Hewlett Packard
Enterprise

7 tips to defend against ransomware attacks

The business of ransomware is booming, and potential damages are growing

With new strains of ransomware and malware threats on the rise and data continuing to grow from edge to the cloud, your enterprise and customer data are more at risk than ever. Although many data protection solutions in the market promise to address the growing demand for cyber resilience, most of them provide only partial protection.

The cost of recovery and the resulting downtime in the aftermath of a ransomware attack, as well as the reputational damage:

59% of organizations were hit by ransomware in the last year[1]

→

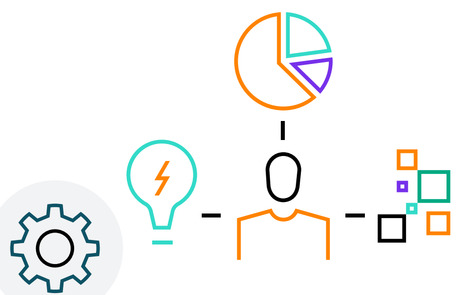
$2.73 million average recovery cost (excluding ransom payment)[2]

→

94% of victims said attackers targeted their backups[3]

It's time to defend your organization against ransomware and modernizing data protection is crucial to ensure business continuity.

Make your data ransomware-proof



1 Use backup and disaster recovery solutions

Ransomware is a disaster scenario; therefore, organizations must also include disaster recovery (DR) along with backup solutions. HPE enables granular recovery checkpoints and the ability to recover entire sites or applications within a few clicks.

2 Enhancing cyber resilience

Deploy a solution that enables secure data protection operations as often as the business requires. Modern solutions offer near-continuous data protection, longer retention periods, and faster recovery time.

3 Rapid recovery

Deploy a solution that provides rapid recovery from ransomware attacks. Hewlett Packard Enterprise helps customers to detect ransomware attacks in seconds and recover in minutes, at scale, to a state, seconds before an attack.

4 Immutable copies

Cybercriminals will attempt to encrypt, modify, or delete your data to force a ransom payment. Immutable copies cannot be altered, keeping your data safe from ransomware.

5 Air-gapped and isolated

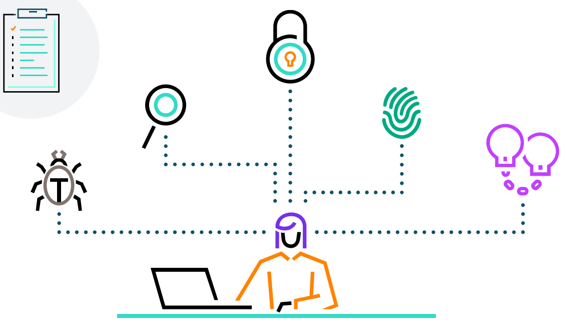
Air-gapped data protection solutions such as tape storage isolate backup data from your infrastructure to prevent ransomware from exploiting the security vulnerabilities of the local environment. HPE also offers an all-in-one Vault solution which is physically air-gapped and stores immutable data copies on secure, high performance, FIPS validated hardware delivering rapid air gapped recovery.

6 Multilayered data protection

One of the timeless data protection rules that can effectively neutralize ransomware threats is by creating an impenetrable multilayered data protection across the edge to the cloud commonly called the 3-2-1-1 rule.

7 Test to ensure recovery

Mimic actual disaster and recovery scenarios to ensure that administrators are following protocols and documentation, especially during ransomware recovery simulations.



Protect your data wherever it lives

By implementing these steps, you can start protecting your organization's data against damaging ransomware attacks. You are in control of the data, and you are no longer vulnerable to the hacker's demands. HPE solutions are secure by design, enabling rapid recovery and helping you to modernize your data protection edge to the cloud to secure your data from ransomware attacks.

Don't wait. HPE keeps your data safe wherever it lives.

[1, 2, 3] "The 2024 ransomware experience," Sophos, 2024

Learn more at

HPE.com/storage/dataprotection

Chat now (sales)