SaaS Security

The most common threats to data in SaaS applications and why Gartner recommends using a cloud access security broker (CASB) to protect data

Download the CASB Magic Quadrant

Today, the majority of organizations use at least one cloud app, and the average number of cloud services used by an organization has more than doubled between the last quarter of 2013 and the last quarter of 2016. Gartner forecasts that worldwide SaaS spending will nearly double from 2016 to 2020, to a $75.7 billion market. Mainstream cloud adoption is driving the need for new security controls.

Unlike traditional approaches to securing applications hosted on premises, SaaS adds another dimension to security — a shared-responsibility model to security between the cloud service provider and the customer. Cloud service providers typically take responsibility for the security of the underlying infrastructure and applications.

However, the customer must ensure the data is used in a secure and compliant manner. This includes how the service is used, who is accessing the data, and how the data is being shared. Cloud access security broker (CASB) solutions come into play to help bridge the SaaS security gap. CASBs are security solutions designed to provide enterprises with greater visibility into and control over their cloud usage.

> *CASBs provide consistent policy and governance concurrently across multiple cloud services, for users or devices, and provide granular visibility into and control over user activities.*
>
> GARTNER, MARKET GUIDE FOR CLOUD ACCESS SECURITY BROKERS, CRAIG LAWSON, NEIL MACDONALD, BRIAN LOWANS, BRIAN REED, OCTOBER 24, 2016

Download the CASB Magic Quadrant

Download the inaugural MQ report that identifies and analyzes CASB leaders

Download Now

Types of Threats in the Cloud

Traditional tools such as firewalls and intrusion-prevention systems are intended to protect the network and the perimeter. They don't adequately protect the data in the cloud because they don't provide the visibility required to secure that data.

On average, an enterprise experiences 23.2 cloud-based threats per month. These include:

- **Data loss due to inappropriate sharing** — 17.7% of documents uploaded to file-sharing services have access permissions that allow anyone in the organizations to view them, while 9.3% of documents shared externally contain sensitive information
- **Insider threats** — scenarios such as employees taking sensitive or proprietary data with them when leaving for a competitor
- **Compromised accounts** — stolen credentials are especially a problem because employees use the same passwords for work and personal accounts, and the massive breaches of several major companies' user login information made these credentials available to bad actors
- **Privileged users** — it's not uncommon for administrators to grant excessive permissions to users, giving employees access to data they don't need for their specific roles
- **High-risk shadow IT apps** — downloading data from secure, company-sanctioned SaaS then uploading them to shadow IT services puts the data at risk

One example of this failure is the breach of 730,000 Morgan Stanley account records. A financial adviser was criminally convicted after confidential data he downloaded and transferred to his personal home server became available online, likely due to a third-party hack of his server. As a result, the Securities and Exchange Commission fined Morgan Stanley $1 million in 2016 for failing to protect customer information and for lacking appropriate policies and procedures.

The frequency of these kinds of incidents will increase as organizations move to the cloud without adopting the right tools and policies to prevent inappropriate and negligent use of their data. Gartner forecasts that through 2020, 95% of cloud security breaches will be the customers' fault. As

part of a shared responsibility model, cloud providers are upholding their responsibilities for platform security, but enterprises lack the tools needed to protect data against user threats.

Moreover, many organizations must satisfy a variety of internal policies and external regulations; however, they may lack adequate cloud governance policies and the means with which to enforce them. One survey found that only 61% of large enterprises have a cloud governance policy. Without a policy in place, IT managers don't have a blueprint for evaluating the risk of new cloud apps.

Security controls needed for the cloud

Governance: There's a multitude of criteria to consider when adopting a new SaaS tool, such as authentication controls, encryption, compliance certifications, IP ownership, DLP methods, etc. Governance policies can limit cloud-use risks by providing a system that restricts use of high-risk services while creating a mechanism for vetting apps.

Data loss prevention: Cloud data loss prevention (DLP) must be approached in the same way as on-premises policies. SaaS is an extension of software that runs on premises, and therefore the same set of DLP policies must apply to both.

If no on-premises DLP policy exists, organizations should start by identifying the sensitive, regulated, and restricted data headed for the cloud across the entire enterprise. Once a classification system is developed, the data can be mapped according to each category, and policies can be developed to mitigate risk.

Threat protection: Technology based on user and entity behavior analytics (UEBA) and machine learning is proving itself a game-changer for threat protection. Using machine learning algorithms, the latest threat protection technology creates models for typical user behavior and detects anomalous activities deviating from typical behavior which may be indicative of a threat.

Effective UEBA tools need to have the following characteristics:

- Visibility into threats across all cloud services
- Self-learning with minimal human input
- Ability to convert behavioral data into a mathematical model
- Automatic grouping of users based on their behavior
- Differentiating behavior by context and across time

Activity monitoring: An audit trail for both user and administrator activity is necessary to ensure compliance with internal policies as well as post-forensic investigations.

Access controls: Today's mobile workforce doesn't conform to the conventions of the traditional workplaces. They access corporate data from their own devices and remote locations. Pervasive security controls must be in place for BYOD and off-network access.

Encryption: Although considered an industry standard for protecting sensitive data such as PII and PHI, encryption is not a standard feature for all SaaS vendors, especially for consumer-grade apps. Yet almost a third of apps used by the average enterprise are consumer services. Enterprises increasingly augment cloud provider controls by encrypting corporate data using their own encryption keys.

Cloud Compliance

HIPAA Compliance | FISMA Compliance | GDPR Compliance | ITAR Compliance | FIPS 140-2 Compliance | Sarbanes-Oxley Compliance | GLBA Compliance | FITARA Compliance | PCI DSS Compliance

Solutions

Cloud Data Loss Prevention | Cloud Encryption

Featured Resources

What is a CASB? | What is a Cloud Security Gateway? | What is Shadow IT? | Tokenization vs Encryption | How Safe is My Data in Office 365? | Office 365 Benefits | SharePoint Online Security Best Practices | OneDrive Security Best Practices | Salesforce Data Security Best Practices | Advantages of the Cloud | Cloud Computing Trends 2017 | Cloud Computing Security Risks | Top Data Loss Prevention Tools? | Incident Response Plan Template | Most Common Passwords | Information Rights Management (IRM)? | Azure vs AWS vs Google Cloud Market Share | Top Cyber Security Companies and Vendors | Box Security Best Practices | What Is HIPAA Security Rule and Privacy Rule? | HIPAA Violations Examples and Cases | Top 5 HIPAA-Compliant Cloud Storage Services | CISM vs CISSP | Top Cloud Security Vendors | 225 IT Interview Questions | 200 IT Security Interview Questions | SaaS Security | Cloud Usage Statistics | CASB RFP | AWS Security Best Practices | AWS IAM Best Practices | AWS Shared Responsibility Model | Gartner's CASB Magic Quadrant