Controlled networks | Technology Focused Cloud Driven.

EVIDENCE & INVESTIGATION

TWELVE MONTHS OF FIREWALL LOGS · ILLUSTRATIVE

STILL ON THE DEVICE



Intrusion begins
The records that explain it are overwritten

Breach discovered
Investigators ask for the logs

~~Month 1 · 02:14:07~~	~~vpn-gateway~~	~~Login accepted from new location~~	~~OVERWRITTEN~~
~~Month 1 · 02:31:52~~	~~file-server-02~~	~~Privileged account created~~	~~OVERWRITTEN~~
Month 12 · 09:03:18	file-server-02	Mass file modification detected	AVAILABLE

FORENSIC LOG RETENTION

The breach was months ago. Do you still have the logs?

Many intrusions are found weeks or months after they start. Forensic Log Retention keeps the evidence: collected off the source systems, protected against tampering and searchable when an investigator, auditor or insurer asks what happened.

WHY THE EVIDENCE IS USUALLY GONE

01

Devices overwrite their own history

Firewalls, servers and switches keep a limited local log and rotate it. The week you need may already be gone.

02

Attackers clean up after themselves

Logs stored on a compromised system can be edited or wiped by whoever controls that system.

03

Scattered logs do not make a timeline

Separate consoles, formats and clocks turn one investigation into a dozen manual searches.

Know what you could prove tomorrow.

800-700-7500
www.controllednetworks.com

What Forensic Log Retention gives you

One protected record of what happened across your environment, kept for as long as your policy, contracts and regulators require.

Centralized collection

Firewall, server, network, identity and application events gathered in one place, off the systems that produced them.

Long-term retention

A searchable tier for recent activity and an archive tier for the long term, sized to your data volume.

Tamper-evidence controls

Access control, integrity checks and protected storage, so any change to a record can be detected.

Incident investigation

Authorized analysts search timelines and correlate sources to reconstruct who did what, and when.

Legal hold

A defined process to freeze scoped records when normal retention has to be suspended.

Evidence export

Controlled delivery of the relevant records with a documented access history and chain of custody.

WHO WILL ASK YOU FOR THE LOGS

Incident responders

To scope what was touched, when it started and whether it is over.

Auditors and regulators

To see that your controls were operating over the whole period.

Cyber insurers

To support a claim with a record of the event.

Legal counsel

To preserve records under hold and answer discovery.

HOW WE WORK

01

Inventory

We map your log sources and find the gaps in coverage.

02

Model

Data volume, retention periods and search-versus-archive tiers.

03

Build

Collection, protected storage, access and integrity controls.

04

Operate

We watch collection health and support investigations and exports.

Request a forensic logging and retention assessment.

We look at what you log today, how long it survives and who could alter it, then show you the gaps.

800-700-7500

www.controllednetworks.com

325 S. River St., 2nd Floor, Hackensack, NJ 07601

Retention periods vary by industry, regulation and contract. Whether records are admissible as evidence also depends on collection method, custody and applicable rules.

© 2026 Controlled Networks Solution LLC (CNS). All rights reserved.