SureDrop

SUREDROP IN ACTION

Biotechnology company requires cybersecurity without compromising workgroup efficiency.

Overview

A security first approach to file-sharing and collaboration

A hybrid workforce (comprising office workers, home workers and remote workers) has become the default model for many organisations. Whilst it offers many benefits, not least of which is a better life/work balance, it means businesses have become more dependent on collaboration solutions and ubiquitous access to business-critical data and applications.

Borderless networks, cloud applications and user-owned devices may provide convenience but they also create risk. The greater the number of gateways into the network, the greater the threat of cyberattack. File-sharing and workgroup collaboration often involves the exchange of confidential or high value information, this data is a prime target for cybercriminals.

Cyber-threats dominate the IT landscape in many industries, especially among those richest in intellectual property and personally identifiable information. The medical research and technology sectors are no exception. The high value nature of the data moving to, from and within their workgroups requires them to adopt a security first approach to file sharing and collaboration.

Cybersecurity experts highlight three primary risk factors arising from file-sharing and collaboration – the use of BYO devices, inherently unsecure Internet connections and innocent user errors. 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 data 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 are increasing constantly. Data exchange via email, public collaboration platforms or critical business applications are vulnerable, both to cyberattack and accidental breach. As such, there is a preference for strong 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.

Customer

Profile:

100+ employees

Supplies over 10 countries

Annual turnover >US$50million

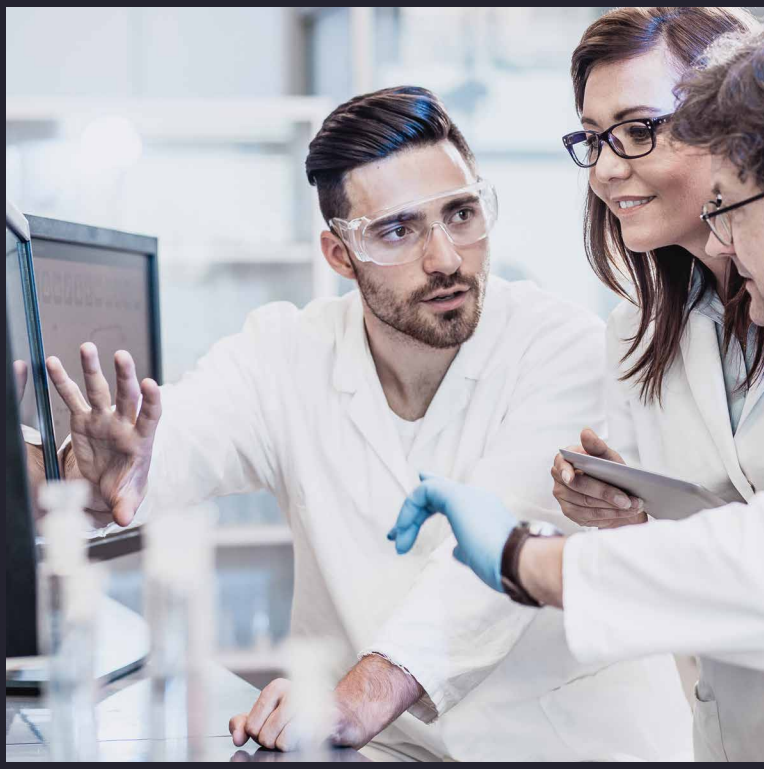
Our customer is a specialist medical research and biotechnology company that manufactures regenerative medicine products used in acute medical treatments. Its proprietary technology has enabled broad clinical applications including complex surgical applications.

Workgroup collaboration is a fundamental activity in both the organisation's continuing medical research and clinical work. Research and clinical workgroup activities require employees to create, share, collaborate on and store numerous sensitive files daily, from patient identities and clinical information to valuable intellectual property. Sharing files within and outside the organisation adds a need for file location control, providing data sovereignty.

The customer recognises the increased cyber-risks through maintaining hybrid workgroups. Any successful data breach resulting from unsecure file sharing and collaboration would come at enormous cost, both in terms of direct costs to remediate, potential regulatory penalties, and reputational damage.

Requirements

- Advanced, standards-based encryption
- Advanced security features - standards-based encryption and file fragmentation across a data storage mesh
- State-of-the-art encryption key management
- Data sovereignty capability
- Intuitive user interface
- Microsoft 365, Azure and Active Directory integration
- Sovereign cloud deployment
- Compatibility with (certified) 'protected' status sovereign cloud data centre
- Integration with AWS (Amazon Web Services)
- Workgroup collaboration features
- Real-time collaboration performance



Evaluation

The customer identified secure collaboration as its primary objective, preferably without compromising user convenience. It elected not to consider collaboration platforms with 'added on' security features.

Due to the proprietary nature of the customer's research and product information, it decided that effective file protection also demanded data sovereignty – enabling 100% control over file storage location to ensure files are stored within the organisation's sovereign territory in a Cloud enabled solution.

The customer's Cloud data storage requirements are:

- Compatibility with (certified) 'protected' status sovereign data storage – where the data's classification mandated both 'protected' status classification and 100% 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-type applications, plus the implementation of best-in-class security.

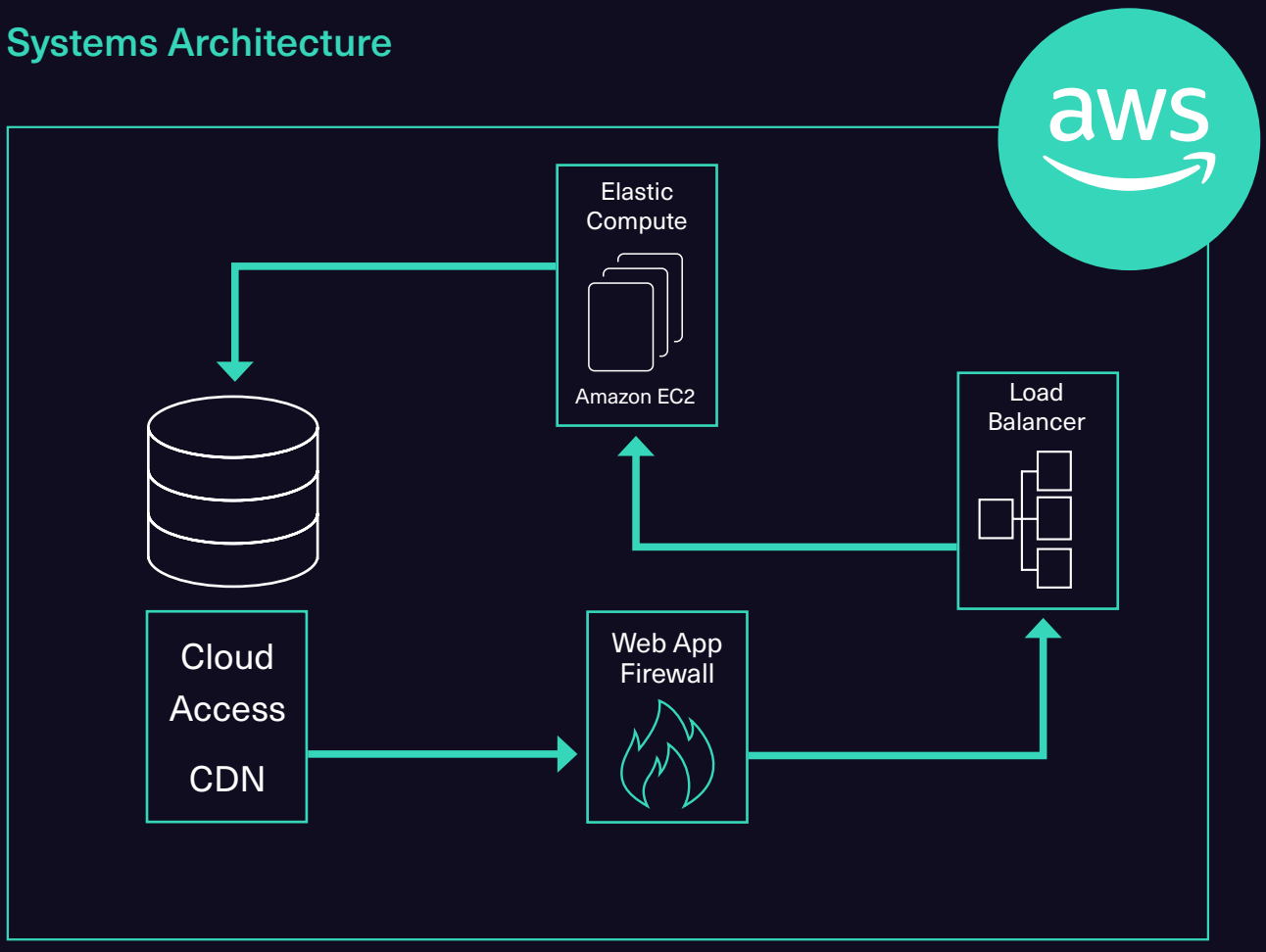
Customer Implementation

- The primary sharing and collaboration platform
- >5Tb of data securely stored
- Secure Cloud deployment
- 100% control over data sovereignty
- AWS cloud storage integration
- Microsoft 365, Active Directory and Azure integration

> "SureDrop met all of our evaluation criteria; secure, sovereign and seamless. We take security very seriously but, at the end of the day, the system has to be user friendly. Otherwise, people just won't use it."

RDS

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

info@suredrop.io T +61(03) 9868 4555