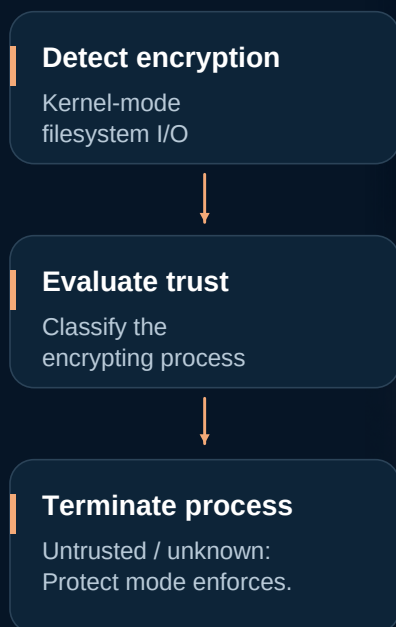


Two attack paths. One added layer.

Filesystem encryption detection and targeted exfiltration-tool controls add an enforcement layer alongside your existing endpoint defenses. [1, 2]

LOGICAL PROTECTION WORKFLOWS

01 / ENCRYPTION



Trusted
continue



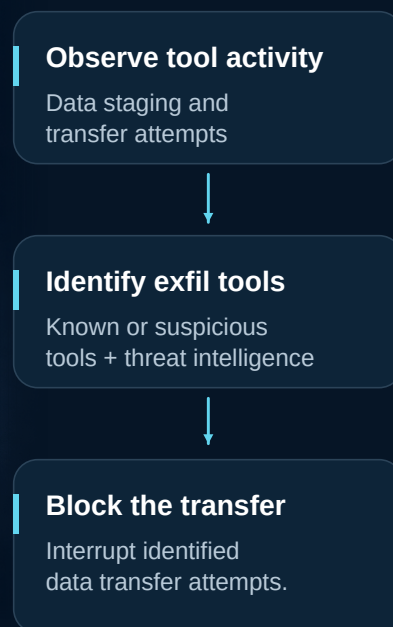
PROTECTED FILES

Windows endpoints + servers

• **ALERTS** Console / SIEM / SOAR / MDR

PROTECT MODE

02 / EXFILTRATION



Logical view. Enforcement and response depend on configured mode and policy.

ENCRYPTION DETECTION [1, 2]

The mathematical algorithm identifies file encryption without malware signatures. Process trust evaluation determines the response.

EXFILTRATION CONTROL [1]

Threat intelligence identifies known or suspicious staging and transfer tools, enabling targeted interruption of data theft attempts.

Deploy with intent. Validate the outcome.

Build the rollout around trusted workloads, enforcement settings and observable results.

01 Enforcement + recovery

Protect: terminates untrusted encryption; restores affected files from local pre-modification backups.

Alert-Only: reports events without termination or recovery. [2]

02 SMB file shares

Deploy agents on the server and clients requiring encrypted writes. Trust checks use bidirectional UDP 55999. Unmanaged clients cannot write encrypted files. [2]

03 Scripts + wiper attacks

Control encryption from unapproved PowerShell, Python and Bash interpreters. Apply Allow, Deny or Alert by agent, group or organization. Wiper protection targets malicious deletion and corruption. [1, 2]

04 SOC visibility

Manage alerts, agent status and configuration centrally. Route Windows System Event 739 or HTTPS webhooks to SIEM and automation. Integrate with existing SOAR, ticketing and MDR workflows. [1, 2]

DEPLOYMENT ESSENTIALS [2]

Platform: 64-bit Windows 10+ / Server 2016+.

Cloud: outbound HTTPS 443, TLS 1.2+.

Disconnected / self-hosted options are available. Validate trust coverage, update delivery and telemetry for the selected deployment.

MEASURE THE CONTROL, NOT JUST THE ALERT

FILES + PROCESSES

Record files affected, termination latency and recovery completeness.

DATA TRANSFERS

Test identified tools, approved workflows and custom transfer paths.

OPERATIONS

Check false positives, EDR coexistence, workload overhead and SOC delivery.

[1] SecuritySnares Datasheet 2.0 (supplied). [2] SecuritySnares User Guide, accessed 22 Sep 2026.

docs.securitysnares.com/docs/user_guide

Put the controls to the test.