SureDrop

SUREDROP IN ACTION

National defence department requires secure team collaboration and real time performance.

Overview

Security is not negotiable

With the continuing, fast pace of government agencies' digital transformation and cloud adoption, they are exposed to a growing cybersecurity threat landscape. Today's cyber-attacks are initiated by motivated and well-resourced organisations, such as those sponsored by rogue nation states, organised crime syndicates or cyber-terrorists. They are typically large, clandestine organisations with significant funding and technical capabilities.

Government agencies are a primary target, as cyber-criminals seek to steal government secrets, citizen identities and other high value data. US cybersecurity sources highlight continuing cyber-attacks on government agencies, such as healthcare, defence and human services and their supply chains. When successful, the data breaches lead to catastrophic harm - ranging from damage to IT systems, disruption to services and even breaches of critical national security information.

Digital transformation efforts are complicated by the widespread adoption of hybrid workforces. As government employees share files and collaborate over the Internet, use unsecure BYO devices and even use public file-sharing services to work remotely, files are exposed to serious cyber-threats. Government agencies need both security and usability, without compromise.

Data exchanges 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 for loss of high-value, sensitive data. When dealing with government and defence networks, the risks could even extend to existential threats.

> "Our workgroup teams share and collaborate on highly sensitive files that in the wrong hands could weaken our national security. As we advance our digital transformation and take advantage of cloud-enabled services, we are mindful of the cybersecurity risks."

Customer

Profile:

500,000+ civil employees

National and international locations

Our customer is a national defence agency with civil employees located throughout the country and in numerous other countries. Like many national government agencies, the defence department has embraced digital transformation to support its remote workers and improve efficiency whilst lowering its overall IT infrastructure overheads.

Defence agency teams' work involves high volumes of file-sharing and regular team collaboration. However, our customer recognised a number of cybersecurity vulnerabilities that required a more secure collaboration platform, something designed from a security first perspective. At the same time, it was important that security didn't come at the cost of performance. There was still a requirement for real time file availability and synchronisation.

The primary risks identified were the potential loss of unencrypted data, attacks on encryption key infrastructure and the danger of malware being introduced to the network. customers' security policies also include the need for total control over file location under its requirement for data sovereignty.

The solution requirements included the need for it to support hybrid Cloud infrastructure and Thales HSM (High Security Module) and CipherNet - providing maximum encryption key management and encryption storage on premises and in the Cloud. The customer also required assurance that the solution would support all file types and sizes, not compromise real time file synchronisation, or the quality of files such as high resolution video and audio.

Requirements

- Advanced, standards-based encryption
- File fragmentation across the data storage mesh
- State-of-the-art encryption key management
- Support for Thales HSM and CipherNet key storage and management
- Real time performance
- Seamless integration with Microsoft 365, Azure, Active Directory
- Support for Votiro Cloud API anti-malware optional integration
- Audit logs and other user security features
- Support for hybrid cloud infrastructure

Evaluation

The customer evaluated a broad range of alternative solutions, none of which could match the primary security features offered by SureDrop. The customer identified secure collaboration as its primary objective, without compromising user convenience and real time performance.

Due to the national security nature of the customer's information, it required 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.

Integration with Thales HSM and CipherTrust secure key storage and management used by the customer was not supported by any alternative solution. The customer was already familiar with the high-assurance hardware encryption products offered by Senetas. CN Series encryption hardware is also compatible with Thales HSM and CipherTrust, and this legacy of best-in-class encryption security had a positive influence on their choice of solution.

Solution

The customer chose SureDrop because of its security credentials - built from the ground up with government and defence grade workgroup secure 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
- >10Tb of data securely stored
- Secure hybrid Cloud deployment
- 100% control over data sovereignty
- Thales HSM and CypherTrust integration
- Planned implementation of Votiro Cloud API anti-malware
- Microsoft 365, Active Directory and Azure integration

> "SureDrop provides the strongest security features available and necessary for secure team collaboration whilst meeting our sovereign file storage control requirement. And it delivers an efficient real time user experience."

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