FORTRA

CASE STUDY (CLOUD DATA PROTECTION)

Lantum Protects Sensitive Data, and Ensures Compliance with Fortra CASB

Workforce platform for healthcare organizations gains visibility into data, devices, and users.

The Objective: Protect Sensitive Data and Ensure Compliance

U.K.-based Lantum unites healthcare providers and their workforces so that they can deliver the best care together. Lantum works with more than 37,000 clinicians, and over 3,000 healthcare organizations and their highly sensitive data. The company required a solution that ensured all sensitive data, including employee and clinician records, is protected. The solution must minimize risk of exposure and ensure compliance with several cybersecurity and data standards such as the International Organization for Standardization's ISO 27001 and the U.K.'s National Cyber Security Centre's Cyber Essentials. Ensuring successful compliance with these regulations is essential to Lantum's business. Without it, Lantum could not continue as a supplier to the NHS — a core customer.

Lantum utilizes Google Workspace and enjoys its flexibility. However, there were security concerns about the sensitive data that could be aggregated within Google Drive. It is necessary to minimize the risk of an employee without the right access controls viewing or storing data on Google Drive, and sharing that data outside of an approved group. Lantum wanted visibility over downloads of sensitive data when, for example, an employee has resigned. According to Gary O'Connor, CTO, Lantum: "It's the things that you don't know about that you worry about the most."

Solution

O'Connor and Lantum's compliance officer were planning to recertify the company for ISO 27001 and refresh its adherence to Cyber Essentials. During this process, they chose to implement Fortra's award-winning cloud access security broker (CASB) solution.

AT-A-GLANCE

Company Lantum

Industry Healthcare IT, Human Resources Software

OBJECTIVES:

- Protect sensitive data in the cloud, minimize risk of exposure, and ensure compliance with both local and international data and cybersecurity standards such as the International Organization for Standardization's ISO 27001 and the U.K.'s National Cyber Security Centre's Cyber Essentials.
- Gain visibility into usage and enforce access policies for Google Workspace data and Amazon S3 storage.
- Protect the organization from insider threats.

CHALLENGES:

- Lack of visibility and control for IT over the data stored in the cloud.
- Lack of adaptive access and data security controls do not allow meeting compliance requirements.

SOLUTION:

Fortra CASB

RESULTS:

- Visibility into usage and access of all corporate data.
- Tracking of PCI and sensitive health data and its usage.
- Audit, control, and redaction of sensitive data.
- Monitor and control user access.
- Ensured compliance with the International Organization for Standardization's ISO 27001 and the U.K.'s National Cyber

According to O'Connor, "When you go through a process like ISO 27001, you must be able to prove that you have strong data protection controls in place. As Lantum's business scaled, we needed to automate certain things that previously were acceptable as a smaller business to do manually. If we can't do what we need to do to maintain ISO 27001 accreditation, we're not going to get into the conversations we need in order to grow revenue."

Fortra CASB protects data stored in all cloud and SaaS applications. Whether sharing the data externally with partners, or internally with employees, the solution provides IT with control and visibility to ensure an organization's data stays protected at all times. With adaptive access and data security policies combined with advanced analytics, Fotra enables organizations to safeguard data against intentional insider threats, accidental data exfiltration, data leakage from compromised accounts and other advanced internet-based threats without minimizing user productivity.

Working directly with a team of cybersecurity consultants and sales engineers, Lantum experienced a seamless and fast deployment of CASB saw immediate results. They quickly implemented policies to restrict unauthorized access and ensure compliance.

According to O'Connor, "One of the things that really helped us was the fact that you could quickly set up the tenant and easily configure it with Google Workspace — in less than an hour. We achieved value really, really quickly, and we've been able to build on top of that value over time."

Lantum has a hybrid work model with most employees spread across the U.K., along with several throughout the U.S. and Eastern Europe. With CASB, Lantum can see which people are accessing its data and from where. Having visibility into the type of data, where the data is located, and the level of sensitivity gives Lantum a better picture of expected or unexpected behavior patterns and markers.

The start of the war in Ukraine was another driving factor to scale Lantum's cybersecurity program. Several organizations were identified as critical infrastructure by U.K. government bodies, including the NHS. These identified organizations were required to review their cybersecurity policies due to concerns about external threats. These time-sensitive requirements cascaded down to all NHS suppliers, including Lantum. O'Connor and the compliance team needed to quickly demonstrate how they were dealing with various security scenarios. O'Connor said, "We quickly saw that screw tighten everywhere in our world because of that event. CASB has helped us deal with more of our cybersecurity matters in a systematic way."

O'Connor added, "Cloud tools like Google Workspace have blurred the boundaries of how we work — more and more business is being accomplished on our employee's mobile devices, which increases the risk of inappropriate data usage. CASB has given us greater visibility and control over our corporate and partner data without disrupting our employees experiencing any disruption in productivity."

> "CASB has been an incredibly valuable investment for Lantum. We now have better insight into what employees are doing with our sensitive data, especially in Google Workspace, and we're able quickly apply controls to that data. Thanks to Fortra CASB we can see a surge in downloads from a particular user or timeframe. It turns out none of them presented a threat, but having insight into this activity gave us peace of mind."
>
> **— Gary O'Connor** (CTO, Lantum)

Results

Fortra CASB has helped Lantum:

- Gain visibility into data, devices, and users
- Ensure continuous monitoring of user and entity behavior analytics and implement advanced data protection controls to help ensure compliance with regulatory requirements
- Protect data stored in Google Workspace apps from misuse and internet-based threats
- Enable employees to securely collaborate in a hybrid work environment