

Benefits

- Significantly reduce your attack surface using threat intelligence to more effectively block known threats and unwanted traffic.
- Reduce staff burden by eliminating alert noise and manual workload.
- Increase the value of threat intelligence by taking action.
- Get more out of your firewall by eliminating noisy known threats ahead of it.

Threat Intelligence-Driven Protection

The Bandura® Threat Intelligence Gateway (TIG™) enables companies of all sizes to leverage the power of Threat Intelligence to more effectively and efficiently protect networks against known threats and unwanted traffic.

Now, all the power of massive Threat Intelligence feeds can be deployed ahead of the network — working like a shield to block cyberattacks inbound, preventing data leakage outbound — and significantly reducing the load on the firewall.

The Problem

At any moment, there are over 10 million known threats. Existing security controls, like firewalls, can typically only process 100,000 threat indicators before significant performance issues occur. This forces organizations to either operate with security coverage gaps due to limitations on the ability to use Threat Intelligence or to overspend on firewalls using expensive, deep packet inspection to tackle the problem. This is compounded by the challenges of manually updating and maintaining threat intelligence feeds, firewall rules and Access Control Lists (ACLs).

Bandura TIG to the Rescue

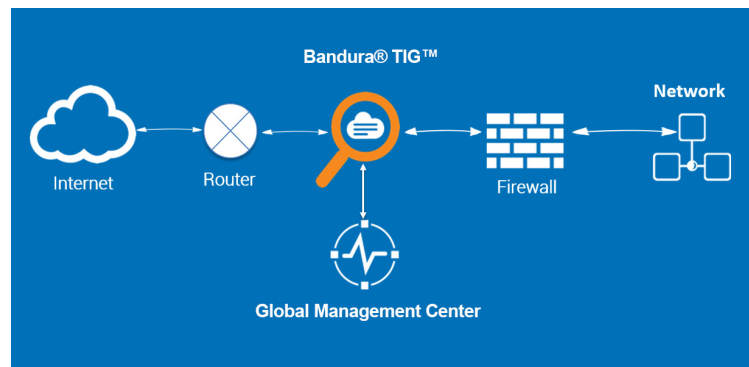
Bandura pioneered Threat Intelligence Gateway (TIG) technology in partnership with the U.S. Department of Defense. Bandura TIG is purpose-built to deliver threat intelligence-based protection at scale. Bandura TIG sits in front of your firewall filtering traffic against a massive volume of threat indicators (IPs and domains) with virtually no latency. Bandura TIG is easy to deploy and manage enabling organizations of all sizes to harness TI power!

Key Features

Threat Intelligence with no limits. Bandura TIG comes out of the box with millions of continuously refreshed threat indicators (IPs and domains) from multiple sources and can filter traffic against over 100 million unique threat indicators with virtually no latency. Traffic can be filtered by threat intelligence category (Command & Control, Botnets, Tor/Anonymizers, etc.), Country, Autonomous System Number (ASN) or any combination.

Automated Threat Intelligence that is easy to use. Threat feeds are automatically updated in near real time and policies automatically applied. Bandura TIG's automation capabilities improve security and increase staff productivity.

Open platform easily integrates with additional threat sources and systems. Want to integrate existing or additional threat feeds into Bandura TIG? Not a problem! Bandura TIG is an open platform that supports STIX and TAXII making it easy to integrate additional threat feeds. Bandura TIG can also be easily integrated with other systems like Threat Intelligence Platforms and SIEMs.



Policy management as granular as you want through an intuitive user interface. Bandura TIG has flexible policy management capabilities that scale to the needs of the user. Leveraging Bandura TIG's automation capabilities, it can be deployed in a low touch "set it and forget it" mode. For more sophisticated enterprises, Bandura TIG offers robust, granular policy management capabilities. No matter which end of the spectrum you fall on, this is all easily accomplished through an intuitive user interface.

Flexible deployment options and centralized management. Bandura TIG can be flexibly deployed as a traditional appliance or as a virtual machine (VM) in private and public cloud environments. Our Global Management Center enables centralized management and reporting for multiple Bandura TIG deployments regardless of form factor.





BANDURA TIG PRODUCT MATRIX

MODEL	BT-500	BT-1G			BT-10G
		Standard (BT-1G)	High Availability (BT-1G-A)	Data Center (BT-1G-X)	
NETWORKING					
Throughput	500 Mb	1 Gb	1 Gb	2 x 1 Gb	10 Gb
Connections per second	10,000	10,000	40,000	80,000	500,000
Concurrent Connections	500,000	500,000	1,000,000	2,000,000	2,000,000
Bridging Interface	Bypass Mode 1 Gb Copper RJ45	Bypass Mode 1 Gb Copper RJ45	Bypass Mode 1 Gb Copper RJ45 or 1 Gb Short-Run Fiber	Bypass Mode 1 Gb Copper RJ45 or 1 Gb Short-Run Fiber	Bypass Mode 10 Gb Copper RJ45 or 10 Gb Short-Run Fiber
Bridge Pairs	Single	Single	Two Bridge Pairs Active/Standby Active/Active	Two Bridge Pairs Active/Standby Active/Active	Two Bridge Pairs Active/Standby Active/Active
Management Interface	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45
Typical Deployment	SOHO	Enterprise	Enterprise	Enterprise, Data Center	Data Center
HARDWARE					
Solid State Drive			✓	✓	✓
Redundant Power Supplies				✓	✓
RAID				✓	✓
DIMENSIONS & POWER					
Mounting	Desktop	1U Rack Mount	1U Rack Mount	1U Rack Mount	1U Rack Mount
Appliance Dimensions	7.25W x 5.5D x 1.7H (in)	17W x 11.5D x 1.7H (in)	17W x 11.5D x 1.7H (in)	17W x 26.5D x 1.7H (in)	17W x 26.5D x 1.7H (in)
Shipping Weight	5 lbs.	15 lbs.	25 lbs.	35 lbs.	35 lbs.
AC Power	100-240 VAC	100-240 VAC	100-240 VAC	100-240 VAC	100-240 VAC

*Full 10 Gbps throughput available Q418

About Bandura Cyber

Bandura Cyber pioneered the Threat Intelligence Gateway in part with the U.S. Department of Defense. Bandura's TIG is the most comprehensive, scalable and granular TIG platform on the market. Organizations worldwide use TIGs for the automation and control needed to operationalize hundreds of millions threat indicators blocking known threats before they even reach the network firewall. Underlying Bandura's robust technology are more than 50 issued and pending patents. To learn more about how Bandura TIG reduces an organization's attack surface, operationalizes threat intelligence and helps get more out of existing security investments, visit banduracyber.com.