PURESTORAGE®

SOLUTION BRIEF

# Five Steps to Combat Ransomware in Healthcare

Safeguard patients, staff and your NHS Trust with modern data protection from Pure Storage®.

In 2020, at the height of the biggest healthcare crisis in living memory, ransomware attacks crippled hospitals and medical facilities across the world. In the UK, the National Cyber Security Centre (NCSC) responded to three times as many ransomware incidents than the previous year.

While these attacks are not new, around 40 NHS organisations and GP practices were hit by ransomware in 2017 including the wannacry attack, which left the NHS with a £73m IT bill! However, NCSC reports an increase in the scale and impact as attacks become ‘more targeted and more aggressive than ever before’.

Alongside the very real impact on patients – doctors unable to access patient records and test results, cancelled operations and departments forced to close – the financial costs of unlocking or decrypting data can be significant and pay outs only further encourage cyber criminals. Plus, should data be stolen, encrypted or deleted, Trusts face potential action by the UK’s Information Commissioner under GDPR regulation.

## IT Recovery Time Impacts Patient Care

When a ransomware attack disables a hospital’s patient record or other data systems, the disruption can be widespread. System downtime hinders clinical decision-making, creates the potential for medical errors and could even be a contributing cause to patient death.

Ransomware attacks on hospitals, clinics and GP surgeries not only impact patient databases, but also the backups used to recover from these breaches. As the sophistication of attacks increases, the NHS needs to address ransomware mitigation and recovery with a modern cyber protection strategy.

### Ransomware Recovery

Pure FlashBlade® with SafeMode™ Snapshots accelerates ransomware recovery by augmenting data protection strategies.

### Data Protection

Introduce your organisation to modern data protection and say goodbye to siloed legacy solutions.

### Backup and Restore

Pure’s modern architecture quickly backs up and restores data when it matters most.

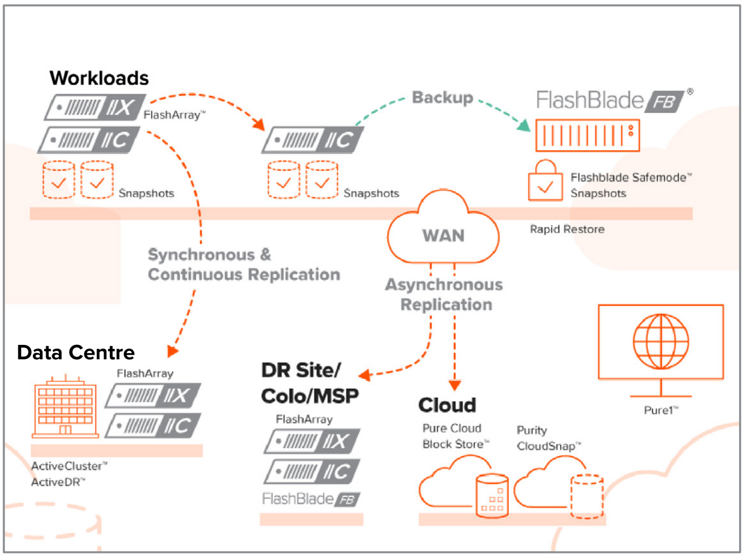
**Level-up Your Cyber Protection with a Five-Step Framework**

- Increase Visibility
- Ensure Control
- Reduce Exposure
- Increase Attack Costs
- Respond and Evolve

Here are five steps you can take to safeguard your data against attack, and how Pure can help:

**Step 1: Increase visibility.** This step is all about knowing what equipment you have and why. That server that no one knows about sitting in your basement just might be the most vulnerable link in your defence. Creating an inventory of assets and points of entry is vital, as is monitoring events on each asset to find anomalies that might indicate intrusion.

- The Pure1 Meta® analytics platform synthesises intelligence from thousands of devices.
- Combining Pure's FlashBlade® with Splunk or Elasticsearch creates a powerful data analytics and security platform.



**Step 2: Ensure control.** Put a virtual fence around your infrastructure to control access. The increase in distributed workforces and work-from-home policies requires a new approach to cyber protection. Pure built FlashArray™ from the ground up to run VDI faster and with greater density than any other product on the market.

**Step 3: Reduce exposure.** This step isn't just about detection. It's also about building an environment that is consistently maintained and monitored, which requires collecting vast amounts of data for complex analytics. That's why it's important to have infrastructure that's architected to provide fast results.

- Take the assessment to see if your organisation is prepared for the next ransomware attack.

**Step 4: Increase the costs of attacks.** Incorporating encryption makes it more difficult and costly for the attacker. At the 2019 RSA Conference, Pure Storage and Thales introduced Vormetric Transparent Encryption for Efficient Storage, the IT and security industries' first end-to-end data encryption framework that realises storage array data reduction. Pure's SafeMode snapshots provide resiliency with immutable backups, making it impossible for an attacker or rogue insider to delete backups, even if administrator credentials have been compromised. Also SafeMode snapshots provide protection to your data if an attack occurs.

**Step 5: Respond and evolve.** Your ability to respond, recover, and evolve as quickly as possible following an attack is critical. Pure FlashRecover™, Powered by Cohesity®, the industry's first jointly architected all-flash modern data-protection solution delivers accelerated backup and rapid recovery at scale.

- Purity ActiveDR™ provides powerful data replication capabilities to ensure quick backups, and FlashBlade delivers rapid restore capabilities of up to 270TB/hour.
- For MEDITECH users, Pure has partnered with BridgeHead Software, Amazon Web Services (AWS), and HealthcareTriangle to deliver backup as-a-service (BaaS), which automates creation, storage and replication of the MEDITECH backup to Pure Cloud Block Store™ in AWS.