Proofpoint CASB
Contrôles d'accès adaptatifs

Sécurisez vos applications cloud grâce à la gestion des accès et des données

DÉFIS

- Prise de contrôle des comptes cloud
- Accès à risque aux applications cloud
- Fuite de données et conformité

PRINCIPAUX AVANTAGES

- Blocage des accès non autorisés à l'aide de contrôles basés sur l'identité et le rôle
- Réduction des risques de conformité à l'aide de contrôles des accès et des données basés sur le terminal
- Protection des fichiers sensibles au moyen d'un système de prévention des fuites de données en temps réel
- Déploiement rapide dans le cloud

PRODUITS

- Proofpoint CASB
- Proofpoint SaaS Isolation

POURQUOI PROOFPOINT ?

- Contrôles de sécurité centrés sur les personnes (Very Attacked People™, utilisateurs à privilèges et utilisateurs plus vulnérables aux cyberattaques)
- Contrôles granulaires basés sur des règles tenant compte du risque, du contexte et du rôle de l'utilisateur
- Threat intelligence directement exploitable (réputation des adresses IP, connexions suspectes à haut risque)
- Déploiement d'une solution robuste et sans agent en quelques heures seulement

Désormais basés dans le cloud et géographiquement dispersés, les effectifs modernes sont devenus une cible privilégiée des cyberattaques. À mesure que le monde du travail traditionnel a gagné en souplesse, tant en termes d'environnement que d'horaires, les menaces ont elles aussi évolué, délaissant le périmètre réseau pour s'attaquer aux utilisateurs ainsi qu'aux données, ressources et systèmes auxquels ils ont accès.

Dans pareil contexte, il est devenu essentiel de sécuriser l'accès aux applications cloud et d'empêcher les fuites de données, le tout sans transiger sur les impératifs de conformité.

Lorsqu'ils travaillent de la maison ou de tout autre site distant, les collaborateurs ne bénéficient plus de la protection de leur réseau d'entreprise. Ils utilisent bien souvent des terminaux non gérés, et il peut leur arriver de télécharger des fichiers contenant des données sensibles sur des terminaux personnels. Ces différents facteurs combinés exposent les entreprises aux cybermenaces, notamment la compromission d'identifiants, qui entraîne à son tour la prise de contrôle de comptes, la fuite de données et toutes sortes d'attaques de phishing comme le piratage de la messagerie en entreprise (BEC, Business Email Compromise).

Ces dangers sont bien réels et ne sont pas à prendre à la légère. Heureusement, Proofpoint CASB peut vous aider à limiter le risque. Facile et rapide à déployer, notre solution protège Microsoft 365 (Office 365), G Suite, Zoom, Box, Salesforce, Workday et bien plus encore.

Les contrôles d'accès adaptatifs de Proofpoint CASB permettent une évaluation en temps réel de la sécurité, en fonction du rôle, du contexte et du niveau de risque. Les tentatives d'accès à partir de sites et de réseaux à risque ou par des cybercriminels connus sont ainsi automatiquement bloquées. Qui plus est, Proofpoint CASB applique aux utilisateurs à haut niveau de risque et de privilèges des contrôles basés sur les risques, notamment l'authentification renforcée, des règles pour les terminaux gérés et la mise en œuvre de réseaux privés virtuels (VPN).

Contrairement aux contrôles statiques de sécurité et de conformité, qui s'appliquent de la même manière à tous les utilisateurs, les contrôles d'accès CASB sont adaptatifs. Vous choisissez donc à qui appliquer tel ou tel contrôle, sans imposer de vérifications inutiles aux utilisateurs à faible risque.

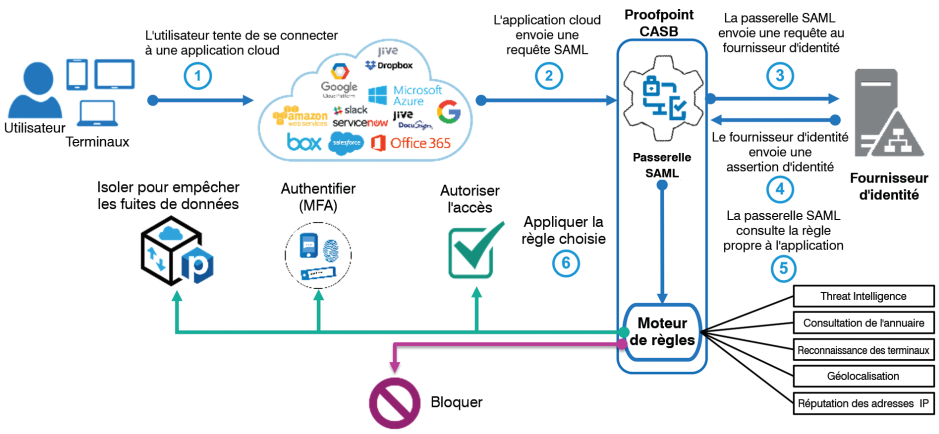

Figure 1. Architecture des contrôles d'accès adaptatifs

PRÉVENTION DES MENACES DANS LE CLOUD

Les identifiants de connexion des utilisateurs représentent la clé de votre royaume. Si des cybercriminels parviennent à compromettre ces identifiants à partir de comptes cloud, ils pourront lancer des attaques à l'intérieur et à l'extérieur de votre entreprise.

Les contrôles d'accès adaptatifs utilisent des informations de threat intelligence sur les cybercriminels connus pour bloquer les connexions suspectes et prévenir la prise de contrôle des comptes. Proofpoint CASB s'appuie également sur des données contextuelles pour vérifier l'identité de l'utilisateur et empêcher les accès à risque. Les données contextuelles examinées sont notamment les suivantes :

- Emplacement de l'utilisateur
- Terminal
- Réseau
- Heure de connexion

Vous pouvez utiliser ces indicateurs de risque pour définir des règles de contrôle d'accès et ainsi empêcher les cyberpirates d'accéder à vos applications d'entreprise.

Règles courantes

Voici deux règles CASB couramment utilisées pour neutraliser les attaques dans le cloud.

Blocage des connexions suspectes à haut risque

Si la signature d'un cybercriminel est connue des services de Proofpoint, vous pouvez empêcher toute connexion à haut risque émanant de ce cyberpirate à l'aide des contrôles d'accès adaptatifs de CASB. Proofpoint traque les connexions suspectes sur des dizaines de millions de comptes et dispose d'une connaissance sans égal des menaces dans le cloud. Ainsi, dès que Proofpoint CASB détecte une tentative de connexion suspecte, vous pouvez bloquer l'accès à vos comptes d'utilisateur les plus exposés.

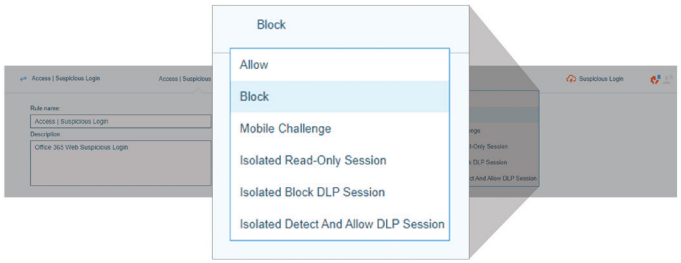

Figure 2. Exemple de règle CASB permettant de bloquer les connexions suspectes

Blocage de l'accès à partir de pays et réseaux à risque

Vous pouvez créer une liste de blocage reprenant les pays où votre entreprise n'est pas présente, mais d'où sont lancées des attaques. Vous pouvez également vous aider de la réputation des adresses IP fournie par Proofpoint pour exiger une authentification à plusieurs facteurs ou bloquer l'accès depuis des réseaux à risque tels que les nœuds Tor, les proxys et autres VPN utilisés par les cybercriminels pour préserver leur anonymat.

ACCÈS CENTRÉ SUR LES PERSONNES

Afin de respecter leurs impératifs de sécurité et de conformité, les entreprises doivent pouvoir sécuriser l'accès de tous les utilisateurs aux applications approuvées et aux données d'entreprise.
Par « tous les utilisateurs », nous entendons les collaborateurs sur site ou distants, mais également les sous-traitants, partenaires et fournisseurs. Mais attention, ce n'est pas parce que le cloud permet un accès universel qu'il faut pour autant se passer de contrôles. Les entreprises doivent pouvoir créer des jeux de règles propres au rôle et aux privilèges de chaque utilisateur, et qui tiennent compte du niveau de sensibilité de l'application et des données qu'elle contient. Les utilisateurs représentent le nouveau périmètre et leur protection demande un haut niveau de connaissance et d'expertise. Proofpoint vous aide à appliquer des contrôles d'accès adaptatifs aux utilisateur/groupes qui relèvent des Very Attacked People™ (VAP, ou « personnes très attaquées ») ou qui disposent de privilèges d'accès à des données, ressources et systèmes critiques de l'entreprise.

Qu'est-ce qu'un VAP ?

Chaque personne est unique. Sa valeur aux yeux des cybercriminels et les risques qu'elle représente pour l'employeur le sont également.

Les collaborateurs ont tous leurs propres habitudes numériques et leurs propres points faibles. Ils sont ciblés par les cybercriminels de diverses manières et avec une intensité variable. Ils disposent en outre de contacts professionnels uniques et d'un accès privilégié aux données, systèmes et ressources.

Ces trois facteurs (vulnérabilités, attaques et privilèges) déterminent leur niveau de risque global.

V : Vulnérabilité. Ils sont susceptibles d'utiliser des terminaux non gérés ou des réseaux non approuvés sans VPN ni contrôles ZTNA. Ils sont plus enclins à ouvrir un email de phishing ou à cliquer sur des liens dangereux.

A : Attaque. Ils sont une cible privilégiée des cyberattaques. Autrement dit, ils subissent un grand nombre d'attaques à caractère unique et particulièrement efficaces, ou sont la proie de cybercriminels particulièrement redoutables.

P : Privilège. Ils ont accès à des données, systèmes et ressources de valeur. Le privilège n'est pas toujours aussi évident qu'il n'y paraît. Un assistant qui ne traite pas de données sensibles de l'entreprise peut en revanche avoir accès aux emails, aux contacts ou encore à l'agenda d'un dirigeant, des éléments très utiles pour les attaques de type BEC.

Un VAP est une personne qui représente un risque supérieur à la normale en vertu de ces critères.

Tous les collaborateurs n'ont pas le statut de VIP.
En revanche, tous peuvent être des VAP.

Règles courantes

Voici des règles CASB couramment employées pour gérer les accès en fonction de la vulnérabilité, du profil d'attaque et des privilèges des utilisateurs.

Mise en place d'une authentification multifacteur pour les VAP

Vous pouvez renforcer la sécurité des utilisateurs à risque. Par exemple, si certains utilisateurs sont « fichés » en tant que VAP d'après les informations de threat intelligence centrées sur les personnes de Proofpoint, vous pouvez soit bloquer leur accès aux applications sensibles, soit renforcer les procédures d'authentification.

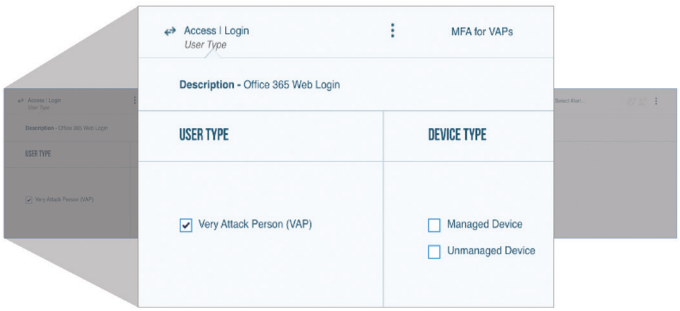

Figure 3. Exemple de règle CASB permettant de définir les terminaux à partir desquels les VAP sont autorisées à accéder à Microsoft 365 en ligne

Mise en place d'un accès via un réseau privé virtuel (VPN) pour les utilisateurs à privilèges d'applications sensibles

Vous pouvez choisir d'autoriser les utilisateurs à privilèges à accéder aux applications sensibles seulement s'ils utilisent un VPN d'entreprise ou un accès ZTNA (Zero-Trust Network Access) tel que Proofpoint Meta. Vous pouvez également définir des plages d'adresses IP pour votre VPN et votre réseau d'entreprise.

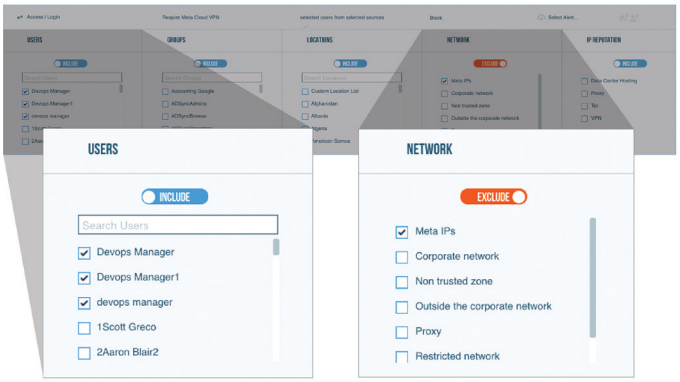

Figure 4. Exemple de règles CASB permettant d'accorder un accès à distance aux administrateurs et utilisateurs à privilèges pour autant qu'ils utilisent un réseau VPN ou ZTNA

CONTRÔLES BASÉS SUR LE TERMINAL POUR UNE PRÉVENTION EN TEMPS RÉEL DES FUITES DE DONNÉES

Les terminaux non gérés et mal protégés comptent parmi les principaux facteurs de risque pour l'entreprise. Lorsqu'un collaborateur accède aux données de l'entreprise par le biais d'un réseau non sécurisé, qui plus est au départ d'un terminal non géré, le risque de fuites ou de pertes monte en flèche. À moins d'avoir déployé les contrôles nécessaires sur les applications utilisées pour consulter, partager et sauvegarder les informations de votre entreprise, ces dernières sont facilement accessibles à toute personne extérieure à l'entreprise et peuvent alors être partagées.

Grâce aux contrôles d'accès adaptatifs de Proofpoint CASB, vos collaborateurs peuvent accéder à vos applications cloud en toute sécurité, où qu'ils soient et sur n'importe quel terminal. Proofpoint CASB :

- détecte les certificats des terminaux ;
- vous aide à mettre en place des règles de sécurité des données pour les terminaux ;
- applique des contrôles en temps réel via l'intégration avec Proofpoint SaaS Isolation.

Vous pouvez permettre aux utilisateurs de parcourir une application à l'intérieur d'un navigateur isolé et sécurisé en mode lecture seule, ou empêcher les chargements et téléchargements de fichiers qui enfreignent les règles DLP.

Dans la plupart des entreprises, les collaborateurs transfèrent régulièrement du contenu de valeur vers le cloud, qu'il s'agisse de dossiers RH ou clients, de formules ou encore de code source. Pouvoir détecter et empêcher les compromissions de données et les infractions aux règles de conformité est donc primordial. Tout d'abord, vous devez vous doter de fonctions de protection des données prenant en compte les risques et capables de prévenir les fuites de données en temps réel au moyen d'analyses. Ensuite, vous devez pouvoir empêcher le chargement de contenus sensibles dans le cloud ou leur téléchargement sur des terminaux personnels.

Règles courantes

Voici deux règles CASB couramment utilisées pour sécuriser les terminaux.

Accès en lecture seule pour les terminaux non gérés se trouvant sur des réseaux non approuvés

Les collaborateurs accèdent aux données de l'entreprise depuis leurs terminaux personnels, via des applications approuvées telles que Microsoft 365, Salesforce ou Atlassian. Ces activités créent de nouveaux risques pour vos données d'entreprise.

En effet, lorsque des données sont téléchargées ou synchronisées sur un terminal personnel, elles quittent leur environnement sécurisé. Et en cas de vol du terminal en question, elles sont perdues.

Voilà pourquoi il peut être intéressant de permettre aux utilisateurs d'accéder aux outils de collaboration à partir de n'importe quel terminal, mais d'autoriser le téléchargement de données uniquement sur les terminaux gérés. Avec Proofpoint CASB, vous pouvez facilement créer une règle qui isole les terminaux non gérés dans une session de navigation sécurisée qui interdit les chargements et téléchargements de fichiers.

Blocage des infractions aux règles DLP pour les terminaux non gérés, même s'ils se trouvent sur le réseau d'entreprise ou un équivalent

Plus de la moitié des compromissions de données sont imputables à un acte malveillant ou une attaque à caractère criminel. Si l'utilisateur se trouve sur un réseau d'entreprise ou un VPN, le risque de cyberattaque extérieure sera moindre. Dans ce cas, vous pouvez choisir d'autoriser le téléchargement de fichiers non sensibles sur des terminaux non gérés, mais de bloquer les transferts de fichiers sensibles.

Avec Proofpoint CASB, vous pouvez créer une règle qui redirige les utilisateurs vers une session isolée où tous les transferts de fichiers sont soumis à des règles DLP. Dès lors qu'une infraction à ces règles est détectée, les transferts sont bloqués.

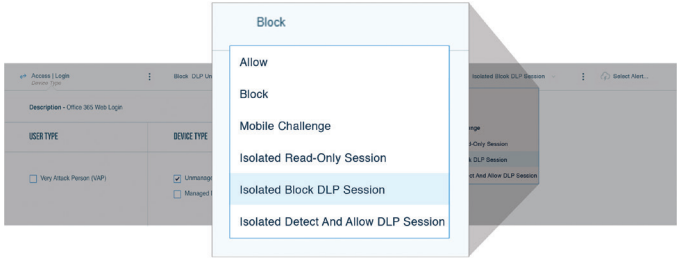

Figure 5. Exemple de règle CASB permettant de bloquer le téléchargement de contenu sensible sur des terminaux non gérés

DÉPLOIEMENT RAPIDE DANS LE CLOUD

Les contrôles d'accès adaptatifs de Proofpoint CASB redirigent les connexions à vos applications cloud vers notre passerelle SAML. Cette passerelle applique un processus d'authentification fédérée en faisant office d'interface entre chaque fournisseur de services et le fournisseur d'identité. Elle est déployée en ligne avec le fournisseur d'identité.

Du point de vue de chaque application, la passerelle SAML apparaît comme le fournisseur d'identité. Du point de vue du véritable fournisseur d'identité (qui gère l'annuaire et les cycles de vie des utilisateurs), la passerelle SAML apparaît comme le fournisseur de services.

L'allocation des ressources aux utilisateurs et les autres fonctions de gestion des workflows d'identité sont du ressort de la solution de gestion des accès et des identités. Ensuite, en fonction de l'analyse réalisée par le moteur de règles, la passerelle SAML applique les mesures de contrôle d'accès requises, notamment l'authentification multifacteur, la protection des sessions ou la prévention en temps réel des fuites de données.

Contrairement aux approches basées sur des proxys inverses et de transfert, notre passerelle SAML présente des avantages architecturaux non négligeables en termes de prévention des fuites de données et de contrôles de compte en temps réel. En voici quelques-uns :

- **Compatibilité avec tous les terminaux.** Vous pouvez sécuriser l'accès aux applications à partir de terminaux personnels ou gérés par l'entreprise, que les utilisateurs se trouvent ou non sur le réseau d'entreprise.
- **Compatibilité avec toutes les applications approuvées par le service informatique.** La passerelle SAML prend en charge toutes les applications cloud approuvées par le service informatique, compatibles avec SAML 2.0 et fédérées par un fournisseur d'identité.
- **Aucun agent de terminal requis.** Comme la passerelle SAML joue le rôle de fournisseur d'identité et analyse la transaction de connexion, aucun agent n'est nécessaire sur le terminal pour acheminer le trafic. Par ailleurs, le fait de ne pas devoir gérer le cycle de vie des terminaux est un véritable plus en termes de rentabilité.
- **Contrôles basés sur des règles.** Les contrôles d'accès adaptatifs permettent la mise en œuvre de flux personnalisables, que ce soit pour les menaces, la prévention des fuites de données ou le contrôle des applications. Ces options vous permettent ainsi de mettre en balance risque et confiance.
- **Robustesse et évolutivité.** La passerelle SAML ne s'appuie sur aucune technique de réécriture d'URL ou de terminaison SSL pour analyser le trafic réseau. Elle se contente d'analyser la transaction de connexion, ce qui se traduit par une faible latence. L'application cloud ne court donc aucun risque, tant en termes d'interruption que de perte de couverture.
- **Confidentialité des utilisateurs.** Contrairement aux autres solutions en ligne, la passerelle SAML n'analyse pas toutes les données et n'a aucune visibilité sur les identifiants de connexion des utilisateurs. Si l'utilisateur est redirigé vers un environnement d'isolation du navigateur afin de prévenir la fuite de données, seuls les transferts de fichiers sont analysés. Et à moins d'une infraction aux règles, aucune donnée n'est conservée. La confidentialité des données de l'entreprise et de l'utilisateur est ainsi garantie.

Solution sans agent hébergée dans le cloud, Proofpoint CASB peut être déployée rapidement sans installer de matériel supplémentaire. Les Services professionnels Proofpoint peuvent aider la plupart des entreprises à implémenter un accès au cloud et des contrôles de données en seulement quelques heures.

PRODUITS

Proofpoint Cloud App Security Broker (CASB)

La solution Proofpoint CASB vous aide à sécuriser les applications cloud, notamment Microsoft 365, Google G Suite et Box. Elle vous protège contre les compromissions de compte, les partages excessifs de données et les risques de conformité dans le cloud. En outre, elle vous permet de mettre en place des contrôles adaptatifs pour sécuriser l'accès à vos applications cloud. CASB vous offre les avantages suivants :

- Visibilité sur les menaces selon une approche centrée sur les personnes
- Fonctions de réponse automatisée
- Fonctionnalités complètes de sécurité des données et de prévention des fuites de données
- Gouvernance des applications cloud et tierces

Notre architecture sans agent offre une valeur ajoutée inégalée et permet l'application des règles en temps réel. De plus, nos analyses puissantes vous aident à octroyer les niveaux d'accès appropriés aux utilisateurs et aux modules complémentaires tiers en fonction des facteurs de risque les plus importants à vos yeux.

Proofpoint SaaS Isolation

Module complémentaire facultatif de Proofpoint CASB, Proofpoint SaaS Isolation sécurise l'accès des utilisateurs aux données et applications cloud en isolant les sessions de navigateur dans un conteneur sécurisé. Cette solution unique permet de sécuriser les chargements et téléchargements de fichiers face à des utilisateurs et des comportements à risque. Elle applique des règles DLP cloud aux transferts de fichiers en temps réel, empêchant ainsi le vol ou la fuite de données sensibles, et contribue à résoudre les problèmes de sécurité, de productivité et de confidentialité liés à l'utilisation d'applications cloud à haut risque. Grâce à son architecture sans agent, SaaS Isolation est compatible avec toutes les applications approuvées par le service informatique. Qui plus est, le déploiement, la gestion et la prise en charge de la solution sont d'une grande simplicité.