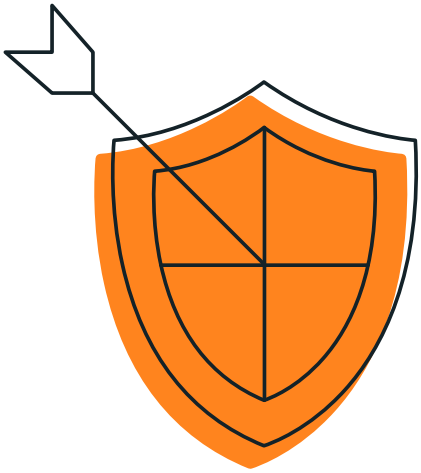
Gigamon® | Trinity Cyber

Neutralize Threats Inflight with Gigamon and Trinity Cyber



THE CHALLENGE

To secure their networks, organizations are often forced to react to threats, using inefficient processes and manual incident response. As a result, network vulnerabilities are overlooked and threats are missed. To enhance security, organizations must actively manage threats with automated processes.

THE SOLUTION

Trinity Cyber and the Gigamon Deep Observability Pipeline work together to improve your overall security posture, enhance appliances and services, save you time and money on incident response and false positives, and improve business continuity. The joint solution is a fundamental component of a Zero Trust Architecture and complements Secure Access Service Edge (SASE) initiatives.

JOINT SOLUTION BENEFITS

+ Provides network detection with endpoint fidelity of in-bound and out-bound traffic at greater than 99.9 percent accuracy
+ Automates detection and response actions in one move
+ Empowers automated response actions at the perimeter beyond block/alert
+ Neutralizes remote code execution, data exfiltration, and embedded malicious code

Introduction

Trinity Cyber offers a breakthrough detection and automated threat response technology that identifies hacking techniques and threats, neutralizes them, and transforms malicious internet traffic in-flight at line speed. Gigamon provides inline traffic acquisition and filtering, powering Trinity Cyber's ability to scan and manipulate packets.

The Gigamon + Trinity Cyber Joint Solution

Key Gigamon Deep Observability Pipeline features that enhance Trinity Cyber include:

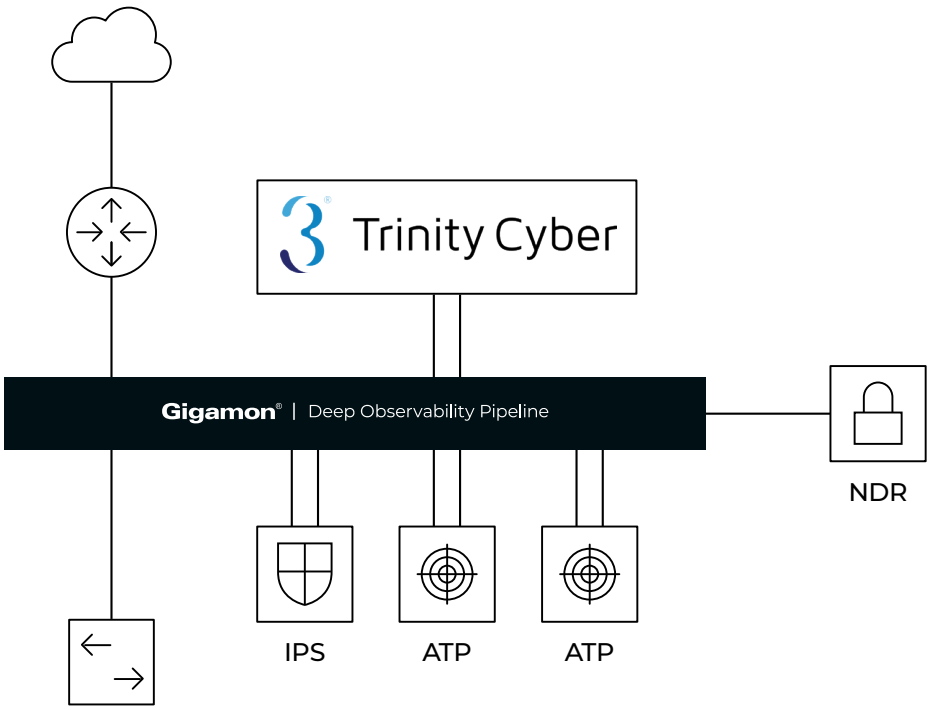
+ **Easy Access to traffic from a physical network:** The Gigamon Deep Observability Pipeline enables traffic from across the network to be managed and delivered to tools efficiently and in the format they need.
+ **Easy access to traffic from a virtual network:** East-West data center traffic is growing increasingly fast. Gigamon can tap this traffic and incorporate it into the Gigamon Deep Observability Pipeline for delivery to the tools you are using on the physical network. That ensures all traffic can be monitored and analyzed together, preventing blind spots, increasing the likelihood of spotting suspicious behavior, and eliminating the need to learn a new set of tooling for virtual environments.
+ **Flow and metadata (NetFlow/IPFIX/CEF) generation:** Gigamon devices can generate unsampled NetFlow/IPFIX flow data and/or IPFIX/CEF metadata for any traffic flow. The Gigamon Deep Observability Pipeline can generate extended metadata records for things like HTTP response codes and DNS queries. This extended metadata can be used to provide far more detailed contextual analysis when looking at network and security events.

How It Works

The Trinity Cyber premise is straightforward: Every Internet session can and should be fully staged, parsed and deeply inspected inline (not in a sandbox) in context, with endpoint and application layer fidelity, before it enters or leaves a customer's control. At the same time, automated processes must be run to remove or alter malicious content from files and protocol fields at speed and scale to affect the outcome in favor of the customer. And, this must be done without introducing latency or degrading the customer's Internet experience. This is what a combined solution with Trinity Cyber and Gigamon provides – a preventive control that delivers clean traffic and files, inline with no noticeable latency.

Customers take advantage of a Gigamon platform to provide inline bypass and service chaining capabilities. Ideally, that Gigamon device will also provide inline SSL (iSSL) decryption capabilities so traffic can be handed off to Trinity Cyber unencrypted. The Trinity Cyber solution applies its patented threat prevention technology to the traffic. Depending on the threat, Trinity Cyber can not only block or allow traffic, but can replace, remove or modify malicious sections of the traffic allowing the remaining benign transmission to continue to its destination. This maintains business continuity in real-time without alerting an adversary to the presence of the protection or exposing network vulnerabilities.

All processed traffic can then be handed back to the Gigamon node for processing through other elements in the service chain.



For more information on Gigamon and Trinity Cyber, visit: gigamon.com and trinitycyber.com.

Gigamon®

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