XMA

PURESTORAGE®

# Understanding Ransomware Recovery with Pure Storage

PURESTORAGE®

# What is Ransomware?

Ransomware is malicious code that infiltrates your systems, encrypts your valuable data, and holds it hostage. To regain access, you're forced to pay a ransom, often in cryptocurrency, where your money disappears into the untraceable dark web. This digital extortion can cost millions in downtime, lost productivity, and potential reputational damage.

A major concern is how planned in advance these attacks may be. When you restore your data, how do you know it's clean? You might receive notification of an attack today, but the breach could have been over 100 days ago. Even if you recover your data, is the breach still there? How far back do you go?

After the initial attack, it can be a slow road to recovery. You need to consider your Recovery Time Objective (RTO). How is your data stored? Recovery takes time, and if you're having to dredge up petabytes of data from your backups, it could take days, months, or even weeks before it's back to business as usual. But by that point, it's not really business as usual, is it? You'll have been delivered a haunting experience that may very well collapse the future of your organisation.

The question is not **IF** you'll be attacked, but **WHEN**.

# Ransomware is on the rise...

In 2022, malware experienced a significant resurgence, with a staggering

**2.8 billion attacks**[1]

and over 270,000[2] new variants identified.

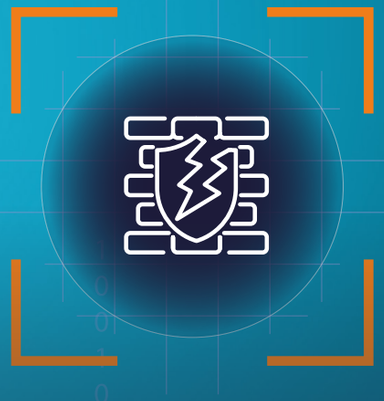
This trend continued into 2023, with threat actors deploying an average of

**11.5 attacks per minute**[3],

including 1.7[4] novel malware samples.

In 2022, **92%** of organisations affected by ransomware did not have effective data loss prevention measures in place, resulting in

**critical data loss**[5].



This highlights the need for robust security protocols and the importance of ethical hacking, which uncovered over **65,000 vulnerabilities** in the same year[6].

The human element remains a significant factor, with

**82% of data breaches**

attributed to

**human error**,

particularly through phishing attacks and stolen credentials[7].

[1]mid-year-update-2022-sonicwall-cyber-threat-report.pdf [2]https://www.sonicwall.com/2022-cyber-threat-report/?elqCampaignId=15400&sfc=7015d000002k7FCAAY
[3]BlackBerry Quarterly Global Threat Report — June 2024 [4]BlackBerry Quarterly Global Threat Report — August [5]Cyber Attack Statistics (Updated August 2024) – Parachute
[6]https://www.hackerone.com/reports/6th-annual-hacker-powered-security-report [7]DBIR Report 2024 - Summary of Findings | Verizon

# Timeline of a ransomware attack

**Ransomware can remain undetected on your network for years at a time collecting data**

**Notified of Breach**

**Ransomware can take days, weeks, or even months to recover from.**

| Delivery | Command and control | Credential access | Canvas | Extortion | Immediate action | Investigation | Containment and Remediation | Post-Incident Activity |
|---|---|---|---|---|---|---|---|---|
| The network is compromised through a phishing email, exploit, or worm. | The ransomware establishes a link with the attacker's server to receive instructions. | The malware remains hidden, stealing credentials and gaining wider access across the network | The virus locates files to encrypt, both on the infected device and any connected networks | Cybercriminals exfiltrate and/or encrypt files, then demand payment for their decryption | **Isolate:** Disconnect compromised servers from the network to prevent further spread.<br>**Report:** Notify relevant legal authorities and stakeholders of the security incident instructions. | **Identify:** Determine the nature of the intrusion (e.g., ransomware, data breach).<br>**Analyse:** Assess the extent of the compromise, including impacted systems and data.<br>**Forensics:** Conduct a thorough forensic analysis to identify the entry point(s) and attack vectors. | **Remove Malware:** Safely eradicate any malicious code or software from affected systems.<br>**Data Analysis:** Examine compromised data to understand the sensitivity and potential misuse.<br>**Restore:** Recover data from the most recent clean backup to minimise data loss.<br>**Patch Vulnerabilities:** Address identified security weaknesses to prevent future intrusions. | **Lessons Learned:** Conduct a comprehensive review of the incident to identify areas for improvement.<br>**Enhance Security:** Strengthen overall security posture by implementing additional controls, employee training, and updated policies. |

# The Pure Storage Advantage

## Step-by-Step Recovery with Pure Storage

While preventing ransomware is the ideal scenario, Pure Storage offers a powerful defence strategy for when the worst happens. Their innovative solutions are designed to minimise the impact of an attack and accelerate recovery.

1

### Detection and Isolation

Pure1®, Pure Storage's AI-driven management platform, acts as an early warning system. It detects unusual file activity, signalling a potential ransomware attack. Rapid isolation of affected systems contains the damage. Pure Storage is constantly monitoring and analysing your data, allowing to pinpoint the exact moment of an attack. This alleviates fears of a breach being hidden in your data, waiting for months before enacting a heist.

2

### SafeMode Snapshots

Pure Storage's SafeMode snapshots are your digital safety net. These immutable copies of your data are immune to encryption or deletion, even by attackers with administrator privileges. They provide a secure, verified starting point for recovery. It’s a fallback for when the worst happens, and an immutable picture of your data before an attack.

3

### Rapid Data Recovery with FlashBlade®

Time is of the essence after a ransomware attack. FlashBlade, Pure Storage's high-performance storage platform, empowers you with Rapid Restore. This feature allows you to recover petabytes of data in mere hours, not days or weeks, minimising downtime. Best of all, you can assign FlashBlade to different sets of data that hold different levels of importance to your organisation. By giving you different levels of recovery time, you can still achieve lightning-fast recovery of your critical data whilst staying within your budget.

4

### Continuous Data Protection (CDP):

Pure Storage goes beyond recovery. With Continuous Data Protection, you create near-instantaneous recovery points, minimising data loss and ensuring your business operations continue with minimal disruption.

# XMA: Your Pure Storage Partner

The cyber threat landscape is ever-changing, but Pure Storage is committed to staying ahead of the curve. Their solutions continually evolve to combat the latest ransomware variants and other cyber threats. By partnering with Pure Storage, XMA delivers the perfect storage solution for you. We work with best-in-class cyber-resilience vendors such as Commvault, Druva, Veeam, and Rubrik, ensuring that you're protected on all fronts, building a pro-active and reactive fortress of defence for your data.

We understand that every organisation has unique needs, and our team of experts is dedicated to helping you assess, design, and deploy a Pure Storage solution tailored to your specific requirements. From initial consultation to ongoing support, we're with you every step of the way.

**Ready to fortify your digital defences? Contact XMA today for a free consultation and discover how Pure Storage can safeguard your valuable data.**

Find out more