Backups are a Top Attack Vector

Learn why backups should be a part of your organization's cyber resiliency plan.

Cyberattacks target your operations and data, as cybercriminals are constantly attempting to encrypt and/or exfiltrate your data for a ransom. They not only target your production environments, they also target your backups

Plan Ahead. Protect Your Data.

Natural Disasters

Cyberattacks

Human Error

Backups Must Be Protected

75% of organizations suffer from cyberattacks

96% of cyberattacks target backups

Backups are a critical part of any incident response plan, making them a valuable target for threat actors. Don't leave backups unprotected — take steps in ensuring your survival.

Business Cost

68% of financial impact is attributed to cost other than the ransom payment

Operations and sales losses are larger than the ransom payment. While even paying the ransom does not guarantee you'll bounce back.

Protect your data and your backups. Avoid the overall cost for the business.

Business Continuity

43% of affected data is not recovered from a ransom encryption

Business-critical data, including sensitive legal and customer data, can all be encrypted and lost.

Secure business-critical information. Meet compliance requirements.

Optimization

63% of organizations want more collaboration between backup and security teams

Their most common solution? Integrate backup and cybersecurity tools.

Optimize teams. Reduce recovery costs.

Trust & Reputation

96% of organizations prioritize clean, recoverable data

Recoverable data matters — so that you can be depended on by those who matter most.

Maintain customer trust. Uphold business reputation.

Veeam believes in a Zero Trust approach that closes security gaps using the 3-2-1-1-0 rule

Backups alone are no longer sufficient. As cybercriminals increasingly target backups, organizations must adopt a new approach to data protection. Teams that have faced ransomware attacks understand the unique challenges of recovery, necessitating a comprehensive strategy that encompasses people, processes, and technology. This is the essence of a data resiliency strategy — ensuring data is always available and ready when needed.

- **3** Different copies
- **2** Different media
- **1** Offsite copy
- \+
- **1** Offline air-gapped or immutable
- **0** No errors after backup recoverability verification

Put yourself in a position to not just bounce back from a cyberattack, but bounce forward

Ransomware attacks will happen — regardless of prevention technologies or employee awareness training. The time is now. Stay ahead of threats, protect your data, and maintain continuous operations. Integrate IT and security teams, form a strong incident response plan, and ensure your backups are clean and reliable.

Learn more with our resources below:

Zero Trust Data Resilience Strategies

Up-level your knowledge for better data protection.

2024 Ransomware Trends Report

Lessons learned from 2,500 cyberattacks globally.

Ransomware Recovery Maturity Assessment

How do you stack up against best practices?