



MSP SiquaL got a customer's business back up and running in less than four hours after a ransomware attack, thanks to ShadowProtect.

Client Profile



Company

SiquaL

Country

France

Industry

Managed Service Provider
(MSP)

Number of employees

19

Solution

ShadowProtect SPX

About SiquaL

SiquaL is an IT Services organisation, offering a broad spectrum of services to its customers, from publishing their ERP to supporting their overall IT infrastructure. With a team of 19 experts, SiquaL generates a turnover of almost 2 million euros a year. Their customers include lawyers, doctors, construction companies and other industries. These organisations rely heavily on IT systems to run their day-to-day business.

SiquaL's vast areas of expertise include storage and data protection solutions, where they have been working with StorageCraft for almost a year. As an MSP, they strive to offer flexible, easy-to-deploy and cost-effective solutions to meet the needs of its small and medium-size business customers.

The Challenge

A few months ago, during an audit for a new client working in the oil industry, SiquaL's experts realised that the backup and data recovery solution deployed by the previous service provider had not been operational for some time, and the client had not been informed. The solution was supposed to protect over 2 terabytes of data, including important HR data, accounts (payroll), as well as their customer database and the sales results, much of which is critical data for the business.

In the event of a system failure or a cyber-attack, the MSP had to be able to act very quickly and roll out a new viable solution to ensure storage and data protection, and above all, business continuity for this company generating a significant amount of revenue.

The Solution

After a successful evaluation and onboarding of the solution into their portfolio, the Siqua's experts naturally recommended StorageCraft ShadowProtect to this particular customer. It offers optimal data protection with a flexible and reliable disaster recovery and ensures that data and systems are always protected and available.

Regular snapshots allow the servers to be restored to the last backup in the event of a disaster. The frequency of these snapshots, that can be set up as needed, was happening every 2 hours for this customer.

The second recommendation was the deployment of an on-premise and off-premise NAS, to better secure the data in the event of a cyber-attack. The MSP offers a private outsourced backup storage with the option of renting a secure location for the off-premise NAS in their own offices.

Siqua uses ShadowControl, a reliable control and management software to monitor and manage the ShadowProtect solution.

“Thanks to StorageCraft, we can offer cutting-edge storage and data protection solutions, while also being able to better monitor our clients' infrastructure. We are delighted with their on-going technical support and guidance. We have full confidence in their engineers who we fully trust. ”

Sylvain Graveron
Technical Manager of IT System
Management, Siqua

The Results

Several months after the successful deployment of ShadowProtect, this client fell victim of a ransomware attack, presumably orchestrated remotely using the RDP protocol, through a user account with insufficient protection.

“No one told us that this privilege had been granted to this particular user after our audit. We discovered it when we were analyzing the data from the attack,” explains Sylvain Graveron, Technical Manager of IT System Management at Siqua. “Neither the protocol nor the authentication criteria followed any IT security best practices.”

After presumably gaining access to the company's data, the hacker started encrypting the file server, which consisted of two virtual machines hosted on a physical server, forcing the company's activity to a complete stop.

The attack took place in the middle of the night, at around 1am. The experts at Siqua were informed by the client the following morning, at around 8 am, and they immediately contacted the StorageCraft Technical Support Team for assistance with the disaster recovery plan.

The last snapshot backup of the data happened at 10:00 pm the night before, which allowed the company to recover its entire information system in less than 4 hours. Most of the 4 hours was spent in restoring data via the network from the local NAS. “As the attack happened overnight, the data was fully restored, nothing was missing!” says Sylvain Graveron.

The ShadowControl monitoring platform has been essential to check the status of the last backup, to gather details about the time of the encryption and ensure a fast and efficient recovery.

The recommended double NAS approach also meant double security since the client’s off-premise NAS was not affected by the attack.

After realising that the company was closed to a major disaster, the management team ran a new security audit of their infrastructure and had to rethink their identity and access management strategy; it was a clear alarm bell about the risks they got exposed to due to weak IT security practices within the organisation. Thanks to this experience, the company is now in a much stronger position with regards to its data resilience.

Siqua’s future projects will largely revolve around Windows 2008 end-of-support and the migration to the 2016 version. Backups will play a key role to ensure a smooth upgrade that that will not affect the company’s data nor applications.

“Backups are the ultimate protection, yet they are still rarely integrated into security strategies. Today, it is vital for all businesses to understand this, and to equip themselves accordingly.”

Sylvain Graveron
Technical Manager of IT System Management, Siqua



Find out more

www.StorageCraft.com/uk



Contact

sales@storagecraft.eu



See more case studies

www.StorageCraft.com/resources