CLOUDIAN®

Ransomware Protection Buyer's Guide

Facts, myths, and real-world examples of how to protect your data from ransomware

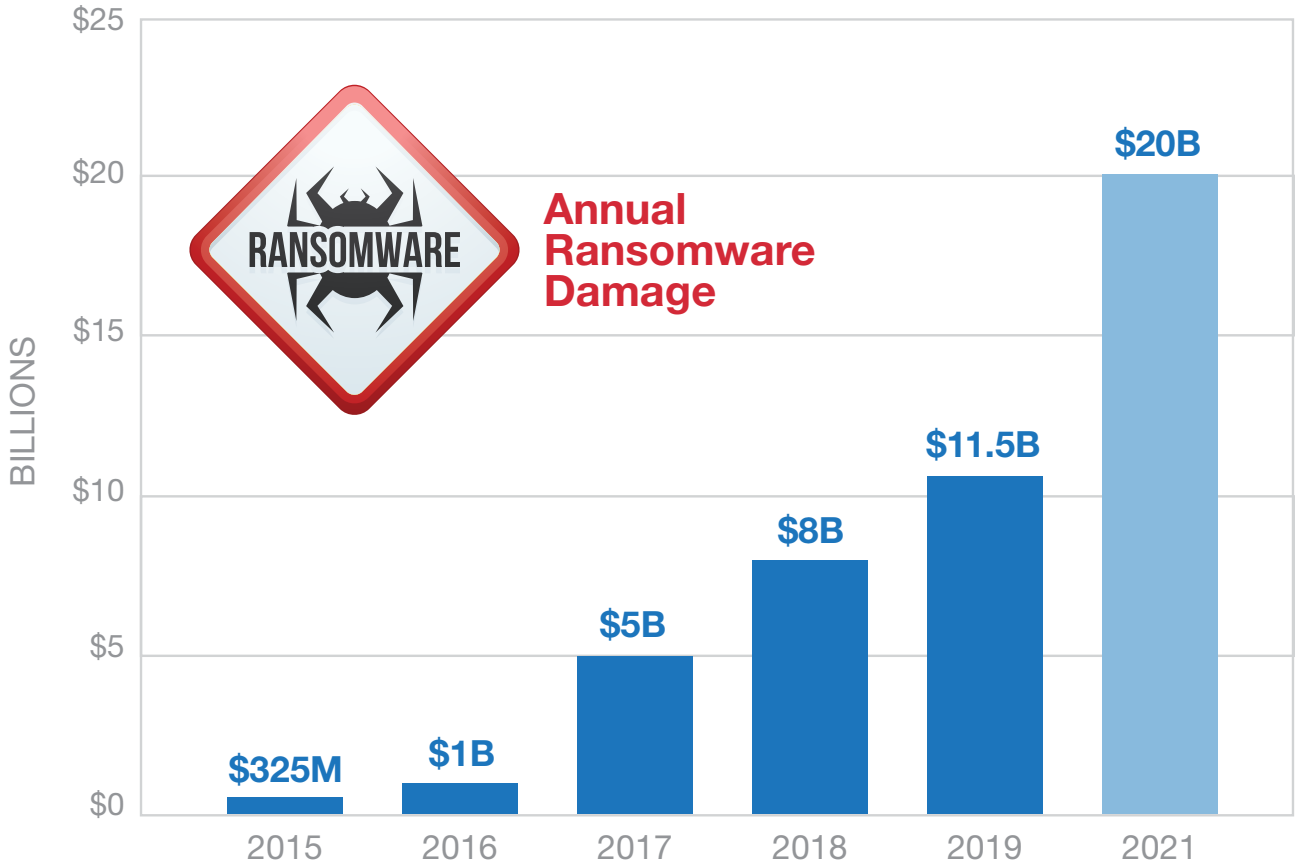
The Growing Need for Ransomware Defense

Ransomware impacts both big and small organizations across every industry. Attacks are on the rise, and their costs continue to soar. In fact, ransomware attacks increased 41% globally in 2019, with 205,000 businesses having lost access to their data. This year, ransomware is expected to cost organizations up to $20B.

Ransomware is a type of malware that holds network data "hostage." It works by reading files to penetrate an organization's IT infrastructure, then encrypts those files and overwrites the original data. The hacker then demands a fee to decrypt the files so the organization can regain access to their data. Data encryption often occurs over the weekend when this malicious background task is less visible to IT staff.

Attacks take many forms, targeting every facet of the infrastructure. One of the most common attack vectors is phishing emails that go after employees, often an organization's weakest attack plane.

Ransomware also targets vulnerabilities on endpoints, searching for out-of-date patches, antivirus software and logging data.



One of the most common attack vectors is phishing emails that go after employees, often an organization's weakest attack plane.

Rise in Ransomware Attacks

With improved encryption capabilities and the growing adoption of cryptocurrency during the past five years, cybercriminals have increased both the volume and variety of ransomware attacks. But the origins of ransomware attacks trace back to the 1980s when malicious actors used floppy disks to install malware on unsuspecting victims.

Since then, ransomware attacks have only grown in complexity and effectiveness thanks in part to the internet. Europol, the European Union-backed organization that fights major crimes and terrorism, recently declared ransomware the second most dangerous online threat to consumers and organizations. The crime-fighting organization also said ransomware attacks show no signs of slowing down.

Unfortunately, it's easier than ever for ransomware affiliates to operate. Security experts recently coined the term "Ransomware-as-a-Service" to underscore how easy it is to launch a ransomware attack by employing 3rd party software. In this SaaS model, cybercriminals do not need any special programming skills. Instead, they just need the motivation and the willingness to spread the malware, which is typically through email botnets that are easy for nonprogrammers to set up. Bad actors can sign up and download a customized ransomware binary that includes custom payment instructions and payment credentials, enabling cybercriminals to engage in ransomware activities with little effort or expertise.

Security experts recently coined the term *"Ransomware-as-a-Service"* to underscore how easy it is to launch a ransomware attack by employing 3rd party software.

Types of Ransomware Attacks

Email

Email is the most common form of ransomware attack. It is a popular cyberweapon because it can exploit social engineering by creating a sense of urgency and legitimacy to perform various actions. Ransomware emails will include attachments that are disguised as innocuous files or links to a software download. Once either the attachment or link is clicked, the victim is infected with malware. While email attacks may seem out-of-date and easy to detect, almost one out of four recipients open phishing emails and, shockingly, more than one out of 10 click on infected attachments or links to phishing messages. (*Source: McAfee Labs*)

Today's email attacks are increasingly sophisticated, with attackers now mimicking emails from trusted associates. In these so-called "whaling" attacks, hackers will masquerade as high-level executives, such as CEOs, to further gain trust of employees. Moreover, these emails will sometimes include personal details, usually gleaned from social media, making it more likely that even a wary individual will fall prey.

Drive-by Download

This ransomware infection is caused by visiting a compromised website, usually with a downlevel browser, software plug-in or unpatched third-party application. The infected website then runs an exploit kit that looks for unpatched vulnerabilities.

Remote Desktop Protocol (RDP)

Internet-exposed RDP sessions are commonly exploited to infect end-user devices. Such sessions are intended to remotely log in to Windows computers and allow the user to securely control the device. Unfortunately, hackers have become skilled at brute force attacking these exposed computers. In compromising RDP vulnerabilities, hackers use these methods and credentials purchased on Dark Web marketplaces.

Free Software

Despite potential benefits, free software can come with a steep price. In this case, cybercriminals prey on people's natural desire for free software and content to bypass firewall filters. Users download pirated games and music, free software tools, adult content and screensavers without realizing these files have been infected with ransomware.

Today's email attacks are increasingly sophisticated, with attackers now mimicking emails from trusted associates. In these so-called "whaling" attacks, hackers will masquerade as high-level executives, such as CEOs, to further gain the trust of employees.

3 Ransomware Myths

Data backups will protect me

Simply having a backup copy is not a defense. Hackers know to target the backup copies first. For backups to be effective, the copies must be unchangeable (or immutable). They are protected from encryption by ransomware only if the data cannot be changed.

Having a copy in the public cloud is protection

In 59% of attacks, cloud-based data was targeted (*Source: Sophos*). Hackers can target your cloud-based data just as readily as on-prem data.

My perimeter defense is up-to-date

A high percentage of attacks occur at firms that have up-to-date perimeter defenses. Attackers routinely skirt that defense by using emails, the most common attack vector, and it only takes a single unguarded moment for an employee to click on a file or link and inadvertently open the door to an attack.

Common Targets

Ransomware has shifted from targeting consumers to primarily impacting businesses and governments. In 2018, enterprises accounted for 81% of ransomware victims. The next year, cybercriminals increasingly targeted government agencies, municipalities, schools, hospitals and healthcare providers, either directly or through managed service providers (MSPs).

Ransomware affiliates became more aggressive, compromising mission-critical systems to intimidate organizations into paying significant fees to get their data back. When an organization chooses not to pay a ransom, they often must replace equipment and start critical business processes over.

Because of this, victimized organizations frequently believe that paying the ransom is the most cost-effective resolution. While this may be true in many cases, it directly funds the development of next generation ransomware and ultimately puts these organizations at greater risk of an attack in the future.

13 Ways to Stop Ransomware — Key Tips

Avoiding Email Attacks

Email attacks are the most common entry point for ransomware, so it's critical to continuously train your employees and users so they can spot suspicious activity.

Never click on unverified links

Avoid clicking links in spam emails or emails from unfamiliar senders. When you click a malicious link and begin a download, your computer can quickly become infected.

Once the ransomware has infected your computer, it will encrypt your data or lock your operating system. At that point, the ransomware has something to hold as hostage, and it will demand a ransom so that you can recover your data. Paying these ransoms may seem like the simplest solution. However, doing so does not guarantee that the perpetrator will give you access to your device or data.

Do not open untrusted email attachments

Another way that ransomware could infect your computer is through an email attachment.

Do not open email attachments from senders you do not trust. Look at who the email is from and confirm that the email address is correct. Be sure to assess whether an attachment looks genuine before opening it. If you're not sure, contact the person you think has sent it and double check.

Never open attachments that ask you to enable macros to view them. If the attachment is infected, opening it will run the malicious macro, giving the malware control over your computer.

Only download from sites you trust

To reduce the risk of downloading ransomware, do not download software or media files from unknown websites. Go to verified, trusted sites if you need to download something. Most reputable websites will have markers of trust that you can recognize. Look in the search bar to see if the site uses 'https' instead of 'http.' A shield or lock symbol may also show in the address bar to verify that the site is secure.

If you're downloading something on your phone, you must also make sure you're doing so from reputable sources.

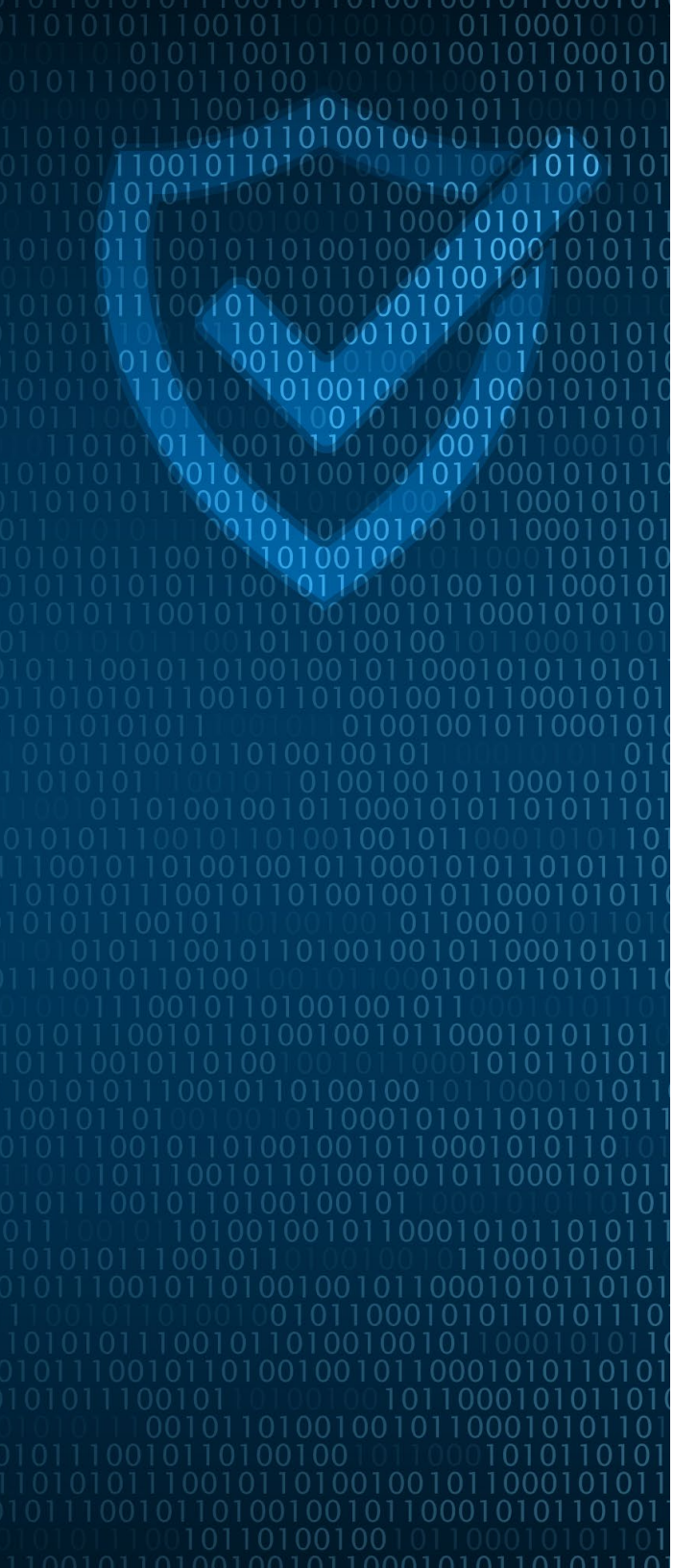
Avoid giving out personal data

If you receive a call, text, or email from an untrusted source that asks for personal information, do not give it out. Cybercriminals planning a ransomware attack may try to gain personal data in advance of an attack. They can use this information in phishing emails to target you specifically. The aim is to lure you into opening an infected attachment or link. Do not let the perpetrators get ahold of data that will make their trap more convincing. If you get contacted by a company asking for information, ignore the request, and contact the company independently to verify it is genuine.

How Cyber Insurance Can Hurt You

Cyber insurance provides protection from ransomware losses. But with claims on the increase, carriers are taking steps to avoid paying out as much as possible. Here are three important facts to remember:

1. **Coverage is not assured:** You may not be able to obtain insurance without a solid ransomware defense that meets your insurer's expectations. The strength of your backup processes and perimeter defenses will matter.
2. **Rates are going up:** A 25% increase in cyber insurance rates was common in 2020. Ask your carrier about discounts if you have an immutable (unchangeable) backup.
3. **Ransom payments are not always covered:** After an attack on Jackson County, Georgia, the local government was responsible for the $400K ransom payment after their cyber insurance carrier refused to cover it.



Defending Other Ransomware Exposures

These perimeter defenses and other tips can also help protect against attack:

Stop ransomware before the endpoint

Keep ransomware from reaching the endpoint in the first place using web-filtering technologies.

Block use of Tor

Tor is software that can provide a means for bad actors to conceal their activity by obscuring identity and point of origin information. To reduce the risk, the Department of Homeland Security recommends that you consider tools that restrict all traffic to and from Tor entry and exit nodes.

Apply all patches

Many ransomware strategies take advantage of vulnerabilities in the operating system or in applications to infect an endpoint. Having the latest operating system and application versions and patches will reduce the attack surface to a minimum.

Spam filtering and web gateway filtering

Again, the ideal approach is to keep ransomware off the network and the endpoint. Spam filtering and web gateway filtering are great ways to stop ransomware that tries to reach the endpoint through malicious IPs, URLs, and email spam.

Allow only whitelisted items to execute

Centrally administer whitelisting to block unauthorized executables on servers and PCs, thus dramatically reducing the attack surface for most ransomware.

Avoid macros

In general, do not enable macros in documents received via email. Microsoft Office turns off automatic execution of macros for Office documents by default. Office macros are a popular way for ransomware to infect your machine, so if a document asks you to enable macros, don't do it.

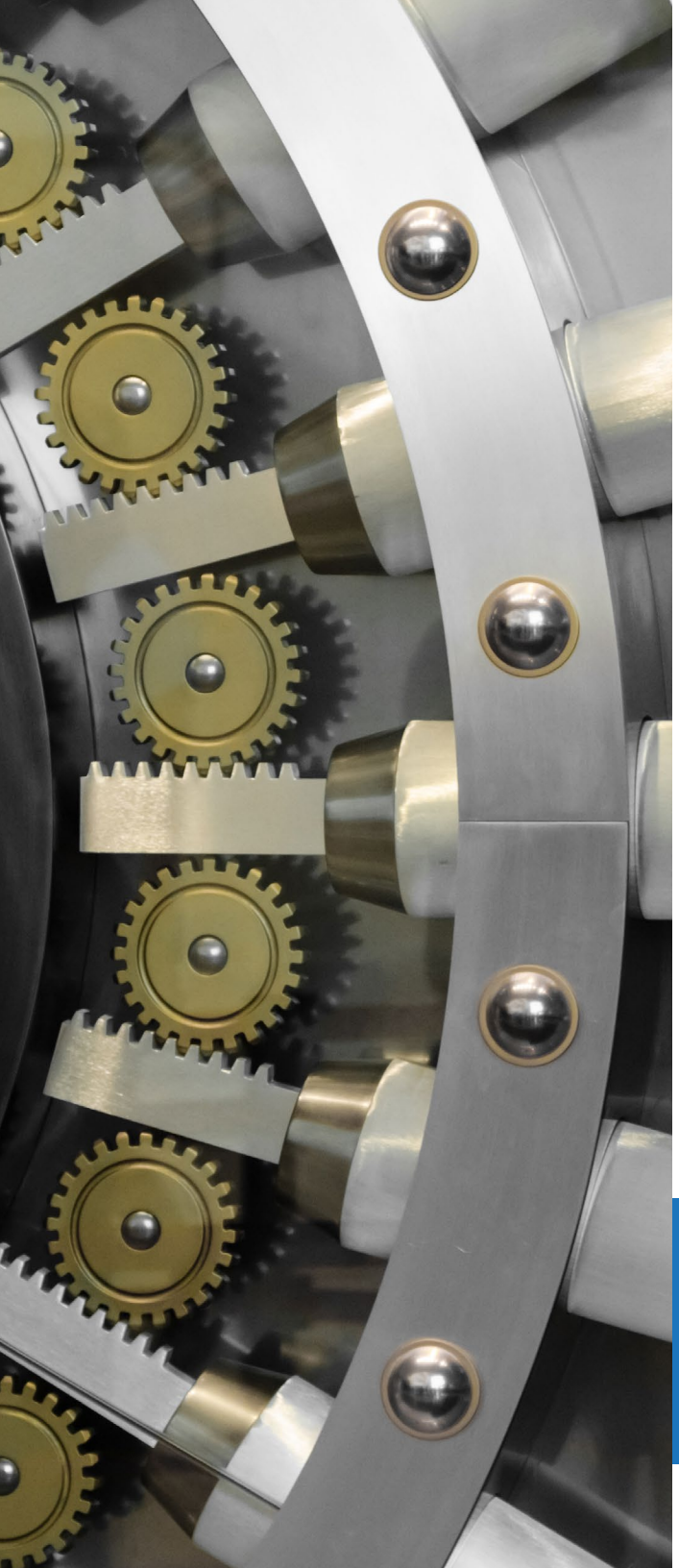
Should You Pay the Ransom?

If you are victim to an attack, the immediate question is, should you pay the ransom?

The most recent estimates are that more than half of victims do pay. But here are 3 reasons not to pay:

1. **Your data might still be lost:** As many as 50% of victims who do pay are not able to recover all their data via the promised decryption.
2. **Paying will encourage future attacks:** Surveys find that over 70% of paying victims are targeted again.
3. **It may be illegal to pay:** Many of the bad actors reside in countries (such as N. Korea) that are currently subject to US sanctions. For US residents, paying them money is against the law, even if you have no knowledge of where the money is going.

"The Treasury Department may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws."



The Best Line of Defense: An Immutable Copy of Your Data

While these tips are important — and should be adhered to — they can all ultimately be defeated. Email attacks have become shockingly convincing and can now fool even highly trained users. Perimeter defenses also have vulnerabilities. Attackers only have to succeed once to hold an entire organization hostage.

There is only one approach that can truly safeguard against ransomware. **Companies must protect data where it resides: at the storage level.** This can be achieved by maintaining an immutable or unchangeable copy of backup data. With a protected copy of the backup data, organizations can mitigate the impact of ransomware attacks. When an attack occurs, they simply need to revert to a backup copy before the malware infected their data. Then, they can restore all affected files.

This can be accomplished in two ways:

1. Tape

Create tape-based backup copies that are physically separate from the infrastructure. While the tape-based method is effective, it is costly in terms of the manual intervention required. Tapes must be managed and maintained, a cumbersome and time-consuming task. And no real-time data searchability means you miss the opportunity to mine and monetize all of that data.

2. Immutable Storage

Use immutable (or WORM) storage for backup data to create a copy which is protected from encryption by ransomware. In the event of an attack, companies will always have an unencrypted data copy to restore from.

There is only one approach that can truly safeguard against ransomware. Companies must protect data where it resides: *at the storage level.*

Object Lock Provides Immutable Storage

The advantage of immutable storage is that it requires no intervention or handling of media. It employs on-prem object storage technology with a feature called Object Lock.

Enterprise Data Storage with Data Immutability

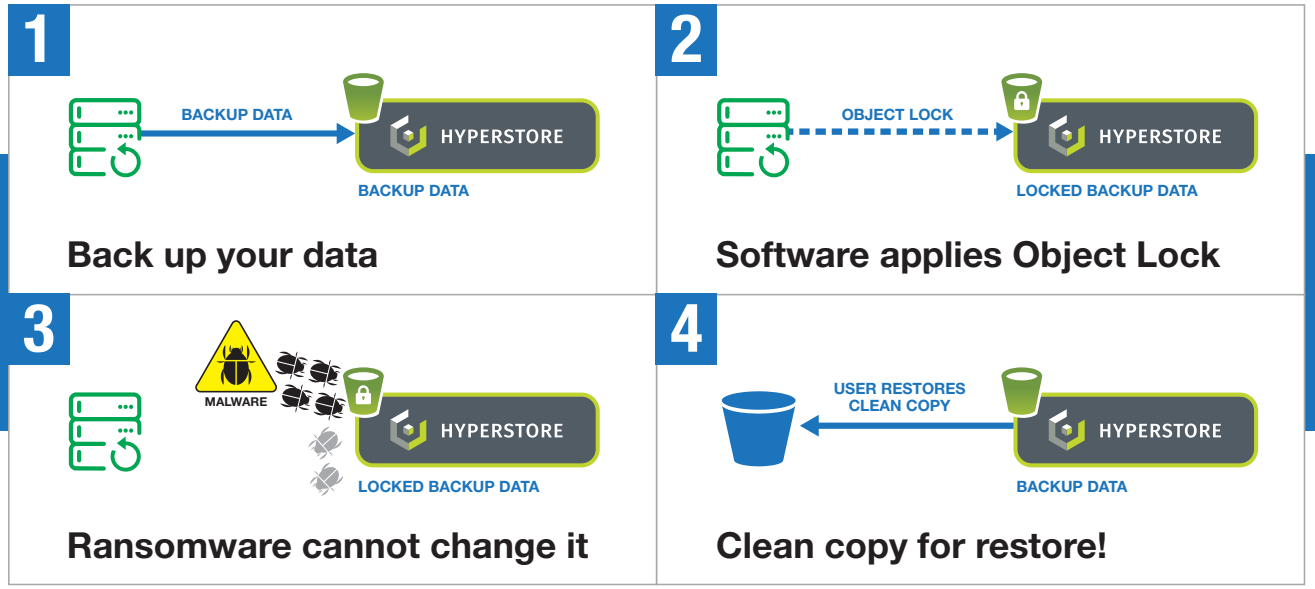
To protect against ransomware attacks, Cloudian HyperStore object storage supports data immutability through a featured called Object Lock. Object Lock permits backup data copies to be made unchangeable for a set period of time, which prevents hacker encryption or deletion and ensures a clean data copy for reliable recovery. The resulting security is comparable to offline storage. Object Lock protects data from ransomware by making it unchangeable for a specified period, thus preventing encryption by malware.

Integrated in a Backup Workflow

Object Lock works as part of a standard backup workflow, so it requires no manual intervention or ongoing management.

Data is backed up using software from leading vendors, such as Veeam and Commvault. Once the Object Lock policy is applied, the data is protected from alteration or deletion for a user-defined period. Data copies are layered, meaning that new backups will be written before the lock expires on the earlier copies. Organizations are always assured they will have an unencrypted copy for restore if an attack were to occur.

Object Lock works as part of a standard backup workflow and requires no manual intervention or ongoing management.



Not all Object Lock Solutions are Created Equal

Cloudian goes beyond simply supporting Object Lock functionality. Cloudian offers a hardened solution that has endured rigorous testing to earn several major government security certifications. With HyperStore, even a rogue IT administrator with management access privileges cannot delete or modify protected data, either by accident or on purpose. The underlying hardware layer is protected too, preventing direct access to storage.

Cloudian HyperStore's security certifications include:

- **FIPS 140-2:** Certified to meet cryptographic components requirements
- **Common Criteria for Information Technology Security Evaluation with EAL2 designation:** Certified to meet federal, state and local government security standards
- **SEC Rule 17a-4(f):** Certified to meet non-rewriteable, non-erasable storage requirements
- **CFTC Rule 1.31(c)-(d):** Certified to meet principles-based requirements
- **FINRA Rule 4511:** Certified to meet data retention requirements

In addition, Cloudian supports AES-256 server-side encryption for data at rest and SSL for data in transit (HTTPS). Fine-grained storage policies — including encryption at object and bucket-levels — permit security settings to be individually configured for different users or data types in a shared-storage environment. Cloudian also offers enhanced security features such as secure shell, integrated firewall and RBAC/IAM access controls to further protect backup copies.

EAL2 Common Criteria CERTIFIED

FIPS Level 1 Validated 140-2

U.S. SECURITIES AND EXCHANGE COMMISSION MCMXXXIV SEC 17a-4

NIST 800-88

Cyber insurance providers require robust ransomware protection and immutable backup

Ransomware attacks were the cause of 41% of the cyber insurance claims filed over the first six months of 2020, according to a report published by Coalition, a cyber insurance vendor that compiled the data based on findings from 25,000 small and medium-sized companies in the U.S. and Canada. Coalition reported a 47% increase in the number of ransomware attacks, with the average size of the demand jumping by 46% over the time period in question.

The emerging ransomware strains Maze and DoppelPaymer are particularly popular among scammers, the Coalition report said. Both kinds of malware are more complex than traditional forms of ransomware, and thus are harder to decrypt, allowing the ransomware affiliates behind the hacks to demand higher payments.

In response, some cyber insurance vendors now demand that customers have robust ransomware protection in place, either charging higher premiums to those that don't, or even refusing to provide coverage. These vendors encourage customers to maintain backup copies that are protected from encryption. Some insurers won't even cover ransomware claims for customers that don't have immutable backup copies.

Cloudian HyperStore S3-Compatible Object Storage

Cloudian HyperStore lets you consolidate enterprise data to a single, limitlessly scalable storage pool. Available as either software or fully integrated appliances, HyperStore enterprise object storage provides unlimited capacity scalability, intuitive management tools, uncompromising data protection and the industry's most compatible S3 API implementation—all at far less cost than traditional disk-based storage systems.

Cloudian is verified compatible with data protection software from all leading suppliers, including Veeam, Commvault, Rubrik, and Veritas. In addition to Object Lock and the industry's broadest array of security certifications, Cloudian HyperStore offers many other capabilities that make it the ideal platform for your enterprise and backup data.

Hybrid Cloud-Ready

For disaster recovery purposes, Cloudian's data management functionality lets users create a remote data copy. Replicate backup data to a second Cloudian site, or to low-cost deep archive storage such as AWS Glacier. With policy-based management, offsite copies will be automatically kept up to date.

Multi-tenancy

Increase efficiency by allowing multiple users to share a single backup and storage infrastructure, without compromising security. Cloudian supports multi-tenancy, giving each client a separate, secure namespace. Integrated billing simplifies management, and QoS controls help you deliver consistent service levels.

Cost-Effective Protection

This level of data protection is surprisingly cost effective. Cloudian offers the lowest TCO of any enterprise storage type, saving over 60% vs traditional enterprise storage or public cloud storage. Complete appliance-based solutions can cost as little as 0.5¢ per GB/mo, including support.

The scale-out architecture lets you start small and grow, rather than buying capacity long in advance. A software-defined-storage model gives you the option of deploying on the hardware of your choice, or on Cloudian's preconfigured storage appliances.

Summary

Ransomware poses one of the most pernicious threats to organizations today, causing significant revenue loss, business downtime and reputational damage. With these attacks growing more frequent and sophisticated, simply adopting security best practices and perimeter defense solutions will not protect companies.

Going to the public cloud won't defend against ransomware either, as the majority of attacks include data in public clouds. Furthermore, organizations cannot just rely on cyber insurance as a fallback plan, as these insurers increasingly refuse to cover claims when they deem that a customer did not take sufficient precautions to guard against an attack.

Companies must protect their data at the storage level through the use of immutable backup copies. They can most securely and economically achieve this by leveraging an on-prem object storage solution with Object Lock functionality. This type of solution ensures that malware cannot change and encrypt backup data, essentially mitigating the impact of any ransomware attack.

Cloudian HyperStore has earned a wide array of government security certifications, validating its reputation as the industry's most secure on-prem object storage platform.

Click **here** to learn more about how Cloudian can protect you against ransomware, or **learn more about a free trial** in your own data center.

Cloudian, Inc. 177 Bovet Road, Suite 450, San Mateo, CA 94402
Tel: 1.650.227.2380 | info@cloudian.com | cloudian.com