Joint Solution Brief

Quickly and Accurately Detect, Block, and Respond to Advanced Malware

The Challenge

Advanced, evasive threats have become more sophisticated, able to penetrate the network and move within it without being detected. Increasing network speeds and traffic loads present a problem of scale. Both of these challenges require a security solution that has the visibility and scalability to monitor across the entire network.

Integrated Solution

Lastline's Advanced Malware Protection Platform integrates with the GigaSECURE® Security Delivery Platform to inspect all traffic for advanced malware and attacks, offering a window into the entire network without speed or load limits. This solution provides instant detection of Advanced Persistent Threats (APTs), Advanced Targeted Attacks (ATAs), and evasive malware, with flexible deployment options.

Key Benefits

- **Complete Visibility into Network Activity Including Virtualized and Encrypted Traffic**—Extends the reach of monitoring tools to significantly improve ROI, more efficiently manage and secure the network, and quickly evolve and scale as network needs change
- **Comprehensive Advanced Malware Protection**—Detects advanced and evasive malware missed by other security products
- **Best-in-class Protection**—Provides instant detection with flexible deployment options against sophisticated and highly-evasive attacks
- **Scale and Extensibility**—Accommodate any traffic speed and load
- **Optimized Incident Response**—Accelerate and simplify incident response with a correlated view of malicious events that shows the complete attack chain

The Challenge

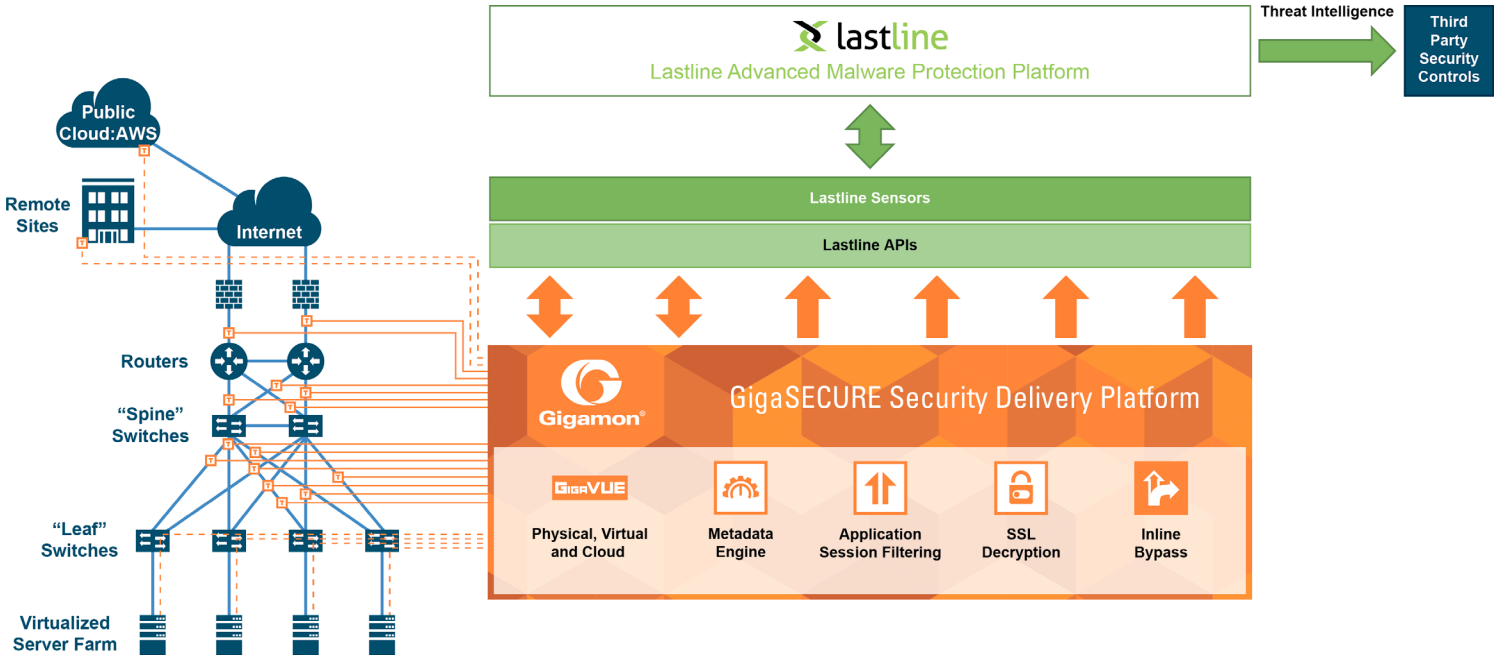
Information security breaches resulting in extensive damages are increasing substantially across the globe. Cyber criminals are updating their strategies and tools to evade agent-based software products, IPS appliances, and even next-generation firewalls and sandboxes. Information security systems must be kept updated and scalable to accommodate the increasing speed and volume of network traffic.

Scalability and robustness of security systems are just as important as efficacy of detection. No security solution can be successful unless it can continuously monitor all network activities in an enterprise. Monitoring only at the edge or endpoint leaves networks vulnerable as malware moves laterally within the network. Traditional SPAN and "TAP-and-agg" technologies are unable to provide the pervasive and active visibility required to detect and mitigate current and future threats, especially as more production traffic moves East-West within virtualized infrastructures.

The Gigamon and Lastline Joint Solution

Gigamon's GigaSECURE Security Delivery Platform helps enable the Lastline Advanced Malware Protection Platform to monitor and inspect content from web, email, and files for advanced threats that other tools miss. This includes North-South traffic in the physical infrastructure as well as East-West traffic between and within virtualized servers.

Deployed out-of-band, the Visibility Fabric™ aggregates and forwards only the relevant production traffic to Lastline sensors. Administrators can define what type of traffic is relevant with Gigamon's patented Flow Mapping® rules. Gigamon's GigaSMART® processing engine can provide deep traffic intelligence, such as Layer 2 – Layer 7 filtering, removal of duplicates, and decryption of SSL traffic. The GigaSECURE platform enables the Lastline Platform to detect advanced, evasive malware in the traffic that meets the criteria set by administrators. Gigamon's GigaStream™ technology distributes traffic among multiple Lastline sensors, which can run on virtual instances or standard servers. This robust and high-performance integration architecture scales to fit growing network speeds and loads.



The Lastline Advanced Malware Protection Platform has been specifically developed to detect and defeat evasive malware operating within a network. It identifies even the most advanced threats, including those developed to evade other security technologies.

The Lastline Platform uses Deep Content Inspection, a unique approach to isolating and analyzing threats to detect malware. Deep Content Inspection thoroughly analyzes the capabilities and behaviors of every object (emails, web traffic, or files). It interacts with the malware, enabling it to evaluate every instruction sent to the CPU and have complete visibility into the malware's behavior.

The Lastline Platform analyzes all unknown objects sent from the GigaSECURE Platform and provides visibility of each object's threat characteristics. It catalogs every stage of the attack chain, from delivery, exploitation, installation, command and control communication, and exfiltration. It provides real-time Threat Intelligence to the Gigamon platform that the IT team can use to help ensure security controls are instrumented against the latest malware, as well as create new workflows to automatically block new threats. Third-party tools can also use the Threat Intelligence from the Lastline Platform to automatically update policies, making them more effective.

Learn More

For more information on the Lastline and Gigamon solution, contact:

lastline
www.lastline.com

Gigamon®
www.gigamon.com

3150-02 03/17