Q

Quarantine Files: Restore, Delete, or Leave Isolated?

Learn what antivirus quarantine does, when an isolated file is safe to leave, and how to decide whether to delete or restore it without creating a security exception.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 What happens when a file is quarantined?

02 Should you delete, restore, or leave the file quarantined?

03 How to check a possible false positive safely

04 Why restoring or excluding a file can be dangerous

05 What to do if the quarantined file may have run

06 Why does the same quarantine alert keep returning?

07 Frequently asked questions

08 Authoritative guidance

Antivirus quarantine is a protected holding area for files that security software has detected or considers suspicious. The product normally blocks the item from running and moves it, renames it, encrypts it, or restricts access to it. A quarantined file is not the same as an active infection, but the alert still needs a decision based on the file's origin and what happened before detection.

In most cases, leave an unfamiliar item quarantined while you investigate. Delete it when it is unwanted or confirmed malicious. Restore it only when you have strong evidence that the detection is a false positive and you trust the exact file, not merely its filename.

01 What happens when a file is quarantined?

Quarantine is containment, not a verdict about every related risk. It prevents the isolated object from executing in its original location. It does not necessarily undo actions performed before detection, revoke stolen passwords, remove another payload, or repair settings changed by malware.

Status or action	What it means	When to use it
Quarantine	The item is isolated and normally cannot run	Default choice while the detection is reviewed
Delete or remove	The quarantined copy is permanently removed	Unknown, unnecessary, or confirmed malicious files
Restore	The file returns to its previous or chosen location	Only a well-supported false positive
Allow or exclude	Future scanning may ignore the file, folder, or behavior	Rarely, and only with a narrow, documented business need

Names vary by security product. For example, an interface may say Restore, Restore and exclude, Allow on device, or Add exception. Read the confirmation carefully: restoring and excluding are materially different actions.

02 Should you delete, restore, or leave the file quarantined?

1. **Identify the exact path and detection time.** A file in an email attachment, temporary directory, crack folder, browser download, or random startup location deserves more suspicion than a signed component in an expected application directory.
2. **Ask whether you intentionally obtained it.** If you do not recognize the file or no longer need it, keep it quarantined and delete it after any required investigation.
3. **Check what occurred before the alert.** If the file ran, a document enabled content, a password was entered, or unusual behavior began, handle the event as a possible compromise rather than a single-file cleanup.
4. **Verify the publisher and source.** Compare the digital signature, hash, version, and download location with the software vendor's official information. A familiar filename alone proves nothing.
5. **Look for independent confirmation.** Update the security product and rescan. Submit the file to the detecting vendor if it may be a false positive. In an organization, ask the security team to analyze it.
6. **Choose the least risky outcome.** Delete unwanted files; leave uncertain items isolated; restore only after the evidence supports it.

03 How to check a possible false positive safely

- Do not open, execute, or upload a confidential file to a public scanning service merely to test it.
- Record the detection name, file path, SHA-256 hash, product version, engine version, and security intelligence version.
- Obtain a fresh installer only from the publisher's official site or your organization's managed software catalog.
- Check the file's valid digital signature and confirm that its signer is the expected publisher.

- Search the detecting vendor's threat database and use its official false-positive submission process.
- For business software, test in an isolated analysis environment and document the approval before restoring.

A detection becoming less common on multi-engine services is not sufficient proof of safety. New malware may initially have few detections, and legitimate tools can be abused. Context, provenance, signature, behavior, and vendor analysis should agree.

04 Why restoring or excluding a file can be dangerous

Restoring makes the object accessible again. Adding an exclusion may also blind future scans to later versions or unrelated files in the same folder. Avoid excluding an entire Downloads, Temp, user profile, drive, or application-data directory. If an exception is unavoidable, scope it to the smallest verified object, record the owner and reason, and set a review date.

If an application stops working because one of its files was quarantined, do not immediately restore the file. Uninstall the affected application if necessary, obtain a clean current installer from the publisher, and reinstall after confirming that the detection is resolved.

05 What to do if the quarantined file may have run

1. Disconnect the device from networks if there are signs of credential theft, remote access, ransomware, or lateral movement.
2. Keep the item quarantined and run an updated full scan. Use the product's offline scan when persistent malware is suspected.
3. Review startup entries, scheduled tasks, browser extensions, recently installed applications, and additional detections.
4. From a known-clean device, change exposed passwords, revoke active sessions, and protect important accounts with multifactor authentication.

5. For a work device, preserve alerts and logs and contact the security team before deleting evidence or reimaging.
6. Rebuild or reset the system if high-impact malware executed, persistence remains, or trustworthy cleanup cannot be demonstrated.

06 Why does the same quarantine alert keep returning?

Repeated alerts can mean that a browser, email client, synchronization service, installer, scheduled task, or another compromised device is recreating the file. Note whether the path and hash stay the same. Remove the delivery source, update the affected application, clear the relevant cache only after preserving needed evidence, and scan connected or synchronized systems.

07 Frequently asked questions

Is it safe to leave files in quarantine?

Generally yes: properly quarantined items are isolated and cannot run normally. Keeping them temporarily is useful for review or restoration of a confirmed false positive. Delete them when they are no longer needed as evidence.

Can a quarantined file infect the computer?

The quarantined copy should be contained. However, it may have executed before detection, and related files or persistence may remain. Review the alert context and scan the system.

Will deleting quarantine damage Windows?

Deleting a genuinely malicious or unnecessary item should not. If a legitimate system or application file was detected incorrectly, deletion may break that component; verify and reinstall it from a trusted source instead of blindly restoring it.

Does uninstalling antivirus release quarantined files?

Behavior differs by product. Do not assume uninstalling restores or safely deletes everything. Resolve quarantined items using the product's documented controls before removal.

08 Authoritative guidance

- Microsoft Defender antivirus and antimalware FAQ
- Malwarebytes: Manage quarantined items
- ESET: Quarantine

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com