JOINT SOLUTION BRIEF

Threat Intelligence-Driven Network Protection from Gigamon and Bandura Cyber Reduces Exposure to Cyberattacks at Scale

The Challenge

Firewalls are getting crushed by the sheer volume of threats that hit them every day — and the number of threats will likely keep growing. The overwhelming amount of known threats leads to security coverage gaps and slower, less efficient firewalls that lack the bandwidth to identify and block complex threats. Enterprises are implementing expensive firewall upgrades more often to keep up with the onslaught, but it's not enough — overwhelmed firewalls are leaving enterprises open to security risks and subject to increased costs.

Integrated Solution

Integrated with the Gigamon GigaSECURE® Security Delivery Platform, the Bandura® Threat Intelligence Gateway (TIG™) automatically defends against tens of millions of potentially harmful IPs and domains at line speeds ahead of firewalls. With Bandura TIG, noisy known threats will be blocked, and your firewall will be able focus its resources on complex threats.

Joint Solution Benefits

- Enhanced visibility and easy access to traffic from physical, virtual and public cloud networks through the GigaSECURE Security Delivery Platform
- The GigaSECURE Security Delivery Platform inline bypass functionality supports failover protection and maintains traffic continuity for the Bandura TIG in the event of a network outage or tool failure
- Automates aggregation and updating of threat intelligence from top global providers and blacklist feeds
- Blocks millions of known threats before they hit the firewall, significantly improving firewall performance
- Reduces the attack surface and alert overload, and stops critical data losses with near-zero latency
- Improves firewalls' ROI and enables a greater return on existing threat intelligence investments

Introduction

Firewalls were not designed to take on the tens of millions of internet threats in play today. At most they can handle a few hundred thousand threat indicators at a time. Now, buckling under the workload, they're slowing down the network and leaving enterprises vulnerable to a broadening scale of cyberattacks.

By leveraging vast threat intelligence repositories, block-list automation and precision geo-IP blocking, the Bandura Threat Intelligence Gateway (TIG™) provides advanced protection ahead of the firewall, ahead of the hacker and ahead of the threat.

The Gigamon-Bandura Joint Solution

Integrated with the GigaSECURE Security Delivery Platform, Bandura TIG gives enterprises an easy way to keep millions of known threats off their infrastructures, helping to make existing security controls more effective and efficient. The joint solution reduces security alert fatigue and restores the ability to control the attack surface.

Bandura TIG's enterprise-class capabilities start with the ability to filter network traffic against more than 100 million unique IPs and domains with virtually no latency. Bandura TIG's open platform, including STIX/TAXII support, can integrate large volumes of threat intelligence from multiple sources and distill down the threat landscape to a single, manageable flow of risk-scored, prioritized data.

This intelligence, coupled with automated security policy adjustments, gives enterprises bi-directional control to take rapid action to block the massive volume of IP and domain threats — before they hit the perimeter — and to stop critical data leaks with near-zero network slowdown. Bandura's cloud-based Global Management Center (GMC) provides single-pane-of-glass management for multiple TIGs.

Key GigaSECURE Security Delivery Platform features that enhance the value of Bandura technology deployments to operationalize the vast amount of threat intelligence on the wire, include:

- **Easy access to traffic from physical, virtual and 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 the Bandura TIG, efficiently and in the correct format, to eliminate blind spots and help ensure collective monitoring and analysis of all traffic.
- **Inline bypass for efficient and resilient deployment**: The inline bypass functionality of the GigaSECURE Security Delivery Platform provides physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure. As required, any number of Bandura TIG devices can be deployed to manage traffic, regardless of the speed and utilization of monitored network connections, or moved in and out of line at the touch of a button.
- **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 Bandura TIG to minimize the number of ports needed. By tagging the traffic, the GigaSECURE Security Delivery Platform can also identify the traffic source.
- **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 avoid unnecessary packet-processing overhead on Bandura TIG, the GigaSECURE Security Delivery Platform removes duplicates before they consume resources and helps balance monitoring coverage.

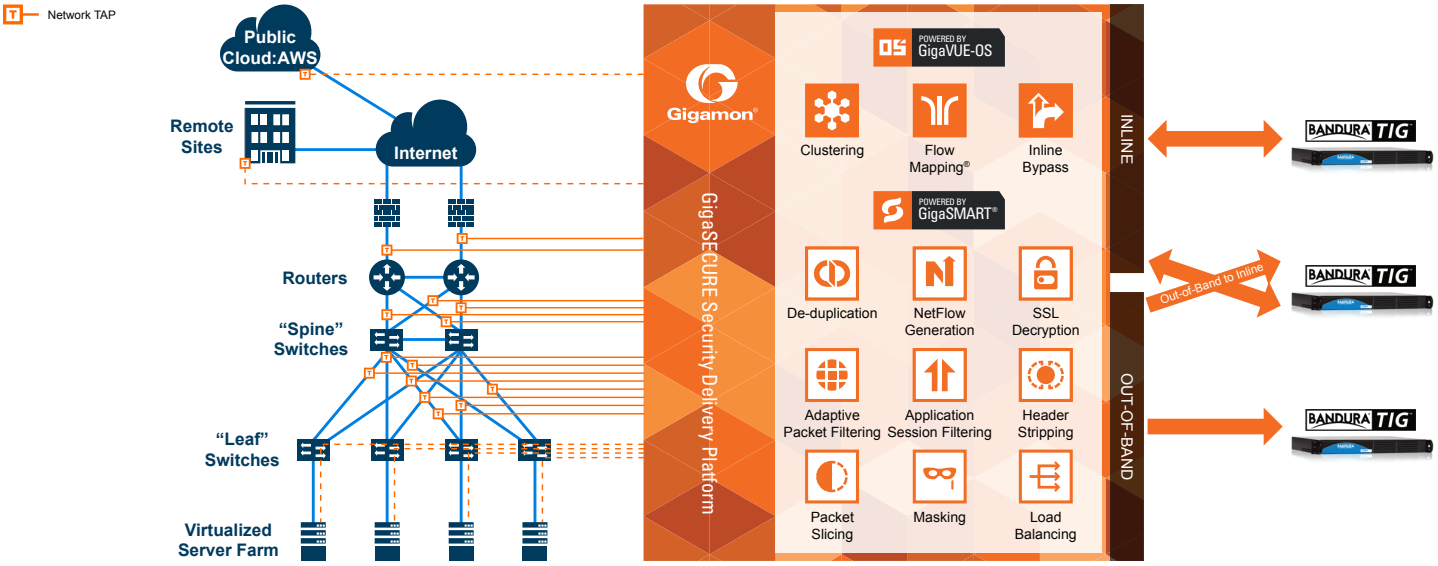

Figure 1: Gigamon GigaSECURE Security Delivery Platform and Bandura TIG Joint Solution.

- **Load balancing to spread traffic across multiple devices:** When traffic flows are larger, the GigaSECURE Security Delivery Platform can split the flow across multiple Bandura TIG instances.
- **Easier control of asymmetric routing to help ensure session information is kept together:** Most security devices require that all the packets in a session be inspected by the same device since incomplete sessions risk being blocked. The GigaSECURE Security Delivery Platform provides an intelligent and efficient way to help ensure this inspection happens in most architectures.

For more information on Gigamon and Bandura Cyber solutions, visit: www.gigamon.com and www.banduracyber.com.

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

3246-01 10/18