, Phish Threat vous aide à protéger vos employés.

SafeGuard Encryption chiffre le contenu dès sa création. Il protège de manière proactive vos données en validant en continu l'utilisateur, l'application et l'intégrité de la sécurité d'un appareil avant d'autoriser l'accès aux données. Il peut ainsi protéger vos données dans un environnement Zero Trust.

Secure Web Gateway facilite la protection avancée du Web, en offrant des niveaux sans précédent de sécurité, de contrôle et d'informations du Web. Au sein d'un environnement Zero Trust, Secure Web Gateway aide à protéger à la fois les réseaux et les workloads.

Sophos Email utilise l'intelligence artificielle pour fournir une sécurité des messageries prédictive et plus intelligente. Au sein d'un environnement Zero Trust, Sophos Email aide à protéger vos réseaux et vos workloads.

Sophos Home est conçu pour protéger vos ordinateurs personnels et est basé sur la même technologie que celle utilisée dans nombre de nos produits commerciaux. Au sein d'un environnement Zero Trust, Sophos Home aide à protéger vos employés à domicile.

Sophos Mobile est notre solution UEM (Unified Endpoint Management) sécurisée pour les entreprises qui souhaitent consacrer moins de temps et d'énergie à la gestion et à la sécurisation des terminaux mobiles et traditionnels. Au sein d'un environnement Zero Trust, Sophos Mobile aide à protéger vos appareils, vos données et vos employés.

Sophos Wireless est une solution simple et efficace de gestion et de protection des réseaux sans fil. Au sein d'un environnement Zero Trust, Sophos Wireless aide à protéger vos réseaux.

XG Firewall offre une protection pare-feu Next-Gen complète qui expose les risques cachés, bloque les menaces inconnues et répond automatiquement aux incidents. Au sein d'un environnement Zero Trust, XG Firewall aide à protéger toutes vos ressources et assets.

L'utilisation de ces technologies est un excellent début pour évoluer vers un modèle Zero Trust. Cependant, comme nous l'avons déjà dit, aucun éditeur ou technologie, y compris Sophos, ne peuvent à eux seuls vous faire évoluer vers un environnement Zero Trust. Pour permettre à vos utilisateurs d'utiliser des services Cloud en tous lieux, vous aurez en outre besoin d'une solution robuste de gestion des identités et des accès (IAM) utilisant l'authentification Single-Sign On (SSO) pour utiliser votre source unique d'identité faisant autorité dans tous les systèmes et services. Cette technologie est un élément clé du modèle Zero Trust.

Apprenez-en davantage sur nos produits et services, et démarrez aisément des démos instantanées sur notre site www.sophos.fr.

Notre vision pour la cybersécurité

Le Zero Trust et notre vision pour la cybersécurité, la Sécurité synchronisée, visent les mêmes objectifs et se complètent mutuellement.

La Sécurité synchronisée est la cybersécurité en tant que système. Elle analyse, adapte et automatise en permanence les tâches informatiques les plus complexes tout en surveillant dynamiquement et en temps réel l'ensemble de l'activité du système, le comportement des utilisateurs, le trafic réseau et les postures de conformité. Toutes les technologies partagent des informations entre elles, en se donnant mutuellement des informations et de la visibilité là où une seule serait aveugle.

Les technologies devraient discuter entre elles. Ce n'est que par ce dialogue que nous pourrons mettre en place les politiques adaptatives et dynamiques dont nous avons besoin, basées sur des sources de données multiples, pour parvenir à un réseau Zero Trust.

Conclusion

Dans l'état actuel des choses, le Zero Trust n'est qu'une philosophie de la cybersécurité, que très peu d'entreprises sont en mesure d'adopter aisément. Néanmoins, comme les périmètres de sécurité s'érodent continuellement, la nécessité d'adopter cette philosophie va devenir de plus en plus pressante. Les cybercriminels ne cessent d'innover et les défenses ont du mal à suivre le rythme. Le modèle Zero Trust constitue un moyen de réduire véritablement les menaces tout en établissant de nouvelles normes en matière de protocole de cybersécurité.

Il est temps de penser différemment. Il est temps d'évoluer.

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

20-03-10 WP-FR (DD)

SOPHOS