netskope

Beyond the Hype: Top CASB Use Cases for Financial Services

Introduction

We know you're seeing a lot of "use cases" hype now. So we'll be brief and to the point.

Cloud services allow organizations to increase productivity and reduce costs. But for organizations in banking, insurance and other financial services, that productivity can entail new risks: you are still responsible for maintaining regulatory compliance and protecting customer data — as well as your own proprietary information — when you outsource functions like data storage to cloud services.

Cloud access security brokers (CASBs) enable organizations to extend their information protection policies and programs from on-premises infrastructure and applications to cloud services.

Here are the top three use cases for financial services organizations that want to take advantage of the increased productivity and cost savings associated with moving to the cloud, while also managing risk:

- Prevent data exfiltration from sanctioned to unsanctioned services
- Safely enable collaboration & social media
- Defend against cloud ransomware

1 Prevent data exfiltration from a sanctioned to an unsanctioned service

For example, detect and block upload of sensitive content into personal cloud storage accounts like Dropbox after its been downloaded from corporate-sanctioned services such as Salesforce, Box, or even AWS S3.

The GLBA Data Protection Rule requires that financial organizations "ensure the security and confidentiality of customer data." Failure to do so can result in civil penalties of up to $100,000 for each violation, as well as fines and/or imprisonment for officers and directors.

Title V of SOX requires that financial institutions avoid conflicts of interest, such as preventing someone from the investment banking team sharing content with anyone in equity research.

GDPR enforcement for failing to secure EU citizen personal data begins in 2018, with penalties of up to €20 Million, or 4% of annual revenues, whichever is greater.

To maintain compliance in the cloud, financial companies need advanced CASB controls that are context-aware, able to differentiate between sanctioned and unsanctioned services, and even between corporate and personal instances of the same service and provide granular and customizable DLP policies.

Functional Requirements

- See and control usage in both sanctioned and unsanctioned services
- Detect sensitive data, e.g., "confidential" using pre-defined or custom DLP profiles
- Identify all unique content in motion and track its movement
- Be aware of context, e.g., activities such as "upload," "download," or "share"
- Correlate users' identities (e.g., bob@netskope.com = bob123@yahoo.com = bobaran@gmail.com)
- Differentiate between internal and external domains
- Know corporate vs. personal accounts
- Recognize and enforce differing policies between service instances, e.g., corporate and personal
- Decrypt SSL and decode the unpublished API to understand the transaction

2 Safely enable collaboration and social media

Collaboration and social media services can be good for productivity, but can also present security risk tied to data loss and non-compliance with FINRA. You can attempt to block these services with legacy security tools or use an innovative security platform like Netskope to safely enable these tools instead.

For example, block any financial employee from posting "guarantee" or "recommend" alongside a stock ticker symbol or company name on any collaboration or social media service like Slack or Twitter, to comply with FINRA and other regulations.

This CASB functionality to intelligently "alert" or "block" on defined activities in specific circumstances enables financial services organizations to take advantage of increased productivity gains from social media and collaboration services, while managing the potential risks.

Functional Requirements

- Integrate CASB with directory services to focus on a specific group, e.g. Investment Banking
- Be aware of context, e.g., activities such as "view," "post," and "create"
- See and control usage in both sanctioned and unsanctioned services
- Detect data violations using advanced DLP features including regular expressions, custom keyword dictionaries, and Boolean operators to focus on specific risky activities (e.g., for FINRA)
- Decrypt SSL and decode the unpublished API to understand the transaction

3 Cloud malware and ransomware protection

Falling victim to a ransomware attack could do irreparable damage to a financial institution's brand. Yet we know ransomware is doing real harm to financial institutions. For example, the recent WannaCry ransomware attack knocked one bank's ATMs offline, in a very public display of security failure. Even if organizations aren't specifically targeted, the synchronization and sharing functionality of popular cloud services makes for a perfect medium for distribution of malware.

Netskope protects financial organizations from ransomware in the cloud with advanced visibility and control. For example, the ability to detect, quarantine, and remediate ransomware downloaded from unsanctioned cloud services in real time.

Functional Requirements

- Inspect, detect, block, and remediate malware in sanctioned cloud services
- Inspect, detect, block, and remediate malware en route to/from unsanctioned cloud services
- Have visibility over cloud traffic even if it's coming from a sync client, native app, or mobile device
- Decrypt SSL and decode the unpublished API to understand the transaction

Conclusion

When evaluating CASB solutions for cloud data governance and regulatory compliance, be sure to verify the vendor's ability to support these top use cases, including the ability to define and enforce policies across all cloud services, including those known to IT and the unknown "shadow IT" services; the ability to monitor and control social media and collaboration services, like Twitter and Slack; and the ability to detect, block and remediate ransomware. Look for vendors who can do all this for data en route to or from cloud services as well as data already resident in the cloud.

About Netskope

Netskope is the leader in cloud security for financial services. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope — security evolved. To learn more, visit www.netskope.com.

Netskope Active Platform | Security Evolved

Want to see cloud security for financial services in action?

www.netskope.com

netskope

©2017 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 07/17 EB-175-1