JOINT SOLUTION BRIEF

Speed Malware Incident Response with Better Traffic Insight and Context from Gigamon and Plixer

The Challenge

Uncovering unwanted or malicious behaviors has never been more difficult. With similar traffic patterns to those of normal communications coming from end systems, low-and-slow attacks and data thefts have become commonplace.

The Solution

Integrated with the Gigamon Visibility Platform, the Plixer Scrutinizer Incident Response System provides the forensic details to perform root-cause analysis in seconds.

Joint Solution Benefits

- Plixer leverages the Gigamon platform's automatic traffic load balancing and aggregation functionality to reduce bottlenecking and port oversubscription
- With the Gigamon platform's real-time SSL decryption functionality, Scrutinizer provides customers with increased visibility into traffic without performance degradation
- The Gigamon platform accelerates processing throughput by effectively filtering and distributing relevant traffic from across the network to Scrutinizer
- Fully integrated with Gigamon Application Metadata to provide Scrutinizer with access to deep insights into network behavior.

Introduction

Security infections and low-and-slow data thefts are no longer merely possible, they are almost a certainty. Not only are they widespread, but the traffic patterns of these bad communications often mimic those of normal, good traffic coming from end systems. For organizations, the ability to separate good from bad has become more difficult than ever before.

When problems arise, whether device-, application-, or security-related, IT teams need better insight and context in order to uncover unwanted or malicious behaviors. In other words, they need Scrutinizer. When coupled with the Gigamon Visibility Platform, Scrutinizer delivers the forensic data necessary to rapidly perform root-cause analysis and help select the best course of action, dramatically reducing time-to-resolution.

The Gigamon and Plixer Joint Solution

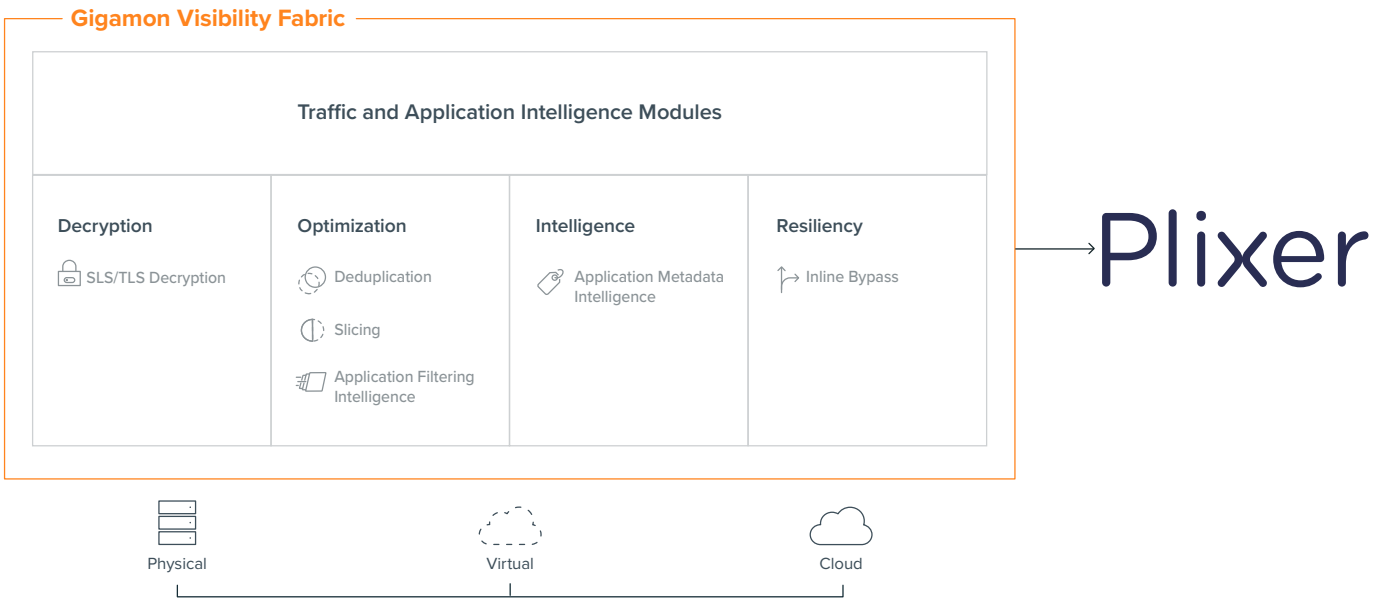
As the foundation of the Plixer incident response and behavior analysis architecture, Scrutinizer performs the collection, threat detection, and reporting of all flow technologies—NetFlow, IPFIX, and metadata—on a single platform. Unlike legacy, all-in-one solutions that cannot keep pace in today's sophisticated and complex threat environments, Scrutinizer excels at delivering real-time context and situational awareness. Detailed forensic analysis is provided through the identification of applications, conversations, traffic flows, protocols, end users, subnets, domains, and countries of origin. Scrutinizer can also create reports on historical network traffic, monitor jitter and latency, and issue alerts on suspicious behavior.

By supporting millions of flows per second, Scrutinizer delivers deep visibility and context into events that organizations can use to quickly identify root cause, minimize the impact of cyber threats, and optimize business application performance. With just a few clicks, IT teams can view a DVR-like graphic replay of events, inclusive of granular, corresponding forensic details, that lets them rapidly respond to incidents. For compliance-minded companies, Scrutinizer can also verify the enforcement of security policies and controls.

Integrated with the Gigamon Visibility Platform, which delivers the right traffic at the right time (including Application Metadata), Scrutinizer analyzes that traffic and metadata to provide deep forensic details and reporting. As critical pieces of any comprehensive security architecture, Gigamon and Plixer move end users from a perimeter-based, static policy-enforcement mindset to one that focuses on internal physical and virtual infrastructure asset monitoring.

Key Gigamon Visibility Platform features that augment the value of Plixer technology deployments include:

Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single tool can manage, the Gigamon platform can be used to split the flow across multiple tools, while keeping sessions together and tool numbers can be incrementally grown by adding new devices to those already connected.



SSL decryption: Real-time SSL decryption integration increases traffic visibility for Scrutinizer, broadening the scope for incident response and behavior analysis.

Filtering traffic to only send relevant traffic: The Gigamon platform can be configured to send only relevant traffic or sessions to Scrutinizer so that it only analyzes traffic that provides security value.

Application metadata: If desired, processing-intensive tasks can be offloaded from data exporters by using the Gigamon platform's functionality for generating unsampled, enhanced metadata (e.g., DNS queries, HTTP response codes) in NetFlow or IPFIX format from any selected traffic stream. Rather than requiring infrastructure devices like routers and switches to generate flow records (NetFlow, IPFIX), the integrated Gigamon Visibility Platform and Scrutinizer solution reduces load on those devices and allows them to focus on their core capabilities, while providing richer data and reporting. This becomes even more valuable in instances when network devices are unable to generate accurate or reliable flow records.

For more information on Gigamon and Plixer, visit:
www.gigamon.com and www.plixer.com

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