

Keep your files. Keep work moving.

An added layer of defense where ransomware strikes: your files.



THE PROBLEM

Hackers can lock, steal or destroy the files your team needs. Orders can stall. Staff may lose access to their work. Recovery costs grow while the clock runs. The damage can reach far beyond the IT team.

THE SOLUTION

RansomSnare watches how files are used. When it finds a harmful task trying to lock them, it stops the task and alerts your team. It adds file protection to the security tools you already use.

THE VALUE

Less damage can mean less time offline, less cleanup and less pressure to pay. The goal is simple: keep useful files within reach and help your team get back to work with less disruption.

— Protection for the files people need to serve customers and run operations.

More protection. Less to recover.

Spots file locking without needing a list of known threats.

01 Protect shared work

Helps protect shared folders where teams read and save files. Controls file changes at the storage layer, where those shared files live.

02 Block data theft tools

Blocks known or suspicious tools used to collect and send files outside your business. This helps close a path used to steal data.

03 Control harmful scripts

Stops unapproved scripts when they try to lock files. These small programs can run many tasks at once, which makes them useful to attackers.

04 Resist destructive attacks

Helps stop attacks that erase or damage files, including attacks that do not ask for money. The aim is to keep usable data intact.

THE BUSINESS

IMPACT

DOWNTIME

Fewer files to restore can help teams resume work sooner.

RECOVERY COST

Less damage can mean less cleanup and lost work.

INSURANCE

Clear test results can support talks about risk and coverage.

EXTORTION

Usable files may reduce the pressure to pay.

Insurance terms vary. Data theft remains a separate risk.

MINIMUM REQUIREMENTS

Processor: 1 GHz | **RAM:** 512 MB | **Storage:** 60 MB

Platform: Windows 10+ / Windows Server 2016+

Coming soon: Linux (RHEL and Debian variants) and macOS.

Send alerts to your security tools, ticketing system or support team. Manage alerts, agent health and settings from one console, with a view across your organization.

See it work. Measure the difference.

Test files affected, time to alert and recovery work in your environment.

[Request a live demo](#)

