

EBOOK

Safeguarding Enterprise Data from the Inside Out

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



Contents

Introduction

Ransomware is a Global Problem.....3

Ransomware

The Rise of Ransomware Attacks4

A Brief History of Ransomware5

The Real-World Impact of an Attack.....6

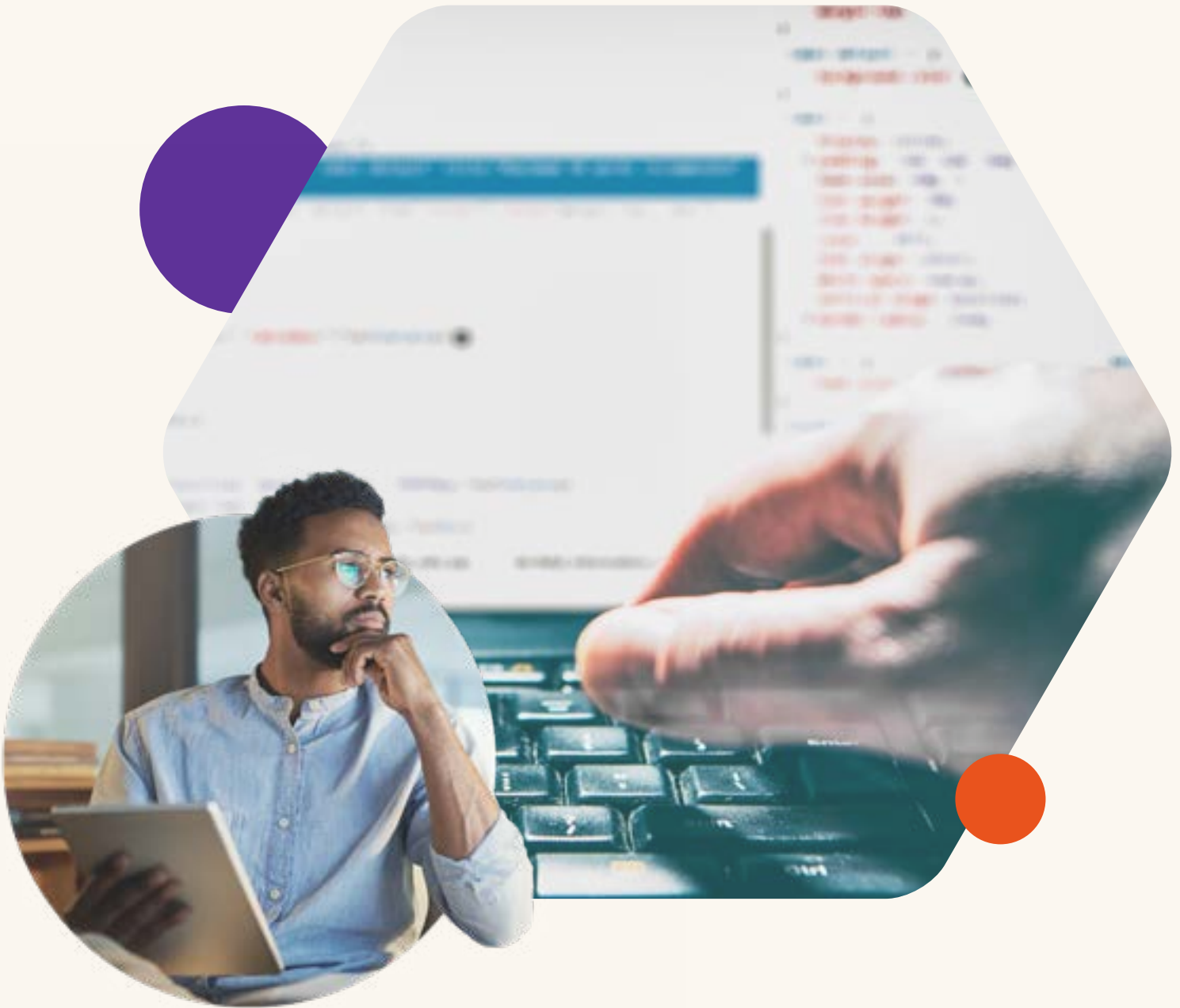
Protection

Develop a Modern Cyberprotection Strategy.....7

Putting Your Data in Safe Mode.....8

About Pure Storage.....9





Ransomware is a Global Problem

With very local implications for organisations across the sector spectrum

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 facing organisations and explores the importance of safeguarding data from the inside out – with a modern cyber protection and recovery strategy.

The Rise of Ransomware Attacks

With the UK's National Cyber Security Centre (NCSC) reporting an increase in the [scale and impact of ransomware attacks](#), the threat to UK businesses is significant and growing.



Last year, the cyber watchdog responded to three times as many ransomware incidents than the previous year. With experts predicting a new ransomware attack on businesses every 11 seconds by the end of 2021¹, this is a significant and growing problem.

While the bulk of ransomware attacks have historically targeted individuals and demanded relatively small payments to unlock devices, attacks are now becoming more focused and more expensive.

Recent figures point to a 100% increase in ransomware demands on small to medium sized businesses², with losses ranging from a few thousand to over £1 million. According to the Coveware Quarterly Ransomware Report Q4 2020, of those firms choosing to pay to get their data unlocked, the average cost was approximately £111,580.

While it may be deemed the lesser of two evils, paying the ransom only encourages eCriminals. The NCSC has seen evidence of [multiple attacks](#) against UK businesses that have paid the ransom.

While the costs of attack may be covered by a company's cyber insurance policy (should they have one), the average IT downtime and the corresponding impact to operations will be hugely disruptive for any organisation.

With ransomware attacks increasing in both speed and sophistication, there is a clear imperative for businesses of all sizes to continue to invest in sound prevention and recovery strategies.

Ransomware: Fast Facts

- Ransomware attacks increased 40% to 199.7 million cases globally in Q3 2020³
- The cyber watchdog NCSC is warning of "more targeted and more aggressive attacks than ever"⁴
- Cybersecurity experts predict one ransomware attack every 11 seconds in 2021⁵
- The global costs of recovery is predicted to exceed \$20 billion by the end of 2021⁶

¹ <https://sensorstechforum.com/ransomware-hit-businesses-11-seconds-2021/>

² <https://www.securitymagazine.com/articles/93609-average-ransomware-demand-increases-100-from-2019-through-q1-2020>

³ <https://www.kratikal.com/blog/ransomware-attacks-increase-to-40-in-q3-2020/>

⁴ <https://www.ncsc.gov.uk/news/annual-review-2020>

⁵ <https://safeatlast.co/blog/ransomware-statistics/>

⁶ <https://safeatlast.co/blog/ransomware-statistics/>

A Brief History of Ransomware

Ransomware attacks are nothing new. The first attacks appeared in the late 1980s. But it wasn't until the early 2010s that attacks began to gather pace against both individuals and organisations.

This also coincided with the development of the Bitcoin cyber currency which made (and continues to make) tracking and recovering payments virtually impossible.

In 2016, a report from security firm Kaspersky estimated that attacks on businesses increased three-fold over the year. More damaging still, of the businesses that did pay the ransom, one in five didn't get their data back.

In 2017 ransomware hit national headlines with the WannaCry virus that infected and encrypted over 230,000 devices and systems in more than 150 countries.

Businesses, healthcare systems and critical national infrastructure utilities were attacked. In the UK, the malware was believed to have impacted around 40 NHS organisations and GP practices, with a total cost of around £92 million according to a 2018 Department of Health and Social Care [report](#).

This, and the similarly virulent NotPetya attack, heralded a potentially lethal change in approach, with attacks originated by state sponsored eCrime groups that appeared to focus on creating maximum disruption rather than financial gain.

Coming right up-to-date, ransomware techniques and approaches have evolved again. In 2020, cybercriminal group Ragnar Locker Team launched a series of Facebook advertisements to put pressure on companies to pay up. These ads threatened to make confidential information public if ransoms were not paid. While this so-called double extortion method is not unusual, the use of social media channels is new.

In the future attacks are expected to grow in sophistication and impact. Cybersecurity Ventures estimates that the cost of cybercrime will increase by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025.

While the stats vary, one thing is clear: a single perimeter security policy will not be sufficient to protect sensitive data and organisations would be wise to employ multiple security strategies to defend in depth.

WannaCry virus infected and encrypted over **230,000 devices** and systems in more than 150 countries

The Real-World Impact of an Attack

When a ransomware attack disables an organisation's corporate, customer or other data systems, the disruption can be widespread — ranging from the need to take industrial or e-commerce platforms offline through to the permanent loss (or theft) of sensitive or proprietary data.

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 businesses ability to operate.

Alongside the very real impacts on business operations, the financial costs of unlocking or decrypting data can be significant. With eCrime groups increasingly stealing data (as well as encrypting and/or deleting it), European-based organisations also 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 on a U.S. financial services firm. It found over 96% of the financial impact was felt "beneath the surface" – in terms of the value of lost contract revenue, damage to their reputation and the lost value of customer relationships.



Develop a Modern Cyberprotection Strategy

Staying ahead of today's known and unknown exploits requires a variety 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 a significant focus is placed on developing strategies that protect the businesses databases and backup environments. Millions may be spent annually to guard entry points to data, but there remains a critical need to defend in depth and develop multi-layered security strategies.

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, maintaining high availability between sites and so on works 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 data is to bring all the disparate silos (data lakes, backup appliances, etc.) together in one place and then create a read only snapshot of the data.


These are then placed into a safe mode so they can't be 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, neither can the IT team (without support).

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



To read our latest blog post on how businesses 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 small and medium sized enterprises, 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 our [ransomware solutions](#) or contact your Pure Storage team on **020 3870 2633** or [email](#) us.

Are You Prepared for a Ransomware Attack?

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



[Take the Assessment](#)



Safeguarding enterprise data from the inside out

EMEA HQ & UK Office

3 Lotus Park
The Causeway
Staines-upon-Thames
Surrey
TW18 3AG

PS2043-01 03/2021
eb-ransomware-uk