asigra

ULTRA SECURE BACKUP

Case Study

Public and Commercial Services Union strengthens cloud backup services with cybersecurity protection across Windows network and Microsoft 365 cloud data

- One of the largest trade unions based in the UK
- Following a significant growth in membership during 2020, and emerging ransomware threats to cloud data, PCS strengthened its recovery capabilities from cyber attacks to enhance their organisational resilience
- Leveraged local partners expertise and knowledge to reduce time to implement.

pcs

DATA2VAULT
SECURE DATA SERVICES

MillerTech
CRM SPECIALISTS FOR NFP

Summary

The Public and Commercial Services (PCS) Union is a nationwide organisation with offices throughout the United Kingdom operating within civil service, government, and privately operated institutions. PCS maintains an extensive distributed hybrid IT environment across the country. With the increasing number of IT platforms, adoption of Cloud services, the growth in cyber security threats and implications presented by General Data Protection Regulation (GDPR), PCS recognised the importance of strengthening their Cloud Backup and Cybersecurity protection to ensure security, recoverability and compliance across their on-premise and Cloud data. As a result, PCS continue to enhance its Cybersecurity services with the support of MillerTech, Data2Vault and Asigra to ensure its primary IT directive of operational continuity.

Customer Overview

PCS is one of the largest trade unions in the United Kingdom with about 300,000 members. The trade union is organised throughout civil service and government agencies, making it the largest civil service trade union in the country. PCS is a democratic organisation, run by members, for members. The collective campaigns for fair pay and conditions, decent pensions for all and equality in the workplace and beyond. PCS is organised into groups that deal with different bargaining units such as Revenue and Customs, Work and Pensions and Law and Justice. With hundreds of thousands of records under management, regulatory requirements related to the General Data Protection Regulation (GDPR) and the growing presence of ransomware, PCS endeavored to audit its IT environment, calling on Data2Vault and Asigra to optimise the security and compliance of its backup and IT continuity infrastructure.

Business Situation

PCS relies on a powerful Oracle-based membership system referred to as Commix which was implemented by MillerTech, a UK-based IT solution provider. The system is maintained to manage memberships, subscriptions, communications, ballots, education, training, reporting, statistics and more. Commix holds the data of more than 300,000 members/contacts of PCS with approximately 15,000 self-service users accessing the system. In addition to Commix, the organisation's computing environment includes distributed VMware systems, databases and Cloud-based data on Microsoft's 365 subscription services, deployed throughout to support workspace requirements. Because of the importance of IT on its operations, PCS has been proactive in monitoring both current and future requirements of its computing infrastructure. After an internal audit, the organisation made the decision to strengthen its security posture

CHALLENGES

- How to minimise the vectors of ransomware attacks, and protect cloud-based data
- Staying current with GDPR compliance
- Insufficient internal resources

ASIGRA CLOUD BASED DATA RECOVERY DELIVERS

- Single integrated solution for all data protection needs
- Policy-based protection based on the organisation's IT environment and recovery requirements
- Optimisation of IT resources for enhanced utilisation
- Data encryption that secures data in-flight and at-rest with full support of compliance requirements
- Agentless architecture
- Signature-less malware detection solution that identifies and quarantines unauthorised or malicious embedded code in backup data across Windows networks and MS365
- Compliant Data Destruction
- High-performance data recovery

and compliance of its data protection environment to safeguard the data of its members.

Cyber attacks on organisations have been on the rise globally, with ransomware at the forefront of threats impacting businesses and non-profits worldwide. In their recent 2020 Breach Insights Report, Beazley Underwriting identified a 131% increase in Cyber insurance claims and attacks by evolving Ransomware was the most common cause. They also identified 24% of these increased claims came as a result of a compromised IT Provider or vendor in their supply chain. The potential impact of such malicious code has meant that PCS escalated the specific protection of their data, in the event of a Cyber attack, to a top priority.

The last line of defense against a ransomware attack is the availability of clean recovery data. However, malicious coders understand this and have developed what is now known as a ransomware Attack-Loop™ to prevent successful recoveries from impacting their bottom line. Attack-Loops occur when hackers insert executable code within the organisation's backup data. When an attack occurs, both primary and secondary data are affected, preventing the possibility of a clean recovery. To hide the code in the backup set, the hacker uses a variety of techniques such as inserting the malware into data objects which are then backed up and stored in the company's secondary storage repository. After a time-delayed detonation, the company restores a pre-attack generation of data only to realise that the recovery data re-inserts the ransomware into the network, recreating the ransomware for a perpetual loop of attacks.

Prior to updating its systems, the procedures PCS used for preventing ransomware from infecting backup data (a.k.a. Attack-loops™) included regular malware scans of network data before a backup was taken. If ransomware was successfully detonated and files became encrypted, the network, systems and backup data were scanned using an anti-malware solution which had limited success in recovering clean data. If older backups were infected with ransomware, meaning it was not possible to recover a ransomware free backup, there would be a serious impact. PCS is a Not for Profit organisation that relies on membership fees for income, anything that disrupts membership billing or collection could be very damaging.

PCS provides a range of time sensitive services to members that include support in legal cases and assistance with employer disputes. Anything that delays or prevents PCS from delivering these services would affect members and damage the union's reputation. With respect to the data under management, PCS oversees and processes a large volume of personal and sensitive data. Therefore, anything that negatively impacts or makes this data inaccessible would constitute a breach under the GDPR, with severe consequences.

With the implementation of Asigra's anti-ransomware capabilities, PCS has changed the process for addressing Attack-Loop based ransomware infections in the backup sets. The inline scanning of backup and recovery data now provides protection against such attacks. Potential backup data deletions or encryptions are countered by the 2FA administration and variable naming to prevent these actions. Asigra gives PCS several new layers of protection, adding further to an effective response should the ICO audit the organisation.

Solution

A longstanding client of data protection provider Data2Vault, PCS called on its trusted managed services partner to review its backup infrastructure for any possible challenges. After an audit revealed the need for security and compliance enhancements, Data2Vault deployed the full suite of Cloud-based data protection services powered by Asigra's Cloud Backup

software. Asigra's platform provides the right blend of enterprise data protection and cybersecurity to address unanswered challenges of security, data privacy and regulatory compliance as they impact data backup and recovery systems. Data2Vault deployed the solution as a service for PCS, providing advanced malware/ransomware protection, GDPR compliance, and high-performance data recovery when required.

> "As a systems specialist for non-profits such as PCS, the time-tested deployment of our Commix system supports the organisation's mission with unprecedented success. The approach of Data2Vault and Asigra in addressing Windows and Linux based data protection complements the overall operation. The combined efforts of this team have played well for PCS."
>
> **Hitesh Sharma, Operations Director**
> **MillerTech**

Data2Vault provides a range of advanced data protection solutions, delivered as secure, managed services that are automated, optimised and simplify core IT operations to help drive efficiency and reduce risk. This MSP understands the economic benefits of Cloud computing and the flexibility it offers, but believes security and managing risk is fundamental to the successful adoption of Cloud based services. Data2Vault has selected the most appropriate award-winning vendors in data protection such as Asigra. The company works closely with industry leaders in risk assessment and channel partners to provide a range of complementary Data Protection and Cyber Security managed services delivered to the most exacting data availability and integrity criteria.

The MSP's data protection suite is powered by Asigra's Cloud Backup software. The Asigra platform converges data protection and IT security for unique and highly effective malware detection and prevention that ensures safe, secure and reliable backup and data recovery whether data resides locally or on Cloud based applications such as Microsoft 365. The solution includes the industry's leading zero-day Attack-Loop™ preventative technology (see figure 1) using signatureless bi-directional malware detection, zero-day exploit protection, variable repository naming, and step-up multifactor authentication (Deep MFA) for a full defensive suite against advanced ransomware and other cyber-attacks on backup data. This is complemented by FIPS 140-2 certification and military-grade data encryption to ensure enterprise-grade data security.

The Asigra platform also includes powerful GDPR compliance enabling features. While the pending regulation requires companies to delete data at the request of the subject, including from backup sets, many organisations lack the ability to easily perform this operation. The long term retention of image-based backups common with many backup platforms require manually intensive processes. With Asigra Cloud Backup Evolved V14, businesses can delete backup data efficiently and in any generation to meet GDPR compliance requirements. It is then possible to provide a data subject with a certificate as evidence, forming part of an effective response to the Information Commissioner's Office (ICO) in the UK.

> "The management at PCS are always proactive in their efforts to protect their systems and the data of their members. With guidance from Data2Vault PCS adopted a more security focused data protection posture to protect against emerging threats such as evolved Ransomware targeting Cloud Data. For any organisation concerned about zero-day malware infecting their data, and in turn their backup files, we provide an early warning service should any of the data becoming infected. This service can be provisioned without disrupting existing backup or malware scanning solutions. I would urge anyone making use of Microsoft 365 subscription services or Windows networks to take a look at the Asigra Cloud Backup platform, it has been instrumental in our efforts to ensure data recoverability against ransomware attacks."
>
> **Mark Saville, Director**
> **Data2Vault**

Results

With the newly provisioned additions to the proven backup services already operational, The IT Disaster Recovery planning at PCS demonstrates the additional resilience and recovery response capabilities of the advanced cybersecurity platform. In the event that PCS is confronted with evolving zero-day malware attacks, compliance audit requests, or a data loss event, the organisation is prepared at many levels to respond quickly and has peace of mind that more disaster recovery scenarios, including recovery from the latest forms of ransomware are catered for. With vital information and systems interconnected across multiple virtual machines, hypervisors, physical servers and Cloud applications, data recovery and operational restoration will be optimised depending on the cause.

The new data protection environment provides powerful enterprise features, including continuous data protection, instant recovery, virtual machine replication, primary site failover with fast recovery time objectives (RTOs) on virtual machines, hypervisors, and physical machines. The service constantly monitors the logical and physical integrity of backup data as it is written to storage, provided through autonomic healing, and now ensures an early warning against ransomware infection, so mission critical data is recoverable when required, irrespective of whether it's in MS365 applications or on-premises servers.

> "Information technology must be able to adapt as business conditions require in order to remain several steps ahead of potential challenges. We have been very pleased with our enhanceddata protection environment as it adds layers of protection that situate the organisation well in the event of any ransomware attacks or compliance audits. We highly recommend MillerTech, Data2Vault, and Asigra to businesses and nonprofits seeking to up their game in IT and data protection."

Head of IT and Facilities,
Public and Commercial Services Union,
Andrew Simpson

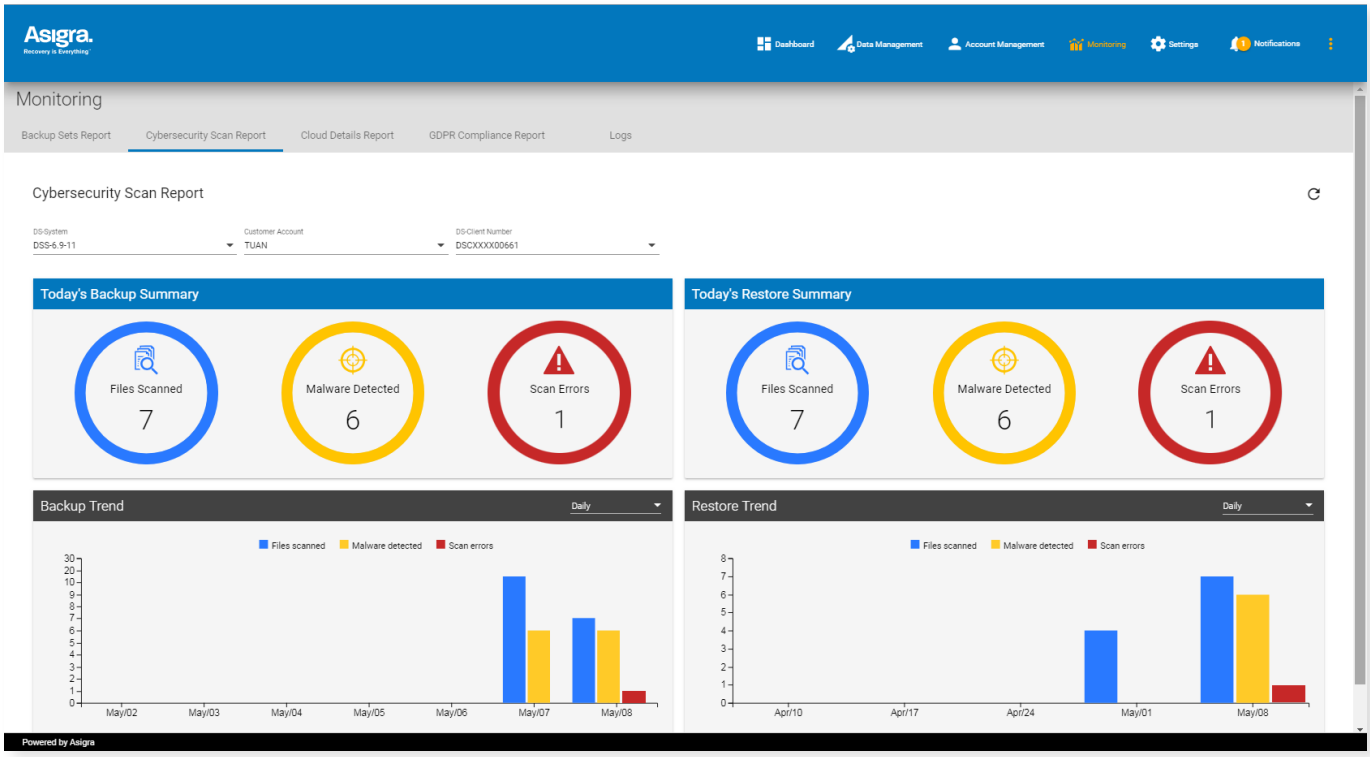

Figure 1 – Cybersecurity Dashboard

About Data2Vault

Our key people have been involved in the secure data protection market since before 2005, working closely with Asigra throughout this time. Our philosophy is simple, security must be at the core of the data protection services we offer, and no one size service fits all. Our objective is to always deliver the data protection services that your organisation needs, securely and in the way that you need it provided. As those needs evolve, then so must our service delivery models, while always retaining a consistent focus on security and management of risk, wrapped up in a high-quality service. We operate from a number of UK Data Centre's to provide high availability continuity of our Data Protection services. The Data Centre's are all ISO9001, ISO27001 and ISO14001 certified, the services we provide are highly resilient and can scale as required to ensure we have no single point of failure at manageable cost.

More information on Data2Vault can be found at www.data2vault.com/.

About MillerTech

MillerTech is a market leader in supplying Membership and CRM systems to the Not for Profit (NFP) sector. We have worked closely with NFP Organisations for over 33 years, delivering effective and innovative solutions which ensure that all your contacts are fully informed and engaged. We have implemented solutions for over 200 NFP organisations including trade unions, charities, associations, friendly societies, professional/regulatory bodies, fundraisers and healthcare providers. Our clients range in size from a few hundreds of members up to millions, with users ranging from a few to thousands.

More information on MillerTech can be found at www.millertech.co.uk/.

About Asigra

Trusted since 1986, Asigra Tigris is a multi award winning backup and recovery technology proudly developed and supported in North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global network of IT service providers. As the industry's most comprehensive data protection platform for servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, and eliminates silos of backup data by providing a single consolidated repository with 100% recovery assurance and antiransomware defense.

More information on Asigra can be found at www.asigra.com

asigra