LUMU | Gigamon®

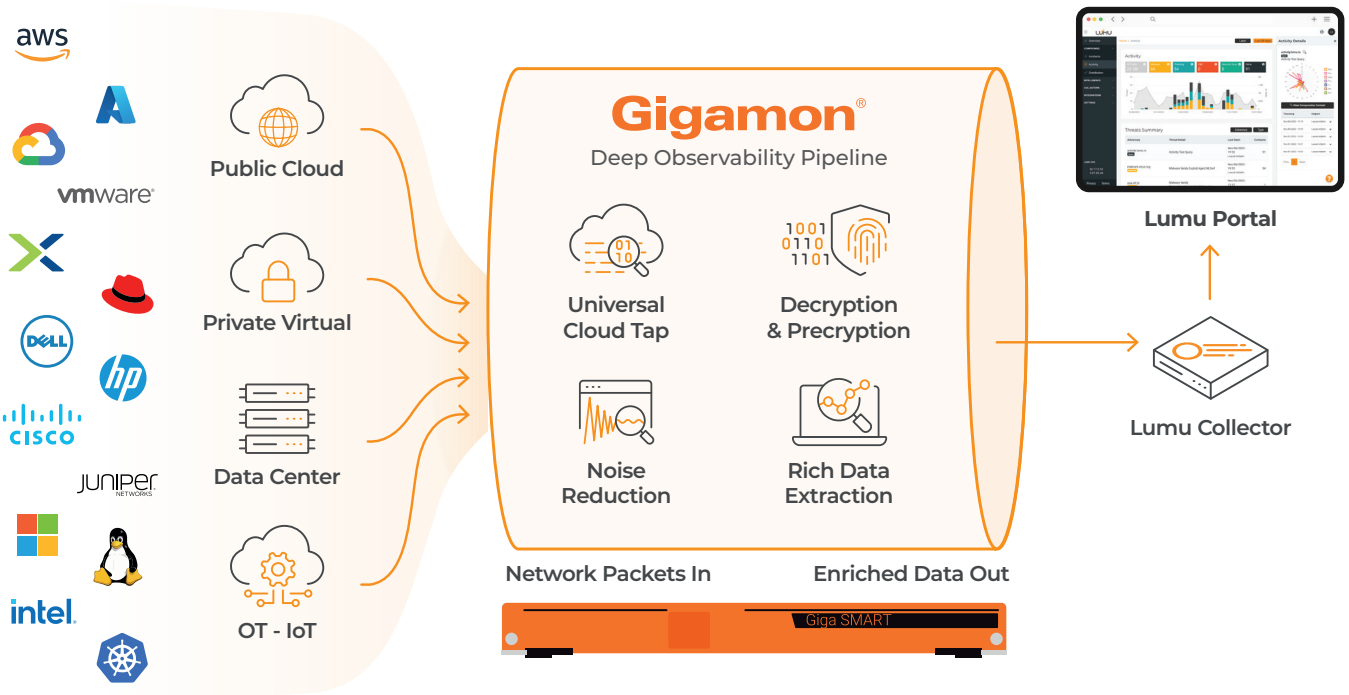
Combining Continuous Compromise Assessment™ and Deep Observability for Seamless Network Detection and Response

OVERVIEW

Organizations face increasingly complex infrastructures, blind spots, and an ever-evolving threat landscape. For those already leveraging Gigamon's Deep Observability Pipeline, Lumu's Continuous Compromise Assessment offers a powerful way to analyze the network metadata being collected and decrypted.

By combining Lumu's ability to assess compromise continuously with Gigamon's simplified visibility into complex systems and efficient data processing, organizations gain a unified solution to combat modern cybersecurity challenges proactively.

HOW IT WORKS



Traffic Capture and Processing

Gigamon captures 100% of network traffic and reduces data complexity through deduplication and flow optimization, but does not identify confirmed compromises.

Metadata Analysis

Gigamon collects and decrypts network flows and feeds it to Lumu, which analyzes it using the Illumination Process™ to detect confirmed compromises in real time.

Threat Response

When Lumu identifies compromises, it triggers an automated response to block or mitigate threats, integrating with existing 3rd party solutions to immediately block threats.

FROM BLIND SPOTS TO ACTIONABLE THREAT DETECTION & RESPONSE

Modern cybersecurity teams face significant challenges due to the growing complexity of infrastructures and the sophistication of threat actors. Key issues include:

- **Decryption Challenges:** Special deployments might require data decryption, adding costs, complexity, and time to achieve full visibility.
- **Complex Networks:** Complex hybrid and multi-cloud environments create blind spots, and duplicated data, complicating data collection and detection.
- **Data Overload:** Redundant or irrelevant data hinders efficiency and increasing storage and processing costs.
- **Inefficient Threat Response:** Data overload delay the detection and mitigation of threats, increasing the risk of breaches and false positive rates.

The integration of Lumu with Gigamon's Deep Observability Pipeline provides a unified approach to addressing these challenges:

- **Centralized Decryption:** Gigamon sends decrypted traffic to Lumu, eliminating blind spots while reducing the burden of licensing and processing costs.
- **Comprehensive Visibility:** Gigamon delivers end-to-end traffic visibility, ensuring no data source is overlooked, from on-premises networks to multi-cloud environments.
- **Optimized Data Processing:** Gigamon reduces data volumes by up to 60% through deduplication and intelligent filtering, ensuring only actionable data reaches Lumu.
- **Real-Time Compromise Assessment:** Lumu continuously analyzes and enriches metadata, identifying confirmed compromises and enabling faster, automated responses.

CHALLENGES OVERCOME

- **Ransomware Defense:** Detect early signs of sophisticated ransomware including lateral movement and command and control. Gigamon decrypts traffic; Lumu identifies threat actors in the network.
- **Encrypted Traffic Visibility:** Gigamon decrypts encrypted traffic for analysis. Lumu uncovers hidden threats and provides actionable insights.
- **Optimized Security Tool Performance:** Gigamon reduces redundant data, increasing cost efficiency. Lumu focuses on actionable insights for faster detection and reduces the cost of storing network logs by offloading them from the SIEM.
- **Compromise Detection in Hybrid Environments:** Monitor hybrid and multi-cloud traffic in real time. Gigamon feeds enriched metadata to Lumu for holistic continuous threat detection.

CONCLUSION

Cybersecurity leaders need good data and good analysis. Gigamon delivers unified visibility across complex environments and all network levels. Lumu provides machine-speed analysis, enriched insights, and the ability to respond to threats in real time. Together, they empower organizations to stay ahead of modern cyber threats.

Lumu Technologies Inc. | 8600 NW 36th St., Suite 150 Doral, FL 33166 | sales@lumu.io | +1 (877) 909-5868