

X P A T T E R N S | BY ATIGEO

Joint Solution Brief

Comprehensive Security Intelligence with Atigeo's xPatterns for Cyber and the Gigamon GigaSECURE Security Delivery Platform

The Challenge

Too often, single-point security solutions can inundate organizations with more alerts than they can manage. This compromises network security and can lead to sensitive data loss, identity theft, and damage to company brand and reputation.

Integrated Solution

Together with the Gigamon GigaSECURE® Security Delivery Platform, Atigeo's xPatterns for Cyber delivers a unified security picture in the right context at the right time, so that organizations can identify, prioritize, and neutralize advanced security threats. xPatterns for Cyber sits on the edge and at the core of networks to seamlessly strengthen existing security solutions and appliances, and delivers predictive forecasting based on historical models, while analyzing data in real-time, near real-time, and forensically.

Joint Solution Benefits

- xPatterns for Cyber leverages the GigaSECURE platform's broad and deep visibility across network traffic to solve complex Big Data problems
- GigaSECURE Security Delivery Platform aggregates, de-duplicates, filters, and masks traffic to pinpoint the important data for xPatterns analysis
- Together, xPatterns for Cyber and GigaSECURE Security Delivery Platform generate NetFlow/IPFIX from any traffic flow and decrypt SSL traffic to minimize unnecessary processing

Introduction

Organizations face the immense technological challenge of defending against evolving security threats that are immune to perimeter firewalls. When these organizations lack the right skillsets and tools to address advanced security threats, many attacks go unnoticed, compromising proprietary information and increasing the likelihood of financial loss.

The advent of Big Data brings with it historically unprecedented potential to accelerate breakthroughs in understanding threat patterns and remediating risk. Atigeo and Gigamon® have teamed up to fortify existing point solutions so organizations can regain control of their security and proactive protection.

The Gigamon and Atigeo Joint Solution

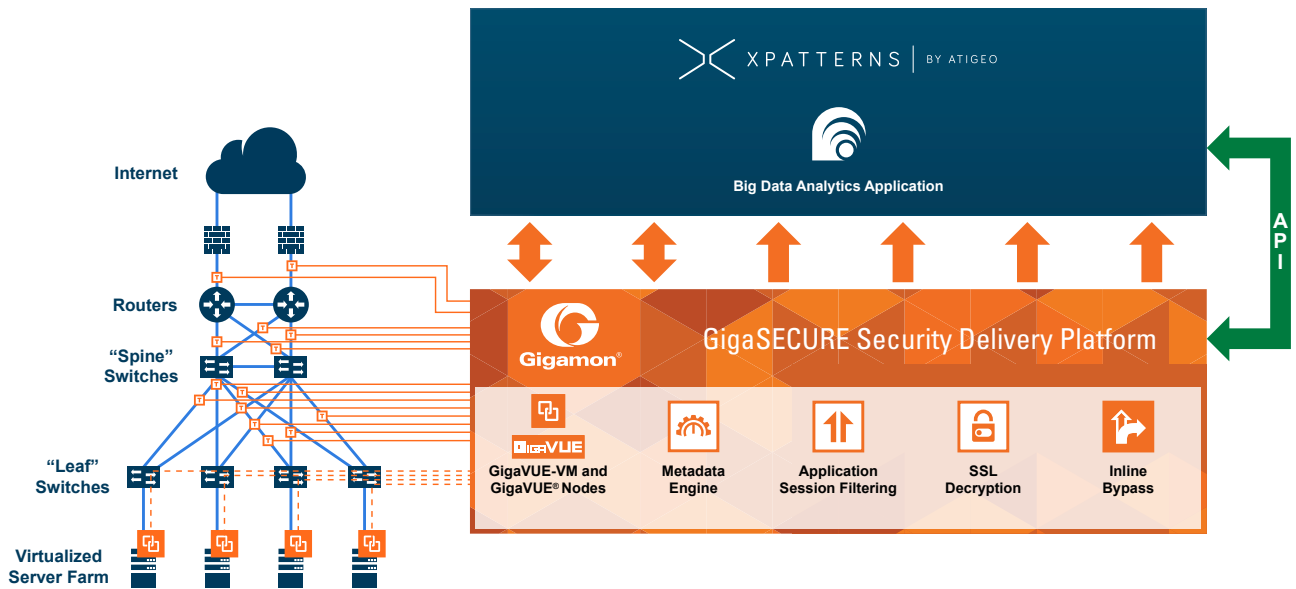
Atigeo has a vision: compassionate technology for a wiser planet. In the realm of cybersecurity, this means protecting the security of the organization, and the privacy of its customers and their data.

xPatterns for Cyber is an adaptive and intuitive solution that fuses historical and real-time data from inside and outside organizations to provide a cohesive and contextual view of security intelligence, network operations, and external information. By applying advanced, autonomous learning capabilities within the cybersecurity domain, the solution works to optimize pattern detection and cross-correlate requisite insights in order to automate cyber risk remediation processes.

Integrated with the Gigamon GigaSECURE Security Delivery Platform, xPatterns for Cyber delivers a unified security picture at high speed. The joint solution, which integrates incident response and remediation for full-scale cyber threat intelligence, surfaces actionable wisdom organizations can use to achieve clarity and make data-driven decisions that support a proactive, rather than reactive, position.

Key GigaSECURE Security Delivery Platform features that augment the value of xPatterns technology deployments include:

Easy access to traffic from physical and virtual networks: The GigaSECURE platform manages and delivers all network traffic to xPatterns efficiently and in the correct format. To monitor east-west data center traffic, Gigamon taps virtual traffic and incorporates it into the GigaSECURE platform for delivery to xPatterns for Cyber on the physical network. This enhances traffic monitoring and analysis and minimizes blind spots.



Aggregation to minimize tool port use: Where links have low traffic volumes, the GigaSECURE Security Delivery Platform can aggregate these together before sending them to the tool in order to minimize the number of ports that need to be used. By tagging the traffic, the Security Delivery Platform enables the source of traffic to be identified.

De-duplication: Pervasive visibility requires tapping or copying traffic from multiple points in the network, which, in turn, means tools may see the same packet more than once. To minimize unnecessary packet processing overhead on xPatterns tools, the Gigamon Visibility Fabric™ has a highly effective de-duplication engine that removes duplicates before they consume resources.

Filtering traffic to only send relevant traffic: The GigaSECURE platform can be configured to send only relevant traffic or sessions to the xPatterns for Cyber solution to filter for traffic that provides security value.

Masking for security: The GigaSECURE Security Delivery Platform is able to mask certain sensitive data (e.g., credit card numbers in e-commerce and patient identification in healthcare) within packets before sending them to other tools where operators or other unintended recipients may see them.

Optimize tool processing throughput: Eliminate the need for tools to undertake complex and processor-demanding traffic transformations (e.g., SSL decryption) prior to processing. With the GigaSECURE Security Delivery Platform, xPatterns for Cyber can concentrate on processing traffic rather than converting it into the right format.

NetFlow generation: If desired, processing intensive tasks can be offloaded from xPatterns for Cyber by using the GigaSECURE platform’s functionality for generating unsampled, enhanced metadata in NetFlow or IPFIX format from selected traffic streams for better analytics and improved forensic capability.

Together, xPatterns for Cyber and Gigamon’s GigaSECURE Security Delivery Platform help provide a cohesive security picture by providing broad network visibility with real-time information organizations need to identify, prioritize, and respond to advanced security threats.

Learn More

For more information on the Atigeo and Gigamon solutions, contact:

