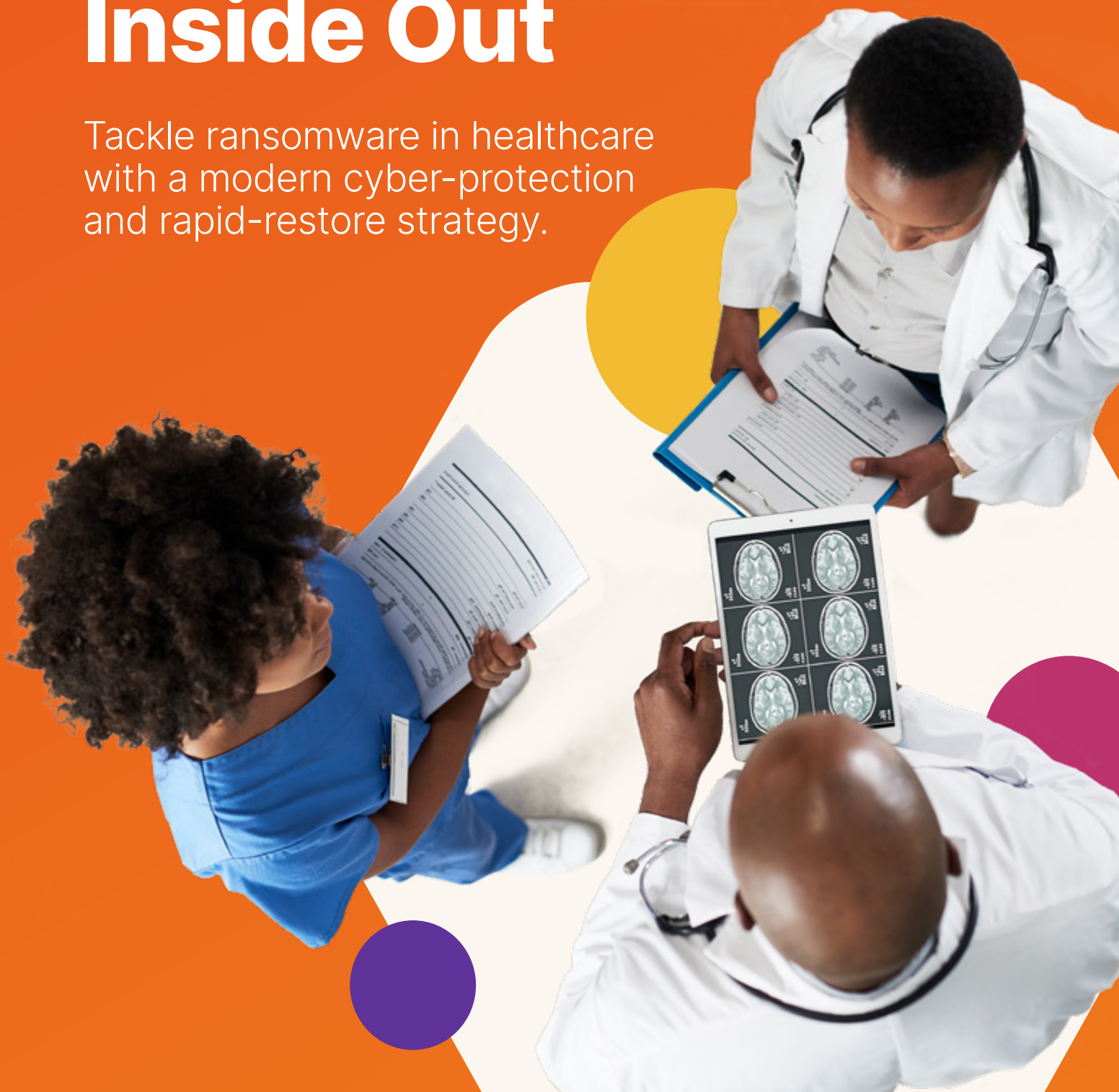
PURESTORAGE®

EBOOK

Safeguard Hospital Data from the Inside Out

Tackle ransomware in healthcare with a modern cyber-protection and rapid-restore strategy.



EBOOK

Contents

Ransomware Is a Global Problem

Hospitals and healthcare providers face very local implications of ransomware.

These sophisticated malware attacks encrypt organisations' files and systems, and then demand payment for restoring access to the data. There is no guarantee that the cyber criminals will honour their terms should the ransom be paid, and data can often be deleted and, increasingly, stolen.

This paper evaluates the latest threats to the healthcare sector and explores the importance of safeguarding data from the inside out – with a modern cyber protection and recovery strategy.

The Rise of Ransomware Attacks in Healthcare

In the UK, the National Cyber Security Centre (NCSC) responded to three times as many ransomware incidents than the previous year – reporting an increase in the scale and impact of attacks.

In November 2020, US federal agencies issued an alert warning of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers" coming in the midst of the biggest global health crisis in living memory, the inability to access patent records and test results, and the inevitable IT disruption would not only impede treatment, but carried a very real risk to life. Which, of course, is exactly why these cyber extortionists chose that moment to strike.

This wasn't an isolated alert. Reports suggest that security systems in some 59 US healthcare providers were successfully breached in 2020, impacting patient care in over 500 facilities. Neither are attacks limited to North America.

In one particularly tragic event linked to ransomware, the failure of IT systems at a hospital in Dusseldorf Germany caused the death of a critically ill patient after she had to be taken to another city for treatment.

With ransomware attacks increasing in both speed and sophistication, there is a clear imperative for healthcare providers and government agencies to continue to invest in sound prevention and recovery strategies.

Ransomware: **Fast Facts**

- **Cyber watchdog NCSC is warning of "more targeted and more aggressive attacks than ever"** [1]
- **Ransomware impacted operations in an estimated 510 US healthcare institutions in 2020** [2]
- **Ransomware attacks increased 40% to 199.7 million cases globally in Q3 2020** [3]
- **Cybersecurity experts predict one ransomware attack every 11 seconds in 2021** [4]
- **The global costs of recovery is predicted to exceed $20 billion by the end of 2021** [5]

[1] https://www.ncsc.gov.uk/news/annual-review-2020
[2] https://apnews.com/article/fbi-warns-ransomware-healthcare-system-548634f03e71a830811d291401651610
[3] https://www.kratikal.com/blog/ransomware-attacks-increase-to-40-in-q3-2020/
[4] https://safeatlast.co/blog/ransomware-statistics/
[5] https://safeatlast.co/blog/ransomware-statistics/

A Brief History of Ransomware: NHS

Ransomware attacks are nothing new. Healthcare Chief Information Security Officers (CISO) have been dealing with these potentially damaging events for upwards of a decade.

According to one report, 65 NHS Trusts have been victims of 'successful' ransomware breaches since 2014. The highest profile and most damaging was 2017's the WannaCry virus, believed to have impacted around 40 NHS organisations and GP practices.

Analysing the impact, a 2018 Department of Health and Social Care report estimated that during the attack, lost output cost the NHS £19 million. Adding the £72 million investment required to restore affected systems and data, the total cost of WannaCry on the NHS reached approximately £92 million.

Swift action was taken, however. And following investments in local infrastructure, a new national Cyber Security Operations Centre and additional spending of £210 million to 2021, the UK's healthcare system is significantly more robust and resilient.

But, while the number of ransomware attacks fell between 2018-19, a white paper presented to the House of Lords by Imperial College London highlighted remaining "weaknesses that compromise patient safety and the integrity of health systems". It seems that there is still work to be done.

The total cost of WannaCry on the NHS reached approximately **£92 million**

Widespread Impact on the Care System

When a ransomware attack disables a hospital's patient record, medical testing or other data systems, the disruption can be widespread.

System downtime not only hinders clinical decision-making and creates the potential for medical errors, it can result in cancelled operations and closed departments. With data from 2020 putting average IT system recovery time at 19 days (up 54% on the previous year), this can have a very significant impact on the hospital's ability to operate.

Alongside the very real impacts on patient care, the financial costs of unlocking or decrypting data can be significant. As we have seen earlier in the paper, the four-day WannaCry attack was hugely costly to the UK healthcare system. Plus, with eCrime groups increasingly stealing data (as well as encrypting and/or deleting it), European-based institutions face the potential of large fines under GDPR regulations.

It is also important to consider the intangible costs of a successful breach. A study of attacks by Deloitte modelled a major data breach for a U.S. health insurer. It found over 96% of the financial impact was felt "beneath the surface" – in terms of the value of lost contract revenue, brand and reputational damage, and the lost value of customer relationships. While these impacts will be more marked for private sector healthcare providers, these reputational and revenue issues may have an impact on national schemes like the UK's NHS where clinical commissioning groups (CCGs) manage and fund primary care.

Develop a Modern Cyberprotection Strategy

Staying ahead of today's known (and unknown) exploits requires a multiplicity of approaches – from advanced endpoint protection and maintaining up-to-date operating systems through to investing in information security training, network audits and vulnerability testing.

It's also critical—because the biggest threat and weakest link is often people—to control access to secure files through data classification, admin rights and privilege management.

Perhaps more than anything else, because ransomware targets data, it's absolutely critical that significant focus is placed on developing strategies that protect hospital databases and backup environments.

The challenge here is that data protection is one of the most complex areas of IT infrastructure. Data has to be quickly copied from multiple sources and quickly secured for restore in the event of a ransomware attack. But it's not easy.

Traditional techniques such as making redundant copies, physical separation, replication, high-availability between sites and so on work well for things like flood or fire, or in the event of human error. But they're not particularly effective in a ransomware scenario. Administrators don't want to be copying compromised data, for example. Nor can organisations rely on backup copies of data because eCrime groups target these systems for encryption too.

There is another,simpler and more comprehensive approach to data **protection and recovery**

Put Your Data in Safe Mode

The key to effectively protecting hospital data is to bring all the disparate silos (data lakes, backup appliances, etc.) together in one place, then create a read only snapshot of the data.

These are then placed into a safe mode so they can't be eradicated (deleted), modified or encrypted by any ransomware.

In practice, this is an automated process and independent of administrator control – which also means the snapshots can't be deleted by accident or by rogue employees.

There's a lot of artificial intelligence, analytics and testing involved in this approach. However, because it's highly automated, it vastly simplifies the process and requires very limited human involvement.

To boost security further, this model requires an authorised individual to work directly with the technology provider to reconfigure the snapshots, make policy modifications and/or manually delete them.

It essentially adds another checkpoint. Not only can the malware not encrypt or delete the snapshots, the IT team can't do so either (without support).

So, by continually creating an unencryptable copy of all the organisation's data, should ransomware make it past the hospital's perimeter defences, the snapshots are safe and can be swiftly recovered – to give clinicians the ability to maintain uninterrupted service delivery.

A recent Forrester study confirms over half of hospital decision-makers recognise that their current approaches of weekly or monthly cloud-based or physical backups are inadequate to meet today's challenges, and are looking to invest in real time backup solutions such as the approach described above. Doing so, they believe, will allow them to focus on caring for patients.

Read our latest blog post on how hospitals can eliminate backup and restore hassles, **recover from ransomware more quickly**, and strengthen their data protection strategy.

Read Now.

About PURESTORAGE®

Pure is Redefining the Storage Experience

We're empowering innovators by simplifying how people consume, interact with, and protect data.

This goal has pioneered the development of the snapshot approach with Pure Storage SafeMode™ snapshots—available with FlashBlade® and FlashArray™ products—to provide the immutability that protects data backups from ransomware attacks.

Enhancing protection and reducing complexity for hospitals and healthcare providers, its solutions are fully customisable and easy to deploy, and expand and upgrade without disruption – integrating with existing backup software. Ransomware also uniquely challenges backup systems to potentially recover massive amounts of data. Crucially, Pure's all-flash solutions are lightening quick, and deliver up to 270TB/hour data-recovery performance.

Find out more about healthcare solutions from Pure.
Or contact hmachen@purestorage.com

Is Your Hospital Prepared for a Ransomware Attack?

The rising sophistication and impact of ransomware is putting healthcare organisations under threat. **Are you prepared?** Find out with this three-minute assessment.

Take the Assessment

Safeguard Hospital Data from the Inside Out

EMEA HQ & UK Office
3 Lotus Park
The Causeway
Staines-upon-Thames
Surrey
TW18 3AG

PS2042-01 03/2021
eb-ransomware-healthcare-uk