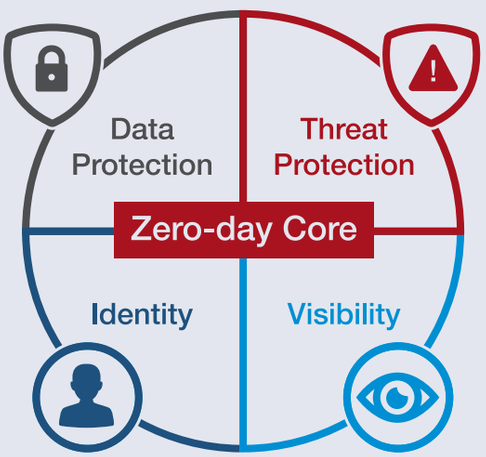
Maximale Sicherheit im Cloud-Umfeld

Mit der «Cloud Access Security Broker»-Lösung (CASB) ermöglicht Bitglass Unternehmen jeder Branche und Grösse, bei der Nutzung von Cloud-Diensten Sicherheitsrichtlinien über die Grenzen der eigenen IT-Infrastruktur hinaus durchzusetzen.

Den Zugriff auf Cloud-Dienste regeln, Daten vor dem Upload in die Cloud verschlüsseln, Datenverluste kontrollieren, Einblicke in auffällige Nutzeraktivitäten erhalten – diese und weitere Möglichkeiten bietet die führende CASB-Lösung von Bitglass.



Der Trend hin zur vermehrten Nutzung von Cloud-Diensten ist unübersehbar. So ist einer branchenübergreifenden, im Jahr 2018 von Bitglass durchgeführten Studie – befragt wurden 135 000 Unternehmen – zu entnehmen, dass bereits 81 Prozent der Firmen Cloud-Services nutzen. Dies hat einschneidende Folgen für die IT-Sicherheit. Denn Cloud-Umgebungen bilden vielfältige Angriffsflächen – gegeben etwa durch eine sich ausbreitende Schatten-IT, die durch eine unkontrollierte Nutzung nicht gesicherter Cloud-Applikationen wie etwa kostenlose Grafikprogramme und private Dropbox-Accounts entsteht. Weitere Schwach- beziehungsweise Angriffspunkte ergeben sich durch die Nutzung privater Smartphones und weiterer mobiler Devices für betriebliche Aufgaben. So bilden verwendete Cloud-Apps vielfältige Angriffspunkte für das Einschleusen von Schadsoftware sowie für den unerlaubten Zugriff auf Unternehmensdaten. Des Weiteren hebeln Cloud-Anwendungen vielerorts ein firmenspezifisches Zugriffsmanagement aus.

Verlassen Daten das Unternehmensnetzwerk, reicht eine Security-Strategie, die sich auf die Sicherung des internen Netzwerks konzentriert, nicht aus. Vielmehr gilt es, die «on premise» geltenden Zugriffsrechte auch in Cloud-Umgebungen durchzusetzen und dafür zu sorgen, dass die übermittelten und in den Cloud-Applikationen genutzten Daten geschützt werden. Dazu dienlich sind unter anderem die Verschlüsselung der Daten sowie ein Zugriffsmanagement, das unrechtmässige Zugriffe blockiert und sämtliche Zugriffe lückenlos dokumentiert.

Next Generation CASB von Bitglass: Cloud Security at its best

Um der beschriebenen Problematik zu begegnen beziehungsweise um Cloud-Umgebungen wirksam zu schützen, empfiehlt sich der Einsatz eines sogenannten «Cloud Access Security Brokers» (CASB). Die in diesem Bereich fortschrittlichste und umfassende «Next Generation»-Lösung stammt von Bitglass. Sie ermöglicht Unternehmen jeder Grösse, bei der Nutzung von Cloud-Diensten Sicherheitsrichtlinien über die Grenzen ihrer eigenen IT-Infrastruktur hinaus durchzusetzen. Demnach bietet die im Leaders Quadrant von Gartner gelistete Plattform einen agentenlosen Zero-Day-, Daten- und Bedrohungsschutz – dies an jedem Standort, für jede Anwendung und für jedes Endgerät. Mit der Unterstützung von SaaS-Anwendungen wie Office 365, IaaS-Plattformen wie AWS und privaten Cloud-Anwendungen sorgt Bitglass für einen umfassenden Echtzeitschutz über alle wichtigen Geschäftsanwendungen hinweg. Ferner bietet die innovative CASB-Lösung ein lückenloses Identitätsmanagement und eine beeindruckende Sichtbarkeit. Dank Bitglass ist es möglich, Compliance-Anforderungen sowie Anforderungen an die Datensicherheit gemäss EU-DSGVO/GDPR in Cloud-Umgebungen einfach einzuhalten.

Zu den Schlüsselelementen der CASB-Lösung von Bitglass gehören Datenschutz, Identitätsmanagement, Bedrohungsschutz und Visibilität. Sie beinhalten unter anderem folgende Leistungsmerkmale:

Identität

Das umfassende Identitätsmanagement-System unterstützt Funktionen wie die einmalige Anmeldung für alle geschützten Anwendungen, Active-Directory-Synchronisation, SMS- und E-Mail-Multifaktor-Authentifizierung, Integration in jedes andere Identitätsmanagement-System sowie Step-up-Authentifizierung.

Kontextbezogene Zugangskontrolle

Die kontextbezogene Zugangskontrolle kontrolliert und sichert den Zugang zu Cloud-Anwendungen – etwa auf Basis von Zugangsmethode (Browser/App), Endgerät (verwaltet/nicht verwaltet), Standort (Land/IP-Adresse) und Gruppenzugehörigkeit.

Schutz vor Datenverlust (Data Leakage Protection, DLP)

Die leistungsstarke, integrierte DLP-Engine bietet die Möglichkeit, Richtlinien frei zu definieren, vom Bitglass-Katalog zu ziehen oder von bestehenden DLP-Lösungen zu importieren.

Erweiterter Bedrohungsschutz

Der optionale erweiterte Risikoschutz (Advanced Threat Protection, ATP) verhindert das Einschleusen und die Verbreitung von unbekannten Angriffen und von Zero-Day-Attacken.

Analyse des Nutzerverhaltens

Die nahtlose Kontrolle über den Zugang zu Cloud-Diensten (API- und proxybasiert) bildet die Basis für eine Nutzerverhaltensanalytik zur Erkennung auffälliger Aktivitäten (gemeldet via Alerts, Dashboard oder SIEM-Integration). Beispiel: Greift ein Anwender aus Zürich auf Slack zu, kann er 30 Minuten später nicht von New York auf Office 365 zugreifen.

Cloud-Verschlüsselung

Die integrierte «Cloud Encryption»-Plattform von Bitglass bietet eine FIPS-konforme 256-bit-Verschlüsselung auf Feld-, Anwendungs- und Datenebene und lässt sich via KNIP in unterschiedlichste Key-Management-Systeme integrieren.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60

info@boll.ch
www.boll.ch