BANDURA® **Smart, Simple, Scalable. Everywhere.**

Benefits

- Strengthen network defense by taking action on threat intelligence and prevent inbound and outbound connections to malicious IPs and domains
- Reduce staff workload by automating IP and domain block listing at scale
- Maximize threat intelligence ROI by making it actionable and increase the ROI and efficiency of existing next-generation firewall investments.

Features

- Bandura integrates threat intelligence from ThreatQ and other sources to block up to 150 million known malicious IPs and domains before they hit your network
- ThreatQ automatically updates intelligence in the Bandura platform, ensuring real time network protection and reduced manual workloads
- Threat intelligence-driven context from the network edge via the Bandura platform enhances the value of ThreatQ threat intelligence with increased visibility into malicious IP and domain activity on your network.

BANDURA® + THREATQUOTIENT

Bandura Cyber and ThreatQuotient have partnered to make threat intelligence more actionable in an effort to further fuel threat-centric security operations. This powerful integration enables organizations to strengthen network defense by proactively using threat intelligence from ThreatQ's Threat Library and the Bandura platform to block IP and domain-based threats before they hit your network.

The ability to take action on threat intelligence is critical to maximizing its value. However, organizations often face challenges integrating threat intelligence into traditional network security controls like firewalls. Most firewalls have limited capacity to integrate third-party threat intelligence indicators, and managing external blocklists in firewalls is complex and time consuming.

Bandura Provides Smart, Simple, & Scalable Network Security Everywhere

Bandura blocks known bad traffic at scale using a combination of simple, innovative technology and best-in-class threat intelligence. We provide 30 million "out of the box" threat indicators from the world's best sources and offer over 50 point-and-click integrations and connectors: ISACs, ISAOs, Threat Intelligence Platforms (TIPs), SIEMs, SOARs, or any other IP or domain based source.

Policy enforcement and blocking is handled by our ThreatBlockr appliances, which can block up to 150M threat indicators in real-time with no latency. ThreatBlockr inspects inbound and outbound traffic and makes simple, policy-based allow or deny decisions based on threat intelligence (IP reputation, block lists, allow lists), GEO-IP, and/or Autonomous System Number (ASN). ThreatBlockr can be flexibly deployed on physical, virtual or cloud appliances, as a cloud-based service or any combination of these. Regardless of deployment, we can protect your users and networks everywhere and our cloud-based Management Portal gives you a central point of visibility and control.

As data flows through ThreatBlockr appliances, the Bandura platform generates a significant amount of data that helps you analyze your security posture, identify and remediate threats in real time, and easily solve for false positives. Non-PII metadata is sent to our Global Management Center to allow quick analysis of your security posture and detailed data is sent to any SIEM, Syslog server or security analytics tool of your choice for further detailed analysis.

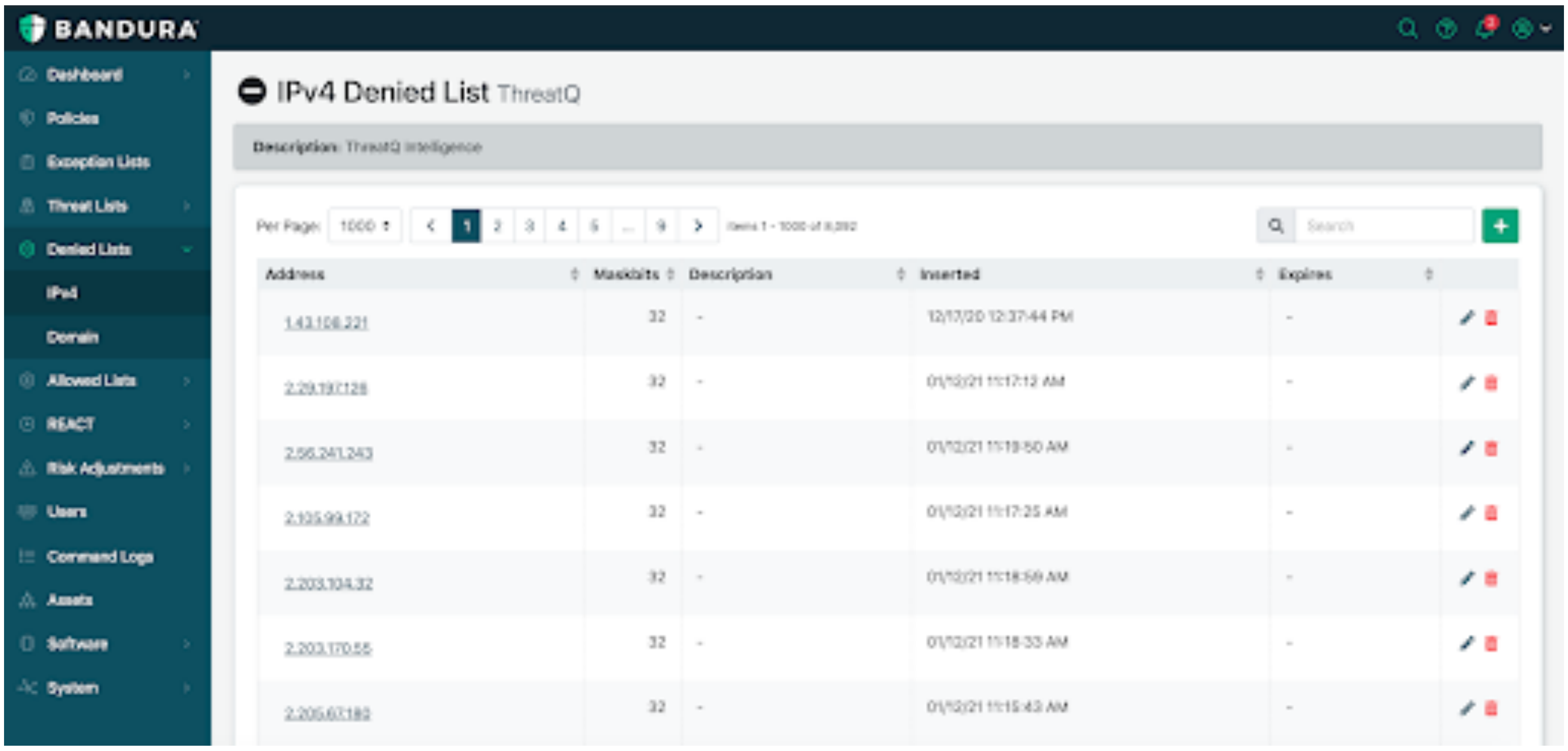
ThreatQ by ThreatQuotient Overview, Features, and Capabilities

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

- Automatically score and prioritize internal and external threat intelligence based on your parameters
- Automate aggregation, operationalization and use of threat intelligence across all systems and teams
- Centralize threat intelligence sharing, analysis and investigation in a threat intelligence platform all teams can access
- Improve effectiveness of existing infrastructure by integrating your tools, teams and workflows.

The Bandura-ThreatQ Integration — Maximizing Threat Intelligence ROI By Making It Actionable

The Bandura platform can easily integrate and take action using threat intelligence from ThreatQ blocking connections to/from known malicious IPs and domains before they hit your network. ThreatQ users can easily create automated IP and domain blocklists, based on prioritized data collections



IPv4 Denied List ThreatQ

Description: ThreatQ Intelligence

Items 1 - 1000 of 8,292

Address	Maskbits	Description	Inserted	Expires
1.43.106.221	32	-	12/17/20 12:37:44 PM	-
2.29.197.128	32	-	01/12/21 11:17:12 AM	-
2.56.241.243	32	-	01/12/21 11:19:50 AM	-
2.105.99.172	32	-	01/12/21 11:17:25 AM	-
2.203.104.32	32	-	01/12/21 11:18:59 AM	-
2.203.170.55	32	-	01/12/21 11:18:33 AM	-
2.205.67.182	32	-	01/12/21 11:15:43 AM	-

The integration of the ThreatQ and Bandura platforms strengthens network security, reduces manual workloads, and maximizes threat intelligence ROI by making it actionable.

For more information about Bandura's solutions contact us at 1.855.765.4925 ext 3, or by email at sales@banduracyber.com.