chrome enterprise

Appliquer une **sécurité zéro confiance** avec Chrome Enterprise et BeyondCorp Enterprise

Introduction

Pendant des décennies, les pare-feu de réseau ont fourni une sécurité de périmètre aux organisations. Cependant, si les récentes affaires de violation de données prouvent une chose, c'est que les acteurs malveillants peuvent franchir les pare-feu les plus robustes et nuire gravement à la réputation et au fonctionnement d'une entreprise.

Alors que les organisations et leurs employés s'orientent de plus en plus vers les appareils mobiles et les technologies cloud, sécuriser les pare-feu est devenu encore plus difficile.

BeyondCorp Enterprise, la solution zéro confiance de Google, transfère le contrôle des accès du réseau vers les utilisateurs individuels. Ce faisant, elle permet un accès sûr et sécurisé aux ressources internes qui s'appuie sur des informations contextuelles concernant l'appareil et l'utilisateur. Que l'utilisateur soit physiquement dans les bureaux d'une entreprise ou travaille chez lui, il ne pourra pas accéder aux ressources du réseau à accès restreint si son appareil ou ses identifiants ne peuvent pas être authentifiés.

Avec BeyondCorp Enterprise, les professionnels de l'informatique peuvent appliquer des contrôles précis pour l'accès aux applications et aux ressources de l'organisation. Les utilisateurs, quant à eux, peuvent travailler à partir de n'importe quel réseau sans avoir à se connecter au réseau à accès restreint par l'intermédiaire d'un VPN classique.

Les protections contre les menaces et la compromission des données de BeyondCorp Enterprise sont intégrées au navigateur Chrome, qui devient le moyen le plus sécurisé d'accéder à des ressources internes sensibles. Les organisations profitent alors de fonctionnalités en temps réel de protection contre la perte de données, de détection des logiciels malveillants et de vérification des URL, ainsi que d'une visibilité sur les activités dans la console d'administration Google.

chrome enterprise

Cas d'utilisation

Pour offrir aux organisations une protection zéro confiance, Chrome Enterprise et BeyondCorp Enterprise combinent les technologies de sécurité les plus performantes de Google, dont l'accès zéro confiance contextuel, la protection des données ainsi que la prévention contre les rançongiciels, les logiciels malveillants et l'hameçonnage.

Les fonctionnalités zéro confiance de BeyondCorp Enterprise permettent aux organisations de profiter d'une protection professionnelle pour de nombreux cas d'utilisation, par exemple :

- Intégrer un nouveau collaborateur ou un nouveau fournisseur et lui fournir un accès sécurisé aux applications d'entreprise sans avoir à recourir à un VPN ou à un agent local
- S'assurer qu'une feuille de calcul contenant des données sensibles ne soit partagée qu'à condition que les règles définies soient remplies, par exemple depuis une adresse e-mail professionnelle et à partir d'appareils bénéficiant de protections professionnelles contre l'hameçonnage et les rançongiciels
- Identifier tous les collaborateurs qui réutilisent leurs mots de passe professionnels sur des sites externes et leur demander automatiquement de les réinitialiser
- Protéger les ressources à accès restreint des attaques malveillantes à l'aide de la validation en deux étapes
- Permettre à un partenaire d'accéder aux ressources à accès restreint du réseau en s'appuyant sur une authentification et sur des informations contextuelles en fonction des renseignements connus sur le partenaire et ses appareils
- Éviter les fuites de données sensibles, telles que les données de santé protégées, grâce aux fonctionnalités de prévention des fuites de données de Chrome OS et du navigateur Chrome
- Bloquer les transferts de logiciels malveillants et les mouvements latéraux par l'intermédiaire d'applications approuvées
- Empêcher les utilisateurs de suivre les URL d'hameçonnage intégrées à des e-mails ou à du contenu d'application

Grâce à ces fonctionnalités, les utilisateurs authentifiés profitent d'un environnement sécurisé de bout en bout pour accéder aux ressources à accès restreint, et ce, avec des répercussions minimes sur leurs performances.

Rôle du navigateur Chrome dans BeyondCorp Enterprise

Le navigateur Chrome étend la sécurité zéro confiance au Web. Des technologies comme la navigation sécurisée, l'isolation de sites et le bac à sable font de Chrome un navigateur sécurisé pour toutes les organisations. Ses mises à jour automatiques et rapides permettent de s'assurer que les utilisateurs bénéficient de la version la plus sûre. Combiné à BeyondCorp Enterprise, Chrome offre également des protections professionnelles supplémentaires contre les menaces externes d'acteurs malveillants, contre les erreurs d'utilisateurs négligents et contre les menaces internes liées aux données sensibles et à l'exfiltration de données.

Les utilisateurs passent un temps considérable à travailler dans leur navigateur Web. Il est donc essentiel qu'il fasse partie intégrante du modèle de sécurité zéro confiance des organisations (figure 1).

En intégrant les fonctionnalités de protection des données et de détection des menaces basées sur le navigateur Chrome à votre stratégie zéro confiance, vous pourrez profiter des avantages suivants :

Créer un inventaire des appareils équipés du navigateur Chrome et de Chrome OS qui accèdent aux données de votre organisation. La validation des points de terminaison liée à l'inventaire des appareils vous fournit de précieuses informations qui vous aideront à assurer la sécurité de l'organisation. Lorsqu'elle est associée à des offres d'accès contextuel, cette fonctionnalité permet d'appliquer un contrôle précis des accès.

Protéger les données de l'organisation en temps réel en évitant l'hameçonnage des utilisateurs. En alliant les derniers renseignements de Google sur les sites malveillants à une analyse professionnelle des URL en temps réel, la navigation sécurisée vous permet de vous assurer que les utilisateurs n'essaient pas d'accéder à des sites malveillants connus (figure 2).

Bloquer les fichiers suspects en temps réel avant qu'ils ne s'immiscent dans votre réseau. Chrome offre des fonctionnalités d'analyse des fichiers en temps réel directement dans Google Cloud (figure 3).

Vous pouvez choisir d'autoriser l'utilisateur à accéder au fichier avant l'analyse ou de l'obliger à attendre que le fichier soit totalement approuvé. Chrome propose également la détection des logiciels malveillants à trois niveaux, avec une détection selon la réputation, une analyse statique et un système avancé de bac à sable cloud.

Empêcher l'exfiltration accidentelle et intentionnelle des données de l'organisation. La protection contre la perte de données s'appuie sur des règles préconfigurées et personnalisées pour bloquer des actions ou alerter l'utilisateur s'il importe des données sur des sites Web et que cela va à l'encontre du règlement. Cette fonctionnalité est particulièrement utile pour les organisations qui gèrent des informations client protégées d'après des mesures de conformité réglementaire (figure 4).

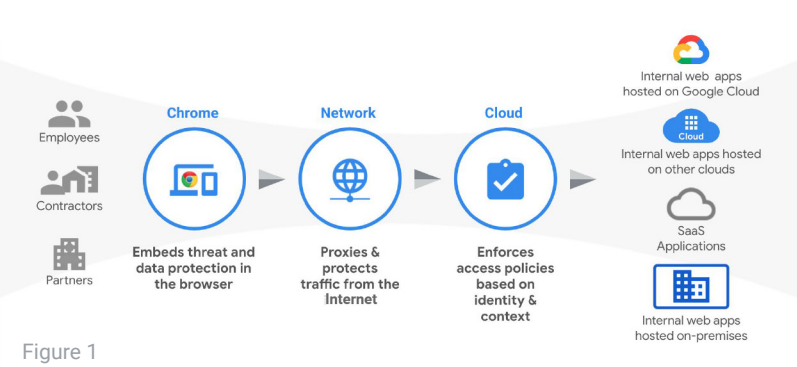


Figure 1

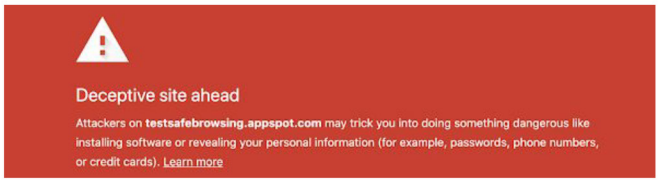


Figure 3

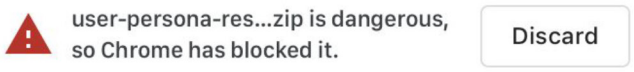


Figure 3

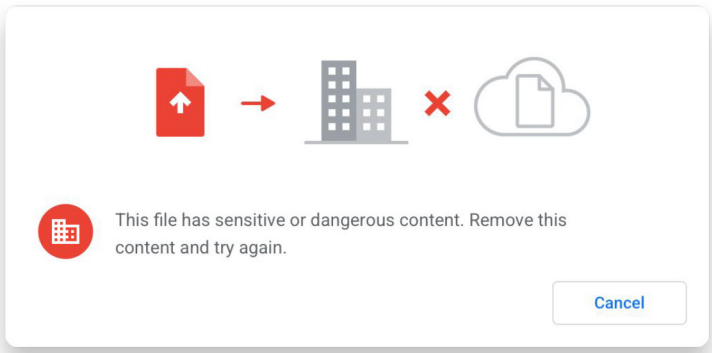
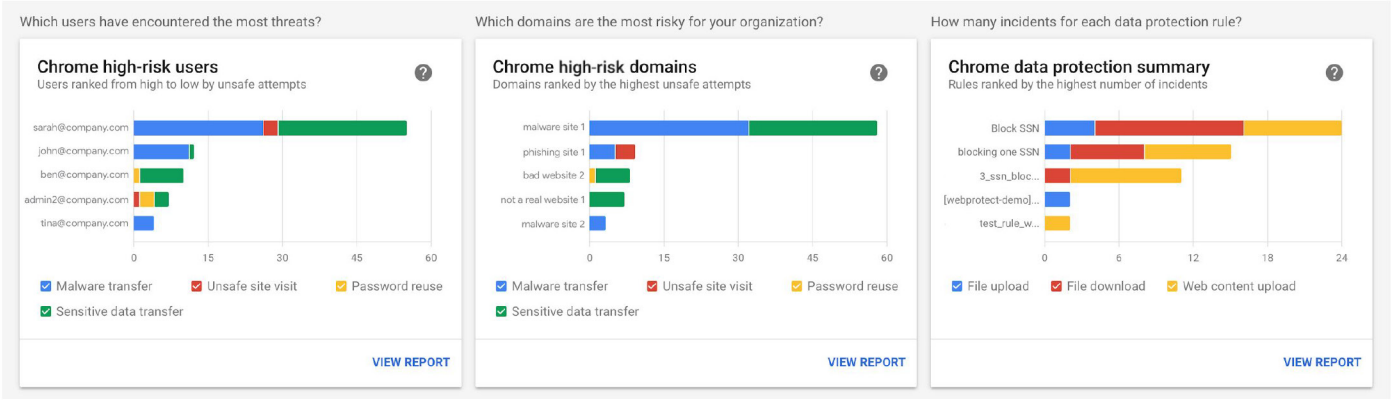


Figure 4

chrome enterprise

Créer des alertes, des journaux et des rapports sur les activités dangereuses. Les équipes informatiques peuvent profiter d'informations supplémentaires sur les événements de sécurité tels que les téléchargements suspects, les visites d'URL à risque, les réutilisations de mots de passe et les fuites de données potentielles. Ces renseignements facilitent leurs efforts de conformité et de sécurité, et leur permettent de repérer les comportements ou les utilisateurs à haut risque.



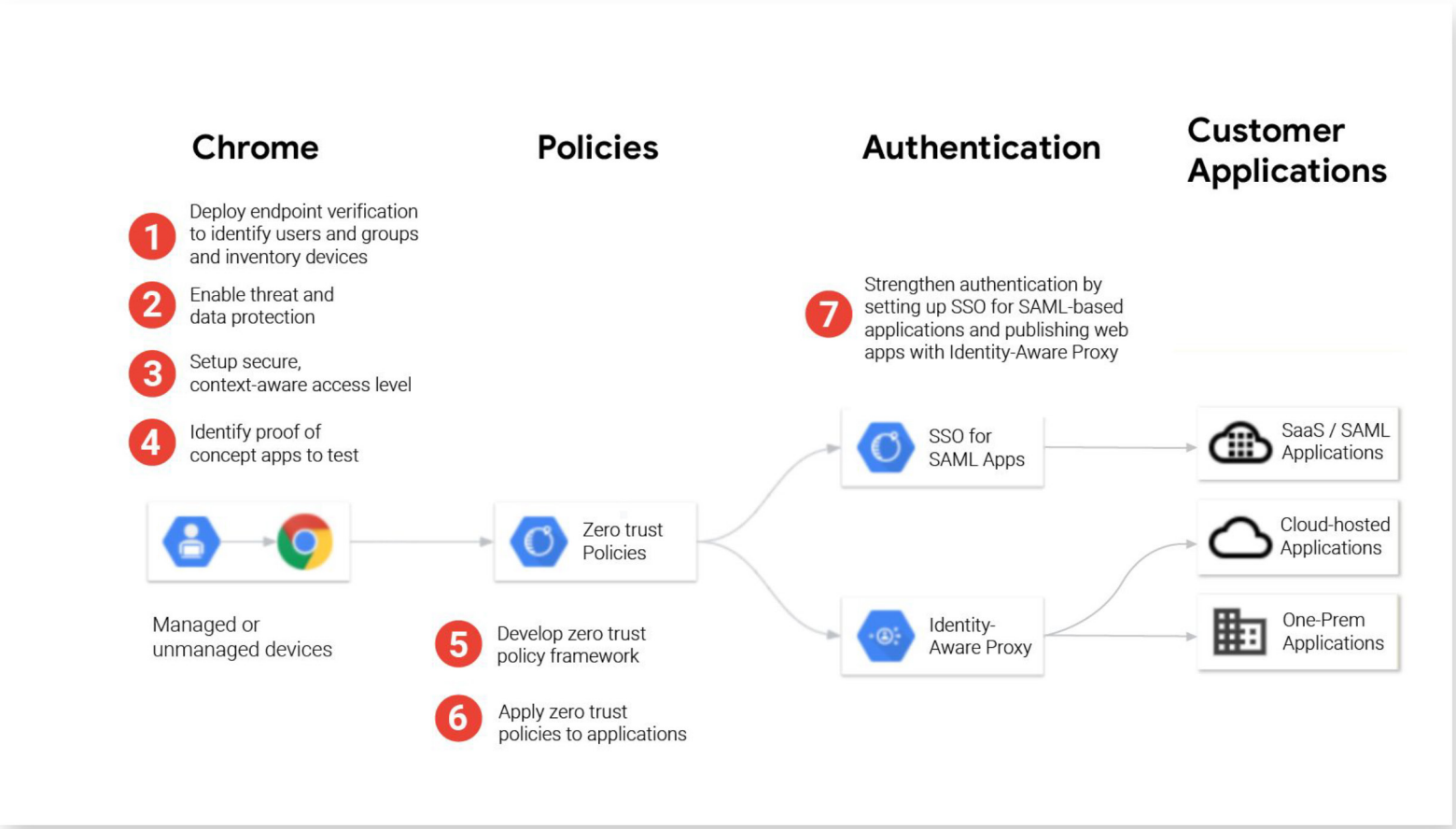
Sécurité zéro confiance renforcée avec Chrome OS

Si vous profitez déjà des protections avancées contre les menaces et la compromission des données intégrées au navigateur Chrome, vous pouvez renforcer encore davantage la sécurité de votre organisation avec Chrome OS. Ce système d'exploitation sécurisé à la conception contribue largement aux modèles de sécurité zéro confiance.

Combiné au navigateur Chrome et à BeyondCorp Enterprise, Chrome OS permet aux organisations d'atténuer les risques tout au long de la chaîne d'utilisation : depuis les appareils jusqu'au Web public en passant par les applications internes et externes.

Migration vers BeyondCorp Enterprise

Faire migrer chaque utilisateur et chaque application du réseau vers le modèle zéro confiance de BeyondCorp Enterprise est un parcours continu. En adoptant une approche de migration par étapes, vous réduisez les risques d'interruption des activités et augmentez les chances de faire passer des groupes importants d'utilisateurs à BeyondCorp Enterprise sans que cela affecte leur productivité.



Conclusion

Chrome Enterprise et BeyondCorp Enterprise aident les organisations à adopter un modèle de sécurité zéro confiance. À l'heure actuelle, les modèles de sécurité de périmètre ne suffisent plus, en particulier avec l'essor du télétravail. Il est indispensable que les effectifs, où qu'ils soient, aient accès aux applications et aux services essentiels pour mener à bien leur travail. Cependant, il peut être difficile pour les organisations d'octroyer ces accès de manière simple et sécurisée.

Avec BeyondCorp Enterprise, les utilisateurs profitent de services de protection contre les menaces et la compromission des données complémentaires au sein même du navigateur Chrome. C'est une couche de sécurité supplémentaire pour les organisations, qui sont protégées contre l'hameçonnage, les logiciels malveillants ainsi que la perte de données, et bénéficient d'une meilleure visibilité sur les activités dangereuses.

Pour en savoir plus sur BeyondCorp Enterprise, consultez g.co/cloud/bce.

chrome enterprise

Ressources

Si vous souhaitez en savoir plus sur le navigateur Chrome, Chrome OS, Chrome Enterprise et BeyondCorp Enterprise, voici quelques ressources qui pourraient vous intéresser :

Navigateur Chrome

- Accédez aux options de téléchargement du navigateur Chrome pour votre entreprise.
- Informez-vous sur la formule d'assistance Enterprise pour le navigateur Chrome.
- Lisez les dernières notes de version sur le navigateur Chrome pour les entreprises.
- Restez informé des dernières mises à jour du navigateur Chrome sur le blog des versions de Chrome.
- Lisez le blog Google officiel sur la sécurité.
- Consultez le Centre d'aide du navigateur Chrome pour les entreprises et le forum d'aide du navigateur Chrome.
- Découvrez les options de la gestion cloud du navigateur Chrome.
- Lisez l'Avis de confidentialité de Google Chrome.
- Lisez le livre blanc sur la confidentialité dans Google Chrome.

Chrome OS

- Renseignez-vous sur le système d'exploitation cloud-first de Google.
- Parcourez le blog Chromium.

Chrome Enterprise

- Découvrez comment Google Chrome Enterprise débloque les capacités professionnelles de Chrome OS, du navigateur Chrome et des appareils Google Chrome.
- Parcourez le blog Chrome Enterprise.

BeyondCorp Enterprise

- Renseignez-vous sur BeyondCorp Enterprise.
- Parcourez le blog BeyondCorp Enterprise.

BeyondCorp Enterprise