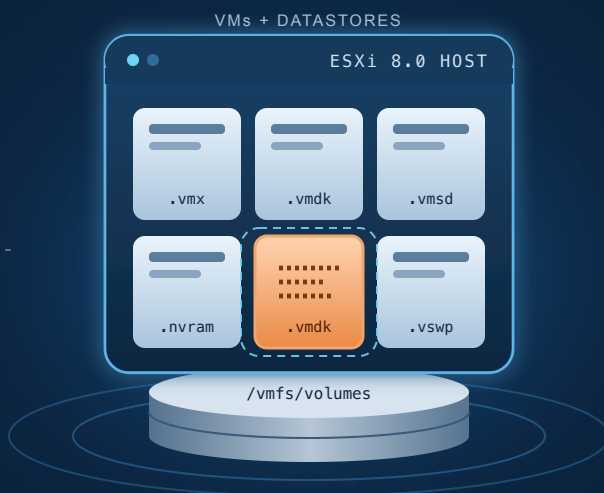
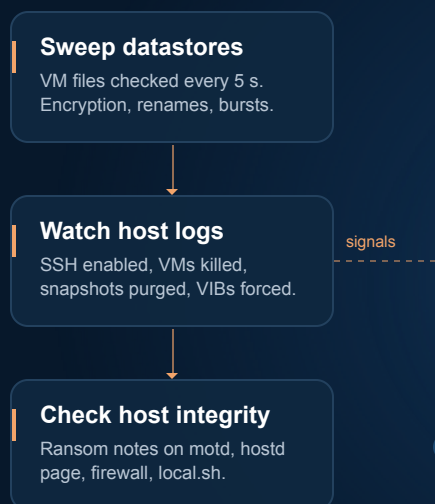


One host sensor. Every VM in view.

A lightweight sensor on each ESXi host monitors VM files, host logs and system files for the moves that come before and during VM encryption. An off-host controller watches for the ransomware TTPs that lead up to encryption and can stop the writer or keep a recovery copy.

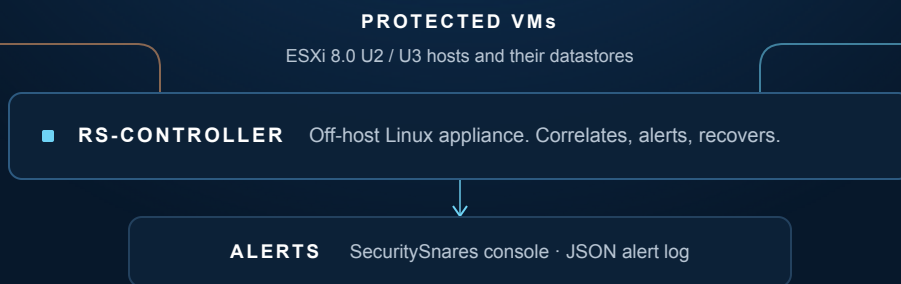
LOGICAL PROTECTION WORKFLOWS

01 / DETECT ON THE HOST



SENSOR + CONTROLLER

02 / WATCH + RESPOND



Logical view. Response depends on the options enabled for each host.

ENCRYPTION DETECTION

Every sweep runs the same mathematical algorithm that detects encryption in the RansomSnare Windows agent. It recognizes encryption itself, so it does not depend on knowing the ransomware family.

RANSOMWARE TTPs

Attackers prepare a host before they encrypt it: enabling SSH, killing VMs, deleting snapshots, loosening host software controls to install unsigned tools. The controller watches for these TTPs on each host and alerts on the build-up to encryption, not only the encryption itself.

Deploy host by host. Prove the response.

Install on each host, turn on response once you trust the detections, and measure the result.

01 Install live, enforce later

Install the rs-sensord VIB with esxcli on a running host, no reboot. Start with response off, review what the sensor detects on your own data, then enable it host by host. Maintenance windows keep patch-day admin work from looking like an attack.

03 Keep a recovery copy

Opt-in: on an attack alert the controller snapshots the affected VM, then clones or relocates it to another host or datastore. If an attacker deletes that snapshot, that raises its own alert. Restoring the copy stays a human decision.

02 Stop the writer

With kill enabled, the sensor terminates the process writing a file the algorithm detects as encrypted. hostd, vpxa and vmx are never killed, and kill pauses inside declared maintenance windows. Off by default.

04 Lightweight by design

The sensor is a small user-world daemon with no kernel module. In lab measurements it held about **4 MB** of memory and used under **0.25%** of one CPU core. It never opens a listening port on the host.

WHAT THE SENSOR WATCHES

A routine admin action alone does not raise an alert. The pattern does.

SOURCE	WHAT RAISES A SIGNAL
Datastores, every 5 s	Encryption of VM files · ransom-suffix renames · bursts of VM file changes
Host logs: preparation	VM power-off and process kill · SSH enabled · root password changed
Host logs: sabotage	All snapshots deleted · host software controls loosened · forced VIB install · execInstalledOnly disabled
Host logs: impact	Encryptor invocation (openssl enc, encrypt scripts) · datastore walks for .vmdk files
Host files	Changes to motd, hostd page, firewall rules, local.sh, esx.conf · ransom notes
Sensor health	Heartbeat every 60 s · a host silent for 3 minutes raises a SensorMissing alert

REQUIREMENTS

Hosts: ESXi 8.0 U2 or 8.0 U3. Any licence, including free hosts.
Host sensor: Secure Boot off; acceptance level CommunitySupported.
Controller: Linux container or VM on the management network; non-root.

CONNECTIVITY

Sensor → controller: 443/tcp, signed and replay-protected.
Controller → vCenter/ESXi: 443, for recovery.
Controller → SecuritySnare cloud: outbound 443.

Source: RansomSnare for VMware ESXi, Deployment and Administration Guide, Early Access, version 2026-10-11. Resource figures are lab measurements on the build tested; results vary with intervals, datastore size and workload.