SureDrop

Global cybersecurity company embraces collaboration without compromise.

Overview

A security first approach to file-sharing and storage

Digital transformation initiatives dominate the IT landscape in many industries. The security, defence and aerospace sectors are no exception. However, the sensitive nature of the data moving to, from and within these organisations means they need to adopt a security first approach to file sharing and collaboration.

An increasingly dispersed workforce, more connected devices and a work from home revolution have combined to place an emphasis on collaboration. Unfortunately, some users will engage in risky behaviour in the name of convenience. This could mean anything from leaving devices logged in to systems to accessing files via unsecure wi-fi networks, or the use of public file sharing apps or email clients for the exchange of sensitive or confidential data.

Today's cybercriminals are better resourced and better funded than ever. Whether they are rogue nation states, financially motivated cyber gangs or state-sponsored cyber-terrorists; the volume and variety of attacks bad actors are capable of launching is increasing constantly.

> *We needed a more secure alternative to mainstream collaboration platforms. We wanted something that featured end-to-end encryption and allowed us to control where our data is stored.*

Data exchange via email, public collaboration platforms or critical business applications is vulnerable, both to cyberattack and accidental breach. As such, there is a preference for robust encryption security; so, in the event of a breach, the data remains confidential.

The consequences of an unsecured breach could be catastrophic, with the potential loss of proprietary IP, personally identifiable information or confidential data leading to business disruption, financial penalties, a loss of reputation and even civil litigation. When dealing with government and defence networks, the risks could extend to existential threats.

Customer

Profile:

10,000+ employees

Offices in over 30 countries

Annual turnover >US$1billion

In this instance, our customer is a large, multinational enterprise providing cybersecurity services to government and commercial customers around the world. Employees create, store, share and collaborate on thousands of files every day; from technical, financial and security documents to government and defence secrets.

Any successful data breach resulting from unsecure file sharing and collaboration would come at enormous cost, both in terms of direct costs to remediate and potential regulatory penalties, not to mention the damage to its reputation as a trustworthy partner.

Requirements

- Advanced, standards-based encryption
- State-of-the-art encryption key management
- Certified data sovereignty capability
- Intuitive user interface
- Microsoft 365, Azure, Active Directory and Outlook integration
- On premises or SaaS cloud deployment flexibility
- Compatibility with (certified) 'protected' status sovereign cloud data centre
- Integration with AWS (Amazon Web Services)
- Workgroup collaboration features
- Compatibility with in-house key management and data storage solutions
- High-volume throughput and real-time performance

Evaluation

Considering the specific requirements of the organisation, the customer identified secure collaboration as its primary objective. They elected not to consider collaboration platforms with 'added on' security features. They also rejected solutions that would lead to high frequency security patching as these may lead to security vulnerabilities and high management costs.

The customer decided that effective protection against shared file data breaches also demanded data sovereignty – enabled by 100% control over file storage location to ensure files are stored within the organisation's sovereign territory in a SaaS cloud enabled solution.

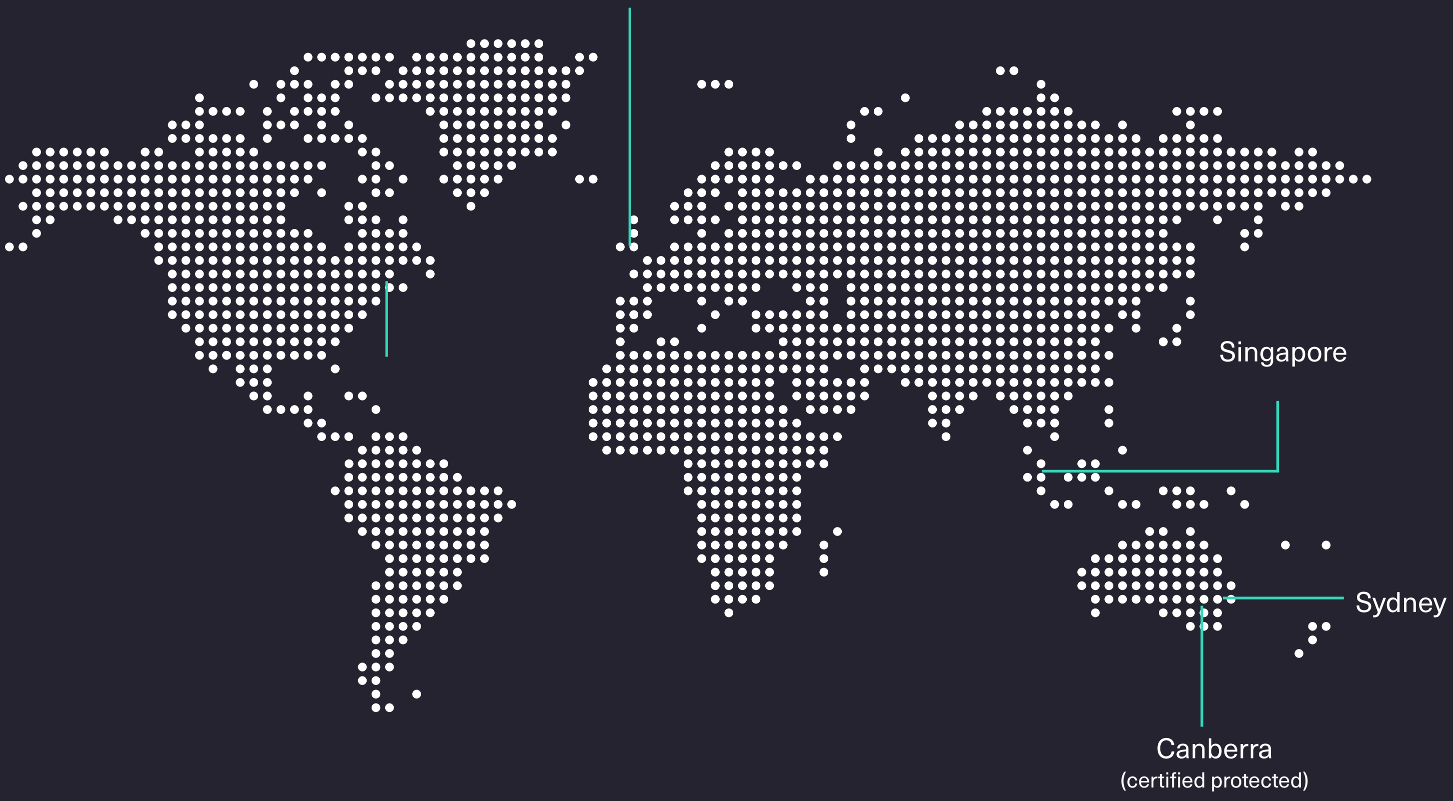
The customer determined the solution must meet two cloud data storage requirements:

- Compatibility with (certified) 'protected' status sovereign data storage – where the data's classification mandated both 'protected' status classification and sovereignty.
- Seamless integration with AWS (Amazon Web Services) cloud data storage without compromising the data's encryption security.

In short, the solution needed to be built from a security first standpoint.

Solution

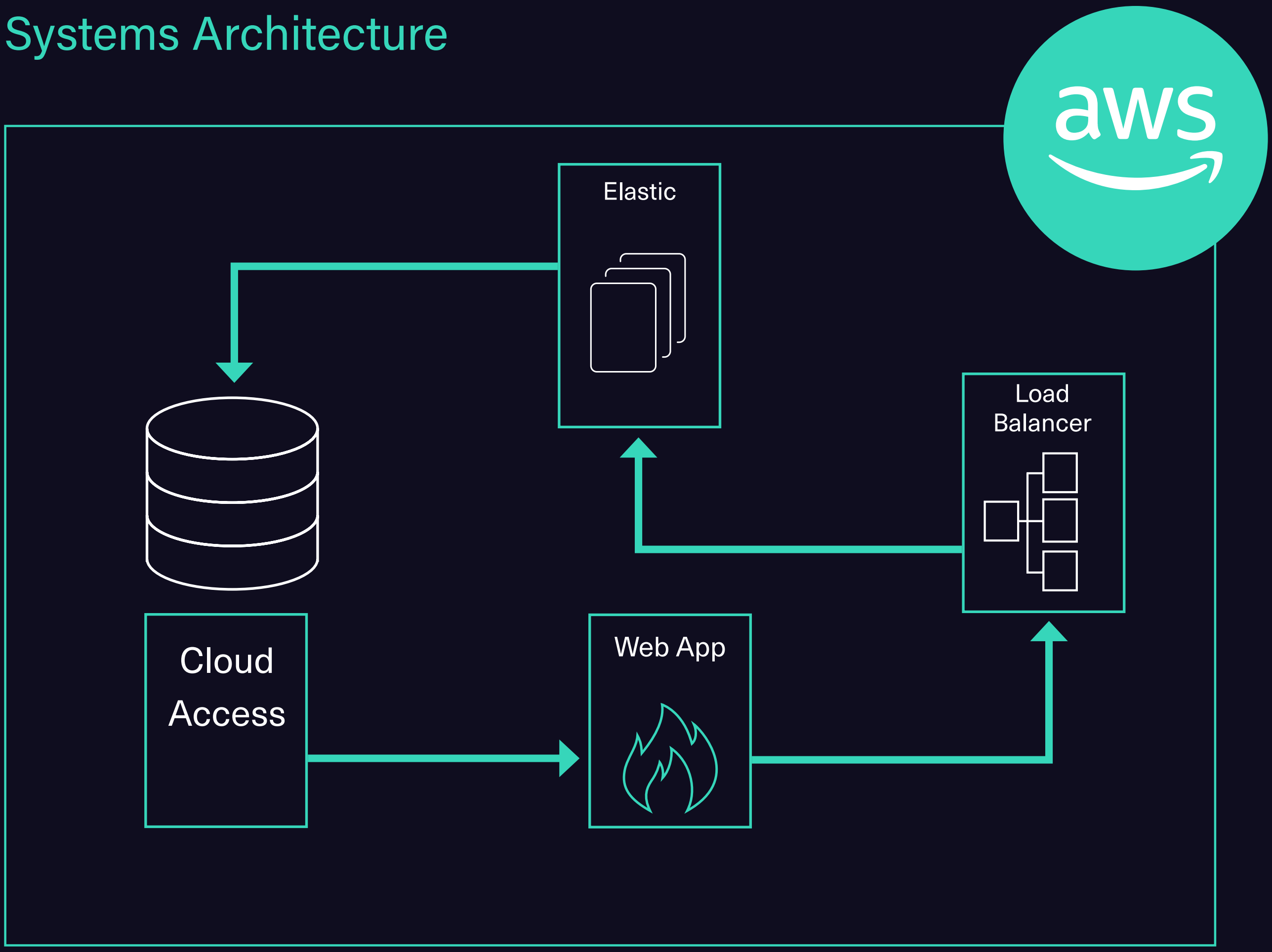
The customer chose SureDrop because it was built from the ground up with secure workgroup collaboration in mind. SureDrop features all the convenience of popular box-style applications, plus the implementation of best-in-class security.



- Primary file-sharing and collaboration platform
- 3 geographic regions
- >10Tb of data securely stored
- Mixed on-premises and cloud deployment
- 100% data location and sovereignty control
- Support AU Cloud certified 'protected' data storage status (locally mandated)
- AWS cloud storage integration
- Over 800 users enrolled
- Microsoft 365, Outlook, Active Directory and Azure integration

> "Not only does SureDrop provide a secure platform for collaboration, it also provides frictionless, real-time access to large volumes of files. As a result, user adoption and satisfaction levels have been high."

Systems Architecture



SureDrop®is brought to you by Senetas Corporation Limited.

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

SureDrop