COMMVAULT

WHITE PAPER

Ransomware Protection: Last Line of Defense, First Step in Data Recovery

Ransomware — the moment of truth

A ransomware attack is a classic ticking-clock scenario. First, critical business data is suddenly taken hostage. Next, hackers use advanced encryption to render it inaccessible – and they demand exorbitant amounts of money to decrypt it.

How will you respond should you face this increasingly common scenario? Can you ensure the safety of your data if you refuse to pay – or even if you do? Do you have a ransomware mitigation plan? If not, your organization could remain paralyzed as you consider your options. Every passing minute increases the pressure to make the right choice as the costs of operational disruption add up. Tick. Tick. Tick.

Ransomware has already struck companies of **all sizes** across industries worldwide. Some were woefully unprepared, while others averted potential catastrophe with confidence. **Ask yourself one career-defining question:**

In this guide, we'll explore the ever-evolving threat of ransomware – and what you can do about it. First, we'll examine ransomware as one of the many **threats to recovery readiness** facing today's organizations. We'll then drill deeper into the nature and potential impact of this **insidious form of attack**. Next, pivoting from awareness to empowerment, we'll explore risk management elements, including planning, protection, monitoring, fast restores, and testing. Finally, you'll learn how recovery readiness can keep you from becoming a victim by providing a critical **last line of defense** against ransomware. Through Commvault Complete™ Data Protection, you'll gain a consistent framework to customize disaster recovery plans to your specific needs.

Your stand against ransomware begins now. Read on.

Threats to recovery readiness

Recovery readiness means being prepared to restore your organization's data and applications quickly, no matter what happens, and adhering to Zero Trust principles helps reinforce best practices for multilayered security. In today's diverse IT environment, that's a significant challenge. But first, you need to understand threats to backup data, which may come in many forms, both inside and outside the company.

Internal threats

People often think of a "threat" as intentional, malicious, and external. However, internal threats to an organization are common and dangerous. Research suggests that insiders are responsible for around 22% of security incidents, costing organizations millions and leading to breaches that expose sensitive customer, client, and company data[1]

While some internal threats are intentional, many are accidental. For example, an employee with legitimate access might simply click the wrong button, leave data exposed, delete the wrong entity, and do untold damage to the organization. Human error is the leading cause of serious insider data breaches, with 84% of organizations experiencing a security incident caused by mistake[2] People are human; stuff happens.

1 Tessian, Maddie Rosenthal, quoting the Verizon 2021 Data Breach Investigations Report in Insider Threat Statistics You Should Know: Updated 2022, June 2021
2 ContinuityCentral.com, Insider cyber incidents: human error is the top cause of serious data breaches, July 2021

External threats

External malicious actors are, in simple terms, bad guys. They're hackers or other individuals seeking to infiltrate your organization for their selfish purposes. Making money is a substantial motivating factor for malicious actors. Cyberattackers often pressure organizations for cash by threatening to publish the sensitive data information they have hijacked, known as double extortion.[3] It's also not unusual for bad actors to take their cyberattacks one step further by demanding ransom from third-party victims, such as company clients, external colleagues, and service providers – a tactic known as triple extortion.[4] Malicious actors may also be motivated by political or competitive reasons, with a goal to delete data, leak data, or disrupt business services.

Whatever their intention, they have a variety of techniques to choose from. Password spraying is a popular one that they use to gain unauthorized access to an organization or system. Another is finding a vulnerability to exploit, then injecting botnets and rootkits to steal data, delete it, or disrupt an organization's ability to function.

That's where ransomware comes in. In a typical attack, the hacker uses malware, often delivered via an infected attachment or link in an email, to encrypt your data. The hacker then demands payment — or you'll never see your data again. Without an effective recovery readiness strategy, your only option is to pay up and hope the attacker shows mercy by releasing your data.

The high cost and rising threat of ransomware

There's a reason ransomware makes the headlines. It's the kind of attack that gets your attention — sudden, brutal, and potentially devastating. In recent years, the rapid rise of ransomware has cast a shadow of anxiety across organizations.

Alarmed business, IT, and security leaders aren't just being paranoid. In a Proofpoint survey, 64% of CISOs feel at risk of suffering a cyberattack in the next 12 months. 20% rate the risk as very high.[5]

And the impact can be devastating:

- Colonial Pipeline, a major American oil pipeline system, suffered a ransomware cyberattack and halted all pipeline operations to contain the attack. Overseen by the FBI, the company paid the amount asked by the hacker group (75 bitcoin or $4.4 million) within several hours. Upon receiving the ransom, the perpetrator provided an IT tool to restore the disabled system. However, the tool had a very long processing time to help get the system backup.[6]
- JBS, the world's largest meat processor, experienced a cyberattack that stopped operations, including meat-packing plants in the U.S., Australia, and Canada. They paid an $11 million (£7.8m) ransom, hoping the payment would head off any further complications, including data theft.[7]
- Brenntag, a global chemical distribution company, fell victim to a ransomware attack in which attackers stole 150GB of sensitive data, including customers' social security numbers, driver's license numbers, and some medical information. The company paid attackers a $4.4 million ransom to receive a decryptor and prevent the attackers from leaking stolen data.[8]

Here are some general considerations:

- The average cost of downtime for large enterprises is more than $11,600 per minute.[9]
- IT workers believe ransomware is as serious as terrorism.[10]
- Cybersecurity Ventures predicts ransomware will cost $10.5 trillion annually by 2025. This is exponentially larger than the damage inflicted by natural disasters in a year.
- It is estimated that an organization suffers a ransomware attack every 11 seconds, and that there will be a new attack on a consumer or business every two seconds by 2031.[11]
- Over 350,000 new cases of malware were discovered every day last year.[12]

3 Venafi, Brooke Crothers, Venafi Survey: Ransomware Evolves—Double and Triple Extortion Now Features in Over 80% of Ransom Demands; February 23, 2022
4 Checkpoint Research, The New Ransomware Threat: Triple Extortion, May 2021
5 Proofpoint, Voice of the CISO 2021 Report, May 12, 2021
6 Bloomberg.com, Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom, May 2021
7 The Guardian for 200 Years, World's biggest meat producer JBS pays $11m cybercrime ransom, June 2021
8 Bleeping Computer, Sergiu Gatlan, US chemical distributor shares info on DarkSide ransomware data theft, July 2021
9 Web tribunal, Branko K., 15+ Scary Data Loss Statistics to Keep in Mind in 2022, March 2022
10 TecRadar Pro, Anthony Spadafora, IT Workers Believe Ransomware is as Serious as Terrorism, January 2022
11 Cyber Magazine, Steve Morgan, 2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics, January 2022
12 Cobalt, Mary Elliott, Top Cybersecuity Statistics for 2022, February 2022

Fighting back

Common countermeasures to ransomware include antivirus, antimalware, and firewall blockers. These are undoubtedly necessary, but they're not enough to keep you safe. The majority of victims already had these solutions in place. That means your ransomware strategy must reduce attack risks while also seeking to mitigate the impact of an attack. Unfortunately, it's all too likely that one will succeed eventually — so you need to be ready.

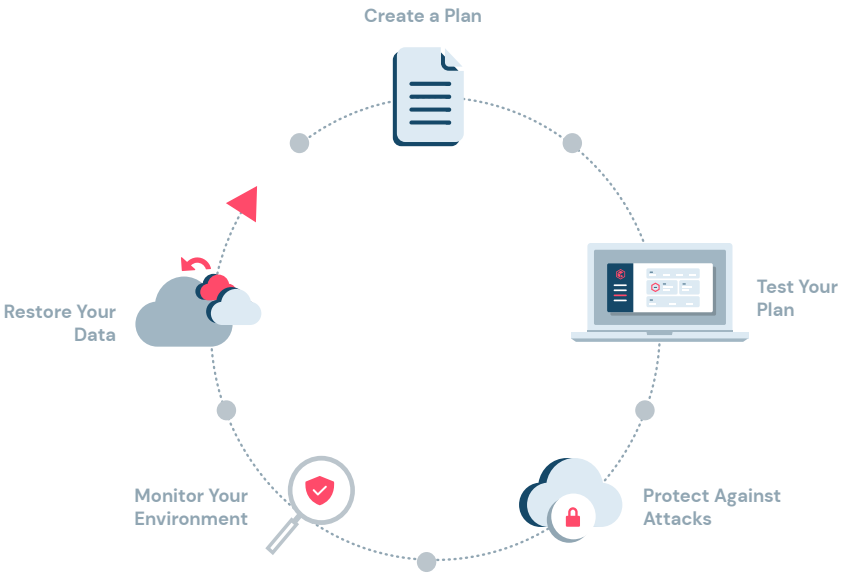
5 Lessons Learned from Ransomware Attacks **Read >**

Learn how to protect against ransomware and manage risk

A complete ransomware strategy includes reducing the risk of a successful attack and lessening the impact of one. You need to do five things: plan, test, protect, monitor, and restore (quickly).

1 Create a Plan

An ongoing attack is no time for improvisation or ad hoc measures. An effective plan is a foundation for a full and speedy resumption of normal operations. Like any disaster recovery plan, an anti-ransomware plan's essential considerations are what, when, and who.



- **What** – Identify and prioritize critical applications to focus on the systems and data you'll need to recover first.
- **When** – Define the Recovery Point Objectives (RPO), Recovery Time Objectives (RTO), and Service Level Agreements (SLAs) for your systems, data, and applications. How soon is soon enough to recover? How far back do you need the restore to go? You can then perform an internal assessment and identify existing gaps in your recovery capabilities based on these metrics. Are there systems or data you're currently unable to recover effectively within the specified parameters? Determining this will help you understand whether you're adequately prepared for a ransomware attack or if there's more work you need to do.
- **Who** – Which players – internal and external – will be involved in your data recovery efforts? How will they be notified? What conditions will trigger an escalation, and to whom? Key participants should include internal IT and line-of-business personnel as well as external suppliers and vendors with relevant roles to play.

You should also decide whether to leverage third-party recovery-readiness expertise and resources as you make your plan. An expert partner can provide recovery-readiness assessment services through implementation, monitoring, management, and response.

Disaster Recovery Solutions **Read >**

2 Test Your Plan

Once you have your plan in place, along with the procedures and technologies to execute it, make sure it will work as needed. Perform frequent tests to verify that you can meet your defined SLAs for critical and high-priority data and applications. Your system should be able to report on metrics such as RPO, actual recovery point, RTO, and estimated recovery time for each of your protected systems. As you identify gaps in your readiness, incorporate the appropriate adjustments into your plan for improvement. For a practical and sustainable testing strategy, you should be able to test your recovery capabilities in real time without impacting staff or disrupting business operations.

Testing can be an excellent area to bring in additional third-party resources – especially if your IT team lacks the bandwidth or expertise to perform regular quarterly reviews. An expert partner can estimate your disaster-recovery settings and operations' effectiveness, validate your backup data integrity, alert you to systems that will miss SLAs, and provide recommendations for corrective action.

3 Protect Against Attacks

While making your organization completely invulnerable is not realistic, every attack you can protect against will save you tremendous pain, time, and cost. There are several ways to go about doing all you can to limit attack success and impact.

Start with user vigilance. Most ransomware – and most malware in general – is delivered via email and triggered by an unsuspecting employee. Preventing this can be as simple as instructing all employees to make sure attachments originated from a known sender or trusted source before opening them. Similarly, users should only download software from legitimate vendors or app stores. All software must be scanned for malware before it's clicked. Measures as simple as these could have stopped many high-profile breaches.

IT needs to act responsibly as well by promptly applying updates and patches. Remember, most successful attacks exploit vulnerabilities for which patches have long been available. Sound IT practices must be non-negotiable.

Once you've reduced the risk of malware entering your environment, the next step is to secure and protect your data against any exploits that might succeed. This should include:

- **Foundation hardening** – Vulnerabilities and configuration flaws in your operating system, database, application, and web server technologies can provide an entry point for all types of cyberthreats. For example, you should disable the use of Server Message Block 1 (SMB 1), which does not support encryption. Hackers can use these vulnerabilities to compromise your data protection platform's integrity and put your backups at risk.
- **Application hardening** –Direct access to applications makes life a lot easier for a cybercriminal. Use the AAA Security framework (Authentication, Authorization, and Accounting) as a guideline for protecting your applications.

AAA Security framework for controlling access		
Authentication	**Authorization**	**Accounting**
Proving and granting access	**Control what level of access is required**	**Tracking and auditing access and capabilities**
For authentication, Commvault integrates with secured LDAP-based directory services and external identity providers via OAuth and SAML protocols. Additional measures include support for two-factor authentication, encryption for credentials and impersonation accounts used for backups, certificate authentication, and Zero Trust controls to protect against threats originating from inside the network.	Fine-grained authorization controls the level of access granted to authenticated users based on their roles and needs. A passkey can be required to perform restores, while a data privacy lock can restrict browse and restore operations to the data owner or other select parties.	Accounting includes tracking and auditing users' data access and capabilities regularly. Remove unnecessary privileges and routinely audit encryption.

- **Ransomware protection** – Make sure the backups in your data protection platform are as safe as possible. This includes keeping the platform itself from being a conduit to spread malware to the backup data it holds. (Keep in mind that your data protection platform isn't designed to scan for or remove malware or prevent it from spreading to backup data from external sources.) There are several ways to protect backup data, each with its advantages and challenges:
  - A backup appliance can harden your architecture with vendor-supplied hardware. This can be a good idea — though you're counting on the vendor to provide regular updates to maintain its effectiveness.
  - WORM (write once, read many) technologies can block illicit encryption attempts by making backup data immutable – in other words, impossible to change or delete. Immutability protects data both within and outside the backup solution. Just make sure it won't pose barriers to the recovery objectives you've defined.
  - Data isolation using air-gap techniques can reduce the exposure of backup data to the risk of malware. If there's restricted network access or read/write access to backup copies of your data, there's no way to breach or corrupt that data, as only verified backup processes can manage those resources. Also, tightly restrict physical access to data — there's always the possibility of an insider inflicting physical damage to your storage library.

4 Monitor Your Environment

No matter how consistent and effective your countermeasures are, you must assume ransomware will eventually enter your environment. At that point, the focus shifts to monitoring: detecting the attack as quickly as possible so you can reduce its impact.

Detection can include scanning servers for anomalies such as unusual file system behavior that can signal an attack is underway. Machine learning has become a key asset in this effort, using historical data to recognize the difference between legitimate activity and potential trouble signs.

Honeypots take detection one step further by creating a hidden file of a type that's especially appealing to hackers and monitoring it for signature changes and other anomalies.

Centralized management and reporting are essential to identify gaps and take proactive action. The IT team should have a single screen to watch for anomalies such as modifications and deletions in file system metrics or the backup index. When potential indicators of ransomware or other threats are detected, real-time alerts can trigger a rapid response through integration with ticket systems or by initiating workflows.

5 Restore Your Data

Fast restores can significantly reduce the impact of a ransomware attack. Not only do you still have an intact copy of your data, you also can make it available to systems and users and help to restore normal business operations as quickly as possible.

There are three ways to backup data, each with different implications for restoration:

- **Traditional backup** operates at the file level. The system works through all the files and directories in the volume to determine whether they've changed and need to be part of the current backup. This can be a time-consuming and resource-intensive approach, though, as the system has to navigate every aspect of the index — an aptly named "tree-walk."
- **Block-level backup** avoids the performance penalties of traditional backup by working on a block-by-block basis. The application doesn't care how many files there are or what your index looks like. This allows faster, more efficient backups, making it feasible to perform backups more frequently.
- **Replication** takes a continuous approach to data backup. One way to do this is through continuous data replication (CDR), which involves logging all file write activity on the source computer, transferring this log to the data recovery platform, and replaying it to create a near real-time replica. Another option is to use incremental replication to continuously apply changes

from a source backup to a backup synced copy. Volume block-level replication (VBR) is often the best approach, combining block-level backup efficiencies with the near-real-time advantages of replication. This allows granular point-in-time recovery, crash-consistent recovery points, application-consistent recovery points, and effective recovery-point lifecycle management.

5 important questions to ask yourself before renewing your backup **Read >**

Taking action against ransomware

Your Commvault data protection and recovery solution can be a valuable part of your anti-ransomware strategy. Advanced technologies powered by artificial intelligence and machine learning make it possible to detect and alert on possible attacks as they happen so you can respond quickly. With Commvault Complete™ Data Protection, you have a powerful backup and recovery software solution for data protection – wherever your data lives. It provides simple, scalable, and comprehensive backup, replication, and disaster recovery orchestration for all your workloads.

We continue to increase data security by adding additional CIS (Center for Internet Security) Level 1 benchmark profiles for both Windows Media Agent and OVA to enhance recoverability in the event of an attack and make it possible to restore backups quickly – to minimize the impact of even a successful ransomware attack.

Opportunity and risk: that's the reality for businesses today and the people responsible for the data. A single event can affect the bottom line or define a career. So how do you prepare? By making sure you're ready.

The State of Colorado used the Commvault platform to recover quickly and fully from a major ransomware attack against its Department of Transportation. In fact, the State first learned of the attack through a Commvault alert – before any of its dedicated security tools had detected the breach. A coordinated response plan across agencies, personnel, and technologies statewide helped immeasurably. **Watch >**

The City of Sparks, Nevada was hit with ransomware that locked its police department shared files and left crucial geographic data inaccessible by agencies across the city. In the past, unreliable backups had raised fears of data corruption, but with Commvault, the city achieved complete data recovery in only 12 hours. **Watch >**

There's never been a more crucial moment to Be Ready with Commvault. For more info, visit **commvault.com/ransomware >**

commvault.com | 888.746.3849
get-info@commvault.com