FORTRA®

CASE STUDY (DATA PROTECTION)

Large Oil and Gas Company Protects HR Data After Cloud Migration

Utility meets security and compliance requirements with Fortra CASB and advanced DLP

When a large oil and gas company based in southeast Europe set out to migrate on-premises data and applications to public cloud infrastructure, they needed help addressing the many security challenges that emerged. Fortra CASB, with advanced data loss prevention (DLP), provided the full breadth of integrated features needed to assure all data security and compliance considerations were met while allowing for open cloud data interaction.

The Challenge

Enterprise cloud migration can be a challenging process, especially in highly regulated industries. For this large oil and gas company with more than 11,000 employees, the transition to the cloud was accelerated when SAP signaled plans for end-of-support of their on-premises Human Capital Management (HCM) solution. Instead, they encouraged customers to migrate to a cloud-based HCM suite. Given this organization's heavy reliance on SAP for all its HR-related processes, along with the need to adhere to strict privacy regulations around employee-centric data, the IT team needed to become quick studies on secure cloud migration.

With this as their first cloud transition project, the team engaged a professional services consultant to assess all possible migration risks. Four key challenges were identified:

- Integrating with existing security solutions, including SAP Identity Authentication Service (IAS) for single sign-on (SSO), Fortra Data Classification, and ArcSight for security information and event management (SIEM)
- Implementing granular control policies that allow only authorized users to access sensitive HR data
- Aligning with data privacy laws, including the European Union's General Data Protection Regulation (GDPR)
- Protecting sensitive data and mitigating the risk of malware, such as ransomware, being uploaded to the infrastructure

AT-A-GLANCE

CHALLENGE:
European oil and gas utility with 11,000+ employees was moving their HR infrastructure to the cloud. They needed to ensure all data security and compliance considerations were met while allowing for open cloud data interaction. A multinational presence also poses data privacy challenges, since candidates submit sensitive data as part of the application process.

SOLUTION:
Fortra CASB with advanced data loss prevention.

RESULTS:
To align with national data privacy laws, personally identifiable information (PII) stored in the cloud is now encrypted. CASB solved the encryption of sensitive data while providing the customer with on-premises custody of encryption keys.

The Solution

The team quickly realized they needed a Cloud Access Security Broker (CASB) solution with advanced Data Loss Prevention (DLP) to help address these immediate items, along with future challenges likely to arise as they migrate more data and applications to the cloud. After a thorough comparison of vendors, they selected CASB with DLP to transition their HCM platform confidently and securely to the cloud.

The next step was to implement granular security controls based on a user's role, device posture, location and type of data requested. Privileges had to be restricted so that no single employee had full control of the system, yet individual users could still get access to the tools they need to be productive from any device or location.

The movement of data (both upload and download) also had to be controlled through data classification labels managed by Fortra. Simply put, data classification is the process of labeling data according to its type, sensitivity and business value so that informed choices can be made about how it is managed, protected and shared, both within and outside the organization.

Once classification is performed, the system can ensure that data unrelated to HR, such as financial and research and development information, cannot be uploaded to the cloud-based tool. The team also had to ensure that sensitive data already stored in the cloud can't be downloaded to untrusted devices or unapproved locations.

Finally, by deploying CASB in reverse proxy mode, the customer could enforce DLP policies that block, limit, or allow access to sensitive HR data from both managed and unmanaged devices. When DLP is used in conjunction with data classification, a zero-tolerance policy can be implemented to block the download of any data identified as sensitive. "When a user tries to download any sensitive data, they need to be denied by default with our security policies," noted their IT Security Architect.

Achieving Compliance With Data Privacy Laws

A multinational presence also poses data privacy challenges, especially when candidates submit sensitive data as part of the application process. "We have lots of sensitive data," said the Head of Data Center Ops, "including national identification numbers, medical information, and other personally identifiable information (PII) that needs to be protected." This data goes straight into the cloud-based tool from SAP.

To align with a myriad of national data privacy laws, personally identifiable information (PII) stored in SAP needed to be encrypted, which brought up the issue of key management. Encryption key management is the administration of policies and procedures for protecting, storing, organizing and distributing encryption keys. In this case, the customer wanted to maintain custody of the encryption keys, including the ability to store them on-premises.

CASB was able to address the encryption of sensitive data while providing the customer with on-premises custody of encryption keys through the Key Management System (KMS). The KMS ensures only authorized employees could access sensitive PII data.

Preventing Malware From Being Uploaded Into The Cloud

Cloud-based applications like SAP support file uploads that carry their own set of security vulnerabilities. For example, candidates applying for a job can upload a resume or CV as part of the job application. All documents uploaded needed to be checked for malware that can enable bad actors to open back doors, acquire authentication for internal systems, steal data or just generally disrupt the business. "We don't allow any documents that haven't been verified and scanned by CASB to be uploaded to the cloud," noted the Head of Data Center Ops.

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.