



Joint Solution Brief

Prevent, Don't Remediate Cyber Threats with Solebit SoleGATE and the Gigamon GigaSECURE Security Delivery Platform

The Challenge

Most of today's network-level cyber protection uses sandboxing technology and inspection built on behavioral analysis to attempt to identify unknown threats. This approach is frequently resource intensive, slow, operating system and client-side application dependent, and even worse, can often be evaded by today's smart attacks.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, SoleGATE provides an accurate and cost-effective, evasion-proof approach for the identification and prevention of zero-day malware and unknown threats.

Joint Solution Benefits

- **Prevent, don't remediate:** Strengthen your cyber defenses dramatically by preventing attacks before they enter and harm your organization, your customers and your brand.
- **Detect the undetected:** Identify any malicious or hidden code within incoming data files whether on your network or in a cloud. What you don't know or cannot see can harm you.
- **Broad and deep visibility:** Across both physical and virtual network traffic helps SoleGATE quickly and easily access and analyze files for unauthorized code.
- **Automatic traffic load balancing and aggregation:** functionality leveraged by SoleGATE to scale your deployment, avoiding bottlenecks and port oversubscription.
- **Real-time SSL decryption:** With the GigaSECURE platform's functionality, SoleGATE gains increased visibility into traffic without performance degradation.

Introduction

Solebit provides a disruptive cyber protection software platform, challenging the norms of currently available technologies that often rely on slow, costly and mostly outdated, ineffective methods of sandboxing, signatures and behavioral inspection.

Many anti-malware solutions are based on dynamic analysis, focus on identifying suspicious behavior, and require opening an object for analysis within a targeted environment. Once opened, however, the malicious code can take control and often evades detection.

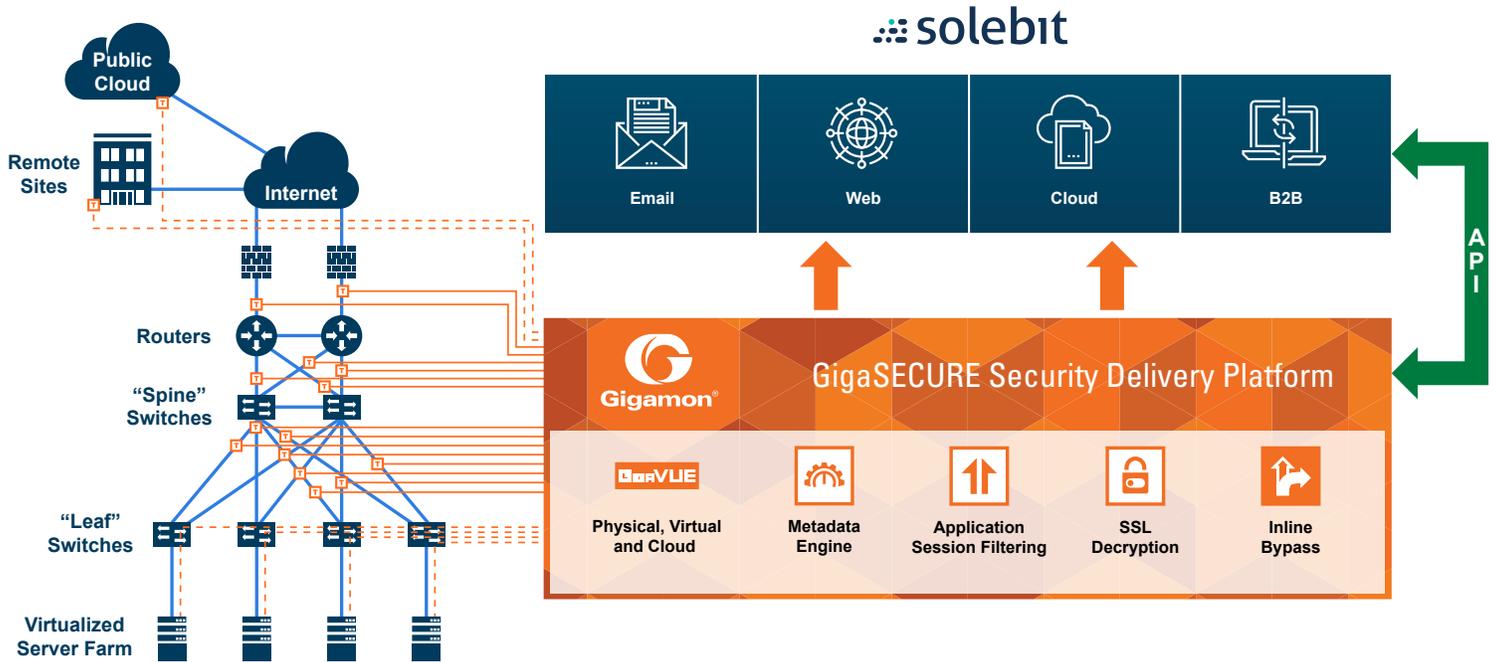
Whether in the form of ransomware, spyware, trojans, rootkits or any other type of malware yet to be defined, SoleGATE will conclusively and in real-time, identify and block the malicious code from infiltrating your organization that other solutions may not even detect.

The Gigamon and Solebit Joint Solution

Together with the Gigamon GigaSECURE Security Delivery Platform, SoleGATE, brings you ground-breaking, evasion-proof protection against modern cyber-attacks before they adversely impact your enterprise.

The SoleGATE Protection Platform is anchored by DvC™, a patented, real-time, signature-less engine. DvC assumes that there is no legitimate reason for executable code to be present in any data file. As such, unlike many competing technologies, it does not rely on heuristics or behaviors. It can definitively identify and terminate any instance of malicious code such as hidden CPU instructions, encrypted and polymorphic payloads, shellcodes and other commands typically buried in data files. DvC also accurately identifies and blocks malicious active content using advanced flow analysis, de-obfuscation techniques and deep content evaluation, to reveal threat intent within any inbound data file covering machine, operating system and application levels, thereby rendering such sandbox-evading attacks harmless to the enterprise.

Moreover, integrated with the GigaSECURE platform, SoleGATE can handle multiple files per second, allowing organizations to process large volumes of data without latency and without causing human-related bottlenecks and queues.



Key GigaSECURE Security Delivery Platform features that augment the value of the SoleGATE solution include:

- Easy access to traffic from physical and virtual networks: The GigaSECURE platform manages and delivers network traffic—in the format required—to SoleGATE. From physical taps, private virtual environments and public cloud deployments. This allows the traffic to be monitored and analyzed together, helping to eliminate blind spots and increase the probability of discovering suspicious behavior and malicious payloads.
- Load balancing to spread traffic across multiple devices: When traffic flows are larger than a single tool can cope with, GigaSECURE can be used to split the flow across multiple tools, while ensuring sessions are kept 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 the SoleGATE solution.
- Protect against network outages: Inline bypass protection maintains traffic continuity and minimizes network outages for maintenance windows.

Learn More

For more information on the Solebit Labs and Gigamon solution, contact:

solebit
www.solebit.io

Gigamon
www.gigamon.com