Forcepoint Zero Trust Content Disarm and Reconstruction

Arrête les menaces connues et inconnues, les attaques zero-day et les malwares.

Forcepoint

Brochure

Forcepoint Zero Trust Content Disarm and Reconstruction

Arrête les menaces connues et inconnues, les attaques zero-day et les malwares.

Qu'il s'agisse d'échanges de courriels, d'interactions sur le Web et les médias sociaux, de téléchargements de fichiers ou d'applications Web : la technologie génère des informations numériques qui sont un véritable nerf de la guerre pour chaque organisation. Ces informations numériques sont partagées et communiquées entre les partenaires commerciaux, les clients, les chaînes d'approvisionnement et les salariés sur site et distants. Le partage d'informations à cette échelle a créé un énorme périmètre d'attaque que les cybercriminels peuvent exploiter en utilisant des malwares dissimulés dans les fichiers, documents et images de tous les jours.

En conséquence, le nombre de technologies défensives a augmenté pour essayer de combattre le problème. Mais ces défenses sont toutes basées, dans une certaine mesure, sur le concept de détection. Le problème des défenses basées sur la détection est qu'elles ne peuvent détecter que ce qu'elles ont « vu » auparavant. Plusieurs tentatives ont été faites pour renforcer ces défenses. Les sandbox peuvent aider, mais les assaillants ont appris à les repérer et ils comptent toujours sur la détection pour essayer d'identifier les menaces. Les algorithmes d'intelligence artificielle et d'apprentissage automatique sont utiles, mais ils ne font en réalité qu'utiliser la puissance de calcul pour essayer de détecter plus rapidement une menace déjà vue. En réaction, les cybercriminels cherchent constamment à attaquer les entreprises avec un malware que les défenses n'ont jamais vu auparavant, et qu'elles considèrent donc comme sûr.

Les défenses basées sur la détection seule ne peuvent tout simplement pas suivre une telle cadence.

La solution Zero Trust Content Disarm and Reconstruction (CDR) de Forcepoint est différente. Plutôt que d'essayer de détecter les malwares, elle part du principe que rien n'est fiable. Elle fonctionne en extrayant les informations commerciales valides des fichiers (en jetant ou en stockant les originaux), en vérifiant que les informations extraites sont bien structurées, puis en construisant de nouveaux fichiers entièrement fonctionnels pour transporter les informations vers leur destination. Zero Trust CDR change la donne pour atténuer la menace des attaques et des exploits zero-day les plus avancés. Passer de la détection à la prévention est particulièrement important avec l'évolution récente des effectifs hybrides et de la transformation numérique, ainsi que de l'utilisation du contenu et des informations électroniques à tout moment et en tout lieu.

Les défenses anti-malwares doivent :

- **Livrer systématiquement un contenu sûr et entièrement fonctionnel** afin que les utilisateurs puissent avoir une confiance totale dans les fichiers qu'ils reçoivent de l'extérieur de l'organisation.
- **Stopper les menaces de type zero-day** sans avoir besoin des derniers patchs ou signatures pour consolider la défense.

Vecteurs d'attaques à protéger :

- **Navigation sur le web**
- **Téléchargements depuis le web**
- **Messagerie Web**
- **Réseaux sociaux**
- **Envoi de fichiers**
- **Courriel**
- **Applications Web**
- **Partage de fichiers**

Données sans malwares

Fichiers parfaits au pixel près, entièrement révisables

Pas de faux positifs

Pas de latence

Stopper toutes les menaces

Le contenu numérique est le vecteur de choix utilisé par les cybercriminels pour les attaques et les exploits à base de malwares. Navigation sur le Web, courriels, téléchargements de fichiers et médias sociaux : le contenu numérique est régulièrement intégré à des menaces connues, ou des menaces de type zero-day, voire totalement indétectables, dissimulées dans les fichiers et les images que nous utilisons chaque heure de la journée de travail.

Depuis plus de 25 ans, l'approche standard pour lutter contre ces menaces consiste à utiliser des cyberdéfenses basées sur la détection. Le problème, c'est que la détection est facile à esquiver. Il suffit de modifier la signature pour que le malware franchisse sans encombre la frontière de sécurité. La détection seule ne suffit plus pour protéger les utilisateurs des menaces connues et inconnues, des attaques de type zero-day et des malwares.

Forcepoint Zero Trust CDR empêche les malwares basés sur des fichiers de pénétrer dans l'organisation sans utiliser la détection. Grâce à la façon unique dont Zero Trust CDR extrait et livre simplement ce qui est bon dans un fichier et n'essaie pas de détecter ce qui est mauvais, il protège les utilisateurs contre les malwares de type « zero-day » et les malwares totalement inconnus. Cette approche de la prévention des malwares n'a pas besoin d'être constamment mise à jour avec les dernières signatures ou les renseignements sur les zero-day dès qu'ils sont disponibles, et ainsi la défense est toujours à jour.

Améliorez l'expérience utilisateur

Alors que les entreprises recherchent de nouvelles solutions plus efficaces pour affronter les malwares dissimulés, elles risquent d'avoir un impact négatif sur l'expérience des utilisateurs. Soumettre les fichiers entrants à plusieurs analyses antivirus ou les retenir et les mettre en sandbox pour un examen plus approfondi peut ajouter de la latence aux processus d'activité. Tenter de rendre les fichiers sûrs en les « aplatissant » – en convertissant le format original révisable en un format fixe non révisable – laisse l'utilisateur professionnel avec des documents qui ne peuvent pas être facilement partagés, modifiés ou mis à jour. Dans de nombreux cas, les intentions sont bonnes, mais le résultat final ralentit les processus d'activité, ce qui amplifie exponentiellement la frustration des utilisateurs.

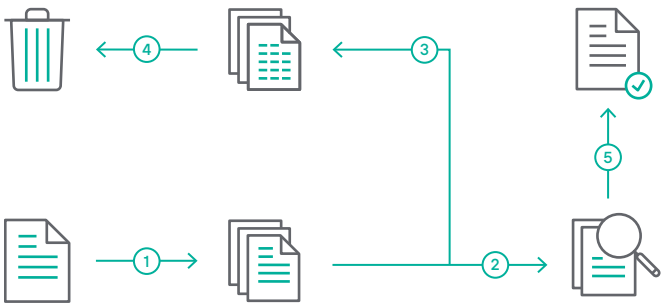
Forcepoint Zero Trust CDR enrichit l'expérience des utilisateurs sans compromettre la sécurité. Le processus CDR de Zero Trust n'utilise pas la détection : cela élimine l'attente due à l'analyse des fichiers et aux tentatives de reconnaissance des menaces connues. Il n'utilise pas de sandboxing, il n'y a donc pas de longs retards dans les processus commerciaux cruciaux pendant que les fichiers sont isolés pour être inspectés. Zero Trust CDR ne demande qu'une fraction de seconde, répondant ainsi au besoin des entreprises de disposer d'informations à la fois sûres et disponibles, sans latence. Loin d'entraver la vitesse à laquelle les utilisateurs peuvent accéder aux fichiers dont ils ont besoin, Zero Trust CDR améliore l'expérience de l'utilisateur, en fournissant des fichiers parfaits au pixel près, entièrement révisables et garantis sans malware.

Libérez le SOC

Même avec les meilleures défenses basées sur la détection, de nombreuses équipes de centres d'opérations de sécurité (*Security Operations Center*, SOC) passent encore trop de temps et d'argent à détecter, analyser et répondre aux incidents de cybersécurité causés par des malwares dissimulés dans des fichiers entrants.

Forcepoint Zero Trust CDR libère l'équipe SOC des corvées quotidiennes de gestion des files d'attente de quarantaine, de gestion des faux positifs, d'application des mises à jour de signatures et de contrat avec les alertes de violation potentielle. Chaque fichier entrant est soumis au processus CDR Zero Trust – qu'il contienne ou non des malwares – et chaque fichier est délivré sans menace.

Principes de fonctionnement



1. Plutôt que d'identifier les malwares connus, Zero Trust CDR prend les données et en extrait les informations utiles.
2. Les informations extraites sont transformées dans un format intermédiaire et vérifiées.
3. Ce processus de sécurisation sophistiqué permet de s'assurer qu'aucune menace ou attaque ne peut parvenir à l'étape suivante.
4. Les données d'origine sont stockées ou jetées avec les malwares, connus ou non.
5. Des données neuves sont ensuite construites de manière normalisée, contenant les informations vérifiées. Les nouvelles données reproduisent les données d'origine, sans malware intégré, et leur sécurité est garantie.

Une protection inégalée

- Efficacité garantie contre les menaces sans données – parfait au pixel près et entièrement révisable.
- Aucun risque, même face aux attaques les plus sophistiquées.
- Pas d'exposition aux menaces de type « zero day ».

Hautement polyvalent

- Fonctionne avec les défenses et les technologies des frontières existantes.
- Transforme un large éventail des formats de fichiers les plus populaires, notamment tous les fichiers Office, les images et les PDF (les formats les plus utilisés par les assaillants).
- Défend un large éventail de vecteurs d'attaque, notamment le Web, les courriels et les téléchargements de fichiers.

Choix du déploiement

- Options de déploiement sur site, virtuel et dans le cloud.
- Peut être déployé et rendu opérationnel en quelques minutes.

Annexe A. Aperçu des éléments de la solution

Forcepoint Zero Trust CDR pour les passerelles web	Forcepoint Zero Trust CDR pour les passerelles web protège les utilisateurs du web des malwares dissimulés dans les téléchargements effectués sur le web, à partir du courriel et via les réseaux sociaux. Il est déployé à la frontière du réseau et s'intègre à la passerelle Web sécurisée (SWG) existante. Les paramètres des politiques de la passerelle Web déterminent les types de fichiers à transmettre à Forcepoint Zero Trust CDR pour qu'ils y soient traités.
Forcepoint Zero Trust CDR pour l'isolation à distance du navigateur	Forcepoint Zero Trust CDR pour l'isolation à distance du navigateur garantit que les utilisateurs qui naviguent sur Internet en utilisant Remote Browser Isolation peuvent télécharger des fichiers sur l'hôte physique en toute sécurité, en sachant qu'ils sont totalement exempts de tout malware.
Forcepoint Zero Trust CDR pour l'envoi de fichiers	Forcepoint Zero Trust CDR pour l'envoi de fichiers protège l'entreprise contre les malwares contenus dans les fichiers téléchargés sur Internet. Cette solution peut être déployée en parallèle d'un proxy Web inversé ou dans le cadre d'une application Web basée dans le cloud.
Forcepoint Zero Trust CDR pour courriel	Forcepoint Zero Trust CDR pour courriel protège les utilisateurs des malwares dissimulés dans les courriels et les pièces jointes. Il est généralement déployé entre la frontière de défense du courriel et le serveur de courriel de l'organisation.
Forcepoint Zero Trust CDR pour le partage de fichiers	Forcepoint Zero Trust CDR pour le partage de fichiers garantit que les fichiers se déplaçant entre les points de stockage de fichiers sur plusieurs réseaux sont exempts de malware basé sur les fichiers.
Forcepoint Zero Trust CDR pour les applications web	Forcepoint Zero Trust CDR pour les applications web garantit que les données structurées qui se déplacent entre les réseaux sont contraintes à correspondre à des schémas prédéfinis, afin qu'elles ne puissent pas être utilisées comme vecteur d'attaque.
API Cloud Forcepoint Zero Trust	En plus d'être disponible sur site, Forcepoint Zero Trust CDR est disponible via des API natives cloud pour les développeurs qui doivent intégrer le désarmement et la reconstruction du contenu dans leurs applications et flux de travail Web.

Annexe B. Types de fichiers rendus sans menace par le Forcepoint Zero Trust CDR

Les types de fichiers suivants sont transformés et rendus sans menace par Forcepoint Zero Trust CDR :

FICHIERS OFFICE	
TYPE DE FICHIER	**EXTENSION**
Image Bitmap	BMP
Document Microsoft Office X	DOCX
Métafichier enrichi de Microsoft	EMF
Message de courriel	EML
Image GIF	GIF
Fichier HTML	HTML
Fichier ICAL	ICAL
JPEG 2000	JP2K
Image JPEG	JPEG
Archive MIME HTML	MHT
Multipurpose Internet Mail Extensions	MIME
Adobe PDF	PDF
Image PNG	PNG
Microsoft Office X PowerPoint	PPTX
Texte enrichi	RTF
Texte brut	TXT
Image TIFF	TIFF
Métafichier Microsoft Windows	WMF
Microsoft Office X Excel	XLSX
Archive Zip	ZIP

FICHIERS DE DONNÉES STRUCTURÉES	
TYPE DE FICHIER	**EXTENSION**
Valeurs séparées par des virgules	CSV
Données structurées JSON	JSON
Google Protocol Buffers 3	Proto3
Données structurées XML	XML

Les formats de fichiers suivants sont également transformés et rendus sans menace en les convertissant d'abord dans un format intermédiaire :

FORMATER	ORIGINAL	TRADUCTION	FINAL
Microsoft Word – ancien	DOC	DOCX	DOC
Microsoft PowerPoint – ancien	PPT	PPTX	PPT
Microsoft Excel – ancien	XLS	XLSX	XLS
Texte OpenDocument	ODT	DOCX	ODT
Tableur OpenDocument	ODS	XLSX	ODS
Présentation OpenDocument	ODP	PPTX	ODP
Texte enrichi	RTF	DOCX	RTF
eXtensible Paper Specification	XPS	PDF	XPS
Format de lecteur de livre EPUB	EPUB	PDF	EPUB
Format ebook Mobipocket	MOBI	DOCX	–
Computer Graphics Metafile	CGM	PDF	–
Adobe Photoshop	PSD	PNG	PSD
Microsoft One Note	ONE	PDF	–
Dessin AutoCAD	DWG	PDF	–
Dessin AutoCAD – ancien	DXF	PDF	–
Microsoft Visio – ancien	VSD	PDF	–
Microsoft Visio	VSDX	PDF	–
XLS Formatting Object	FO	PDF	–
archive 7Zip	7Zip	ZIP	7Zip
Archive BZip2	BZip2	ZIP	BZip2
Archive GZIP	Gzip	ZIP	GZip
Archive Z	Z	ZIP	Z
Archive TAR	TAR	ZIP	TAR
Archive Microsoft CAB	CAB	–	ZIP

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données. Son objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Nos solutions à facteur humain s'adaptent en temps réel à la façon selon laquelle les individus interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables protégeant des milliers de clients dans le monde entier.