FORTRA

CASE STUDY (CLOUD DATA PROTECTION)

Protecting Data Shared with Thousands of Contractors

Fortra CASB helps a large construction firm protect intellectual property shared between employees, partners, and contractors

Large construction firms rely on a vast network of architects, engineers, project managers, contractors, and suppliers to collaborate on projects of all sizes and complexities. While the digitization of the construction industry has made it easier for these project teams to share information, it also expands the cyber-attack surface.

One of the country's largest commercial and civil contractors needed help improving cybersecurity efficacy and reducing business risk. The firm regularly shares documents between employees and third-party partners, including architectural plans, technical drawings, and other sensitive information, through Box and Google Drive. Sensitive project data stored in Salesforce is also widely accessible. While replacing onsite paper-based workflows with digital solutions has helped unlock operational efficiencies, it also puts intellectual property at risk of being stolen or compromised.

The firm realized that its cloud-based tools (Box, Drive, and Salesforce) offered limited security controls insufficient for broad-based third-party access to sensitive information. Its three main areas of concern were:

- The ability to protect sensitive documents downloaded onto an unmanaged partner or BYOD device, both on the site and after they've finished the job
- The use of unsanctioned IT applications that may expose sensitive documents
- Protection against viruses or malware that could infect files uploaded into these cloud solutions by a partner

Native data protection in a single, cloud-delivered platform

After a thorough evaluation, the firm turned to Fortra CASB to provide efficient and secure access for its third-party partners. CASB with native data loss prevention (DLP) and enterprise digital rights management (EDRM) provided a complete set of features needed to secure broad-based, third-party collaboration — all in a single, cloud-delivered platform.

AT-A-GLANCE

CHALLENGE:
Sensitive documents such as architectural plans, technical drawings, and other sensitive information are regularly shared between employees and third-party partners through Box and Google Drive.

SOLUTION:
Fortra CASB with native data loss prevention (DLP) and enterprise digital rights management (EDRM).

RESULTS:
CASB now provides discovery, management, and enforcement of shadow IT apps. CASB tracks more than 16,000 known apps in its extensive knowledge base. If an employee accesses any of those apps, it'll be shown in the traffic log. Once discovered, IT can address each unsanctioned and prohibited app on a case-by-case basis. The firm and its third party partners can work safely together without worrying about malicious content.

The initial implementation included CASB for Box, Google Drive, and Salesforce in an API-based deployment. The CASB serves as a visibility and policy enforcement tool, operating between user devices and the cloud applications they're accessing. It enables the firm to take a granular approach to data protection, making it possible to utilize cloud services for third-party collaboration safely.

Use it, then lose it

As a national builder, the firm maintains more than 4,000 employees and thousands of contractors spread across multiple job sites. While contractors are independently employed, they still require access to sensitive documents on the job site. The IT team had to implement security controls across this broad set of users while facilitating seamless collaboration.

For consistency, a common set of DLP policies had to be created and enforced across Google Drive and Box. DLP policies act as guardrails to help prevent users from unintentionally exposing sensitive data. The system can take actions such as removing public links, quarantining data, and watermarking sensitive files based on policy decisions.

EDRM added the ultimate level of protection. With its file encryption and access policy enforcement capabilities, EDRM enables partners to create, view, and modify information securely while protecting it from unauthorized access, use, and distribution. For example, files with a .vsd extension, which might hold CAD drawings, charts or images, can be encrypted and shared with partners while on the job. IT can revoke access based on various parameters such as the domain, email address or the timeframe it's accessed. Detailed, correlated, and normalized logs provide the firm's IT security team visibility to who opens a document, what device it's opened on, and where it's viewed.

In the shadows

With data shared across numerous third parties using personal or unmanaged devices, there's an inevitable risk of information leaking to apps that aren't sanctioned or supported by the firm's IT team. Known as "Shadow IT" this is a widespread challenge that's grown exponentially in recent years with the adoption of cloud-based apps. Simply put, if IT isn't aware of an app, they can't support it or ensure that it's secure.

Since shadow IT can introduce serious security risks and result in the loss of sensitive information, the firm's IT team depends on CASB to provide discovery, management, and enforcement of shadow IT apps. CASB tracks more than 16,000 known apps in our extensive knowledge base. If an employee accesses any of those apps, it'll be shown in the traffic log. Once discovered, IT can address each unsanctioned and prohibited app on a case-by-case basis.

Protecting against external threats

With data moving fluidly between the firm and its network of contractors, there was a real possibility that someone might upload files containing malware, trojans, or viruses onto Google Drive and Box. Once cloud storage systems are infected, these threats spread quickly to other users and devices. The firm deployed our Anti-Virus and Anti-Malware (AVAM) solution to mitigate this threat. AVAM automatically blocks infected files from being uploaded and quarantines the suspect file for further investigation by the internal security team.

With AVAM, partners can work safely together without worrying about malicious content. After deploying CASB, the firm's IT team was alerted to a ransomware threat from a partner integration. CASB detected abnormal behavior and quarantined the malware before it spread and inflicted lasting damage.

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.