Joint Solution Brief

Real-time, Automated Detection and Remediation of Known and Unknown Threats with Seceon and Gigamon

The Challenge

Current security solutions, such as next-gen firewalls, SIEMs and antivirus software, often work well to detect known threats, but can fall short at real-time detection of zero-day and targeted advanced persistent threats (APTs).

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, the Seceon Open Threat Management (OTM) platform helps organizations quickly see and stop known and unknown cyber threats through behavioral threat detection modeling and machine learning.

Joint Solution Benefits

- Real-time visualization, detection and elimination of cyber threats.
- Enhanced visibility and easy access to traffic from physical, virtual and public cloud networks through the Gigamon GigaSECURE Security Delivery Platform.
- The Gigamon GigaSECURE Security Delivery Platform's real-time SSL decryption functionality increases traffic visibility for Seceon OTM.
- Filtering and distribution of relevant traffic to Seceon OTM accelerates processing throughput and time to resolution.

Introduction

Traditional point security solutions work well to uncover known threats. However, they don't always work as well with unknown threats, leaving organizations vulnerable to today's increasing zero-day and targeted APT attacks.

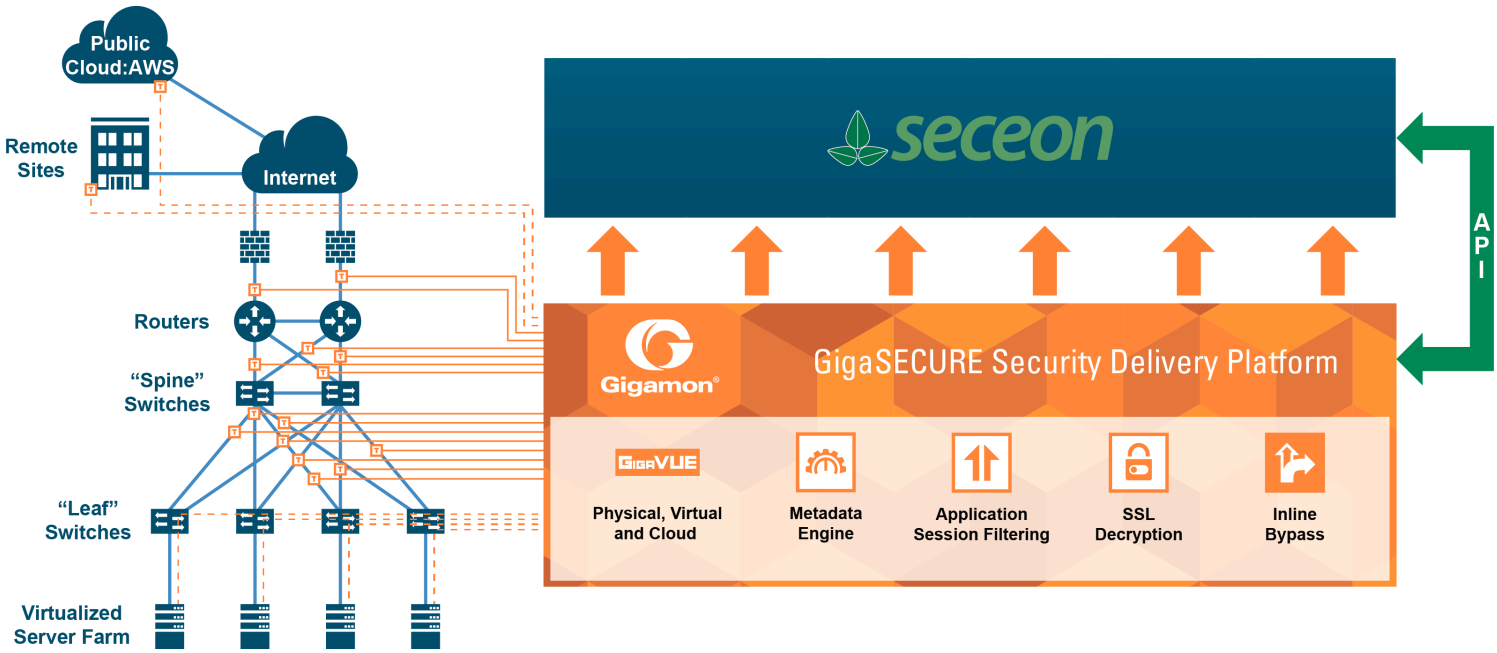
Seeing the need for a new approach to detect and remediate both known and unknown threats, Seceon developed its fully-automated OTM platform. Powered by advanced data collection and analysis, machine learning and patent-pending predictive and behavioral analytics, the subscription-based, agentless solution uncovers recognized and never-before-seen zero-day threats and threat actors based on how they behave. It surfaces only threats that matter and reduces white noise for minimal monitoring and reduced operational expense.

What's more, Seceon OTM was purpose-built for operational efficiency and ease of installation. Organizations of any size can deploy it in any environment – on-premises or private, hybrid and public clouds – within a few short hours and it requires little to no cybersecurity expertise. In other words, it acts as a SoC-in-a-Box™.

The Gigamon and Seceon Joint Solution

Combined with the Gigamon GigaSECURE Security Delivery Platform, Seceon OTM offers unparalleled real-time, holistic cybersecurity. It automates the analysis and correlation of threat indicators from security products like security information and event management (SIEM) systems, next-generation firewalls and server, network and application logs. It processes these events and correlates them with various threat feeds – in seconds and with minimal false positives – surfacing only alerts that need attention, improving speed to detection and response and lowering data breach costs.

By anticipating attacker behavior and stopping attacks as they happen, the joint solution delivers immediate ROI, saving companies the tens of millions of dollars typically spent addressing data loss, clean-up and customer mitigation issues. It also lowers capital expense by reducing multiple cybersecurity tool subscriptions and minimizes operational costs by reducing operational time and resources spent on building out threat-monitoring capabilities.



Key Gigamon solution features that augment the value of Seceon technology deployments include:

Easy access to traffic from physical, virtual and public cloud networks: The GigaSECURE Security Delivery Platform manages and delivers all network traffic – including east-west data center traffic and private and public cloud workloads – to Seceon OTM, efficiently and in the correct format. This eliminates blind spots and helps ensure that all traffic is monitored and analyzed together.

Traffic filtering: The GigaSECURE Security Delivery Platform sends specific traffic or sessions, for example, HTTP, HTTPs and email, to Seceon OTM so it does not become overloaded with irrelevant traffic that would only be dropped at a later point.

Metadata generation: GigaSECURE Security Delivery Platform can be used to generate unsampled, enhanced metadata – such as DNS queries and HTTP response codes – in NetFlow/IPFIX format from any selected traffic stream for more detailed contextual analytics and improved forensics and send them to Seceon OTM.

SSL Decryption: Real-time SSL decryption integration increases traffic visibility for Seceon OTM.

Learn More

For more information on Seceon and Gigamon solutions, contact:

seceon
www.seceon.com

Gigamon®
www.gigamon.com

3246-01 09/17