

Topics

1. What is Ransomware?
2. What are the Types of Ransomware Attacks?
3. How Ransomware Affects a Business
4. The Cost of Ransomware Attacks for Business
5. Can Antivirus Detect Ransomware?
6. How to Prevent Ransomware
7. How to Detect Ransomware
8. How to Stop a Ransomware Attack
9. How to Remove Ransomware
10. How to Recover from Ransomware Attack?
11. How to Protect Yourself From Ransomware
12. Ransomware Attacks on Businesses Statistics

The reality of ransomware recovery

First response: Contain the damage

Assess the fallout: How bad is it?

Ransomware data recovery options

The ransomware debate: To pay or not to pay?

Rebuilding your environment

Lessons learned: Post-recovery actions

People also ask

The bottom line: Prevention beats recovery

Share    

How to Recover from Ransomware Attack?

Published: June 25, 2025

By:  **Brenda Buckman**

Key Takeaways

- Preparation is key: Strong backups and a well-tested response plan help organizations recover much faster.
- Act fast to contain the threat: Disconnect infected systems immediately to stop the ransomware from spreading.
- Keep records of everything: Detailed documentation helps with insurance claims and legal issues.

Ransomware continues to reign as one of the most devastating weapons in the cybercriminal arsenal—a full-blown digital hostage situation that can bring organizations to their knees. One minute, your systems are humming along and then the next, your files are locked up and bad actors are demanding a ransom in Bitcoin, complete with a countdown clock for dramatic effect.

The bad news? Ransomware attacks are getting more sophisticated, with bad actors spending months exploring networks before striking. The good news? You don't have to be a sitting duck. This guide breaks down exactly how to recover from a ransomware attack.

[Try Huntress for Free](#)
[Get a Free Demo](#)

The reality of ransomware recovery

Modern ransomware attacks have evolved far beyond simple encryption. Today's ransomware operators exfiltrate your sensitive data, disable security controls, and establish persistent access to your network—hogtying your entire organization.

Think of it like a housebreak. If burglars break in, you don't just replace the stolen TV. You change the locks, install security cameras, and maybe even get a guard dog. Recovery involves more than just getting your files back. It's about kicking the bad guys out, securing your systems from top to bottom, and making sure they can't slip in through a forgotten backdoor. This is the necessary mindset for effective ransomware recovery.

First response: Contain the damage

The first few minutes after [detecting ransomware](#) are critical. Here's what you need to do to [stop a ransomware attack](#).

1. Pull the plug: Disconnect compromised devices from the network to prevent lateral movement. Ransomware can tear through a network in minutes, so every second counts.
2. Preserve evidence: Take forensic snapshots, save logs, and document everything for legal and insurance purposes.

for legal and insurance purposes.

3. Alert the right people: Notify your IT team, stakeholders, and law enforcement if necessary.
4. Resist the panic payoff: Paying the ransom doesn't guarantee file recovery, and it funds future attacks. Explore alternatives first.

Think of this phase as digital triage. You're stopping the bleeding before beginning the healing process. The decisions made here lay the foundation for ransomware file recovery success.

Assess the fallout: How bad is it?

Once the fire is under control, assess the damage:

- ✓ Which systems and files are affected?
- ✓ Has sensitive data been stolen or leaked?
- ✓ How did the ransomware get in?
- ✓ What's your best path to recovery?

This step is like checking your house after a storm. Before you can rebuild, you need to know what's broken. This recon builds the backbone of your server ransomware recovery strategy.

Ransomware data recovery options

Restore from backups

The fastest and safest way to recover from ransomware is through clean, verified backups. Your backups should be:

- ✓ Stored offline or in immutable storage where ransomware can't touch them.
- ✓ Tested regularly, especially to avoid corruption.
- ✓ Comprehensive, covering all critical data and systems.
- ✓ Following necessary retention policies that balance storage costs with recovery needs.

Decryption tools

In some cases, security researchers release free decryption tools for specific ransomware strains. Check resources like [No More Ransom](#) to see if your variant has a solution, potentially saving you from dealing with the whole rigmarole.

Professional recovery services

If backups are unavailable and decryption isn't an option, [Huntress's specialized ransomware recovery services](#) can help. Our team enables quick ransomware detection and removal to reduce risk and maximize uptime.

The ransomware debate: To pay or not to pay?

Paying the ransom is like negotiating with terrorists. It's risky, ethically questionable, and there's no promise you'll get your data back. Before considering payment, think about this:

- ✓ Many attackers take the money and run (and provide non-functional decryptors).
- ✓ Payment encourages more attacks and funds criminal enterprises.
- ✓ Some jurisdictions don't allow ransom payments.
- ✓ Insurance policies may have limitations on covering ransomware payments.

Rebuilding your environment

After you recover your files, you need to strengthen your security posture so this doesn't happen again.

- ✓ Reinstall clean systems: Start fresh with secure, patched software. Never trust potentially compromised systems.
- ✓ Enhance security: Deploy endpoint detection, multifactor authentication, and strict access controls.
- ✓ Segment networks: Prevent an attack on one system from taking down your entire organization. Network segmentation is like having fireproof doors throughout your building.
- ✓ Train employees: Phishing remains a top ransomware entry point. Train your team to spot red flags. Your people can be your strongest defense or your weakest link.
- ✓ Enable ransomware canaries: Tools like [Huntress's Ransomware Canaries](#) provide early warning before encryption spreads, giving you precious time to respond before the situation becomes critical.

Lessons learned: Post-recovery actions

After a ransomware attack, don't just breathe a sigh of relief and move on. Take time to:

- ✓ Conduct a post-mortem analysis looking at how this happened and what gaps need fixing.
- ✓ Update incident response plans based on lessons learned.
- ✓ Review cyber insurance policies to see if your coverage adequately protects against ransomware.
- ✓ Implement ongoing security awareness training.

People also ask

Is it possible to recover ransomware?

Yes. Recovery depends on factors like backup quality, available decryption tools, and expert assistance.

What's the only way of recovering from a ransomware attack?

There's no single recovery method that works universally. The most reliable approach is restoring from clean, offline backups and implementing a thorough incident response strategy.

How long does it take to recover from a ransomware attack?

It depends. Some orgs recover in days, while others take months. Well-prepared organizations with strong backups recover fastest.

What's the first action after a ransomware attack?

Immediately isolate infected systems, preserve evidence, and activate your incident response plan.

The bottom line: Prevention beats recovery

Recovering from [ransomware](#) is possible, but preventing an attack in the first place is the smarter move. Save yourself the chaos, financial loss, and the stress of dealing with an attack so you can recover from ransomware if there's an actual incident.

Try Huntress and discover our [Ransomware Canaries](#) for faster detection of potential ransomware incidents.



Brenda Buckman

[Read More >](#)

[Continue Reading](#)

How to Protect Yourself From Ransomware >

Protect What Matters

Secure endpoints, email, and employees with the power of our 24/7 SOC. Try Huntress for free and deploy in minutes to start fighting threats.

[Try Huntress for Free](#)



Platform

Huntress Managed Security Platform

Managed EDR

Managed EDR for macOS

Managed ITDR

Solutions

Phishing

Compliance

Business Email Compromise

Education

Why Huntress?

Managed Service Providers

Value Added Resellers

Business & IT Teams

24/7 SOC

Resources

Resource Center

Blog

Upcoming Events

Support Documentation

About

Our Company

Leadership

News & Press

Careers

Managed NDR

Managed SIEM

Managed Security
Awareness Training

Book A Demo

Finance

Healthcare

Manufacturing

State & Local Government

24/7 SOC

Case Studies

Contact Us



© 2025 Huntress All Rights Reserved.
[Privacy Policy](#) | [Cookie Policy](#) | [Terms of Use](#)

Free Trial

