ADVANCING SECURITY AUTOMATION
NEAR-ZERO LATENCY

The ProAct™ Server
*We Know Your World™*

At any given moment there are over 10 million recognized IP threats. Your security team painstakingly weeds through an overwhelming abundance of "actionable threat intelligence" to determine the true risk, then manually manages firewall rules and policies based on the top priorities of today. ProACT™ solves this challenge by rapidly aggregating multiple threat feeds and intelligently determining risk-levels. In near real-time, this data directly feeds to a PoliWall™, which takes immediate action to block threats bi-directionally based on your own defined level of acceptable risk!

Schedule a demo or request a free trial!

sales@bandurasystems.com
1 (636) 265-3110
www.bandurasystems.com

CONTACT US TODAY!
Learn how ProAct™ risk-scoring engine gives real-time threat precision—with action.

Speed and Precision
ProACT is an auto-adjusting IP risk-scoring and threat aggregation engine that processes tens of millions of threats at line speeds with no network slowdown. ProACT's risk-scored threat information automatically feeds into PoliWall where, with near-zero latency, real-time action is taken to stop cyber threats and data leakage.

Multi-Feed Aggregation
ProACT™ aggregates IP threat intelligence data from multiple 3rd-party sources and intelligently assigns IP risk scores based on the compiled data and IP reputation analytics in real-time through a fully automated process.

Intra-Network Threat Feed
Internal threat information from firewalls, IDS, and SIEM is aggregated with external threat feeds for threat identification precision. ProACT™ then feeds the threat data in near real-time to the PoliWall™, which automatically blocks malicious connections at your network perimeter.

Intelligent IP Risk Scoring
ProACT™ automatically assesses risk in real time based on the changing regional and organizational threat posture associated with your enterprise network activity. Real-time assessment alleviates risk of blocking or allowing outdated or re-assigned IP addresses.

Easy Integration
ProACT integrates with existing information systems via a robust REST API, augmenting existing systems and significantly reducing security management time.
ADVANCED SECURITY FOR YOUR WORLD.

Take action against cyber-attack with ProACT™ server and PoliWall® security platform.

Cyber Threats Target Everyone

The ever-increasing number of cyber threats from cyber criminals, fraudsters, nation-state; international competitors; and the growing complexity of compliance with stringent security regulations compels financial services, education, healthcare, energy, and retail and government sectors to protect against online fraud, network intrusion, and web service disruptions.

The sheer number of cyber criminals finding and exploiting vulnerabilities has caused the US government to impose rules and regulations that mandate organizations to proactively secure their infrastructure and ensure data privacy. In response to FFIEC audits, PCI DSS, the Gramm-Leach-Bliley Act, HIPAA, FERC, NERC and numerous other regulations and guidelines, organizations of all sizes are adopting measures to prevent the theft of information and digital assets by malicious attackers.

Reduce Risk Exposure by Controlling the Attack Space

Networks are overwhelmed with the number of threats hitting the network. Of the 10 million IP threats identified at any given moment globally, firewalls can only process 50-100 thousand of those threats before the network slows down—choke. PoliWall processes over 100 million IP threats from multiple sources ahead of the firewall, dropping up to 90% of threats at line speed, before they hit the firewall—rapidly reducing the attack space! It is the Firewall’s Firewall™.

Auto-Action-Auto Update—Threat intelligence companies provide “actionable intelligence”—meaning someone has to pull through the information and then make entries into firewalls or other devices to stop the threat. There is too much actionable intelligence—too many firewall incident reports to review, most of which are just noise and ignored. ProACT’s auto-threat aggregation consumes the threat intelligence and feeds into PoliWall that automatically blocks the threat inbound and outbound—blocking the noise and reducing the attack vector by up to 90% ahead of the firewall as reported by customers. IP Threat intelligence is auto-updated in near real time and auto-blocking is done according to your unique risk policy easily set in the PoliWall.

Ease of Use - Quick Time Value

Current security systems are complex and labor-intensive. PoliWall is plug-and-play, with no network configuration change required and can be up and running in minutes. Patented, easy-to-use graphical interfaces allow country blocking with a click on a map, and using easy slider technology, select your own acceptable level of risk. ProACT’s auto-aggregation of threat intelligence from multiple sources—feeds you own or we can license to you from vendor partners—is combined with threat information found inside your own network—-for auto-block and auto-threat distribution to all PoliWalls in the system. Opt-in, real-time sanitized threat info-sharing possible between ProACT users.
Financial, Healthcare, Energy, Retail and other members of the Critical Infrastructure must maintain compliance with numerous government regulations and cyber security guidelines. Audits are made easy with PoliWall’s graphical interfaces and granular log files. A quick look at a map for easy-to-read logs to verify compliance, and the check is in the box.

**Technology Behind the Security**

With PoliWall you reduce the attack space with near-zero latency, set your exceptions, determine an IP’s real-time threat risk, and stop block cyber-attacks and outbound data leaks automatically. PoliWall IP Platform blocks threats as they emerge, and re-allows when the threat is gone in near real time. Three core PoliWall technologies help administrators balance the demand of blanket policies with the need for granular control:

1. **HIPPIE** (High-speed Internet Protocol Packet Inspection Engine) blocks country of origin at lines speeds and auto-updates country IP address ranges. This eliminates the need to maintain hundreds of country-based access control lists (ACLs), significantly reducing the burden on system administrators, firewalls, and routers in the network.

2. **Dynamically-Compiled Exception Lists (DCELs)** (pronounced Diesel) engines allow you to integrate very large IP Reputation Threat lists blocking large groups of IP’s.

3. **ProACT™** server aggregates multiple sources of threat intelligences to give you the most accurate picture of the threat landscape and dynamically assesses the risk posture on the network and adjusts the access control policy accordingly. Opt-in threat information sharing with other ProACT users in real time, provides unique industry threat data not yet seen on commercially available feeds.

**Real-Time Risk-Scoring**

ProACT server does patent-pending real-time risk scoring based on outside threat intelligence and internal network events. ProACT allows our customers to share intelligence events across all PoliWall’s in the architecture for threat identification precision not available with other products. ProACT solves the false positive problem by allowing each customer to tailor their acceptable risk levels.

ProACT is an auto-adjusting IP risk-scoring and threat aggregation engine processes tens of millions of threats at line speeds with no network slowdown. ProACT’s risk-scored threat information automatically feeds into PoliWall where, with near zero latency, real-time action is taken to stop cyber threats and data leakage.

ProACT Community Opt-in threat information sharing (available January 2016) with other ProACT users in real time, provides unique industry threat data not yet seen on commercially available feeds.

No express or implied warranties are provided for herein. © 2013 Bandura, LLC. All rights reserved. Bandura, the Bandura logo, PoliWall, DCELs, and ProACT are trademarks of Bandura, LLC.