THREATBLOCKR® splunk>

Smart, Simple, Scalable. Everywhere.

The integration of ThreatBlockr and Splunk Enterprise Security combines security information and event management (SIEM) with network security powered by real-time threat intelligence. ThreatBlockr blocks known bad traffic at scale using a combination of simple, innovative technology and best-in-class threat intelligence.

Splunk Enterprise Security is widely used by leading security organizations to detect, analyze, and respond to threats quickly. The combination of the two platforms provides improved protection from cyber threats and more effective and efficient threat detection, investigation, and response.

BENEFITS

- Comprehensive visibility into your security posture
- Improve threat detection
- Reduce the time to investigate and respond to security incidents

FEATURES

- Leverage Splunk Enterprise Security for long-term storage of ThreatBlockr logs
- Aggregate logs from multiple ThreatBlockr appliances in Splunk
- Use more customizable and advanced analytics, visualization, and reporting capabilities
- Correlate ThreatBlockr logs with logs from other security controls and systems

ThreatBlockr Provides Smart, Simple, & Scalable Network Security Everywhere

ThreatBlockr 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.

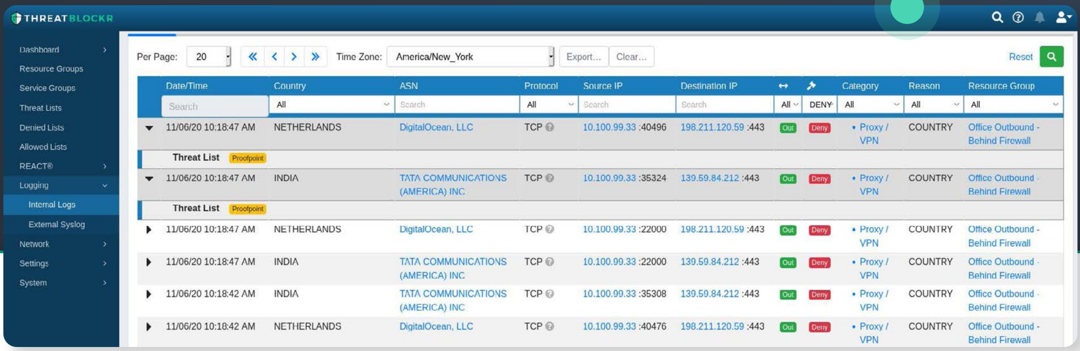
Policy enforcement and blocking is handled by ThreatBlockr, which can block up to 150M threat indicators in real-time with no latency. ThreatBlockr inspects inbound and outbound traffic and makes simple, policy-based allow or deny decisions based on threat intelligence (IP reputation, block lists, allow 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, the 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 Admin Console 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.

ThreatBlockr Logs Provide Powerful Data & Syslog Export Capabilities

One of the many powerful features of the ThreatBlockr platform are powerful logging capabilities with ThreatBlockr logging every connection (allowed or denied). Logs allow you to look at inbound and outbound connections and quickly see things like:

- Source and destination IP
- What country is an IP from? What network is it from based on Autonomous System Number (ASN)?
- Was it Allowed or Denied?
- Why was it Allowed or Denied? Was a connection denied because it was a malicious IP on a threat intelligence feed? The result of a Country (GEO-IP) policy?
- What threat intelligence feeds are an IP or domain on?



Date/Time	Country	ASN	Protocol	Source IP	Destination IP	↔		Category	Reason	Resource Group
Search	All	Search	All	Search	Search	All	DENY	All	All	All
11/06/20 10:18:47 AM	NETHERLANDS	DigitalOcean, LLC	TCP	10.100.99.33 :40496	198.211.120.59 :443	Out	Deny	• Proxy / VPN	COUNTRY	Office Outbound - Behind Firewall
Threat List Proofpoint										
11/06/20 10:18:47 AM	INDIA	TATA COMMUNICATIONS (AMERICA) INC	TCP	10.100.99.33 :35324	139.59.84.212 :443	Out	Deny	• Proxy / VPN	COUNTRY	Office Outbound - Behind Firewall
Threat List Proofpoint										
11/06/20 10:18:47 AM	NETHERLANDS	DigitalOcean, LLC	TCP	10.100.99.33 :22000	198.211.120.59 :443	Out	Deny	• Proxy / VPN	COUNTRY	Office Outbound - Behind Firewall
11/06/20 10:18:47 AM	INDIA	TATA COMMUNICATIONS (AMERICA) INC	TCP	10.100.99.33 :22000	139.59.84.212 :443	Out	Deny	• Proxy / VPN	COUNTRY	Office Outbound - Behind Firewall
11/06/20 10:18:42 AM	INDIA	TATA COMMUNICATIONS (AMERICA) INC	TCP	10.100.99.33 :35308	139.59.84.212 :443	Out	Deny	• Proxy / VPN	COUNTRY	Office Outbound - Behind Firewall
11/06/20 10:18:42 AM	NETHERLANDS	DigitalOcean, LLC	TCP	10.100.99.33 :40476	198.211.120.59 :443	Out	Deny	• Proxy / VPN	COUNTRY	Office Outbound - Behind Firewall

This log data can be analyzed to provide valuable information to help organizations analyze their security posture, identify and remediate threats in real time, and easily solve for false positives.

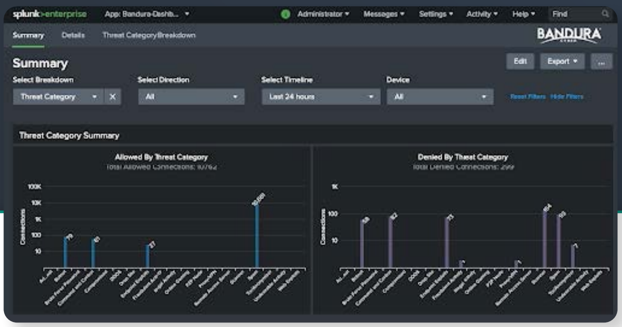
ThreatBlockr stores a limited amount of log data in memory on the device. To enable organizations to support more comprehensive security monitoring and analytics efforts and satisfy compliance requirements, the platform provides powerful syslog export capabilities. Syslog export, in the ThreatBlockr platform, is not only RFC-compliant but also includes intelligent formatting including embedded CSV and key/value pairs.
This makes it easy to export logs to SIEMs and data analytics platforms like Splunk for aggregation and long-term storage of logs, advanced analytics and reporting capabilities, and the ability to centrally view and correlate logs from multiple security controls and other systems.

Syslog export in the ThreatBlockr platform is also customizable enabling users to control which logs to export to one or more external SIEM tools. Each syslog export is independently configurable such that it can be filtered by Log Type, Resource Group, Verdict (Allowed or Denied), and Direction (Inbound vs. Outbound). This enables users to control what data they are sending to SIEMs helping them control SIEM costs, which are often driven by the volume of data the SIEM is ingesting.

ThreatBlockr Cyber App for Splunk

The ThreatBlockr App for Splunk automates the process of integrating ThreatBlockr log data into Splunk Enterprise and Splunk Enterprise Security and provides pre-built dashboards that visualize log activity from one or more ThreatBlockr appliances.

Summary dashboards provide a holistic view of your security posture where you can easily see what traffic is being allowed or denied by Reason, Threat Category, Country, and Autonomous System Number (ASN).



Summary

Select Breakdown: Threat Category

Select Direction: All

Select Timeline: Last 24 hours

Device: All

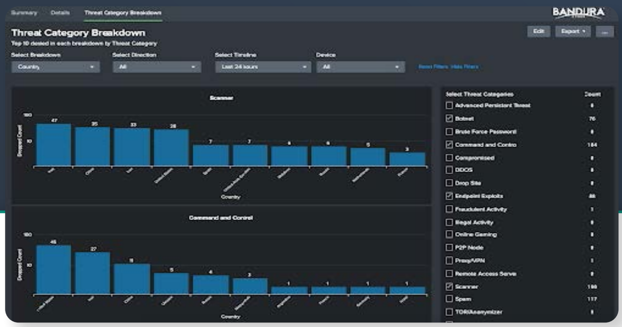
Threat Category Summary

Allowed By Threat Category

Total Allowed Connections: 10762

Denied By Threat Category

Total Denied Connections: 299



Threat Category Breakdown

Top 10 denied in each breakdown by Threat Category

Select Breakdown: Country

Select Direction: All

Select Timeline: Last 24 hours

Device: All

Select Threat Categories	Count
☐ Advanced Persistent Threat	0
☑ Botnet	76
☐ Brute Force Password	0
☑ Command and Contro	184
☐ Compromised	0
☐ DDOS	0
☐ Drop Site	0
☑ Endpoint Exploits	48
☐ Fraudulent Activity	1
☐ Illegal Activity	0
☐ Online Gaming	0
☐ P2P Node	0
☐ Proxy/VPN	1
☐ Remote Access Serve	0
☑ Scanner	198
☐ Spam	117
☐ TOR/Anonymizer	0

Detailed dashboards provide more granular data helping you to identify, investigate, and remediate threats.

These dashboards provide connection details over time allowing you to see trends in allowed and denied connections by Reason, Threat Category, Country, and ASN. The Threat Category Breakdown dashboard gives you visibility into the Top 10 denied by Threat Category. For example, the Top 10 Countries being blocked in the Command and Control threat category.

The ThreatBlockr App for Splunk has passed all relevant Splunk certifications including Splunk AppInspect and can be downloaded and installed directly from Splunkbase:

DOWNLOAD AND INSTALL