FORTRA

CASE STUDY (CLOUD DATA PROTECTION)

Leading Financial Technology Company Improves Security and Compliance

Firm secured their AI-powered, online financial platform hosting more than a million customer accounts with Fortra CASB

When a leading financial technology provider began posting record success and rapid customer growth, it needed a holistic security strategy to protect its customer data and comply with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the California Consumer Privacy Act (CCPA).

Business Growth brings a variety of challenges

In 2021, the firm's platform delivered a record-breaking year — facilitating hundreds of thousands of new accounts amounting to billions of dollars in personal loans. As the platform scaled and new features were added, the need for proper visibility into cloud data and application usage became increasingly apparent to the firm's IT and security teams.

The teams identified three key challenges:

Managing multiple security solutions and enforcing uniform data protection policies across all apps was arduous and inefficient.

- Aligning with compliance regulations became increasingly difficult as the customer base and volume of sensitive compliance-related data each grew.
- Ensuring proper configuration of Amazon Web Services (AWS) cloud infrastructure and various AWS services, including S3 cloud object storage, was difficult and prone to error.
- Convergence without compromise

The firm needed help securing their AI-powered, online financial platform hosting more than a million customer accounts. With cloud-native Fortra CASB, they were able to consolidate multiple point solutions into a single integrated platform, reducing network and security complexity while increasing organizational agility.

AT-A-GLANCE

CHALLENGE:
FinTech firm needs to protect customer data and comply with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the California Consumer Privacy Act (CCPA).

SOLUTION:
Fortra CASB with native data loss prevention (DLP).

RESULTS:
Consolidating DLP point products into a converged platform, the firm was able to reduce risk, realize cost savings, and most importantly, have confidence in their data security.

CASB with native Data Loss Prevention (DLP) was deployed to secure customer data while ensuring regulatory compliance. All traffic from the customer flows through a common inline proxy where it can be intercepted and monitored. From this vantage point, security admins can apply a cohesive package of advanced data security controls through a common set of IT security policies.

Once the customer saw the value of DLP protecting data in their SaaS apps, their next step was to deploy Cloud Security Posture Management (CSPM), which enables users to visualize and minimize the risk of security misconfigurations in their AWS infrastructure.

The Power of Simplicity

A DLP policy defines how organizations share and protect data. It provides guidelines on how data can be used in decision making without exposing it to anyone who shouldn't have access.

As the firm's SaaS portfolio expanded to include Slack, Box, Microsoft 365 and GitHub, configuring and maintaining DLP rules became increasingly complex. With each app offering its own DLP features, the resulting DLP tool sprawl led to:

- Multiple owners of DLP capabilities
- Unnecessary or overlapping policies
- Holes in data visibility and coverage
- Decreased operational efficiency and security

CASB provided the firm's IT and security team with a converged platform that offered complete data visibility, consistent policies and operational efficiency across all apps. It provided a common interface through which uniform DLP policies could be defined across all SaaS apps. Because these policies are context-aware, they're able to adapt based on the data and applications being accessed, the user's risk score and the risk posture of the device. With pre-configured policy templates, the customer was able to create consistent rules for protecting sensitive data across all apps.

By consolidating DLP point products into a converged platform, the firm was able to reduce risk, realize cost savings, and most importantly, have confidence in their data security.

Implementing a Privacy Compliance Program

Facilitating personal loans and credit cards requires collecting personal information such as bank accounts, credit history, social security numbers (SSNs) and home addresses. This sensitive data, stored in cloud storage solutions including Box and Microsoft OneDrive, is also shared internally via Slack messaging. A data security policy must be established to correctly identify and protect the customer's data privacy and comply with regulatory requirements.

Security policies enable IT admins to define and enforce rules and take action at various enforcement points in the system. Actions such as masking, redacting, watermarking or encrypting the data ensure that it stays protected even if it moves outside the company's boundaries, whether intentionally or unintentionally. For example, individual security policy rules can be set up to block a sensitive document from passing through Slack to unauthorized recipients based on predefined attributes. Because security systems are only as effective as the policies that guide their actions, policy management must be as intuitive and straightforward.

Typically, an admin would have to go into each cloud application individually to configure a uniform set of policies via different user interfaces. This approach was both complex and incredibly inefficient.

CASB consolidated this myriad of DLP engines into a single, unified system where a common set of IT security policies could be applied and enforced. This model offered the best security and overall user experience. The firm was able to streamline the workflow needed to create policies, increasing efficiency while reducing the risk of human error.

Reduce Risk with Continuous Monitoring

Like many organizations, the firm uses Amazon Web Services (AWS) for reliable and scalable cloud computing and storage. Data is stored in Amazon Simple Storage Service (Amazon S3) as objects within "buckets".

Misconfigured or "leaky" AWS S3 storage buckets can expose massive amounts of data to the internet. In fact, Amazon S3 buckets have been at the heart of countless data breaches in the last few years. It's common for "leak hunters" to use automated search tools to find thousands of open S3 buckets that include data companies would not want public.

CASB introduced Cloud Security Posture Management (CSPM) as part of the same unified security platform to help organizations correctly and appropriately secure the data they hold in cloud storage instances. CSPM is an IT security tool designed to identify misconfiguration issues and compliance risks by continuously monitoring cloud infrastructure for gaps in security policy enforcement.

With large amounts of private data stored in S3, CSPM helps the firm ensure that their AWS resources are properly configured and sensitive data is protected from public access. It provides actionable reporting on exactly which resources failed the assessment and how to remediate those issues.

CSPM can also be applied to other cloud platforms such as Azure, Microsoft Office 365 and Salesforce. Knowing these foundational resources are correctly configured provides IT and Security teams the certainty they need to perform their day-to-day tasks with confidence that customer data is safe and in regulatory compliance.

Secure future growth

As the customer grows, the volume of data they collect will only increase. It can be challenging to ensure that all data is protected and compliant as the digital footprint rapidly scales with a high-growth company like this. The customer is confident that Fortra will provide them the scalability, visibility and security necessary to grow and help them understand how to do so effectively.

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.