Ransomware: The moment of truth for data protection.

A ransomware attack is a classic ticking-clock scenario. It has already struck companies of all sizes across industries around the world. Yours could be next. Are you ready?

Learn how to protect against ransomware and mitigate risk

A successful ransomware strategy includes both reducing the risk of a successful attack and lessening the impact of an attack that does succeed. There are five things you need to do:

Create a plan

An effective plan is the foundation for a full and speedy resumption of normal operations.

Prevent attacks

Preventative steps include foundation hardening, application hardening, and ransomware protection.

Monitor your environment

Constantly be on the lookout for any anomaly, detecting the attack as quickly as possible to reduce its impact.

Restore your data

Perform fast restores with an intact data copy to quickly resume normal business operations and reduce the ransomware impact.

Test your plan

Perform frequent tests to verify you can meet your defined SLAs for high-priority data and applications.

Commvault data protection and recovery can be a valuable part of your anti-ransomware strategy. In fact, EIC value survey statistics1 illustrate the difference Commvault makes for customers:

- up to 49% improvement in average recovery time for messages, files, and VMs as well as Exchange, Oracle, SharePoint, and SQL applications.
- up to 392% improvement in data coverage for protection, analytics, encryption, and reporting.
- up to 61% reduction in annual exposure to compliance failures, audit failures, and/or data theft or breach.

Hear from our customers

Every day, across industries, companies are using our tools to protect their data and keep their business running. Learn how Commvault could work for you by watching these success stories:

When ransomware hit the City of Sparks, Nevada, police department shared files were locked. City employees could not access the geographic information system. With Commvault backup and recovery, the municipal government was able to complete data recovery from the ransomware attack in just 12 hours.

Watch the video >

Don’t let ransomware make your organization a victim. The five steps outlined here can help you maintain a constant state of recovery readiness. By keeping your backups safe and ready for rapid restoration, you can save time and keep your business out of harm’s way — and out of the news.

2 Gartner, “Avoid Ransomware Disasters with a Better Backup and Recovery Strategy, Published: 22 July 2019, ID G000392054
3 Quantifying the Business Value of Commvault Software, IDC 2018, US40773815