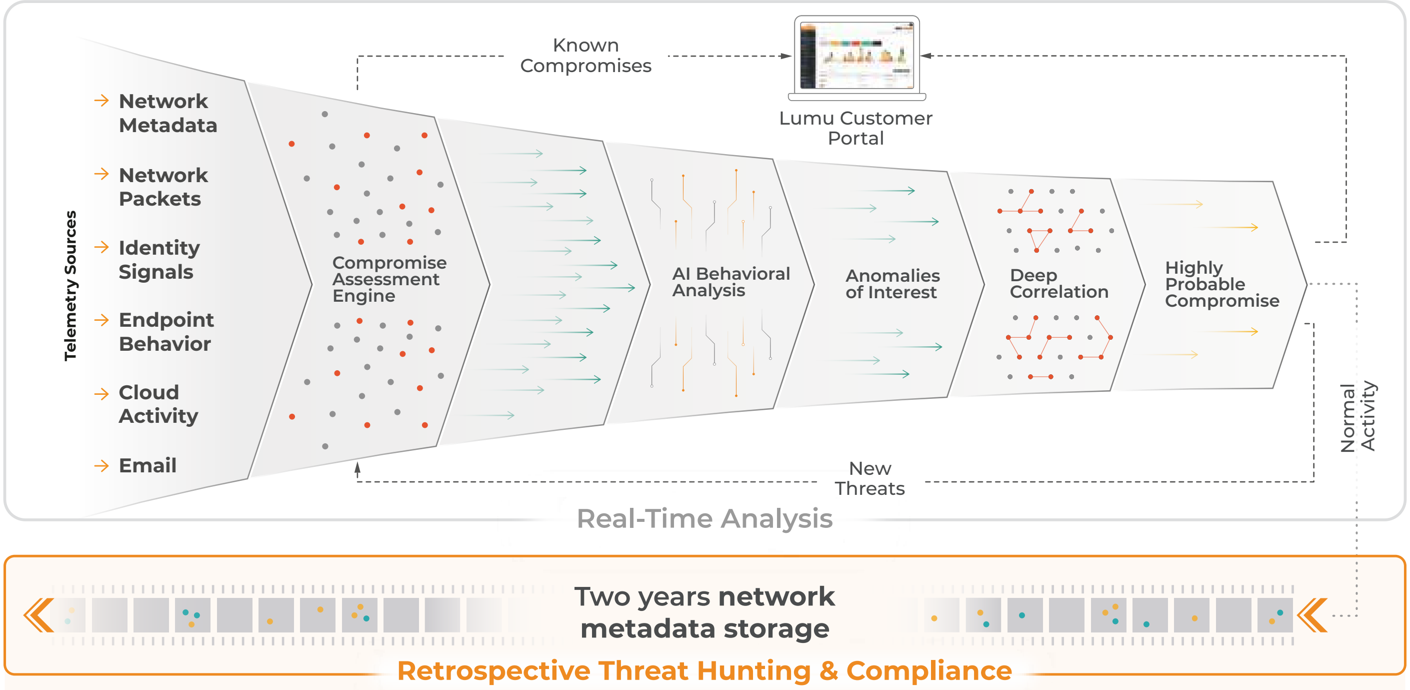
Lumu Archive

Log retention is required for compliance. Lumu Archive is a feature that collects, analyzes, and stores network logs, turning them into actionable threat intelligence.

How It Works



Lumu Defender analyzes network metadata in real time to identify confirmed compromises. Archive takes this further by storing network data for up to two years and continuously cross-referencing it against emerging threats. This ensures security teams detect past compromises linked to evolving attack techniques.

Network Log Storage

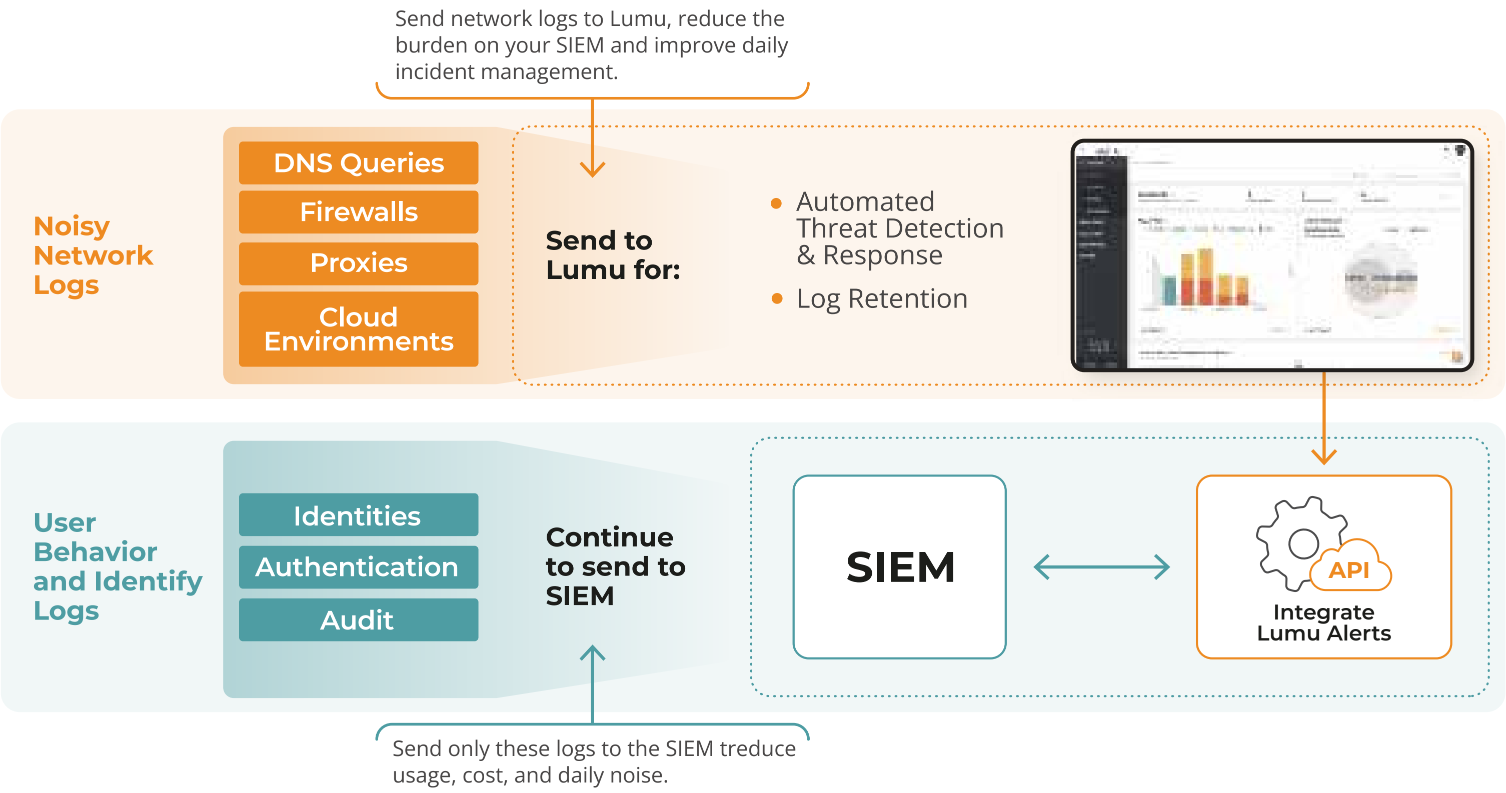
An optimized approach to retaining noisy network logs, like DNS, firewall, proxies, and cloud data for up to two years, ensuring compliance and visibility.

Retrospective Analysis

Uncovers novel attacks and zero-day attacks by continuously analyzing historical network logs and comparing them against the latest threat indicators.

Offload Noisy Logs to Lumu Archive

Lumu Archive offloads high-volume network logs like DNS, firewall, and proxy data, reducing SIEM storage costs while preserving full security visibility. It ensures continuous analysis of historical data against emerging threats, optimizing both cost and threat detection.



Send network logs to Lumu, reduce the burden on your SIEM and improve daily incident management.

Send only these logs to the SIEM treduce usage, cost, and daily noise.

Key Benefits

Retrospective Threat Detection

Even the newest, most sophisticated attacks leave clues. Lumu scans your historical logs for emerging IoCs, uncovering previously hidden threats and zero-day attacks.

Unlimited Log Access

Your logs are always available. Query and analyze them anytime, with no limitations on log requests.

2-Year Log Retention

Maintain compliance and support investigations with up to 2 years of log storage.

Reduced SIEM Storage

Offload your network logs to Lumu and eliminate the need to store duplicates in your SIEM, reducing costs and complexity.

Compliance Enablement

No matter which frameworks, Archive ensures that you comply with requirements for network log storage.

Faster Incident Response

Quickly query historical data to pinpoint the source and scope of an attack, accelerating your response and minimizing damage.