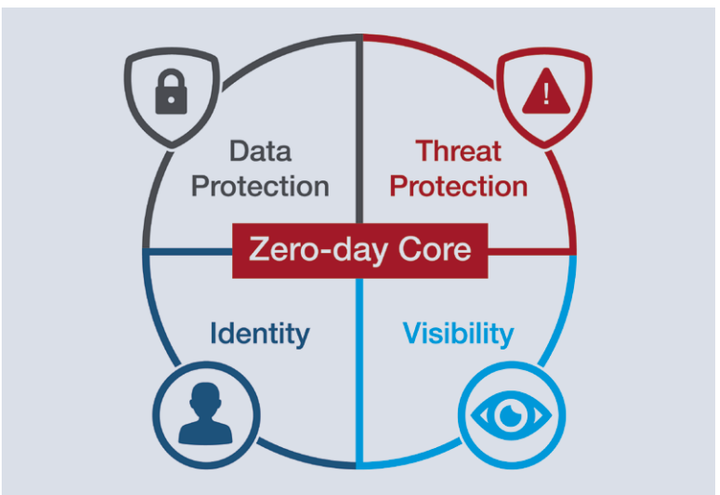
Sécurité maximale dans l'environnement Cloud

Avec sa solution «Cloud Access Security Broker» (CASB), Bitglass permet aux entreprises de toutes tailles et de tous secteurs d'activité d'appliquer des politiques de sécurité au-delà des frontières de leur propre infrastructure informatique lors de l'utilisation des services Cloud.



La tendance à l'utilisation accrue des services Cloud est évidente. Selon une étude interprofessionnelle menée par Bitglass en 2018 auprès de 135'000 organisations, 81% des entreprises utilisent déjà les services Cloud. Avec un impact dramatique sur la sécurité informatique. En effet, les environnements Cloud forment une variété de surfaces d'attaque, en raison notamment d'une shadow IT qui ne cesse de s'étendre avec l'utilisation incontrôlée d'applications Cloud non sécurisées, telles que les programmes graphiques gratuits et les services de partage de données. D'autres faiblesses et vecteurs d'attaque résultent de l'utilisation des smartphones privés et autres appareils mobiles pour des tâches professionnelles. Les applications Cloud utilisées offrent une variété de surfaces d'attaque pour l'infiltration de logiciels malveillants et pour l'accès non autorisé aux données de l'entreprise. En outre, en de nombreux endroits, les applications Cloud exploitent la gestion des accès propre à l'entreprise.

Si les données quittent le réseau de l'entreprise, une stratégie axée sur la sécurisation du réseau interne ne suffit pas. Il est plutôt nécessaire de faire respecter les droits d'accès qui s'appliquent «on-premise» aux environnements Cloud et de veiller à ce que les données transmises et utilisées dans les applications Cloud soient protégées. Via notamment le chiffrement des données et une gestion des accès permettant de bloquer un accès non autorisé et de répertorier tous les accès.

CASB Next Generation de Bitglass: Le meilleur de la sécurité Cloud

Afin de contrer ce problème et de protéger efficacement les environnements Cloud, il est conseillé d'utiliser un «Cloud Access Security Broker» (CASB). La solution «Next Generation» la plus avancée et la plus complète dans ce domaine vient de Bitglass. Elle permet aux entreprises de toutes tailles d'appliquer des politiques de sécurité au-delà des frontières de leur propre infrastructure informatique lors de l'utilisation des services Cloud. La plate-forme, répertoriée dans les Leaders du Quadrant de Gartner, offre une protection sans agent contre les menaces Zero-Day, ceci sur tous les sites, pour toute application et pour tout périphérique. Avec la prise en charge d'applications SaaS telles qu'Office 365, de plates-formes IaaS telles que AWS et d'applications de Cloud privé, Bitglass offre une protection complète et en temps réel pour toutes les principales applications métier. La solution innovante CASB offre également une gestion complète de l'identité et une visibilité impressionnante. Bitglass permet de répondre facilement aux exigences de conformité DSGVO/GDPR et de sécurité des données dans les environnements Cloud.

La protection des données, la gestion des identités, la protection contre les menaces et la visibilité font partie des éléments clés de la solution CASB de Bitglass. Ils présentent notamment les caractéristiques suivantes:

L'identité

Le système complet de gestion des identités prend en charge des fonctions telles que l'authentification unique pour toutes les applications protégées, la synchronisation Active Directory, l'authentification multifactorielle SMS et e-mail, l'intégration avec tout autre système de gestion des identités et l'authentification renforcée.

Contrôle d'accès contextuel

Le contrôle d'accès contextuel sécurise l'accès aux applications Cloud - par exemple en fonction de la méthode d'accès (navigateur/application), du terminal (géré/non géré), de l'emplacement (pays/adresse IP) et l'appartenance à un groupe.

Protection contre les fuites de données (DLP)

Le puissant moteur DLP intégré permet de définir librement des stratégies, les extraire du catalogue bitglass ou d'importer à partir d'autres solutions DLP existantes.

Protection contre les menaces avancées

La protection optionnelle contre les menaces avancées (ATP) empêche l'infiltration et la propagation d'attaques inconnues et d'attaques Zero-Day.

Analyse du comportement de l'utilisateur

Le contrôle transparent de l'accès aux services Cloud (API et proxy) constitue la base de l'analyse du comportement des utilisateurs pour détecter les activités suspectes (signalées via des alertes, des tableaux de bord ou une intégration SIEM). Exemple: Si un utilisateur accède à Slack depuis Zurich, il ne peut pas accéder à Office 365 depuis New York 30 minutes plus tard.

Chiffrement Cloud

La plate-forme intégrée «Cloud Encryption» de Bitglass offre un chiffrement 256 bits conforme à la norme FIPS pour les applications et les données et peut être intégrée dans une large gamme de systèmes de gestion de clés via KNIP.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch
www.boll.ch