Proven Ransomware Detection Techniques For Improved Security

by MaKenna Hensley
Published: 18 March 2025

Ransomware isn't just a cybersecurity issue—it's a business killer. One attack can lock up critical files, disrupt operations, and force companies into a brutal decision: pay up or lose everything. And it's not just businesses.

Individuals, hospitals, government agencies—no one's off-limits. The best shot at stopping it? Recognizing the warning signs before it takes hold. Organizations and individuals must have effective ransomware detection mechanisms in place to avoid such attacks and their consequences.

In this article, we'll look at tried-and-true ransomware detection mechanisms that can significantly improve security and repel such harmful attacks.

Understanding Ransomware and Its Impact

To properly understand how to find ransomware, it is first necessary to know what it is and how it can damage computers. If you don't pay a certain amount of money or "ransom," this bad software will lock you out of your computer or encrypt your files. People and businesses can suffer a lot from this because sensitive data and critical systems can be held hostage.

Finding and stopping ransomware as soon as possible is key to lessening its effects. By using strong ransomware detection methods, businesses can greatly lower their chances of being hit by these attacks and limit damage. That said, we'll now look at these methods and strategies for detection, including their pros and cons and some real-life examples of each.

Traditional Ransomware Detection Techniques

Traditionally, the default method of detecting ransomware has been pattern matching—recognizing malware by known signatures. It is excellent for already studied threats, but fresh ransomware doesn't play by those rules. New variants, obfuscation schemes, and rapid evolution make signature-based detection progressively less trustworthy day by day. Although such mechanisms prove successful against well-known variants of ransomware, they may not be as effective against fresh and emerging variants.

Below is a listing of some of the traditional detection mechanisms most frequently used, along with each mode of operation.

Signature-based Detection

Signature-based detection involves identifying known patterns and signatures of ransomware using antivirus and antimalware software. This technique relies on recognizing specific characteristics of known ransomware variants to identify and block them before they cause harm. However, this approach has limitations as it is reactive and may need to be more effective against new or evolving ransomware strains.

Example: An antivirus software detects a file with a signature matching a known ransomware variant and quarantines it before executing and encrypting the system's data.

Heuristic-based Detection

Instead of searching for a specific ransomware signature, heuristic detection looks at behavior. If a program begins encrypting files in bulk, changing system processes, or trying to close security software, that's suspicious. It doesn't even matter if it's a brand-new strain—if it acts like ransomware, it's caught. That adaptability makes it harder for attackers to get through.

Example: If a piece of software exhibits suspicious behavior, such as encrypting a large number of files at a rapid pace, the system will prevent it from being executed.

Behavior-based Detection

What then is behavior-based detection all about? Rather than searching for particular ransomware signatures, it searches for odd activity—things like a program suddenly encrypting hundreds of files at once, changing system settings, or viewing documents it shouldn't be reading. Should it spot something dark, it stops the process before it may cause damage. It picks up irregularities, including mass file encryption, illegal process execution, and unexpected CPU spikes. This method helps to find malware that avoids signature and heuristic-based detection.

Example: A security solution identifies an application attempting to access multiple files and promptly sends an alert, blocking the process.

Advanced Ransomware Detection Techniques

Legacy methods cannot match the pace of modern ransomware. Attackers evolve constantly, so defenses also need to be nimble. For just this reason, newer detection models rely on machine learning, AI, and real-time analysis. Instead of reacting to known threats, these solutions learn, adjust, and forecast potential attacks prior to their occurrence.

These innovative technologies improve ransomware detection by utilizing machine learning, artificial intelligence, and test environments to identify and mitigate new threats.

Machine Learning Based Detection

How can ransomware be prevented using machine learning, analyzing large datasets, and identifying patterns that people would overlook? By spotting minute behavioral clues, these adaptive systems improve ransomware detection.

For instance, early detection and mitigation are triggered when a machine learning model trained on past ransomware attacks identifies a pattern of file access and alterations that resemble ransomware activity.

Sandboxing

Sandboxing is like a test lab for suspicious programs. It runs them in a secure, isolated environment where security teams can study their behavior without putting the real system at risk. For example, if a suspicious email attachment is opened in a sandbox, the system monitors its actions closely. If it shows signs of ransomware—such as attempting to encrypt files or communicate with unknown servers—the sandbox blocks it before it can cause harm.

Artificial intelligence-based detection

AI is not static rules when it comes to ransomware detection. Instead of being signature-based, it's trained on actual activity—watching network activity, file changes, and system interactions. When something doesn't feel right—like strange file encryption, unauthorized login, or suspicious traffic—it alerts the activity and acts fast. It doesn't need to have seen a specific strain of ransomware before to know that something's wrong, so it's much more effective at handling newer, constantly evolving threats. The moment AI detects suspicious behavior, it acts to prevent the threat from spreading.

Detection Strategies

Effective ransomware detection requires a combination of methods to examine different parts of the system and network. Organizations that use a variety of detection tactics can better detect and react to ransomware assaults before they cause serious damage. To help strengthen defenses against ransomware, we have included some of the most common detection methods below.

Network-based Detection

Network-based detection can monitor anomalous communication patterns, attempts to encrypt data, and other signs of ransomware activity. It is a preventative approach that can identify potential dangers before they impact specific systems, averting potential damage.

Suspicious network activity is one of the first signs of a ransomware attack. An intrusion detection system (IDS) scans the network for unusual traffic spikes—especially those headed to suspicious or blacklisted destinations. Upon detecting something unusual, it blocks the connection immediately and alerts the security team to investigate

Host-based Detection

Host-based detection focuses on monitoring and analyzing activities on individual devices to identify signs of ransomware. Host-based detection strategies can detect ransomware early and prevent data encryption by closely monitoring system behavior, file access, and modification activities.

An example of this would be a host-based antivirus solution that detects an unauthorized process attempting to modify any files, triggers an alert, and prevents potential ransomware encryption.

Cloud Backup Disaster Recovery

Cloud security acts as a watchtower, keeping an eye on ransomware threats across multiple devices at once. By analyzing massive amounts of data in real-time, cloud-based systems can spot unusual activity before an attack spreads. If ransomware is detected on one device, the cloud security system can immediately isolate it and prevent further infection. With cloud backup disaster recovery solutions in place, businesses can quickly restore lost data and minimize downtime.

For instance, a cloud-based security platform detects a ransomware attack on one device within a network and immediately disseminates threat intelligence and mitigation measures to other connected devices, effectively containing the spread of the ransomware.

Best Practices for Ransomware Detection

A good defense against ransomware includes both finding it and having a plan for backing up and recovering data. Reliable backups make it easy to get back lost data quickly, which cuts down on downtime and damage.

Ransomware threats can be found and stopped with good detection tools, but they are only one part of a full security plan. Finding threats isn't enough; companies must also follow best practices to stop them and lessen the damage they do. Companies can make their defense against malware stronger by using strong detection tools along with smart security procedures.

The following best practices enhance security posture and provide additional layers of protection against ransomware attacks:

Disaster Recovery Plan

Once ransomware locks up your files, there's no undo button. Either you restore from backups, or you're stuck deciding how much the data is worth. Solid disaster recovery planning means you're never in that position. Regular, automated backups let you wipe infected systems and restore clean data without scrambling for solutions or paying a ransom. The difference between a minor inconvenience and a full-scale disaster is whether that plan is in place before the attack happens.

Backup and Recovery

Regular backup testing ensures data integrity and minimizes risk. Disaster recovery software like Google Workspace Backup offers extra security with key apps and data remaining accessible even in the case of an attack. A disaster recovery plan includes secure off-site storage combined with regular testing to stop ransomware from disrupting business processes.

To lessen the impact of ransomware attacks, off-site storage, and frequent backups must be implemented in secure locations. Clean and recent backups can facilitate speedy system and data restoration in the event of such assaults, hence diminishing the strength of the ransomware attacker.

Software and Patch Management

Outdated software is a goldmine for ransomware. Every missed update leaves a security gap, and attackers know exactly where to find them. The longer a system goes without updates, the more vulnerable it gets. Keeping software, operating systems, and security patches up to date shuts down those entry points and keeps threats from taking hold in the first place. Patch management can be considered a proactive measure because it proactively reduces the attack surface and improves the security posture of a network or system.

Employee Education and Awareness

Employees are the first line of defense against ransomware. The majority of ransomware campaigns start out not with some complex exploit. They start with an email. A false invoice, a plea from someone who looks to be a manager, a seemingly harmless link. Someone clicks and, ta-da, the malware starts.

Security tools can only do so much if employees aren't trained to recognize these tactics. A well-trained team stops attacks before they ever have a chance to get past the inbox. So, security awareness training stops phishing and social engineering attacks via which ransomware is typically delivered. Additionally, regular phishing simulations and security drills make employees able to detect and avoid threats before they can cause any damage.

Keep Learning About Ransomware Protection

Ransomware threats continue to evolve. Combining traditional and advanced detection techniques enhances cybersecurity and reduces risks. A comprehensive business continuity and disaster recovery solution plan ensures resilience against attacks.

To further strengthen your knowledge and security posture, explore the following resources:

- ✓ Learn how a comprehensive system for email security can prevent advanced threats, such as spear phishing or ransomware.
- ✓ Learn how you can protect your business from ransomware.
- ✓ Get the latest digital security updates.

Subscribe to Blog RSS

Must Read Blog Posts

Demystifying Phishing Attacks: How to Protect Yourself in 2025

Must Read - How Phishing Emails Bypass Microsoft 365 Default Security

Must Read - Shortcomings of Endpoint Security in Securing Business Email

Must Read - What You Need to Know to Shield Your Business from Ransomware

Must Read - Email Virus: Complete Guide to Email Viruses & Best Practices

Must Read - Microsoft 365 Email Security Limitations You Should Know in 2025

Latest Blog Articles

8 Enterprise Email Security Best Practices to Prevent Cyberattacks

Understanding the Importance of Data Security in HRIS

The Hidden Risk: Leaked Employee Emails

Giovanni Bechis' Bold Plans to Transform SpamAssassin

Boost Your Network Security with These Proven Techniques

A Guide to Email Security: Training to Keep Your Team and Business Secure

Enhancing Email Security: The Role of Unified Observability in Microsoft 365

The Cloud Advantage: Boosting Your Business Email Security

Mastering Multi-Factor Authentication (MFA): A Step-by-Step Guide for IT and Security Admins

Speak with an Email Security Specialist

Let Guardian Digital help you accomplish your strategic business goals by safeguarding your most valuable assets — your employees — and your business information.

First Name

Last Name

Business Email Address

Contact Us

Have Questions or Comments?

☎ 1-866-435-4689

✉ hello@guardiandigital.com

f 𝕏 in

Subscribe to our Behind the Shield Newsletter

Email

Stay Informed!

Company

Customer Success Stories

About Us

Media Center

Press Releases

Resource Center

Our Philosophy

Partner Programs

Our Open-Source Philosophy: Development Without Limits

Newsletter Sign Up

Contact Us

Cyber/Email Security Resources Hub

Solutions

Advanced Threat Protection

Multi-tiered Security & Policy Controls

EnGarde Cloud Email Security

Microsoft 365 Protection

Real Estate and Title Companies: Secure Email Against Wire Transfer Fraud

Legal: Protect Email Against Cyberattacks and Data Leaks

Information Protection

Incident Response

Microsoft 365 Email Security

Google Workspace Email Protection

Guardian Digital vCISO Email Security Services

Services

Premium Support Services

Professional Engineering Services

Sign Up for Free Trial

Guide: Choosing a Business Email Security Solution

Email Risk Assessment Tool

Guardian Digital

Terms of Service / Privacy Policy / Cookie Statement / Site Map