# Proofpoint pour se protéger des ransomwares

## Comment empêcher les ransomwares de s'implanter et de se propager dans votre entreprise

### Produits

- Proofpoint Advanced Threat Protection
- Proofpoint Cloud Security

### Principaux avantages

- Prévention de l'infection initiale
- Prévention de la reconnaissance, du déplacement latéral et de la persistance
- Prévention de l'exfiltration de données

Le ransomware est l'une des formes de cyberattaque les plus déstabilisantes. Il interrompt les activités de ses victimes, contraint les hôpitaux à renvoyer les patients chez eux et met les pouvoirs publics complètement à l'arrêt. Il n'a cessé d'évoluer pour devenir l'une des cybermenaces actuelles les plus redoutables. Rien que l'année dernière, les États-Unis ont recensé plus de 65 000 attaques de ransomwares. Cette menace figure au nombre des principales préoccupations des RSSI et est devenue un problème de sécurité nationale. Bien plus alarmant encore, de nombreuses entreprises sont totalement désarmées face à une attaque de ransomware. Seulement 13 % des experts informatiques interrogés par le Ponemon Institute considèrent que leur entreprise est en mesure de prévenir une attaque de ransomware. Plus de 68 % s'estiment « vulnérables » ou « très vulnérables »[1].

Les emails et le Web sont les principaux vecteurs d'attaque utilisés par les ransomwares. À l'heure actuelle, la plupart de ces attaques se déroulent en plusieurs phases. La messagerie et les sites web compromis jouent un rôle déterminant dans les premières phases de la chaîne d'attaque. Ils sont utilisés pour distribuer la charge virale initiale, généralement un téléchargeur de malwares. Ces charges virales sont conçues pour infiltrer le système de l'utilisateur, le plus souvent pour dérober des identifiants de connexion et accéder au réseau. Les opérateurs de ransomwares utilisent également des identifiants de connexion volés pour accéder à des services Internet. Parmi les tactiques courantes figurent les emails de phishing d'identifiants de connexion, les attaques par force brute de mots de passe et les compromissions par téléchargement à l'insu de l'utilisateur (drive-by).

Une fois l'accès initial obtenu, les opérateurs de ransomwares s'implantent durablement, mènent des opérations de reconnaissance et se déplacent latéralement. Dès qu'ils sont à l'intérieur, les cybercriminels peuvent chiffrer les fichiers sensibles, mais aussi exfiltrer des informations stratégiques dans le cadre d'une double extorsion.

Dès lors que les mesures de sauvegarde et de restauration parviennent à déjouer les attaques de ransomwares, les tactiques des cybercriminels évoluent pour les contourner. C'est ainsi que les cybercriminels utilisent désormais des ransomwares « à double extorsion », une tactique consistant à exfiltrer des données sensibles, puis à chiffrer

1 The Ponemon Institute, « The Rise of Ransomware » (L'essor du ransomware), janvier 2017.

les fichiers. Si l'entreprise victime refuser de payer la rançon, le cybercriminel dispose de trois options pour obtenir ce paiement :

- Menacer la victime de divulguer les données en ligne
- Vendre les données au plus offrant
- Envoyer des emails aux clients et partenaires de la victime en les menaçant de divulguer leurs données

La messagerie étant le point d'infection initial de la plupart des attaques de ransomwares, bon nombre de celles-ci débutent, directement ou indirectement, par un email de phishing. Ces emails incitent les utilisateurs à ouvrir une pièce jointe dangereuse ou à cliquer sur une URL malveillante. Seules des solutions avancées sont à même de détecter et de bloquer de telles menaces avant qu'elles ne s'emparent des identifiants de connexion des utilisateurs. En raison de la migration à grande échelle des données d'entreprise vers le cloud, de plus en plus de fichiers de mots de passe et d'informations sensibles y sont stockés. Il est donc important de limiter l'exposition des données dans le cloud pour réduire le nombre d'informations susceptibles de tomber entre les mains de cybercriminels.

D'après les observations de Proofpoint, les attaques de ransomwares sont de plus en plus ciblées, dévastatrices et perturbatrices pour l'activité des entreprises. Proofpoint Advanced Threat Protection et Proofpoint Cloud Security peuvent vous aider à les prévenir. Nos plates-formes intégrées complètes réduisent le risque d'attaques de ransomwares grâce à plusieurs niveaux de contrôles visant plusieurs objectifs :

- Prévenir l'infection initiale
- Détecter l'accès initial et empêcher la reconnaissance, le déplacement latéral et la persistance
- Empêcher l'exfiltration de données

## Prévenir l'infection initiale

Pour vous aider à prévenir les infections initiales, Proofpoint Advanced Threat Protection et Proofpoint Cloud Security exécutent différentes tâches :

- Détection et prévention des ransomwares et des téléchargeurs de malwares à l'origine de la distribution de ransomwares
- Prévention de la compromission d'identifiants de connexion
- Visibilité sur le risque d'attaques de ransomwares
- Isolation des clics sur les URL en fonction du risque
- Formation des utilisateurs afin qu'ils repèrent et signalent les emails malveillants
- Automatisation de la neutralisation des menaces véhiculées par email

### Détection et blocage des ransomwares et des téléchargeurs de malwares

La plate-forme Proofpoint Advanced Threat Protection détecte et bloque les ransomwares au stade de la charge virale initiale. Elle bloque également les malwares à l'origine de la distribution de ransomwares. Nos multiples moteurs basés sur l'apprentissage automatique détectent les malwares, le code malveillant et les techniques de contournement des dispositifs de détection afin de protéger les utilisateurs des sites Web malveillants et des fichiers infectés par des ransomwares.

La plate-forme procède à une analyse de la réputation et du contenu. Elle exécute également des analyses approfondies en environnement sandbox des URL et des pièces jointes susceptibles de dissimuler des menaces. Des fonctionnalités d'analyse prédictive permettent d'identifier et d'isoler en environnement sandbox les URL suspectes en fonction de l'évolution des tactiques des cybercriminels. Par exemple, étant donné que les cybercriminels utilisent souvent des sites légitimes de partage de fichiers pour héberger leurs malwares, la plate-forme analyse systématiquement les URL de ces sites en environnement sandbox. Les solutions qui s'appuient uniquement sur l'analyse de réputation passeront inévitablement à côté de ces attaques.

### Prévention de la compromission d'identifiants de connexion

Les cybercriminels recourent à différentes tactiques pour dérober des identifiants de connexion : phishing, attaques par force brute, Dark Web ou encore informations exposées dans l'espace de stockage cloud de l'utilisateur. Une fois les identifiants de connexion obtenus, l'envoi d'un téléchargeur devient superflu. Il suffit au cybercriminel d'utiliser vos identifiants de connexion pour se connecter à votre VPN ou à des services Web. Il peut alors dérober des données confidentielles ou chiffrer des fichiers à sa guise. En multipliant leurs services cloud, les entreprises s'exposent à ce que des utilisateurs négligents transfèrent des fichiers de mots de passe et autres données sensibles dans le cloud.

Proofpoint Advanced Threat Protection détecte et bloque les emails de phishing grâce à plusieurs moteurs de détection, notamment des classificateurs tirant parti de l'apprentissage automatique pour inspecter les URL. Proofpoint Cloud Security permet d'identifier les informations sensibles exposées dans les comptes cloud susceptibles d'être exploités par des cybercriminels.

### Visibilité sur le risque d'attaques de ransomwares

Proofpoint vous offre une visibilité sur vos VAP (Very Attacked Person™, ou personnes très attaquées), c'est-à-dire les collaborateurs de votre entreprise les plus exposés aux attaques. Vous pouvez ainsi établir qui sont vos collaborateurs les plus ciblés et par quelles menaces. Fort de ces informations, vous pouvez alors adapter votre stratégie de défense aux menaces spécifiques ciblant vos VAP.


Figure 1. Trois niveaux de protection

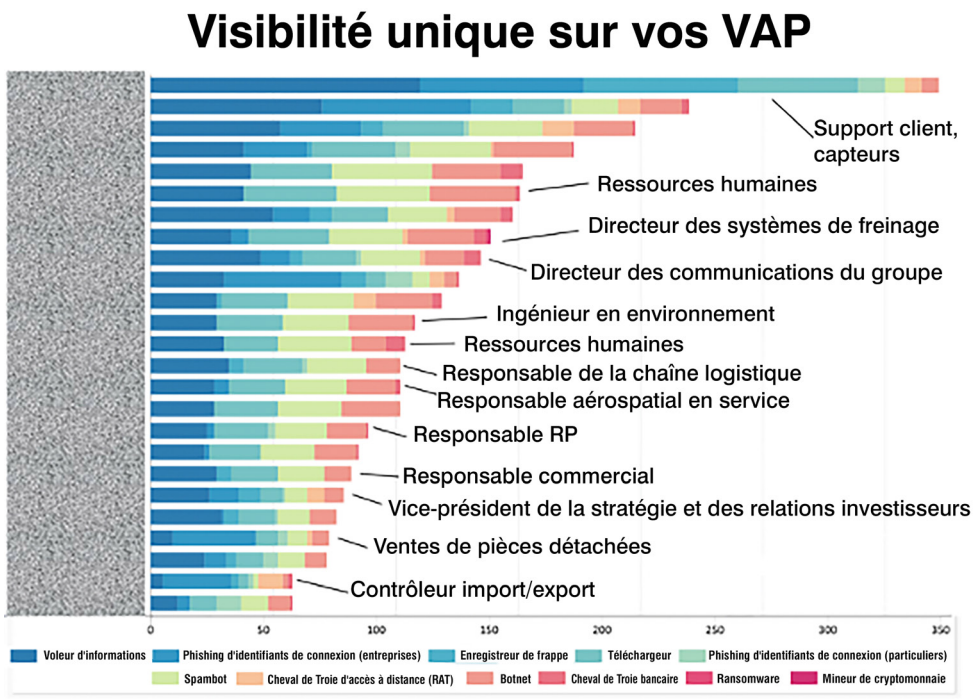


Figure 2. Proofpoint vous offre une visibilité sur vos VAP (Very Attacked Person, ou personnes très attaquées).

Proofpoint fournit également des informations détaillées sur les menaces et les campagnes. Le tableau de bord Threat Insight présente des données d'investigation numérique approfondies sur les cybercriminels, leurs méthodes de propagation, des exemples de message, les destinataires visés, la progression de l'attaque, et bien plus encore.

## Réduction de l'impact grâce à l'isolation intégrée de la messagerie

Les cybercriminels piègent parfois les URL après la remise du message, une stratégie qui leur permet d'échapper à la détection initiale. Proofpoint Browser Isolation réduit les conséquences de l'activation d'URL malveillantes par les utilisateurs. Il offre une protection au moment du clic sur les URL contenues dans des emails d'entreprise et isole l'activité de navigation dans un conteneur sécurisé qui affiche uniquement une version sécurisée aux utilisateurs. Il prévient également les téléchargeurs initiaux et le vol d'identifiants de connexion, ce qui permet de briser la chaîne d'attaque.

Vous pouvez mettre en place un environnement d'isolation basé sur les risques selon les règles définies et les informations au sujet de vos VAP, et transférer les URL les plus à risque vers des sessions de navigation isolées. Vous pouvez également définir des règles plus strictes pour les personnes ciblées en isolant tous leurs clics, de même qu'adapter ces règles en fonction du niveau de risque de l'utilisateur et de l'URL sur laquelle il clique.

## Sensibilisation des utilisateurs à la sécurité informatique

Il est essentiel de former vos collaborateurs à la prévention des attaques de ransomwares. Ils constituent en effet la dernière ligne de défense de l'entreprise. Pour qu'une attaque de ransomware aboutisse, il faut qu'un utilisateur clique sur un lien ou télécharge une pièce jointe. Selon le rapport d'enquête 2021 de Verizon sur les compromissions de données, 85 % des compromissions survenues l'an passé ont nécessité une intervention humaine[2].

La plate-forme Proofpoint Threat Protection comprend une formation de sensibilisation à la sécurité informatique conçue pour sensibiliser les utilisateurs aux attaques de ransomwares afin qu'ils évitent de cliquer sur des messages suspects. Vous pouvez proposer une formation plus approfondie aux utilisateurs les plus ciblés et à ceux qui ont déjà succombé à une attaque. Pour consolider la formation des utilisateurs finaux, vous pouvez également utiliser les ressources de notre vaste bibliothèque de contenus dans vos communications internes et vos alertes de sécurité. N'hésitez pas également à lancer des simulations d'attaques à l'aide de modèles élaborés à partir de leurres réels observés dans les milliards de messages analysés par Proofpoint. La plate-forme propose des mécanismes simples pour signaler les emails suspects, comme le bouton PhishAlarm et l'affichage d'avertissements.

## Automatisation de la neutralisation des messages malveillants

Souvent, les équipes de sécurité manquent de personnel et sont submergées d'alertes, qu'il faut trier et analyser rapidement. La plate-forme Proofpoint Threat Protection propose des solutions d'orchestration, d'automatisation et de réponse aux incidents de sécurité visant la messagerie (mSOAR). Elle automatise l'investigation et la neutralisation des emails malveillants ou indésirables signalés par les utilisateurs.

Ces messages sont automatiquement analysés et enrichis par de nombreux systèmes de threat intelligence et de réputation. Si le message s'avère malveillant, il est automatiquement mis en quarantaine, de même que tout message connexe.

2 Verizon, « DBIR: Data Breach Investigations Report » (Rapport d'enquête sur les compromissions de données), 2021.

Les identifiants de connexion des utilisateurs représentent la clé de votre royaume. Il suffit d'un nom d'utilisateur et d'un mot de passe pour qu'un opérateur de ransomware puisse lancer des attaques à l'intérieur et à l'extérieur de votre entreprise.

Il est donc désormais inutile d'analyser chaque alerte et de neutraliser manuellement les messages malveillants, ce qui permet à votre équipe de sécurité de gagner un temps précieux et d'économiser bien des efforts. Les utilisateurs reçoivent quant à eux un email personnalisé confirmant la nature malveillante du message, ce qui contribue au renforcement des bons comportements.

La plate-forme Proofpoint Threat Protection analyse les messages même après leur remise. Si un élément malveillant est identifié après la remise, la plate-forme extrait automatiquement le message de la boîte de réception de l'utilisateur, de même que les messages transférés à d'autres utilisateurs ou envoyés par le biais de listes de distribution.

## Détecter l'accès initial et empêcher la reconnaissance, le déplacement latéral et la persistance

Proofpoint Cloud Security détecte les attaques de ransomwares de diverses façons :

- En surveillant et en identifiant les comptes cloud compromis
- En surveillant les chargements de fichiers malveillants vers des comptes cloud
- En protégeant vos systèmes des infrastructures de commande et de contrôle grâce à Proofpoint Web Security

### Détection de la prise de contrôle de comptes cloud

Les identifiants de connexion des utilisateurs représentent la clé de votre royaume. Il suffit d'un nom d'utilisateur et d'un mot de passe, en particulier pour des applications cloud telles que Microsoft 365 ou Google Workspace, pour qu'un opérateur de ransomware puisse lancer des attaques à l'intérieur et à l'extérieur de votre entreprise. La solution CASB de Proofpoint Cloud Security propose des contrôles d'accès adaptatifs en temps réel basés sur le risque, le contexte et le rôle de l'utilisateur. Les tentatives d'accès à des applications cloud à partir de sites à risque ou par des cybercriminels connus sont ainsi automatiquement bloquées. Proofpoint CASB s'appuie également sur des données contextuelles pour vérifier l'identité de l'utilisateur et empêcher les accès à risque. Ces données incluent notamment l'emplacement de l'utilisateur, le terminal utilisé, le réseau et l'heure de connexion. Vous pouvez définir des contrôles des règles d'accès, comme l'application de l'authentification multifacteur et la restriction de l'accès à partir de terminaux non gérés pour vous protéger des opérateurs de ransomwares.

Proofpoint vous offre la visibilité nécessaire pour mettre au jour les déplacements latéraux ainsi que les risques qui pèsent sur vos données à la suite de la compromission d'un compte. Vous pouvez déterminer si une connexion suspecte est associée à un compte à l'origine de l'envoi d'emails malveillants. Vous pouvez également voir si un cybercriminel a tenté d'installer un accès persistant en définissant des règles de transfert et de délégation d'emails ou en utilisant des jetons OAuth. Enfin, vous disposez d'une visibilité sur les activités suspectes associées à des fichiers.

### Prévention de la distribution de ransomwares depuis des applications cloud

Un ransomware peut se propager via le partage de fichiers infectés et la synchronisation automatique, ce qui peut avoir de lourdes conséquences pour votre entreprise, vos partenaires et vos clients. Proofpoint Cloud Security surveille activement les partages de fichiers cloud et vous alerte en cas de fichier suspect. Grâce à l'environnement sandbox de Proofpoint et à l'analyse des fichiers dans les applications cloud, vous pouvez confiner ces fichiers malveillants dans le cloud via une mise en quarantaine automatisée et d'autres mesures de correction.

## Protection contre les infrastructures de commande et de contrôle grâce à Proofpoint Web Security

Dès lors qu'un terminal est compromis, il envoie un signal aux serveurs du cybercriminel. Ce dernier envoie alors le jeu d'instructions suivant. Grâce au contrôle du terminal, l'opérateur de ransomware peut effectuer différentes actions, comme distribuer le ransomware ou exfiltrer des données.

Les solutions Web Security et Browser Isolation de Proofpoint Cloud Security bloquent les connexions à des sites compromis. Elles empêchent ainsi l'opérateur de ransomware de contrôler le terminal et de causer d'autres dégâts. Les informations de threat intelligence sont optimisées par le graphique des menaces Nexus de Proofpoint, qui combine des billions de points de données en temps réel sur plusieurs vecteurs de menaces au niveau mondial, des technologies avancées d'intelligence artificielle et d'apprentissage automatique et une équipe internationale de chercheurs afin de vous permettre de garder une longueur d'avance sur les cybermenaces les plus dangereuses.

## Empêcher l'exfiltration de données

Proofpoint Advanced Threat Protection et Proofpoint Cloud Security empêchent l'exfiltration de données de diverses façons :

- En étant attentif aux premiers signes d'exfiltration de données
- En détectant et en empêchant tout mouvement de données non autorisé

Les solutions Web Security et Browser Isolation de Proofpoint Cloud Security proposent des fonctions de protection des données prenant en compte les risques afin de prévenir les fuites de données en temps réel. Combiné à Proofpoint Browser Isolation, Proofpoint Web Security offre un contrôle granulaire des données (accès en lecture seule, par exemple), ainsi que des fonctionnalités d'autorisation et de blocage des applications cloud et des sites Web. Proofpoint Browser Isolation sécurise l'accès des utilisateurs aux données et applications en isolant les sessions de navigateur dans un conteneur sécurisé.

Proofpoint CASB vous permet en outre de bénéficier d'une visibilité instantanée sur les activités suspectes des fichiers, qui sont mises en corrélation avec les connexions suspectes. De cette façon, les équipes de sécurité peuvent rapidement différencier les activités des fichiers initiées par un cybercriminel de celles exécutées par un utilisateur et intervenir à temps.

Proofpoint ne se contente pas de protéger les données sensibles dans les applications cloud, il peut également bloquer l'exfiltration de contenus sensibles via des infrastructures de commande et de contrôle, leur téléchargement sur des terminaux non gérés (appartenant à l'opérateur de ransomware) et leur envoi par email.

## EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

**À PROPOS DE PROOFPOINT**

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.



proofpoint.

0203-004-01-03 12/21