Forcepoint

Présentation succincte

Forcepoint Zero Trust Content Disarm and Reconstruction for E-mail

Le courriel sans danger, tout simplement

Défis

- Lutter contre les attaques de phishing – CISCO a indiqué en 2021 que 90 % des fuites de données étaient dues au phishing.
- Failles Zero-day

La Solution

- Renforcez la sécurité de votre courriel avec Désarmement et reconstruction Zero Trust – Zero Trust Content Disarm and Reconstruction (CDR) : Le seul moyen de vaincre les menaces connues, inconnues et de type zero-day dans le contenu lorsqu'il franchit la frontière du courriel.

Avantages

- Livraison sécurisée des courriels et des pièces jointes exemptes de menaces à travers la frontière du réseau, sans qu'il soit nécessaire de détecter la menace ou d'isoler les utilisateurs du contenu professionnel dont ils ont besoin. Les failles zero-day, les ransomwares, la stéganographie, les malwares sans fichier et les menaces inhérentes aux fichiers polymorphes, tout cela est supprimé.
- Fonctionne avec vos passerelles de sécurité du courriel, vos filtres anti-spam et votre technologie antivirus périmétrique existants. S'intègre de façon transparente dans le périmètre de la cyberdéfense et offre une solution à faible risque et à faible coût, pour une protection totale contre les menaces transmises par le contenu.

En général, les utilisateurs en entreprise disposent d'un système de courriel leur permettant d'échanger des messages électroniques depuis leur lieu de travail avec des utilisateurs au sein de leur organisation, et des utilisateurs sur Internet. Les courriels peuvent contenir un contenu enrichi, les utilisateurs envoyant souvent des pièces jointes tout en utilisant le HTML ou le Rich Text pour créer des messages incluant du formatage, des hyperliens, des couleurs et des images, ainsi que des pièces jointes. Cela crée un risque pour l'organisation que les courriels transmettent des malwares cachés dans ce contenu enrichi.

Les passerelles traditionnelles de sécurisation du courriel reposent sur la détection de la menace potentielle. Elles s'avèrent inadéquates pour le niveau actuel de sophistication des attaques.

Neutralisez les menaces inconnues

Les défenses périmétriques existantes du courriel et les passerelles (combinant anti-virus, le renseignement, le sandboxing et le filtrage du SPAM) fournissent une première ligne de défense, détectant les menaces connues en recherchant les signatures d'exploits 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 ne puissent les rattraper, ou par des menaces entièrement inconnues qui atteignent leur objectif sans jamais avoir été correctement identifiées.

Zero Trust CDR pour courriel est le seul moyen de vaincre les menaces identifiées, mais également les menaces zero day et inconnues insérées dans le contenu ou ayant franchi la frontière du courriel, car cette solution ne repose pas sur la détection ou la détonation par sandboxing. Au lieu de cela, il utilise un processus de transformation unique pour assurer une protection totale.

Transformez votre sécurité courriel

Zero Trust CDR pour courriel fonctionne en extrayant les informations commerciales des courriels et des pièces jointes à la frontière. Les données portant les informations sont éliminées en même temps que toutes les menaces. De tout nouveaux messages et pièces jointes sont alors recréés et remis 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.

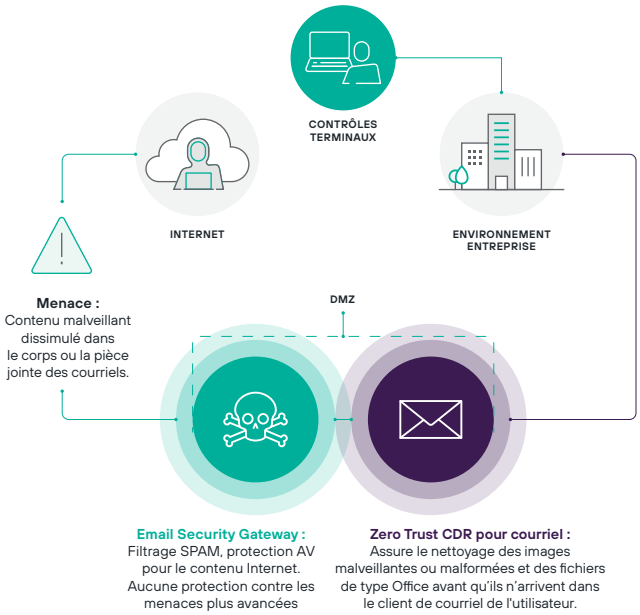
Ce processus est ce que l'on appelle la transformation. Il ne peut être tenu en échec : l'équipe de sécurité est satisfaite parce que la menace est éliminée, tandis que les utilisateurs professionnels sont satisfaits parce qu'ils obtiennent les informations dont ils ont besoin.

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.

Amplifier votre défense existante

Zero Trust CDR pour courriel déploie une passerelle Email Security Gateway et un serveur de messagerie existants pour éliminer les menaces provenant des corps de courriel et des types de fichiers couramment utilisés qui sont joints aux courriels (images, documents Microsoft Office et PDF). Zero Trust CDR pour courriel peut être déployé sur site et dans le cloud.

Zero Trust CDR pour courriel complète les contrôles de sécurité des courriels existants en interposant un élément supplémentaire dans le flux du trafic des courriels entrants et sortants.



Intégration transparente

Zero Trust CDR pour courriel est exécuté sur un serveur côté entreprise appartenant à une passerelle de sécurité de courriel existante. Les courriels entrants sont acheminés depuis la passerelle Email Security Gateway vers Zero Trust CDR pour courriel, où les messages sont transformés pour garantir qu'ils sont exempts de menaces avant d'être remis au serveur de messagerie de l'entreprise.

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 courriel est le vecteur parfait pour l'infiltration. Zero Trust CDR pour courriel permet aux salariés de l'entreprise d'utiliser le courriel en toute tranquillité d'esprit, grâce à un processus unique de transformation des messages. Chaque document et chaque image sont soumis à une transformation et chacun est exempt de toute menace.

Proxy de la couche d'application

Zero Trust CDR pour courriel fonctionne comme un proxy de couche d'application à double hébergement pour vos protocoles SMTP. Il déploie une frontière sécurisée entre le réseau de l'entreprise et les systèmes externes, agissant comme un hôte intelligent à la fois avec la passerelle de sécurité des courriels, pour les messages entrants, et avec le serveur de messagerie, pour les messages sortants. Tout le contenu, y compris MIME (Multipurpose Internet Mail Extensions) et les pièces jointes, est transformé par Zero Trust CDR pour garantir une livraison sécurisée dans le réseau de l'entreprise. Zero Trust CDR transforme les demandes et les réponses du portail de l'utilisateur pour accéder aux documents et pièces jointes protégés par mot de passe pour qu'ils soient récupérés.

Zero Trust CDR pour courriel transforme le contenu qu'il reçoit en une représentation interne de l'information. Les données originales sont éliminées et de nouvelles données "sûres" sont créées à partir de ces informations. Ainsi, les attaques incluses dans les contenus sont supprimées, même si elles sont inconnues, tout en permettant à l'information d'atteindre sa destination. Ce processus est exécuté pour tout le contenu, qui sera ainsi transformé.

Pièces jointes protégées par mot de passe

Dans certaines organisations, les utilisateurs protègent par mot de passe les documents qui sont ensuite envoyés sur Internet en tant que pièces jointes. Ces documents représentent une menace potentielle, car ils ne peuvent pas être transformés et rendus sans menace.

Pour garder l'équilibre entre les besoins de l'entreprise et la sécurité, Zero Trust CDR pour courriel peut être configuré pour ne pas distribuer les messages contenant des pièces jointes protégées par un mot de passe ou pour expurger des messages les pièces jointes protégées par un mot de passe. Il est également possible de configurer des canaux entre des utilisateurs ou des groupes d'utilisateurs spécifiques pour contourner le processus de transformation, si la capacité d'envoi de pièces jointes protégées par un mot de passe est considérée comme essentielle.

Messages signés et chiffrés

S'il est nécessaire de prendre en charge les messages signés et/ou cryptés en utilisant S/MIME ou PGP, cela peut être pris en charge au niveau de la passerelle. Les messages sont d'abord purgés des menaces en utilisant Zero Trust CDR, puis transmis à un serveur de garde distinct de Forcepoint, pour être signés ou cryptés par le garde lui-même.

Macros et contenus exécutables

Dans certaines organisations, les utilisateurs échangent des documents Office contenant des macros en utilisant le courriel. Ces documents représentent une menace potentielle, car les macros sont des contenus exécutables qui ne peuvent être pas être exempt de danger par transformation.

Pour garder l'équilibre entre les besoins de l'entreprise et la sécurité, Zero Trust CDR pour courriel peut être configuré pour ne pas distribuer les messages contenant des macros pour Office, ou pour modifier les messages ayant des pièces jointes contenant des macros Office. Il est également possible de configurer des canaux entre des utilisateurs ou des groupes d'utilisateurs spécifiques pour contourner le processus de transformation, si la capacité d'envoi de documents Office contenant des macros est considérée comme essentielle.

Pour plus d'informations, consultez Forcepoint Zero Trust CDR

forcepoint.com/contact