Case Study

How Lantum, a Workforce Platform for Healthcare Organizations, Protects Sensitive Data, and Ensures Compliance With Lookout Secure Cloud Access

The Objective — Protect Sensitive Data and Ensure Compliance

U.K.-based Lantum, the pioneer of Connected Scheduling™, unites healthcare providers and their workforces so that they can deliver the best care together. With more than 37,000 clinicians onboarded to its platform, in 2021 Lantum supported over 3,000 healthcare organizations, including nearly 150 COVID-19 vaccination centers, with their staffing needs. This saved the U.K.'s National Health Service (NHS) more than £30 million.

Lantum works with highly sensitive data. The company required a solution that ensured all of this 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 can't continue as a supplier to the NHS — a core customer.

The Customer

Headquartered in London, Lantum is on a mission to radically improve how the healthcare industry connects with the workforce so that they can provide better patient care. The Lantum platform uses advanced technology to help healthcare organizations manage their workforce and connect with a large network of healthcare professionals to fill shift gaps.

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.

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 imperative 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."

> "It's the things that you don't know about that you worry about the most."
>
> - **Gary O'Connor,** CTO, Lantum

Insider threats could cause serious problems down the line and without the right controls in place, the IT team could potentially struggle to work out who was responsible. Being proactive is key.

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.

The Solution: Lookout Secure Cloud Access, a cloud access security broker (CASB) solution.

The 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 Security Centre's Cyber Essentials.

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 decided to implement Lookout Secure Cloud Access, an award-winning cloud access security broker (CASB) solution.

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."

Lookout Secure Cloud Access 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, Lookout 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 Appurity's team of cybersecurity consultants and Lookout sales engineers, Lantum experienced a seamless and fast deployment of Lookout Secure Cloud Access — and saw immediate results. The customer quickly 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 Lookout tenant and easily configure it with Google Workspace — within under an hour. We achieved value really, really quickly, and we've been able to build on top of that value over time."

[1] ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS) and their requirements.

[2] The U.K.'s National Cyber Security Centre's Cyber Essentials regulation helps organizations guard against the most common cyber threats and demonstrate their commitment to cyber security.

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 Lookout, 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 of 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. Lookout 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. Lookout Secure Cloud Access has given us greater visibility and control over our corporate and partner data without disrupting our employees experiencing any disruption in productivity."

Lookout Secure Cloud Access is one element of the Lookout Cloud Security Platform, which converges security service edge (SSE) and endpoint security to protect users and data wherever they reside. It continuously monitors the risk posture of users and devices to provide dynamic and granular zero-trust access based on the sensitivity level of apps and data, enabling organizations to protect its workers, their devices, apps, and data from unauthorized access as well as from modern day internet-based threats. The platform provides customers the ability to leverage the threat intelligence from mobile endpoints to make more informed decisions for cloud security services.

Built on the Company's patented technologies, the Lookout Cloud Security Platform combines the following security services:

- Lookout Secure Cloud Access, the Company's CASB solution, provides seamless security across all cloud and SaaS apps with unified policies, trusted data security and validated standards compliance, offering complete visibility and control.
- Lookout Secure Private Access is a cloud-delivered zero trust network access (ZTNA) solution built on the principle of zero trust that provides seamless access to private enterprise applications no matter where the user or the app may be located. Unlike a VPN, Lookout Secure Private Access connects users to apps and not the network, a core principle of a zero-trust architecture.
- Lookout Secure Internet Access is a cloud-delivered secure web gateway (SWG), which includes firewall as a service (FWaaS), built on the principles of zero trust to protect users, underlying networks and corporate data from internet-based threats and prevent data leakage.
- Lookout Mobile Endpoint Security enables secure productivity from mobile devices – personal, managed, and unmanaged iOS, Android and Chromebook devices – by protecting against socially engineered phishing campaigns, malicious apps, risky network connections and full device compromise.

> "The ability to audit what you've done, and what data you have, has been incredibly useful to us."
>
> – **Gary O'Connor,** CTO, Lantum

Results

> "Lookout's 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."
>
> - **Gary O'Connor,** CTO, Lantum

Lookout Secure Cloud Access 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

About Appurity

Appurity is a team of cross-platform mobility consultants specialising in assessing security environments and delivering best-in-class mobile and application security solutions. Built for the modern and dispersed workforce, Appurity's solutions adhere to data protection and cybersecurity schemes and regulations such as Cyber Essentials and ISO. It works with companies to develop and implement impenetrable security strategies that utilize the latest technologies and security frameworks including ZTNA, SSE, CASB and MTD.
Its solutions are built to offer unparalleled protection — endpoint to cloud — while improving productivity for users.

> "Thanks to Lookout Secure Cloud Access, 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

About Lookout

Lookout, Inc. is the data-centric cloud security company that uses a defense in-depth strategy to address the different stages of a cybersecurity attack. Data is at the core of every organization, and our approach to cybersecurity is designed to protect that data in the modern threat landscape. With a focus on people and their behavior, the Lookout Cloud Security Platform ensures real-time threat visibility, and quickly halts breaches from initial phishing attempts to data extraction. To learn more, visit www.lookout.com and follow Lookout on our blog, LinkedIn and X.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo