Forcepoint

Présentation succincte

Zero Trust Content Disarm and Reconstruction for Web Gateways

La navigation sur le Web en toute sérénité

Défis

- Les entreprises sont infiltrées par des menaces de type « zero day » qui s'insinuent dans l'organisation avant que les défenses basées sur la détection ne puissent agir suffisamment vite, ou par des menaces totalement inconnues qui atteignent leur objectif sans jamais être correctement identifiées.
- Les téléchargements Web peuvent contenir des menaces qui perturbent le fonctionnement des applications et permettent aux assaillants de prendre le contrôle des systèmes de l'entreprise.
- Les téléchargements vers le Web peuvent contenir plus d'informations que ce qu'une organisation ne souhaite divulguer, nuisant à l'entreprise en révélant des informations sensibles.

La Solution

- La technologie unique Zero Trust CDR de Forcepoint part du principe que toutes les données sont dangereuses ou hostiles. Elle n'essaie pas de distinguer les bonnes des mauvaises. C'est ce qui en fait la seule véritable solution Zero Trust.
- Zero Trust CDR s'intègre à votre défense Web existante en quelques instants.

Avantages

- Livrez systématiquement un contenu sûr et sans menace à travers les frontières du Web
- Neutralisez les menaces inconnues
- Transformez votre sécurité Web
- Enrichissez l'expérience de navigation
- L'intégration est transparente
- Stoppez les malwares
- Déjouez la stéganographie
- Profitez d'une protection sans équivalent

Les entreprises sont dépendantes du Web pour partager des informations, renforcer les processus commerciaux clés et effectuer des transactions. Les défenses Web périmétriques existantes (passerelles Web et firewalls) ne parviennent pas à faire face à l'assaut de menaces connues, inconnues et de type « zero-day » dissimulées dans des documents et des images nécessaires à l'activité. Si l'on n'y prend garde, ce vecteur d'attaque constitue une menace existentielle pour les entreprises. Les documents et les images que les utilisateurs téléchargent contiennent des menaces qui perturbent le fonctionnement des applications et permettent aux attaquants de contrôler les systèmes de l'entreprise. Les documents et les images téléchargés peuvent contenir plus d'informations que l'entreprise ne souhaite pas divulguer, susceptibles de lui nuire en dévoilant des informations sensibles. À ce jour, personne n'a trouvé le moyen d'endiguer le flux des menaces.

Neutralisez les menaces inconnues

Les défenses Web périmétriques, les passerelles et les firewalls existants constituent une première ligne de défense, en détectant les menaces connues et en recherchant les signatures de failles de sécurité ou de comportements dangereux rencontrés précédemment. Mais les entreprises sont souvent victimes des menaces de type « zero day », qui pénètrent dans l'organisation avant que les défenses basées sur la détection soient capables d'agir, ou par des menaces entièrement inconnues qui atteignent leur objectif sans jamais être correctement identifiées.

Zero Trust Content Disarm and Reconstruction (CDR) for Web Gateways est le seul moyen de vaincre les menaces identifiées, mais également les menaces zero day et inconnues insérées dans le contenu lorsqu'elles traversent la frontière du Web, car cette solution ne repose pas sur la détection ni l'exécution dans un sandbox. Au lieu de cela, il utilise un processus de transformation unique pour assurer une protection totale.

Transformez votre sécurité Web

Zero Trust CDR pour passerelles web fonctionne en extrayant les informations commerciales des documents et des images présents dans le flux de navigation Web. Les données portant les informations sont éliminées en même temps que toutes les menaces. De tout nouveaux documents et images sont alors recréés et livrés à l'utilisateur. Rien ne voyage de bout en bout, si ce n'est un contenu sûr. Les attaquants ne peuvent pas entrer et l'entreprise obtient ce dont elle a besoin.

Ce processus est ce que l'on appelle la transformation. Il ne peut être tenu en échec : l'équipe de sécurité est satisfaite parce que la menace est éliminée, tandis que les utilisateurs professionnels sont satisfaits parce qu'ils obtiennent les informations dont ils ont besoin.

Zero Trust CDR est le seul moyen de garantir que les menaces soient supprimées du contenu. Abandonnant les paradigmes périmés de la détection et de l'isolation des menaces, la technologie unique Zero Trust CDR de Forcepoint part du principe que toutes les données sont dangereuses ou hostiles. Elle n'essaie pas de distinguer les bonnes des mauvaises.

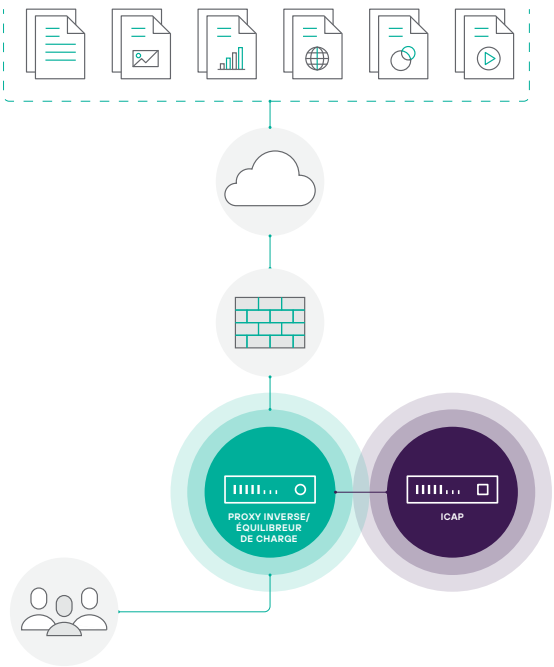
Enrichissez l'expérience de navigation

L'utilisateur professionnel reste la principale victime dans le combat que livrent les équipes de sécurité face à des cyberattaquants qui semblent toujours avoir une longueur d'avance. Le temps passé à vérifier les faux positifs ou à attendre que les documents soient vérifiés et libérés entrave les processus commerciaux et limite la productivité. Et lorsque les choses tournent mal, les mesures correctives sont coûteuses et prennent du temps.

Zero Trust CDR pour passerelles web enrichit l'expérience de l'utilisateur avec le Web et les médias sociaux, car il obtient en temps voulu l'accès aux informations commerciales qu'il doit lire et peut partager et effectuer des transactions, sans aucun risque de compromission du contenu consommé.

Garantir un contenu numériquement pur

Alors que l'utilisation du Web et des médias sociaux devient un aspect crucial des activités, il n'a jamais été aussi important de s'assurer que le contenu véhiculé est sûr, pur et sans menace. Toute entreprise capable d'établir une réputation de sécurité auprès de ses utilisateurs, partenaires commerciaux et clients, offrant l'accès à un contenu garanti sans danger se démarquera dans ce qui devient rapidement un univers cybernétique en marge de la loi.



Zero Trust CDR pour passerelles web offre une telle garantie, en veillant à ce que les entreprises puissent profiter des avantages de l'utilisation du Web et des médias sociaux, avec l'assurance que le contenu professionnel traité est exempt de menaces.

Intégration transparente aux défenses existantes

Zero Trust CDR pour passerelles web s'intègre de manière transparente aux défenses Web périmétriques existantes, aux passerelles Web et aux firewalls d'application en utilisant le protocole ICAP standard de l'industrie. Déployée en tant que « sidecar », la solution est configurée de manière à ce que la passerelle Web ou le firewall transmette les documents et les images à un serveur Gateway eXtension (GX) de Forcepoint via ICAP, où ils sont transformés pour éliminer toute menace cachée, puis renvoyés à la passerelle pour être remis à l'utilisateur.

L'intégration avec le périmètre de défense Web existant ne prend que quelques instants, et des fichiers d'intégration pré-écrits sont disponibles pour de nombreuses passerelles Web et firewalls populaires, pour faciliter l'adoption.

Stoppez l'infiltration des malwares dans le contenu

Les documents Office, les fichiers PDF (Adobe Portable Document Files) et les images sont désormais pour les malwares les supports les plus courants. La complexité de ces formats de fichiers et des applications qui les manipulent en fait une cible naturelle pour les assaillants. Quel que soit le malware – ransomwares, chevaux de Troie bancaires, kits d'accès à distance et enregistreurs de frappe – les cybercriminels connaissent le meilleur endroit pour dissimuler leur toute dernière menace de type « zero-day » dans un document d'entreprise ordinaire. Des techniques telles que l'utilisation de malwares sans fichier et le polymorphisme des fichiers rendent encore plus difficile la gestion de la cybersécurité conventionnelle basée sur la détection, et le Web est le vecteur parfait pour une telle infiltration.

Zero Trust CDR pour passerelles web garantit que les utilisateurs professionnels peuvent charger et télécharger des documents et des images dans le cadre de leur activité sur le Web en toute sérénité, grâce à la façon unique dont ces fichiers sont transformés. Chaque document et chaque image sont soumis à une transformation, et chacun est exempt de toute menace.

Stoppez la perte de données dissimulée grâce à la stéganographie

La stéganographie consiste à dissimuler des données dans des fichiers apparemment inoffensifs. Il s'agit d'un moyen d'encoder un message secret à l'intérieur d'un autre message, appelé le porteur, que seul le destinataire souhaité peut lire. Mais l'utilisation de Stegware, une version de stéganographie utilisée comme arme par les cyberattaquants, est en hausse. Elle est proposée par défaut dans des kits de malware en tant que service sur le Dark Web. Stegware a été utilisé dans des campagnes de malvertising pour extorquer de l'argent à des milliers d'utilisateurs, et a mis à genoux des sites d'information réputés. Il a été utilisé conjointement avec des sites Web de médias sociaux pour voler des actifs financiers de grande valeur, dissimulés dans des images apparemment inoffensives. C'est une mauvaise nouvelle pour les professionnels de l'informatique qui utilisent des outils permettant d'identifier les données non sécurisées, car la stéganographie est impossible à détecter.

Zero Trust CDR pour passerelles web garantit que chaque image vue par un utilisateur naviguant sur le Web ou communiquant via des médias sociaux est entièrement exempte de tout contenu dissimulé en utilisant Stegware. Le processus de transformation détruit tout contenu caché, désarmant ainsi l'image envoyée par l'attaquant. Zero Trust CDR pour passerelles web renforce l'application des initiatives existantes de prévention des pertes de données et de gouvernance, telles que le Règlement général sur la protection des données (RGPD), car il stoppe entièrement la perte de données secrètes par stéganographie d'images.

Perturbation des canaux Command and Control (CnC)

Les cyberattaques les plus sophistiquées et pernicieuses impliquent généralement l'établissement d'un canal de commande et de contrôle (CnC) entre l'assaillant distant et un ou plusieurs postes de travail au sein du réseau de l'entreprise. Souvent, ces canaux sont établis lorsqu'un poste de travail précédemment compromis contacte un serveur distant, par exemple par le biais d'une image sur un site de médias sociaux, ou lorsque des malwares inconnus sont introduits en étant déguisés comme un document de travail valide.

Zero Trust CDR pour passerelles web garantit que les tentatives d'établissement d'un CnC sont interrompues. Le processus de transformation élimine toute menace qui pourrait être dissimulée dans les documents, les images Web et les médias sociaux. Un tableau de bord d'analyse criminalistique permet de voir les copies « avant et après » des documents et des images, ce qui facilite l'identification des comportements suspects et aide à responsabiliser les utilisateurs.

Élaborer une solution gagnante

En collaboration avec nos partenaires revendeurs Forcepoint, l'équipe des solutions Forcepoint fournit une large gamme de services professionnels qui vous aident à maximiser votre investissement dans la technologie Zero Trust CDR. Nous pouvons vous aider à définir la portée, à planifier, installer, configurer et gérer votre solution Zero Trust CDR pour passerelles web.

Assurez-vous que tout s'exécute sans problème pendant et après le déploiement, avec le support technique de Forcepoint. Notre équipe Solutions hautement qualifiée dispose d'une grande expertise et de toutes les informations. Vous pouvez compter sur elle pour agir comme une extension naturelle de votre équipe interne.

Résumé : Profitez d'une protection sans équivalent

Nous sommes à l'aube d'une révolution technologique. Face à des cyberattaques incessantes et concertées, les entreprises sont forcées de réévaluer chaque aspect de la manière dont elles acquièrent, partagent et effectuent des transactions numériques.

Pour plus d'informations, consultez Forcepoint Zero Trust CDR

forcepoint.com/contact