THREAT BLOCKR

THREAT RISK ASSESSMENT

RISC Technology Advisors

LOG START DATE
Thursday February 3, 2022

LOG END DATE
Friday February 4, 2022

DURATION OF ASSESSMENT PERIOD: 1 day, 23 hr, 58 min

FIREWALL VENDOR
Watchguard

This report shows the number of known-bad connections and IP addresses allowed through your firewalls **that would have been blocked by ThreatBlockr.** In today's threat landscape, it only takes one malicious connection coming into or leaving your network to cause a cyber attack.

Overall Risk Assessment

High

Assessment Summary

Total Known Bad Connections allowed by your firewall that ThreatBlockr would have blocked	202972
Known Bad Connections per day allowed by your firewall that would have been blocked by ThreatBlockr	101557
Total Known Bad IP addresses allowed by your firewall that ThreatBlockr would have blocked	951

Assessment Details

	Inbound	Outbound
Unique **Public IP addresses** that your firewall allowed	2568	9765
Known **Bad Connections** that your firewall allowed and ThreatBlockr would have blocked	21202	181770
Known **Bad IP Addresses** that your firewall allowed and ThreatBlockr would have blocked	807	144
Number of **unique ASN's** where known bad traffic was found	167	35

THREAT BLOCKR

THREAT RISK ASSESSMENT

RISC Technology Advisors

LOG START DATE

Thursday February 3, 2022

LOG END DATE

Friday February 4, 2022

DURATION OF ASSESSMENT PERIOD: 1 day, 23 hr, 58 min

FIREWALL VENDOR

Watchguard

Assessment Details *(continued)*

Known Bad traffic that was allowed by your firewall came Inbound from **these Countries**

Argentina, Australia, Austria, Bangladesh, Belgium, Bolivia, Bulgaria, Canada, China, Colombia, Denmark, Dominican Republic, France, Germany, Greece, Hong Kong, Hungary, Iceland, India, Indonesia, Iraq, Ireland, Israel, Italy, Japan, Kenya, Kuwait, Latvia, Luxembourg, Macedonia, Malaysia, Mexico, Mongolia, Myanmar, Netherlands, Nigeria, Norway, Panama, Peru, Philippines, Poland, Portugal, Puerto Rico, Romania, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Trinidad and Tobago, Tunisia, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela

Known Bad traffic that was allowed by your firewall went Outbound to **these Countries**

Austria, Canada, Finland, France, Germany, Luxembourg, Netherlands, United Kingdom, United States

Known **Threat categories** identified from Inbound traffic

Endpoint Exploits, Fraudulent Activity, Proxy / VPN, Scanner, Spam, TOR / Anonymizer

Known **Threat categories** identified to Outbound traffic

Botnet, Command and Control, Endpoint Exploits, Fraudulent Activity, Proxy / VPN, Spam

Notes

1. *A known bad connection is defined as a connection where either the source or destination IP address is known with high-confidence to be malicious by one or more of our industry-leading partner sources.*
2. *This assessment analyzes known bad IP addresses only and does not include other ThreatBlockr features such as Domain Blocking, Geo-Blocking, ASN-Blocking, Custom Blocking lists, etc.*