IMPERVA®

Imperva CounterBreach

FICHE TECHNIQUE

Protégez vos données contre les menaces

La plus grande menace pour la sécurité de l'entreprise provient de ses employés. Pour faire leur travail, les employés, les entrepreneurs, les consultants et les fournisseurs doivent avoir un accès légitime aux données critiques et sensibles figurant dans les bases de données de l'entreprise, les serveurs de fichiers et les applications SaaS. Toutefois, lorsque des initiés abusent de cet accès, ou sont exploités par des criminels extérieurs, les données de l'entreprise sont exposées. La détection et le confinement des menaces d'initiés nécessitent une compréhension experte des utilisateurs et de leur utilisation des données de l'entreprise.

Les employés doivent avoir accès aux ressources d'informations pour accomplir leurs tâches, mais les accès autorisés abusifs (par ignorance ou à de mauvaises fins) sont à haut risque et difficiles à détecter.

GARTNER, BEST PRACTICES FOR MANAGING 'INSIDER' SECURITY THREATS, ANDREW WALLS, 17 JUIN 2014

Imperva CounterBreach

Imperva CounterBreach protège les données de l'entreprise figurant dans les bases de données de l'entreprise, les serveurs de fichiers et les applications SaaS, contre le vol et la perte causés par des utilisateurs compromis, négligents ou malintentionnés. Par l'apprentissage dynamique des tendances d'accès normal aux données, puis l'identification de tout accès abusif ou inapproprié, CounterBreach alerte promptement les services informatiques de tout comportement dangereux. CounterBreach utilise également des technologies d'autodéfense pour identifier de façon déterministe les appareils finaux compromis par les criminels extérieurs, ajoutant ainsi du contexte à l'apprentissage des accès aux données.

AKERVA

Les stratégies de sécurité de l'information doivent passer d'une stratégie ascendante centrée sur les réseaux et les appareils à une stratégie descendante privilégiant les informations.

GARTNER, PREVENTION IS FUTILE IN 2020: PROTECT INFORMATION VIA PERVASIVE MONITORING AND COLLECTIVE INTELLIGENCE, NEIL MACDONALD, 27 JANVIER 2016

Détecter les accès dangereux aux données sensibles

CounterBreach détecte les éventuelles violations en localisant les accès risqués aux données, ainsi que les utilisateurs associés.

CounterBreach Behavior Analytics

CounterBreach Behavior Analytics utilise l'apprentissage machine et les analyses de groupes de pairs pour détecter automatiquement tout accès anormal aux données. Cela établit une base de référence contextuelle complète des accès types aux tables de bases de données, aux fichiers figurant dans les partages de fichiers et aux objets stockés dans les applications de cloud computing. Les accès anormaux sont ensuite détectés et hiérarchisés. Grâce à une compréhension experte des utilisateurs et de leur accès aux données, les entreprises disposent du contexte et de la précision nécessaires pour détecter les violations de données. Grâce à CounterBreach, les équipes responsables de la sécurité peuvent rapidement discerner les accès malveillants des accès normaux, afin d'identifier immédiatement les comportements à risque et d'agir en conséquence.

L'identification précise des violations potentielles de données nécessite une profonde compréhension contextuelle de l'activité de l'utilisateur, des données auxquelles il accède et de son mode d'accès. Sans visibilité sur les données elles-mêmes, et une compréhension des indicateurs d'usage abusif des données, la moitié de l'équation est manquante. Le tableau ci-dessous affiche des exemples communs d'indicateurs de violation de données, ainsi que les informations nécessaires pour les identifier, en termes d'utilisateur et de données.

INDICATEURS D'ABUS DE DONNÉES	DÉTAILS UTILISATEUR ACQUIS	DÉTAILS D'ACCÈS AUX DONNÉES ACQUIS
Accès aux données d'applications suspects Signale les utilisateurs interactifs (hors application) qui accèdent aux données d'applications sensibles sur une base de données.	Identité d'utilisateur Adresse IP client IP serveur Application client	Nom base de données Nom tableau Sensibilité des données Schéma Opération SQL Type d'opération SQL
Accès excessif aux bases de données Détecte les utilisateurs qui accèdent à un nombre exceptionnellement élevé de bases de données, compte tenu de leur activité normale et celle de leur groupe de pairs.	Identité d'utilisateur Service de l'utilisateur	Nom base de données Sensibilité des données Nom tableau Schéma Nombre de lignes impliquées dans l'opération Opération SQL
Abus de compte de service Détecte toute connexion d'un utilisateur interactif (hors application) à une base de données par le biais d'un compte de service.	Identité d'utilisateur Adresse IP client IP serveur Application client	Nom base de données Tendances d'accès aux bases de données Tendances d'opérations SQL Type d'opération SQL
Accès lent aux fichiers Identifie les utilisateurs qui consultent ou copient un certain nombre de fichiers de manière inhabituellement lente.	Identité d'utilisateur Service de l'utilisateur	Opération de fichier Chemin de fichier Nom de fichier Type de dossier Nom du partage de fichiers Délai de l'opération
Accès à un nombre de fichiers excessif Signale les utilisateurs qui consultent ou copient un nombre anormalement élevé de fichiers à partir de leur dossier personnel, d'un dossier de leur service ou d'un partage de fichiers réseau à partir de plusieurs hôtes.	Identité d'utilisateur Service de l'utilisateur	Opération de fichier Chemin de fichier Nom de fichier Type de fichier Nom du partage de fichiers

AKERVA

CounterBreach met en lumière les utilisateurs, hôtes clients et serveurs les plus risqués pour que les équipes de sécurité puissent se concentrer sur les incidents les plus graves.

Fonctionnalités clés

- Détecter l'utilisation abusive de données critiques
- Raccourcir les délais de réponse aux incidents
- Simplifier les enquêtes

CounterBreach Deception Tokens

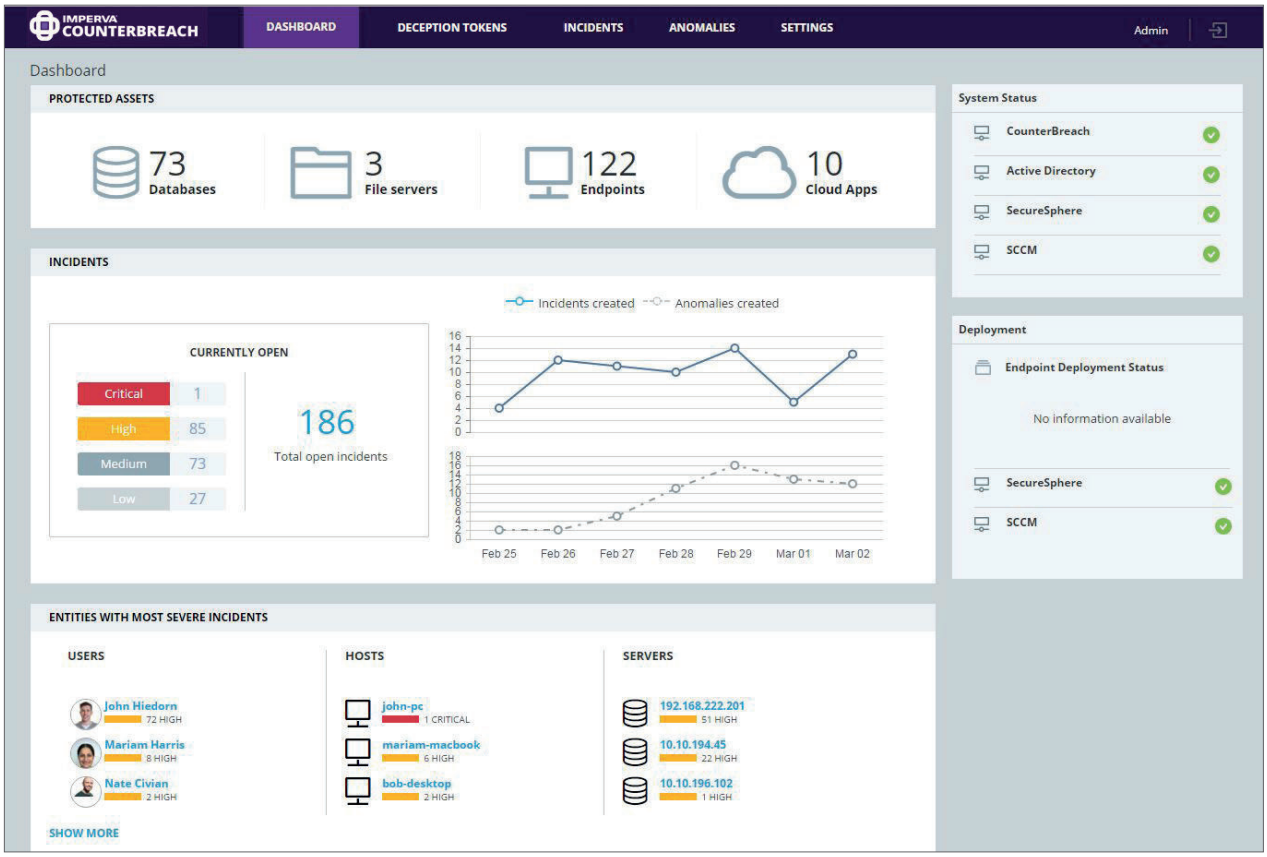
Les CounterBreach Deception Tokens détectent les points d'accès compromis par les cybercriminels. Lorsqu'un point d'accès est compromis, la menace se déplace directement de l'extérieur vers l'intérieur de l'entreprise. Cette identification déterministe des points d'accès compromis ajoute du contexte à CounterBreach Behavior Analytics.

Cette technologie brevetée leurre les criminels vers la toute première étape d'une cyberattaque, au moyen de jetons d'information fictifs sondés pour accéder au réseau interne. Les Deception Tokens comprennent des identifiants d'accès fictifs aux bases de données, des raccourcis attrayants vers les fichiers et des cookies de navigateur web. Entièrement passifs, ces jetons sont installés sur les postes de travail utilisateur et apparaissent comme authentiques, aussi bien pour l'entreprise que pour les pirates informatiques. Si un criminel tente d'utiliser un Deception Token pour accéder à des référentiels de données d'accès, CounterBreach signale l'incident en temps réel. Les jetons étant de nature déterministe, les équipes de sécurité peuvent s'assurer que les alertes générées sont très précises et indiquer une intention délibérée d'accéder aux données de l'entreprise, et de les détourner.

Fonctions clés de CounterBreach

Détection des abus de données critiques

Les incidents détectés par la fonction Behavior Analytics et les Deception Tokens sont répertoriés dans un tableau de bord intuitif. CounterBreach repère les utilisateurs, hôtes clients et serveurs les plus risqués, de sorte que le service informatique puisse se concentrer sur les violations de données les plus graves. Les analystes en sécurité peuvent également accéder à une vue de tous les incidents ouverts, pour passer au crible les informations relatives à un événement spécifique.



Le tableau de bord CounterBreach regroupe les indicateurs de menace pour toutes les données de l'entreprise.

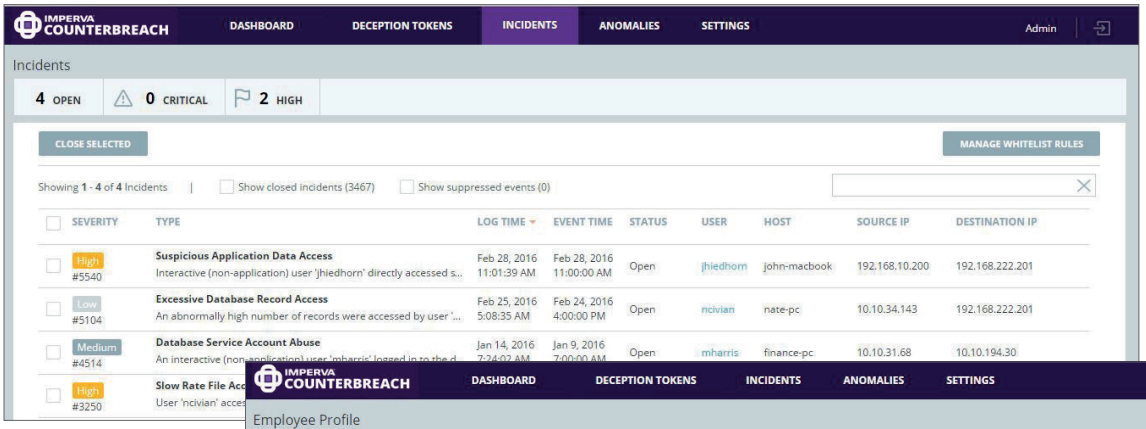
AKERVA

Accélération des délais de réponse aux incidents

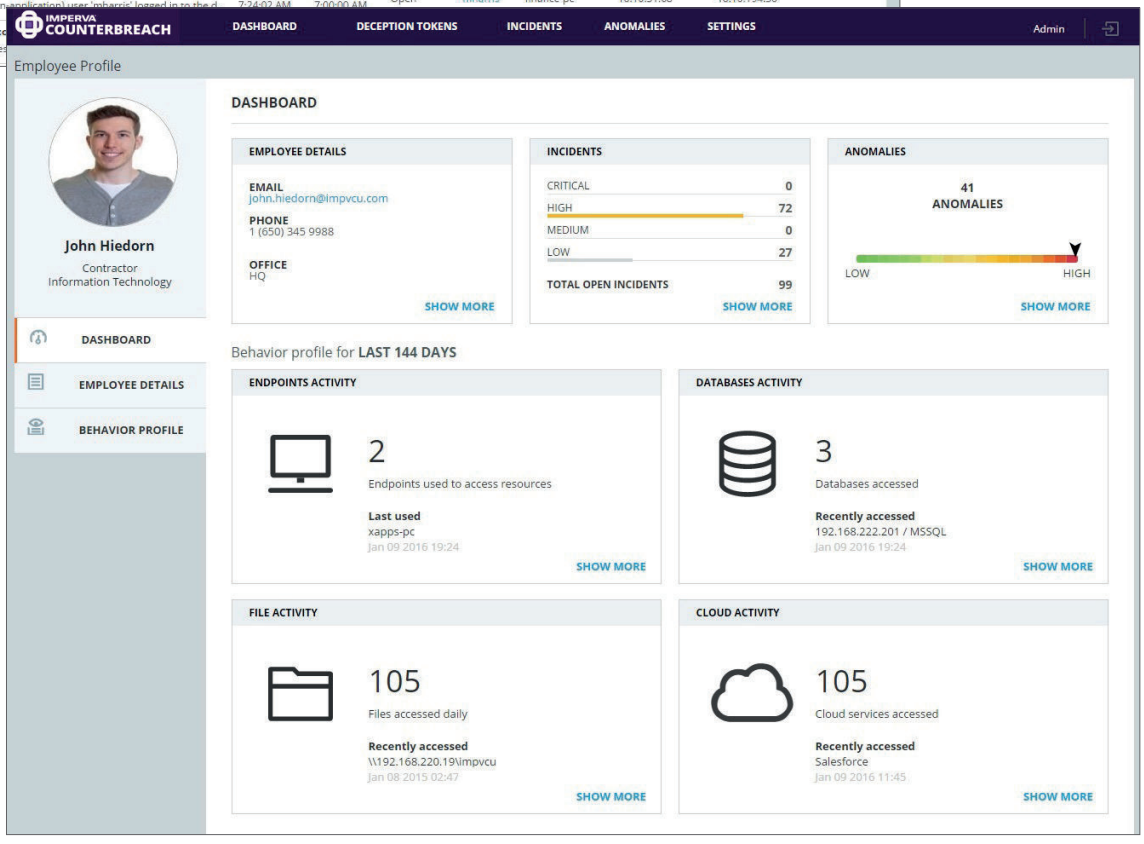
Les équipes de sécurité peuvent étudier efficacement les accès aux données les plus risqués, en filtrant les incidents ouverts par gravité, ainsi que par utilisateur serveur ou hôte client spécifique. Les utilisateurs peuvent alors se pencher d'avantage sur un incident spécifique, pour examiner une description détaillée de l'événement et afficher des informations sur l'utilisation granulaire et les données consultées. Ensuite, le personnel du SOC (Security Operations Center) peut clore l'incident ou mettre sur liste blanche l'incident qui est autorisé ou ne peut être corrigé dans l'immédiat.

Simplification des enquêtes

Les équipes de sécurité peuvent analyser les tendances d'accès aux données d'utilisateurs particuliers, grâce au tableau de bord des utilisateurs. Grâce à une vue consolidée des activités liées aux bases de données, aux fichiers et aux applications de cloud computing, les analystes disposent d'un tableau précis de l'accès aux données de l'entreprise par l'utilisateur. Les équipes de sécurité peuvent enquêter sur les incidents et les anomalies spécifiques à l'individu, puis consulter son profil comportemental et afficher son activité type, avant de les comparer à celles de ses pairs.



L'écran d'incidents CounterBreach affiche les anomalies d'accès aux données critiques par ordre de priorité, de gravité critique à faible.

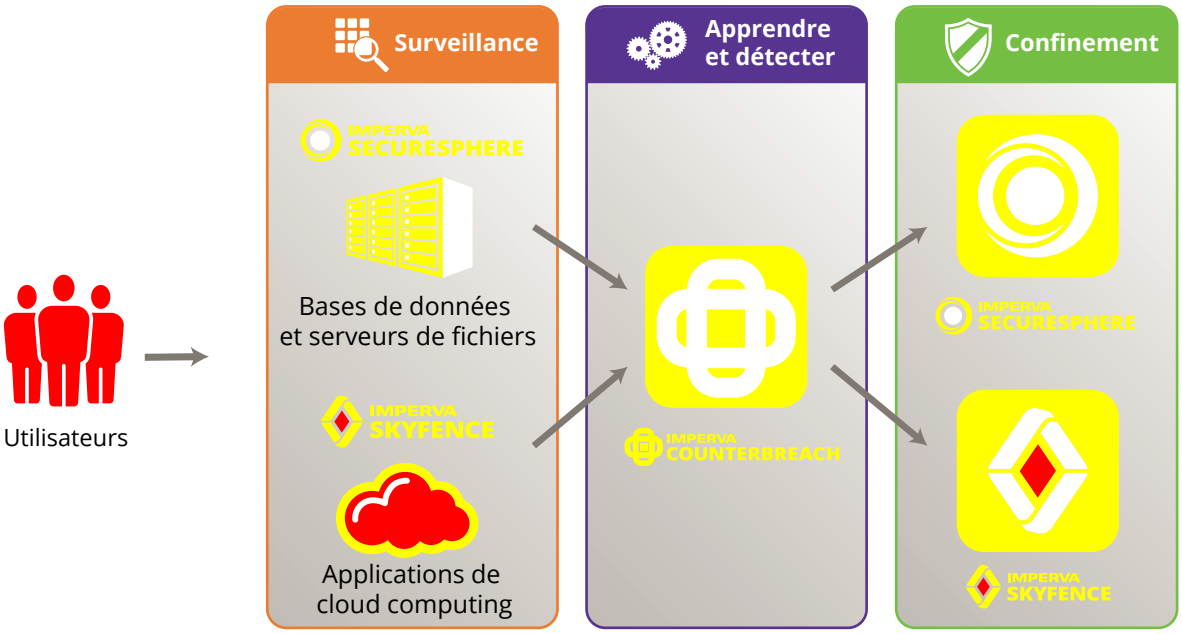


L'écran utilisateur CounterBreach fournit un aperçu des accès individuels aux données de l'entreprise et met en évidence les comportements d'utilisateurs risqués.

AKERVA

Prévention des violations de données avec Imperva

Pour détecter et contenir les violations de données, les entreprises doivent savoir précisément qui accède à leurs données, comprendre si cet accès est légitime et réagir immédiatement si ce n'est pas le cas. CounterBreach s'intègre aux solutions Imperva SecureSphere et Imperva Skyfence pour détecter les anomalies critiques qui indiquent une utilisation abusive des données d'entreprise stockées dans les bases de données, les serveurs de fichiers et les applications de cloud computing.



CounterBreach s'intègre aux solutions Imperva SecureSphere et Imperva Skyfence pour détecter les anomalies critiques qui indiquent une utilisation abusive des données d'entreprise

Surveillance

Les solutions de protection des données Imperva surveillent directement tous les accès utilisateur aux référentiels de données sur site ou dans le Cloud. SecureSphere offrant une visibilité quant à l'accès des utilisateurs accèdent aux at serveurs de fichiers et aux bases de données, les services informatiques savent qui accède aux informations sensibles, quel est le mode d'accès et à quel moment elles sont consultées. Skyfence surveille en permanence les chargements, téléchargements et partages des données sensibles dans les applications de cloud computing telles que : Office 365, SalesForce, Dropbox, etc.

Apprendre et détecter

CounterBreach allie l'expertise d'Imperva en matière de surveillance et de protection de données à un système d'apprentissage machine avancé pour détecter tout accès dangereux aux données. Sur la base des rapports granulaires de SecureSphere et de Skyfence, CounterBreach établit une base d'accès utilisateur typique, puis détecte les accès exceptionnellement anormaux. CounterBreach signale ces accès dangereux de manière proactive pour qu'ils fassent l'objet d'une enquête immédiate.

Confinement

Grâce à la solution CounterBreach, les équipes de sécurité peuvent contenir les fuites de données potentielles avant qu'elles ne se transforment en incidents majeurs. Une fois les anomalies dangereuses détectées, les entreprises peuvent rapidement mettre en quarantaine les utilisateurs à risque afin d'empêcher ou de contenir promptement les fuites de données.

AKERVA

Sécurité cybernétique Imperva CounterBreach

Imperva CounterBreach protège les données de l'entreprise figurant dans les bases de données de l'entreprise, les partages de fichiers et les applications de cloud computing, contre le vol et la perte causés par des utilisateurs compromis, négligents ou mal-intentionnés.
Par l'apprentissage dynamique des tendances d'accès normal aux données, puis l'identification de tout accès abusif ou inapproprié, CounterBreach alerte promptement les services informatiques de tout comportement dangereux.

IMPERVA COUNTERBREACH

Configuration système

Configuration requise pour CounterBreach

CounterBreach nécessite l'un des produits Imperva suivants pour la surveillance et le confinement : SecureSphere Database Activity Monitor, Database Firewall, File Activity Monitor et File Firewall. En outre, Imperva Skyfence peut être intégré à n'importe quel déploiement CounterBreach.

Applications virtuelles CounterBreach

CounterBreach est déployé facilement sous forme d'applications virtuelles qui n'interfèrent pas avec les structures Skyfence ou SecureSphere existantes. La configuration minimale requise par hôte physique et pour chaque application virtuelle invitée est indiquée ci-dessous.

	HÔTE PHYSIQUE		APPLICATION VIRTUELLE HÔTE				
	Hyperviseur	Processeur	Processeur	Mémoire	Espace disque	Système d'exploitation	Système de fichier
CounterBreach Admin Server[1]	Serveur double cœur Intel VTx ou AMD-V	VMWare ESX/ESXi 4.x/5.x/6.x	2	4 Go	50 Go		
CounterBreach Analytics Server[2]			4	16 Go	500 Go		
CounterBreach Deception Sensor Admin Server[2]			2	4 Go	160 Go		
CounterBreach Deception Sensor Server[2]			2	4 Go	40 Go		
Deception Target Server[3]			2	4 Go	40 Go	Serveur 64 bits avec licence Windows 2012 R2	NTFS

[1] Admin Server est requis pour les outils Behavior Analytics et Deception Tokens. Imperva intègrera les logiciels aux applications virtuelles préconfigurées, selon les spécifications indiquées ci-dessus.

[2] Imperva intègrera les logiciels aux applications virtuelles préconfigurées, selon les spécifications indiquées ci-dessus.

[3] Imperva livrera le logiciel Deception Target aux clients par le biais d'un programme d'installation. Une machine virtuelle avec les spécifications indiquées ci-dessus doit être fournie par le client.

Plates-formes prises en charge

COUNTERBREACH BEHAVIOR ANALYTICS	
Plates-formes de bases de données	Oracle, Microsoft SQL Server
Systèmes de fichiers	Systèmes de stockage de fichiers CIFS, périphériques NAS
Systèmes d'exploitation de fichiers	Microsoft Windows Server
Applications de cloud computing	Toutes les applications prises en charge par Skyfence notamment Office 365, AWS, Salesforce, Google Apps, Box, Dropbox, NetSuite, Workday et Microsoft Azure.
COUNTERBREACH DECEPTION TOKENS	
Systèmes d'exploitation	Windows 7
Système de distribution logicielle	Microsoft SCCM

AKERVA