

Why Partner with Bandura?

- Gain exposure to the fast-growing Threat Intelligence Gateway (TIG) market opportunity.
- Provide your customers a solution that is easy to deploy and delivers significant out-of-the-box value by improving security and alleviating operational pain points.
- Drive incremental revenue while improving the ROI of customers' existing security investments including firewalls, unified threat management (UTM) solutions, SIEM, and Threat Intelligence.
- Improve the effectiveness & efficiency of your Managed Security Services offerings.
- Influence and shape the Bandura Channel Program.

Program Highlights

- Attractive Product Discounts
- Deal Registration
- Dedicated Account Manager
- Partner Portal Access
- Sales & Technical Training
- Demo (NFR) Equipment Discount
- Dedicated Account Manager
- Product & Marketing Collateral
- Joint Marketing Initiatives

JOIN OUR MISSION!

partner@bandurasystems.com

Welcome to Threat Intelligence-Driven Protection

Bandura's mission is to enable all companies to use Threat Intelligence (TI) without limits to protect networks in a simple & automated way. We know this mission is impossible to achieve without the help of partners like you. So we're glad you're here! We think you will find that the Bandura Channel Partner Program provides you with an attractive growth opportunity for your security business.


The Problem

- ▶ Traditional network security controls don't provide the volume of TI required to protect today's networks. At any moment, there are over 10 million known threats. Firewalls can only process 100,000 threat indicators before significant performance issues occur leading to security coverage gaps.
- ▶ Most companies lack the staff & resources to effectively and efficiently utilize TI, leaving TI to be primarily the domain of large enterprises with significant resources. Companies of all sizes need TI.
- ▶ Organizations lack the ability to take action with TI in an automated way. Managing TI enforcement with firewall rules and access control lists (ACLs) is manual, time consuming, and not scalable.

PoliWall Threat Intelligence Gateway (TIG) to the Rescue

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

PoliWall TIG enables companies of all sizes to leverage the power of TI to more effectively and efficiently protect networks against known threats and unwanted traffic. All the power of massive TI feeds can be deployed as the first and last line of defense, blocking malicious and unwanted traffic both inbound and outbound.



| | |
|--|---|
| <p style="text-align: center; margin: 0;">Access</p> <ul style="list-style-type: none"> 10M "out of the box" threat indicators from multiple sources ~20 threat categories including Botnets, Command & Control, etc. Country IPs & Company IPs (ASNs) | <p style="text-align: center; margin: 0;">Aggregate</p> <ul style="list-style-type: none"> Multiple threat feeds consolidated into a single feed Unified risk scoring based on category Analytics enable dynamic risk adjusting |
| <p style="text-align: center; margin: 0;">Automate</p> <ul style="list-style-type: none"> Threat feeds dynamically updated in real time Policies automatically applied No updating firewall rules or ACLs | <p style="text-align: center; margin: 0;">Act</p> <ul style="list-style-type: none"> Block known threats & unwanted traffic Detect threats & alert Respond to threat indicators from SIEMs, TIPs, and other systems |