Keeping vital services up and running

Solution components

- **Predatar Ultimate**
- **IBM Storage Protect**
- **IBM Storage Protect Plus**
- **IBM Cloud Object Storage (ICOS)**

One of the UK's largest utilities providers enhances its cyber protection with IBM Predatar and IBM to ensure uninterrupted essential services.

Maintaining a continuous supply of essential services to households and businesses is one of the highest priorities in a modern economy. The utility provider, which supplies more than 5.2 million homes and 150,000 businesses, wanted to minimise the risk of service interruptions by protecting critical systems. Facing the growing threat of ransomware, how could they defend against the malicious encryption of its data?

What happens when backups are infected?

Everyone understands the vital importance of backing up data, but what happens when your backups include the malware you've just been infected with? Restoring from infected data will simply result in reinfection. Of course, you can - and should - run test recoveries for all backups, but that's a huge operational challenge. When systems are down and the clock is ticking, how quickly can you set up the infrastructure to run those tests - and how much will it cost you?

One of the reasons that many organisations have not yet solved the challenge of cyber-resilient backup is that infrastructure and security are handled by different teams, so it's not clear who's responsible. As a forward-thinking organisation, our customer united these teams to find a way to increase its ability to recover business-critical systems and data effectively following a potential cyber-attack.

And it's not just about customer service and revenues: as an operator of critical infrastructure, the company is subject to stringent government regulations around service continuity. And while it had deployed an advanced data storage and backup solution relatively recently, rapid advances in the incidence and sophistication of cyber-attacks meant that the customer felt it could do more to protect systems and data from external threats. Equally, it recognized that some cyber threats can come from inside the organisation.

Beyond the inconvenience of an interrupted supply to millions of their customers, an equally important issue is the financial impact of a potential breach. According to IBM's Cost of a Data Breach 2022 Report, the average post-ransomware remediation cost for a critical-infrastructure business is almost £4 million: around £800,000 greater than the average for other types of business.

Head of Technology at the utilities company says:

"The cyber threat is always evolving, and we take our responsibility as a critical-infrastructure business extremely seriously. We wanted to improve our cyber-resiliency with a solution that would integrate with our existing IBM Storage environment."

Supply of critical services to over

5 million

homes protected

Time to recover reduced by an estimated

300%

through pro-active recovery testing in the cloud

Gaining cyber-resilient backup capabilities

To achieve cyber-resilient backup and recovery, The customer chose the Predatar SaaS solution running on IBM Cloud to create and manage an offsite, airgapped third copy of backup data. The Predatar solution is integrated with the existing IBM Storage Protect environment, enabling the customer to continue driving value from its existing investment.

“The Predatar solution on IBM Cloud met all our requirements around encryption, airgapping, role-based access controls, and the ability to scan and remove viruses in an isolated environment. With Predatar, we are following best practice by having a different copy on different media in a different location, but also we benefit from ongoing malware scanning and recovery testing.”

Predatar uses built-in antivirus tools to scan backups for malware. Crucially, the solution tests any suspected anomalies in a sandbox environment, rather than simply rolling back to an early version of the backup. This means that - unlike some competing solutions - Predatar validates possible threats to avoid false positives and unnecessary disruption. In addition, thanks to the solution’s use of machine learning for anomaly detection, it can intelligently determine that some potential red flags are actually normal behaviour for your organisation.

“It’s still early days for us with Predatar, but what we’ve seen so far gives us great confidence that we’re better protected against the worst-case scenarios. In the coming months, we’ll be setting up different tiers of backups in Predatar so that we can prioritise recoveries according to the criticality of systems.”

Mitigating risk for critical systems

The Predatar solution provides an additional layer of protection to the customer, adding cyber-resilience to its existing backup and recovery capabilities. As a result, the company is more confident in the ability to recover systems and data quickly, reliably and cost-effectively from the third copy on IBM Cloud. The solution automatically performs test recoveries in isolated virtual environments based on a schedule set by the user. The organisation can also run ad hoc test recoveries.

“Predatar gives us additional peace of mind that we’re protected against serious impact from a malware infection. The solution increases the resilience of key systems and data, helping reduce the risk of a lengthy and difficult recovery in the event of a serious breach.”

Predatar automates many common backup administration tasks and cyber-resiliency processes, so the solution eases the strain on the internal team. The airgapped backups are protected by rigorous access controls that require senior approval from two managers for any changes.

“Predatar integrates fully with our existing IBM Storage Protect environment, which makes the solution easy to deploy and manage. Working with the team from Predatar has been a great experience, and the solution has delivered on our primary objective of reducing cyber risk around backup and recovery.”

Ultimately, the ability to recover faster and at lower cost to a known good copy of a system will reinforce the customer’s ability to provide uninterrupted supply to the households and businesses it serves - even in the event that the organisation suffers a cyber-attack.

Find out more about recovery assurance for your business. Visit www.predatar.com