E-GUIDE

Don’t fall victim to daylight data robbery

Keep sensitive police data secure and maintain public trust with NetApp, your protection partner.

NetApp

Overview

It's a sad fact that data breaches are becoming increasingly common, putting the personal information of thousands at risk each time. Because of this, privacy and data security policies are getting stricter, especially where the police force is concerned. Failure to stay on top of these can mean steep regulatory fines and PR challenges that damage public trust.

This explains why, as part of the National Policing Digital Strategy (sounds fancy), you're planning to define a secure-by-design model for IT infrastructure that aligns to security standards and better protects sensitive data—no matter where it's stored.

Challenge

299

The average number of data breaches per UK police station from 2016 to the end of April 2021

Source: Info-security Magazine, 2021

Given the nature of the job and the type of data it collects, it's easy to see why you'd be on high alert when trying to safeguard applications and information. A big chunk of the work you do is sensitive and needs guaranteed security and governance to protect it from breaches while remaining compliant with data regulations.

However, the data silos created within a traditional on-prem—or cloud—solution mean IT teams often end up managing and maintaining security and compliance in every single location, for every single application. No easy feat.

Having the right tools on hand is crucial for centralising your data protection approach, letting you cater for all eventualities and respond quickly. Access to our backup and disaster recovery tools will give you the ability to monitor data protection, privacy, and compliance, and develop incident-response procedures to smooth operations on prem and in the cloud. Sound good?

Solution

Back up your defences using robust protection

We know siloed data is a thorn in the side of solid data protection. Add to that the sensitivity of operational data sources like intelligence and evidence—that should only be accessed by certain people and can't be copied—and it can feel like a minefield.

At NetApp, we arm you with powerful data protection capabilities that work across any IT environment. Features like anomaly detection based on AI and a zero-trust framework enable you to analyse data patterns and identify threats in real time. Combined with our backup and restore capabilities, we can enable the availability and long-term archive of data, making sure it's protected against local, site-wide, and region-wide failures and attacks.

Always put compliance first

You need the right tools to be ready for Professional Standards Department and HMICFRS inquiries and audits. You also need to able to proactively clamp down on cybercriminals. That's where we come in. We help you analyse your data with ease—whether it's in the cloud, on prem, or both.

Use custom policies to build dashboard analytics, receive alerts if anything needs your attention, and identify and secure sensitive data. They can also help you automate data categorisation and reporting so you receive vital data health and protection reports in minutes. Together this provides you with a simple way to maintain governance and compliance across your hybrid cloud environments.

Want to keep sensitive data under lock and key?

Chat to us

NetApp

NA-808-0322