eBook

RANSOMWARE 101

COMMVAULT

CONTENTS

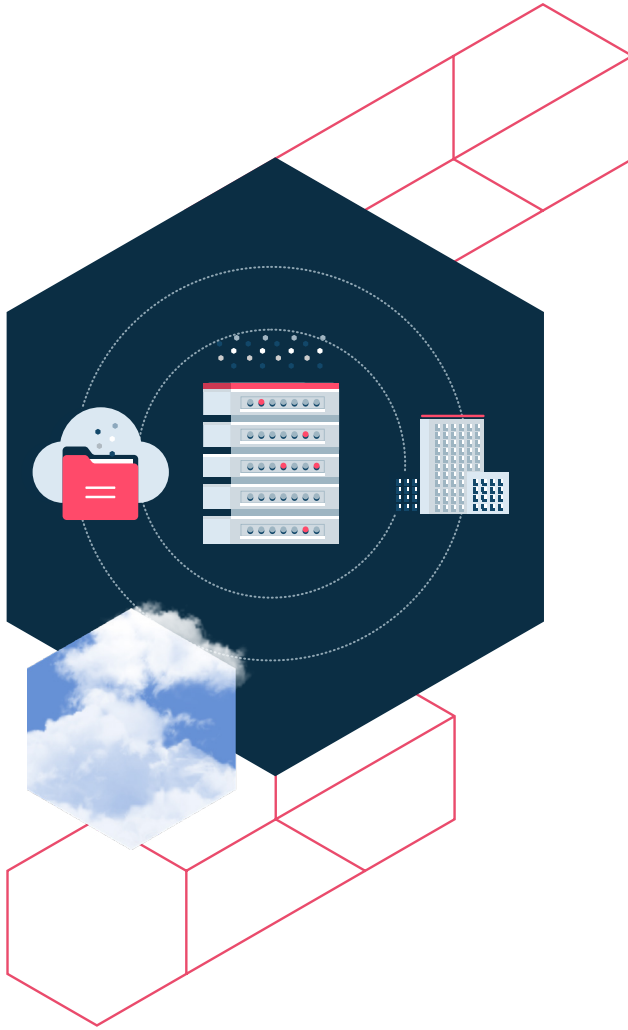
Time Accelerates in a Ransomware Attack

A ransomware attack is a classic example of a ticking clock. Your critical business data is suddenly taken hostage. Hackers use advanced encryption to render it inaccessible — and they demand money to decrypt it. How will you respond? Can you ensure the safety of your data if you refuse to pay — or even if you do? While you consider your options, your organization remains paralyzed. Every passing minute increases the pressure to make the right choice.

This scenario has already struck companies of all sizes across industries worldwide. **Yours could be next.**

Are you ready?

What Is Ransomware Protection?



The cyberthreat landscape, including ransomware, has transitioned to a case of when – not *if*. To ensure you can recover your data, you need the right solution with the best technology, the right people, and proven processes.

Organizations require tools such as anomaly detection, immutable backups, air gaps, and multi-factor authentication (MFA) controls to continually measure and protect their recovery readiness state. These tools help expose and remediate problems, validate data and business applications' recoverability, and improve security to reduce risk. In the event of a successful attack, fast restores are essential to resume business operations quickly.

A recovery solution is only viable if it is resilient across various failure modes. For example, one scenario may call for a data recovery event to revert to the prior instances before the corruption. Another may require the complete recovery of business applications to a new location. Designing recoverability across environments and providing simplified automation to test and validate each scenario helps build the recovery readiness state. Knowing that mission-critical data and applications have already been validated for recovery by an automated process completes the needed security, compliance, and comfort level.

LEARN MORE >

By 2031, it is anticipated that ransomware attacks against businesses will occur

every 2 seconds

up from every 11 seconds in 2021.[1]

1 CYBERSECURITY VENTURES, Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031, David, Braue, June 3, 2021.

What Is a Ransomware Attack?

Gartner defines a ransomware attack as "cyber extortion that occurs when malicious software infiltrates computer systems and encrypts data, holding it hostage until the victim pays a ransom."[2]

There's a reason ransomware attacks make the headlines. They are sudden, brutal, often highly profitable, and leave the victim feeling helpless. In recent years, the rapid rise of ransomware has cast a shadow of anxiety across organizations. Alarmed businesses, IT staff, and security leaders aren't just being paranoid.

A staggering

84% of organizations

experienced phishing or ransomware attacks in the last year. The average ransomware payment was over

$500,000.[3]

2 Gartner, 6 Ways to Defend Against a Ransomware Attack, by Manasi Sakpal, November 16, 2020.

3 Security Intelligence, Everything You Need To Know About Ransomware Attacks and Gangs In 2022, by Mark Stone, January 2022.

Types of Cyberattacks

It is easy to assume that all ransomware attacks are similar and that one size fits all in terms of prevention and preparation. However, because each type of ransomware is usually developed to infiltrate different, targeted networks, they can be very different in how they operate. Therefore, it is essential to understand the different types currently being used (keeping in mind that attackers are capable of combining multiple types of ransomware).

The strength of protection against any ransomware attack is in your defense strategy – especially given the rise in zero-day vectors with no known tactics, techniques, or procedures (TTP).

06 TYPES of Ransomware

01 **CryptoWall** is responsible for a high percentage of ransomware attacks – typically through phishing emails. The WannaCry ransomware virus is a derivative of the Crypto family and was at the core of the largest cyberattacks ever perpetrated. Unfortunately, the creators of CryptoWall continue to release new versions designed to avert security protections.

02 **Locky**, as the name implies, locks you out of files and replaces the files with the extension .lockey). However, its name doesn't describe the most damaging part of this type of ransomware: its speed. Locky has the distinction of spreading to other files throughout the network faster than other ransomware strains.

03 **Crysis** takes data attacks to a new level, actually hijacking your data and moving it to a new, virtual location. The significance of this aspect of the attack is that it qualifies as a breach if your company works with personal data; organizations must contact anyone who may have information on your network to stay compliant with local, state, and federal guidelines.

04 **Samsam** attacks unpatched WildFly application servers in the internet-facing portion of their network. Once inside the network, the ransomware looks for other systems to attack.

05 **Cerber** attacks the database server processes to gain access instead of going straight after the files. Its creators sell the ransomware software to criminals for a portion of the ransom collected, i.e., Ransomware-as-a-Service.

06 **Maze** is a variant of ransomware representing the trend in what is called "leakware." After data is encrypted, bad actors threaten to leak ransomed private data on the dark web unless the ransom is paid.

Safeguarding against ransomware must be at the forefront of organizations' security efforts.

Who Are These Bad Actors?

External malicious actors are, in simple terms, villains. They are hackers or other individuals seeking to infiltrate your organization for their nefarious purposes. What drives them is anyone's guess. However, one of these motives usually comes into play:

Greed. Making money is a substantial motivating factor. For example, cryptojacking has become a popular method of stealing compute resources within an organization for mining cryptocurrency.

Political. Malicious actors may be motivated by political reasons, including using ransomware to fund terrorism.

Competitive. Some bad actors may want to delete data, leak data, or disrupt business services simply to gain a competitive advantage over a rival.

Whatever their intention, they often use password-spraying techniques to gain unauthorized access to an organization or system. Or they might try to exploit vulnerabilities or inject botnets or rootkits to steal and delete data or disrupt an organization's ability to function.

That is where ransomware comes in. In a typical attack, the hacker uses malicious software (malware) to encrypt your data, often delivered via an infected attachment or link in an email. As in a flesh-and-blood ransom situation, the hacker then demands payment – or you'll never see your data again! Without an effective recovery strategy, you may think your only option is to pay the ransom and hope for the best.

How Does Ransomware Spread?

Ransomware is most often spread through email phishing messages containing malicious links. It can also disseminate via drive-by downloading that happens when a user unintentionally visits a contaminated site, and malware downloads onto the user's computer or mobile device. A drive-by download usually exploits a browser, application, or operating system that is outdated or has a security flaw. Ransomware then uses these vulnerabilities to find other systems in which to spread.

In any organization, the goal is to reduce risks and minimize the effects of ransomware. Ransomware mitigation requires a combination of best practices, constant vigilance, and a layered security approach.

Ransomware protection does not have to be complex.

With the proper preparation starting with creating a plan, constant monitoring, and a robust backup and recovery solution, you can mitigate the risk of ransomware.

10 TIPS to Minimize Ransomware

01 **Plan, plan, and more planning for ransomware protection and recovery:** Plan for the worst and hope your plans are never put to the test. It is imperative to have a multilayered security strategy in place. Remember: recovery readiness is critical.

02 **Employees are critical to a good defense; conduct employee security training:** Educate employees on avoiding ransomware and detecting phishing campaigns, suspicious websites, and other scams. Unfortunately, employees are still a leading cause of malware despite their best intentions.

03 **Ensure patches are up to date:** Keep software, firmware, and applications up to date to reduce the risk of ransomware exploiting common vulnerabilities.

04 **Install antivirus and antimalware protection:** Use antivirus software with active monitoring designed to thwart advanced malware attacks.

05 **Implement multi-factor authentication:** The process of authentication requires each user to have a unique set of criteria for gaining access. Enabling MFA methods makes it highly unlikely that a valid user account can be impersonated.

06 **Segment your networks to prevent lateral movements:** If a cyberattack is successful, don't give the perpetrator unlimited access within your network. Instead, divide your network into smaller segments to prevent lateral movement and contain the damage.

07 **Know your data to safeguard your data**: Identify business-critical data and sensitive data across your environment. Then determine if data is exposed to vulnerabilities. Using data insights, you can efficiently remediate these risks by removing, moving, or securing exposed data to reduce the chances of costly breaches and ransomware attacks.

08 **Perform regular backups:** Employ a backup and recovery solution that offers a multilayer framework for protecting, monitoring, and recovering from threats. The solution must support a 3-2-1 backup strategy for rapid recovery and secure cloud copies for added protection. 3-2-1 is 3 copies of your data, on 2 different media types with 1 copy offsite and preferably air-gapped.

09 **Test, test, and test:** Once you have your plan in place and the procedures and technologies to execute it, make sure it will work as needed. Perform frequent tests to verify that you can meet the SLAs you've defined for critical and high-priority data and applications.

10 **Enable the Security Health Assessment Dashboard (if you are a Commvault customer):** Use the Security Health Assessment Dashboard to identify, assess, mitigate, and monitor security controls within the Commvault data protection environment.

How to Mitigate Ransomware Attacks

When a ransomware attack occurs, the best approach is to have a validated copy of your backup data restored quickly to resume business operations. Organizations need a layered security approach encompassing multiple security tools, resources, controls, best practices, and strategies for a trusted and protected backup data copy. These security controls are applied within and around the data protection infrastructure to ensure the backup data is secured and recoverable.

These steps provide the confidence that when an attack occurs, your backup data is protected and ready.

What Are the Risks of Paying the Ransom?

To pay or not to pay a ransom is a highly debated topic. Only you can decide what is best for your organization. Factors to consider:

- Many government security services recommend not paying. For example, the U.S. government strongly prefers that you not pay a ransom because doing so encourages cryptolock attacks.[4] In March 2022, the U.S. government established the Consolidated Appropriations Act 2022, which requires a 24-hour reporting on any ransomware payments to the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and a 72-hour requirement to report all covered cyber incidents to CISA.[5]
- The kits for Ransomware as a Service often fund organized crime.
- Once you've paid, will the bad actors provide the keys to get your files back? Will they leave malware behind to strike again? It is easy to assume that all ransomware is similar, and it is not uncommon to think that one size fits all in terms of prevention and preparation.
- If leakware is involved, the EU's General Data Protection Regulation (GDPR) considers it a data breach once discovered, and you have 72 hours to devise a plan and report it.
- Do you become a future target for your willingness to pay?

Remember, even if you pay the ransom, there is no guarantee that you will recover all of your data. Only 8% of victims who pay ransomware get back all their data, and only 29% get back even half.[6] And even with the encryption keys, it may take several days, weeks, and even months to restore it all.

4 Richmond Times-Dispatch, Leading-Edge Law: Is it illegal to pay ransomware?," by John Farmer, December 2021
5 Inside Privacy, President Biden Signs Critical Infrastructure Ransomware Payment and Cyber Incident Reporting into Law, by Ashden Fein, Robert Huffman, Moriah Daugherty & Hensey A. Fenton III, March 2022
6 Richmond Times-Dispatch, Leading-Edge Law: Is it illegal to pay ransomware?", by John Farmer, December 2021

How Commvault Fights Ransomware

Commvault data protection and recovery can be a critically-important part of your anti-ransomware strategy. Commvault multilayered security is built on zero trust principles and based on the National Institute of Standards and Technology (NIST) cybersecurity framework to protect data and recover quickly in the event of a ransomware attack. Commvault helps protect and isolate your data, provides proactive monitoring and alerts, and enables fast restores. Advanced technologies powered by artificial intelligence and machine learning, including honeypots, make it possible to detect and provide alerts on potential attacks as they happen so you can respond quickly. By keeping your backups out of danger and making it possible to restore them within your Service Level Agreements, you can minimize the impact of a successful ransomware attack so you can get back to business right away (and avoid paying expensive ransoms).

Protecting and isolating your backup copies is critical to data integrity and security. Therefore, Commvault has taken an agnostic approach to immutability. With Commvault, you do not need special hardware or cloud storage accounts to lock backup data against ransomware threats. If you have Write-Once, Read Many (WORM), object lock, or snapshot-supported hardware (which Commvault fully supports), you can still use Commvault's built-in locking capabilities to complement and layer on top of existing security controls. The ability to layer security controls across different infrastructure types sets the Commvault immutable solution ahead of its competitors.

LEARN MORE >

Zero Loss Strategy

Commvault also offers a zero loss strategy, designed to help you reduce the threat of ransomware and recover quickly. This strategy is built on zero trust principles and implemented through our multilayered security framework. It provides end-to-end data visibility, protection, and recovery, the ability to identify and eliminate data gaps, and the capacity to easily scale and protect workloads – all through a single landscape.

LEARN MORE >

Commvault's Security Protection Layers

With every environment having a mix of different infrastructures, securing backup data against random unauthorized changes can seem challenging. Just like securing your house, you need to identify the vulnerabilities and enable protection and monitoring capabilities to match your needs.

Many experts recommend having a layered antimalware and ransomware strategy. Commvault has built these security capabilities into our data protection software and policies without the incremental management overhead of other solutions. The Commvault data protection and management platform includes five security layers: **"Identify, Protect, Monitor, Respond, and Recover."** Commvault multilayered security consists of feature sets, guidelines, and best practices to manage cybersecurity risk and ensure readily available data. Learn more about our multilayered security framework HERE ›

It is essential to understand that these capabilities are part of Commvault's core platform experience, Commvault Complete™ Data Protection. There are no special licensing fees, additional costs, or required hardware or software. The layered security depth is enhanced through greater integration with Metallic® Recovery Reserve™, Commvault HyperScale™ X, Commvault® File Storage Optimization, and Commvault® Data Governance for customers seeking the simplicity of Backup as a Service, data protection appliance, and/or gaining data insights and identifying business-critical and sensitive data, respectively.

Risk always accompanies opportunity – that's the reality for businesses today and those responsible for the data. A single ransomware event can threaten the bottom line or define a career. So how do you prepare? To assess your level of protection against ransomware attacks, take the free Commvault Risk Assessment. Learn more about ransomware and recovery HERE ›

Allina Health Embraces Flexible Data Protection With Commvault

BACKGROUND

Allina Health is a not-for-profit healthcare system dedicated to preventing and treating of illness and enhancing the greater health of individuals, families and communities throughout Minnesota and western Wisconsin. They struggled to complete backups consistently and needed a solution that was easier to manage and better supported.

CHALLENGE

The need for a hardware refresh prompted Allina Health to seek another data protection and management solution that could handle the data they needed to protect now and scale to growth.

- Inconsistent backups for critical systems created data gaps and risk of data loss
- High overhead to manage the system and prepare for complex annual licensing renewal
- Poor support experiences and critical issues not prioritized by the technology vendor

Consistent backup success with Commvault of greater than 99.9% over the last 5 years

Flexibility and granularity to recover only what they need, when they need it

Accelerated backups protect extreme database sizes in the same day

Reduced storage requirements with deduplication

Vastly improved support experience with access to technical resources and proactive guidance on solution use

CONTINUED ON NEXT PAGE

Allina Health

SOLUTION

Commvault was able to align with Allina's Health business strategies and objectives and Commvault Intelligent Data Services was chosen for its flexibility, agility, and the ability to quickly enable a forward-looking data management strategy.

- Commvault Complete™ Backup & Recovery for agile data protection and flexible, granular recovery
- Commvault's snapshot management technology for quicker, easier, more affordable protection across multivendor environments
- Enhanced services with Commvault Enterprise Support Program (ESP)

> ***We used to manually engineer redundancy to avoid data loss. Commvault provides the needed flexibility and granularity for fast restores.***

Jeff Burrell
Senior Infrastructure Engineer
Allina Health

READ THE CASE STUDY >

Kuveyt Türk Participation Bank Cuts Administrative Time by 80% and Upgrades Security

BACKGROUND

Kuveyt Türk Participation Bank (Kuveyt Türk) – a subsidiary of Kuwait Finance House (KFH) – is the 11th largest bank in Turkey. They wanted to grow the bank into the top 10 and therefore had to improve the operational efficiency of its backups and ensure it could defend against cybersecurity threats like ransomware attacks.

CHALLENGE

Kuveyt Türk wanted to simplify maintenance and administration of backups and free staff to focus on initiatives that support business growth.

- Needed a single backup software to simplify management of critical data across core banking applications and more than 500 virtual machines
- Wanted to spend less time troubleshooting data issues
- Wanted greater ease in managing scripts and creating more consistent snapshots

KUVEYTTÜRK

- **80% reduction in weekly time spent on backup administrative tasks**
- **Easier and faster troubleshooting with integrated Commvault workflows**
- **Installation completed in just one week, compared to months with competing vendors**
- **Eliminated the dependency on hardware vendors by gaining the flexibility to use any disk for backup**
- **Greater ease in managing scripts and creating consistent snapshots**

CONTINUED ON NEXT PAGE

KUVEYTTÜRK

SOLUTION

The Turkish Bank needed a centralized data protection solution to streamline backup and recovery and chose Commvault to help its enterprise grow faster.

- Commvault Complete™ Backup & Recovery
- Integration of workflow with Commvault platform

> ***We looked at EMC Networker and Veritas NetBackup, but Commvault Complete Backup and Recovery was easier to operate, easier to troubleshoot and it gave us the flexibility to use any disk for back up without tying us to a specific hardware vendor. Commvault was the only solution that gave us all these advantages.***

Ali Yazici
IT Service Manager
Kuveyt Türk

READ THE CASE STUDY >

Arvest Bank Slashes Time and Expense of Data Backup With Commvault

ARVEST

BACKGROUND

Arvest Bank has expanded to 135 communities in Arkansas, Kansas, Missouri, and Oklahoma – earning it a spot on the list of largest U.S. banks. They provide financial services, loans, deposits, asset management, insurance, and credit cards. Arvest Bank needed to keep their customers' data safe and in compliance adhering to bank regulations.

CHALLENGE

Arvest Bank follows strict compliance regulations. It needed to keep data for a specific amount of time while ensuring that data software would be backward compatible and provide the highest level of protection.

- 95% of data was being written to tape
- Required multiple days to achieve a single complete backup
- Difficulty complying with ever-changing banking regulations
- Pressure to meet internal SLAs: maintain two current copies of backups at all times

Reduced data backup time from 3 days to 3 hours

Increased backup schedule from 5 days per week to 7 days per week

Cut time to complete backups by 75%

Cut storage by 90% with deduplication

Able to get secondary copies offsite nearly 72 hours faster than writing locally to tape

75% to 85% deduplication rates allowed storage of 3.6 PBs data on 571 TBs of disk

Saved hundreds of thousands of dollars in disk cost alone

CONTINUED ON NEXT PAGE

ARVEST

SOLUTION

Arvest Bank chose Commvault for their backup/data management solution that provides stability and supports backups for the newest technologies.

- Replicates deduplicated data to another location using Commvault Complete™ Data Protection
- Uses Commvault snapshot management technology to allow VMs to be quickly protected
- Saves significant time by using disk-based deduplication copy replication

> ***The savings here is in the hundreds of thousands of dollars in disk cost alone.***

Chase Hale
Network Systems Engineer
Arvest Bank

READ THE CASE STUDY >

To assess your level of protection against ransomware attacks, take the Commvault Risk Assessment **HERE ›**

To learn more about ransomware and recovery, visit **COMMVAULT.COM/RANSOMWARE ›**

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

COMMVAULT