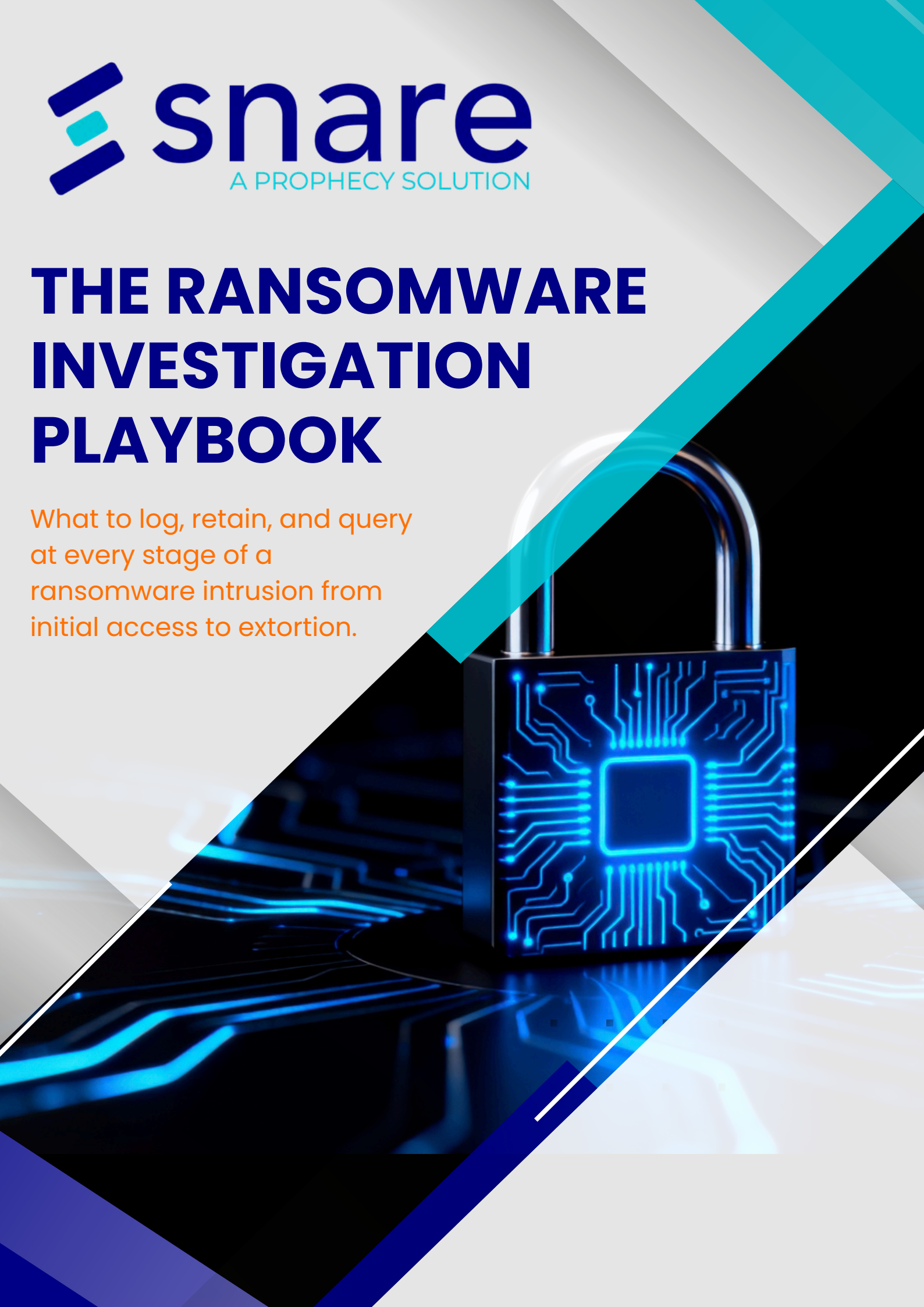
snare
A PROPHECY SOLUTION

THE RANSOMWARE INVESTIGATION PLAYBOOK

What to log, retain, and query at every stage of a ransomware intrusion from initial access to extortion.



Why This Playbook Exists

Ransomware has stopped being a single event. It is a multi-stage intrusion that, by the time encryption begins, has usually already involved credential theft, lateral movement, and data exfiltration.

Google Threat Intelligence Group found that 77% of the ransomware intrusions Mandiant responded to in 2025 involved suspected data theft, up from 57% in 2024, and virtualisation infrastructure was targeted in roughly 43% of incidents, up from 29% the year before. [1]

At the same time, Mandiant's M-Trends 2026 puts the mean time to exploit a newly disclosed vulnerability at negative seven days — down from 63 days in 2018 — meaning the reconnaissance-to-encryption clock is now frequently running before most organisations even know they have a problem. [2]
Encryption is the moment ransomware becomes visible. It is rarely the moment it began. Waiting for an encryption alert to start an investigation means starting the investigation last.

This playbook works backwards from that problem. It breaks a modern ransomware intrusion into seven stages, and for each one sets out:

- What the stage typically looks like in practice.
- The log sources that provide evidence of it — before, during, and after the fact.
- How long that evidence needs to be retained to still be useful.
- The specific questions an analyst should be able to answer once an investigation starts.

Throughout, we reference a real June 2026 intrusion — publicly documented by Symantec's Threat Hunter Team as the “Spirals” ransomware incident — in which attackers moved from an exposed IIS web server to full network encryption in under 24 hours. It is a useful spine for this playbook precisely because it was fast: every stage happened, but few of them had time to be noticed. [3]

How to use this playbook

Each stage chapter stands alone — use it as a reference the next time you're scoping log sources for a specific control, or work through it end-to-end as an audit of your current ransomware readiness. A consolidated log source matrix appears near the end for quick reference during tabletop exercises or actual incident response.

The Anatomy of a Modern Ransomware Intrusion

The seven stages below are not always sequential in the real world, attackers loop back, skip steps, or run several in parallel, but together they cover the evidence trail investigators most often need to reconstruct.

Stage	What Happens
1. Initial Access	Attacker gains an initial foothold, an exposed service, a phished credential, a vulnerable edge device.
2. Discovery, Credential Access & Persistence	Attacker maps the environment, dumps credentials and establishes a way back in.
3. Privilege Escalation & Defense Evasion	Attacker elevates access and starts disabling or blinding security controls.
4. Lateral Movement	Attacker spreads across the network using legitimate admin tools and tunnels.
5. Backup & Virtualisation Targeting	Attacker locates and disables recovery paths before deploying the payload.
6. Data Staging & Exfiltration	Attacker collects and exfiltrates data to support double-extortion.
7. Encryption & Extortion	Attacker deploys the payload and issues a ransom demand.

Stage 1 of 7

Initial Access

Every ransomware intrusion starts somewhere specific: an exposed service, a phished credential, or a vulnerable edge device. This is also the stage most likely to leave a clean, early signal, if the right logs are being collected.

Field Example, "Spirals" Ransomware, June 2026

The Spirals intrusion began at 22:21 local time when attackers compromised an internet-facing Microsoft IIS server and uploaded an ASP.NET web shell to establish a foothold, the single event the rest of the 24-hour intrusion depended on. [3]

What the Evidence Trail Looks Like

- Unusual inbound connections to internet-facing services outside normal patterns.
- Unexpected file uploads to web-accessible directories.
- New or modified files in web application directories shortly after suspicious inbound activity.
- Authentication attempts from unfamiliar geographies, ASNs, or at unusual hours.

Stage 1 of 7

Initial Access

Log Sources to Prioritise

- Web-access and application logs for internet-facing servers.
- Web application firewall (WAF) and reverse-proxy logs.
- File-integrity monitoring on web root and application directories.
- VPN and remote-access authentication logs.
- Edge device (router, firewall, VPN concentrator) configuration-change logs.

Retention guidance

Web-access and authentication logs for internet-facing systems should be retained for a minimum of 12 months, long enough to cover the negative mean-time-to-exploit window, where the record of first access may predate any detection.

Key Investigative Questions

1. What was the first anomalous request or authentication event and from where did it originate?
2. Was a new file created in a web-accessible directory in the hours before other suspicious activity began?
3. Were any internet-facing systems running software with a known, unpatched vulnerability at the time of access?
4. Did the same source IP or credential appear anywhere else in the environment afterward?

Stage 2 of 7

Discovery, Credential Access & Persistence

Once inside, attackers need to understand the environment and secure a way back in, even if their initial foothold is discovered and closed.

Field Example, "Spirals" Ransomware, June 2026

Within roughly three hours of establishing the web shell, the Spirals operator executed commands through the IIS worker process, spawning cmd.exe and PowerShell for reconnaissance, bypassing User Account Control, enabling Remote Desktop and creating a local persistence account. The attacker also dumped the SAM registry hive and LSASS process memory to extract credentials. [3]

What the Evidence Trail Looks Like

- Process execution from an unusual parent process (e.g. a web server process spawning a command shell).
- Access to credential stores, the SAM registry hive, LSASS process memory, or password managers.
- Creation of new local or domain accounts outside change-management processes.
- Reconnaissance commands: user, group and network enumeration.

Stage 2 of 7

Discovery, Credential Access & Persistence

Log Sources to Prioritise

- Endpoint process-creation and command-line logging.
- Windows Security event logs (account creation, credential access events).
- EDR/antivirus alerts and quarantine actions.
- Directory-service (Active Directory / identity provider) audit logs.

Retention guidance

Process-creation and command-line logs are high-volume and often the first candidate for aggressive filtering, but they are also the evidence most often needed to establish a credential-access timeline. Retain at least 90 days centrally, with the ability to extend retention on affected hosts once an investigation opens.

Key Investigative Questions

1. Did any process access LSASS memory or the SAM registry hive outside of expected administrative tooling?
2. Were any local or domain accounts created in the period surrounding the suspected initial access?
3. What commands were executed from the process that first showed anomalous behaviour?

Stage 3 of 7

Privilege Escalation & Defense Evasion

With a foothold and some credentials secured, attackers work to gain higher privileges and reduce the chance of being seen, often by disabling or bypassing the very tools meant to detect them.

What the Evidence Trail Looks Like

- UAC bypass techniques or unexpected elevation to SYSTEM/administrator context.
- Security-tool tampering: EDR or antivirus disabled, uninstalled, or its logging paused.
- Remote-access features enabled that were not previously in use (e.g. RDP turned on).
- Shadow-copy or Volume Shadow Copy Service (VSS) deletion commands.
- Local Windows Security event log cleared or its size/retention policy altered.

Stage 3 of 7

Privilege Escalation & Defense Evasion

Log Sources to Prioritise

- Endpoint protection platform (EPP/EDR) management console logs, tamper and status-change events specifically.
- Windows Event Logs for service start/stop and configuration changes.
- Windows Security Event Log clearing events (Event ID 1102) — the direct signal that an attacker has wiped the local event log, and the specific event this stage's retention guidance is written to defend against.
- Endpoint process-creation logging (Event ID 4688) to capture shadow-copy deletion commands such as vssadmin delete shadows and wmic shadowcopy delete.
- Group Policy and configuration-management change logs.
- Local firewall and RDP configuration-change events.

Retention guidance

Security-tool management and tamper logs — including Event ID 1102 log-clearing events — should be routed to a destination the attacker cannot reach or clear from the compromised host itself. Centralisation is the control here, not just retention length: a log the attacker can delete locally is only useful if a copy already left the host.

Key Investigative Questions

1. Was any security control disabled, uninstalled, or tampered with and by which account?
2. Were remote-access services enabled on hosts where they are not normally used?
3. Was shadow-copy deletion attempted on any host and did it succeed?
4. Was Event ID 1102 recorded on any host, and did centralised logging still capture that host's activity after the local log was cleared?

Stage 4 of 7

Lateral Movement

Attackers rarely stop at the first system. They move, usually with legitimate administrative tools, which is exactly what makes this stage hard to distinguish from normal IT activity.

Field Example, "Spirals" Ransomware, June 2026

The Spirals operator used WMI for remote execution alongside tunnelling and proxy tools, including revsocks, Chisel and Cloudflare tunnels, to move across more than a dozen systems before deploying the encryptor. [3]

What the Evidence Trail Looks Like

- Use of PsExec, WMI, or similar remote-execution tools outside their normal operational pattern.
- New outbound tunnelling tools (e.g. reverse-proxy or tunnelling utilities) connecting to unfamiliar external endpoints.
- A single account authenticating to an unusually large number of hosts in a short window.
- SMB or RDP connections between hosts that do not normally communicate.

Stage 4 of 7

Lateral Movement

Log Sources to Prioritise

- Windows Event Logs for logon type and remote-service execution (Events 4624, 4648, 7045).
- Network flow data (NetFlow/IPFIX) or firewall connection logs for east-west traffic.
- DNS query logs for unfamiliar or newly registered domains.
- Endpoint process-creation logs for remote-execution utilities.

.

Key Investigative Questions

1. Which hosts did the compromised account or process touch and in what order?
2. Were any unfamiliar tunnelling or remote-access utilities introduced onto the network during this period?
3. Is there a common administrative tool or credential linking activity across multiple hosts?

Stage 5 of 7

Backup & Virtualisation Targeting

Modern ransomware operators assume you have backups and they go looking for them, along with the virtualisation layer that can multiply the impact of a single compromise across dozens of systems at once.

What the Evidence Trail Looks Like

- Use of PsExec, WMI, or similar remote-execution tools outside their normal operational pattern.
- New outbound tunnelling tools (e.g. reverse-proxy or tunnelling utilities) connecting to unfamiliar external endpoints.
- A single account authenticating to an unusually large number of hosts in a short window.
- SMB or RDP connections between hosts that do not normally communicate.

Stage 5 of 7

Backup & Virtualisation Targeting

Log Sources to Prioritise

- Backup software management-console audit logs.
- Hypervisor (e.g. vCenter, Hyper-V) administrative and authentication logs.
- Storage-array and datastore access logs.
- Privileged access-management logs covering backup and virtualisation admin roles.

.

Retention guidance

Virtualisation infrastructure was targeted in roughly 43% of the ransomware incidents Mandiant responded to in 2025, up from 29% the year before, this stage's logs are frequently the ones organisations discover, too late, that they never collected centrally.

Key Investigative Questions

1. Were backup jobs, schedules, or retention settings modified or deleted and by whom?
2. Did any account access the hypervisor management plane outside its normal pattern?
3. Are immutable or offline backup copies confirmed intact and unaffected?

Stage 6 of 7

Data Staging & Exfiltration

In the large majority of ransomware intrusions today, data theft happens before, or instead of, encryption. This stage is the evidentiary basis for understanding exactly what was taken, which drives regulatory notification obligations as much as it drives the security response.

Field Example, "Spirals" Ransomware, June 2026

The Spirals attackers stole data before encrypting the network, then used the theft as extortion leverage, the ransom note (RECOVERY_SECTION.log) threatened to leak the stolen data within six days if the ransom went unpaid. [3]

What the Evidence Trail Looks Like

- Large-scale file enumeration or bulk access to file shares outside normal usage patterns.
- Compression or archiving of large volumes of data shortly before outbound transfer.
- Unusually large or sustained outbound data transfers, particularly to cloud storage or file-sharing services.
- Use of legitimate but unexpected exfiltration channels (cloud sync clients, remote-access tunnels).

Stage 6 of 7

Data Staging & Exfiltration

Log Sources to Prioritise

- File-share and NAS access logs (who accessed what and how much).
- Data loss prevention (DLP) alerts and network egress logs.
- Cloud storage and SaaS application audit logs (uploads, sharing events).
- Proxy and firewall logs for outbound data volume by destination.

Retention guidance

Outbound data-volume and file-access logs should be retained for at least 12 months, this is the evidence set regulators and legal counsel will ask for first, often well after the initial incident response has concluded.

Key Investigative Questions

1. What data was accessed and can the scope be bounded by file share, database, or application?
2. How much data left the environment, to which destination and over what time window?
3. Does the exfiltration timeline overlap with the credential-access and lateral-movement evidence gathered earlier?

Stage 7 of 7

Encryption & Extortion

By the time encryption begins, the investigation's most important work, establishing entry point, scope and data exposure, should already be well under way. This stage confirms impact and triggers recovery, but it should rarely be the first indication that something is wrong.

Field Example, "Spirals" Ransomware, June 2026

Spirals is written in Rust and encrypts files using a separate AES-128 key per file, wrapped with an attacker-controlled ECDH P-256 public key; files larger than 5 MB are encrypted in chunks to speed up the process. From the initial IIS web shell to full network encryption, the entire intrusion took under 24 hours. [3]

What the Evidence Trail Looks Like

- Mass file-modification events across multiple hosts in a short window.
- New or unfamiliar file extensions appearing on a large number of files simultaneously.
- Ransom-note files created in multiple directories or hosts near-simultaneously.
- A sudden spike in disk write activity across many endpoints at once.

Stage 7 of 7

Encryption & Extortion

Log Sources to Prioritise

- File-integrity monitoring and mass file-modification detection.
- Endpoint telemetry for the encryption process itself (parent process, command line, file-write patterns).
- Centralised logging infrastructure status, confirm collection was not disrupted during the encryption event.
- Network logs covering the final hours before encryption, to close any remaining gaps in the timeline.

.

Key Investigative Questions

1. Which host encrypted first and does that align with the lateral-movement evidence gathered earlier?
2. Was the logging pipeline itself disrupted or targeted during this stage?
3. Is there a complete, end-to-end timeline from initial access through to encryption and where are the remaining gaps?

The Snare Perspective

Building an Investigation-Ready Logging Architecture

Every stage in this playbook depends on the same underlying requirement: the right events, from the right sources, retained for long enough and searchable quickly once an incident begins. That is an architecture problem, not just a retention-policy problem.

Sending every available event into the SIEM at full volume does not solve it, it usually makes the searches slower and the signal harder to find. Snare helps organisations manage the full logging lifecycle so that the evidence in this playbook is there when it's needed:

SNARE AGENT	Collect detailed security and audit events from endpoints and systems close to the source, including the process-creation, credential-access and file-integrity events every stage of this playbook depends on.
SNARE CENTRAL	Centrally manage logging policy so backup, virtualisation, edge-device and identity sources are collected consistently, not just the sources that happen to be easiest to reach.
SNARE REFLECTOR	Filter, transform and route log data so high-value evidence reaches the SIEM and long-term storage without the noise that drives up cost and slows down search.
ASKSNARE	Turn the investigative questions in each stage of this playbook into natural-language queries against retained log data, reducing the time spent translating a question into platform-specific syntax.

Quick-Reference: Log Source Matrix

A consolidated view of the sources referenced throughout this playbook. Use it as a checklist during a tabletop exercise, or as an audit of your current collection against a ransomware scenario.

Log Source	Relevant Stage(s)	Min. Retention*	Priority
Web-access / WAF logs	1. Initial Access	12 months	Critical
VPN & remote-access auth	1. Initial Access	12 months	Critical
Endpoint process-creation	2, 3, 7	12 months	Critical
Windows Security event logs	2, 3, 4	12 months	High
Directory-service audit logs	2	12 months	Critical
EDR/EPP tamper & status events	3	12 months	Critical
Network flow / firewall east-west	4	90 days+	High
DNS query logs	4	90 days+	Medium
Backup management console audit	5	12 months	Critical
Hypervisor admin & auth logs	5	12 months	Critical
File-share / NAS access logs	6	12 months	High
DLP & network egress logs	6	12 months	High
Cloud storage / SaaS audit logs	6	12 months	Medium
File-integrity monitoring	1, 7	90 days+	High

*** Minimum retention reflects the evidence window needed to investigate, not a compliance minimum, align final retention with your regulatory obligations and Snare Reflector routing policy. PCIDSS and other standards do call for a min of 12 months for most logs.**

Next Steps

This playbook maps the evidence a ransomware investigation needs. Whether you're auditing current coverage, building a tabletop exercise, or responding to a live incident, the same underlying question applies:

> **if this happened to you tonight, could your team answer every question in this playbook by tomorrow morning?**

Put this playbook into practice

See how Snare Agent, Central, Reflector and AskSnare work together to keep this evidence collected, retained and queryable, before you need it.

Request a Snare and AskSnare demonstration
|Download the Investigation-Ready Logging Checklist
| Read Snare Insider Issue 13

References

[1] Google Cloud Blog / Google Threat Intelligence Group, "Ransomware Tactics, Techniques and Procedures in a Shifting Threat Landscape," 16 March 2026. https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape
[2] Google Cloud Blog / Mandiant, "M-Trends 2026: Data, Insights and Strategies From the Frontlines," 23 March 2026. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026
[3] BleepingComputer, "New Spirals ransomware encrypts victim network in under 24 hours," 16–17 July 2026, reporting on analysis by Symantec's Threat Hunter Team. https://www.bleepingcomputer.com/news/security/new-spirals-ransomware-encrypts-victim-network-in-under-24-hours/amp/
[4] Cybersecurity and Infrastructure Security Agency (CISA), NSA, FBI and MS-ISAC, "#StopRansomware Guide." https://www.cisa.gov/resources-tools/resources/stopransomware-guide

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

snare
A PROPHECY SOLUTION