Gigamon ThreatINSIGHT Retention Options Overview

Gigamon ThreatINSIGHT™ retention options are designed to meet all security and incident response use cases to combat cyber adversaries in the present, the future and the past. Built by responders, for responders, ThreatINSIGHT collects, indexes and stores near PCAP-level network metadata in the INSIGHT Cloud Data Warehouse to facilitate behavioral threat detection and rapid, informed response. All metadata is further enriched with entity and third-party intelligence to provide the added context for both detections and response actions.

Within the INSIGHT Cloud Data Warehouse, the ThreatINSIGHT solution's machine learning, behavioral analysis and threat intelligence detection engines are applied against each client's individual network metadata, as well as collective crowdsourced network metadata to identify emerging and otherwise unknown threats.

The INSIGHT Cloud Data Warehouse also enables advanced investigation and threat hunting capabilities through robust metadata query and faceted search results. With an average client query response time of 1.5 seconds, ThreatINSIGHT provides incident responders the ability to rapidly discover and understand a threat actor's complete activity to facilitate informed response.

To fit the requirements for all clients, ThreatINSIGHT offers three metadata retention options:

Metadata Retention Options	Description
Unlimited detection | 7-day investigation	• Unlimited storage of all detection related enriched network metadata • 7 days retention of all enriched network metadata activity to enable threat hunting and complete incident investigation
Unlimited detection | 30-day investigation	• Unlimited storage of all detection related enriched network metadata • 30 days retention of all enriched network metadata activity to enable threat hunting and complete incident investigation
Meta Stream | Unlimited historical metadata acess	• Optional: In addition to either the 7- or 30-day investigation options, Meta Stream enables the export of all enriched network metadata for long-term historical analysis and retention requirements • Indefinite retention of all detection related enriched network metadata

The key benefits of each option include:

Metadata Retention	Unlimited Detection 7-Day Investigation	Unlimited Detection 30-Day Investigation	Meta Stream
High fidelity threat detections	✓	✓	
Threat triage	✓	✓	
Threat investigations	7 Day	30 Day	
Threat hunting	7 Day	30 Day	
Full scope of threat actor's activity		✓	
Long-term historical analysis			✓
Compliance retention requirements			✓

Learn more at gigamon.com/threatinsight.

REQUEST A DEMO AT GIGAMON.COM/DEMO.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com