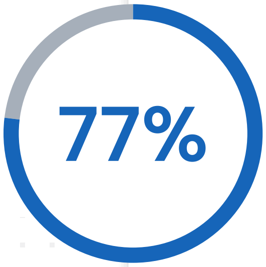
Helping MSPs Deliver Actionable Threat Intelligence

Threat Intelligence-Powered Network Protection Services for MSPs

It should not be a surprise that many small- to medium-sized businesses (SMBs) are asking more questions about cybersecurity and looking to their Managed Service Providers (MSPs) to help answer their questions. Cybersecurity became a hot topic in 2019 and continued to gain popularity in 2020.

According to Datto's 2020 State of the MSP Report, cybersecurity is expected to be a key driver of MSP growth opportunities and after economic uncertainty, client cybersecurity was the top issue keeping MSPs up at night. According to Kaseya's 2021 Global MSP Benchmark Survey Report, 77% of MSPs reported that their clients were hit with a cyberattack and a majority of MSPs said clients are now looking to the MSP to advise them on how to protect themselves. In fact, an MSP's ability to address cybersecurity challenges and mitigate risk is increasingly playing a larger role in the MSP selection process. Finally, according to the The State of SMB Cybersecurity in a 2020 report from ConnectWise, 86% of SMBs viewed cybersecurity as the top or one of the top five priorities in their organization. And, 91% of businesses would consider using or moving to a new IT service provider if they offered the 'right' cybersecurity solution for their organization's needs.

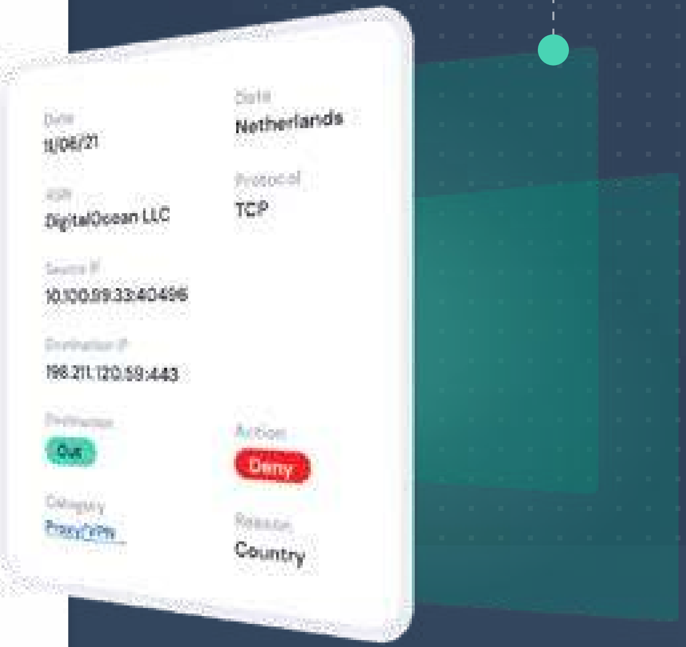
As the data shows, cybersecurity continues to be a significant growth opportunity for Managed Service Providers. In order to protect customers from cyber threats, MSPs need to provide a layered security approach that provides coverage across the multiple vectors attackers use to target users, applications, and data. While protecting endpoints is important, it's equally important that MSPs protect the networks being used by users to access applications and data.



of MSPs reported that their clients were hit with a cyberattack

When it comes to network security, many MSPs continue to rely on traditional network security controls, like next-generation firewalls. However, firewalls are having a tough time keeping up with threats because they operate with too narrow a view of threat intelligence. The result is the need for a more intelligent network security layer that is powered by threat intelligence from multiple, diverse sources.

Intelligent network security is exactly what ThreatBlockr provides. The ThreatBlockr platform blocks known bad traffic at scale using large volumes of threat intelligence from best-in-class providers and sources. MSPs are using ThreatBlockr to deliver managed intelligent network protection services that can be deployed on any network—on prem, cloud, and remote networks. MSPs are also using ThreatBlockr to deploy threat intelligence services to customers and to generate their own actionable threat intelligence based on activity across their customer bases. MSPs deploy ThreatBlockr not only because of the powerful capabilities and value the platform provides, but also because it is easy to deploy and manage, highly automated, and affordable. ThreatBlockr also complements MSPs existing managed security service offerings, including EDR, email security, firewalls, among others.



Date
11/06/21

ASN
DigitalOcean LLC

Source IP
10.100.99.33:40496

Destination IP
198.211.120.59:443

Direction
Out

Category
ProxyVPN

[illegible]
Netherlands

Protocol
TCP

Action
Deny

Reason
Country

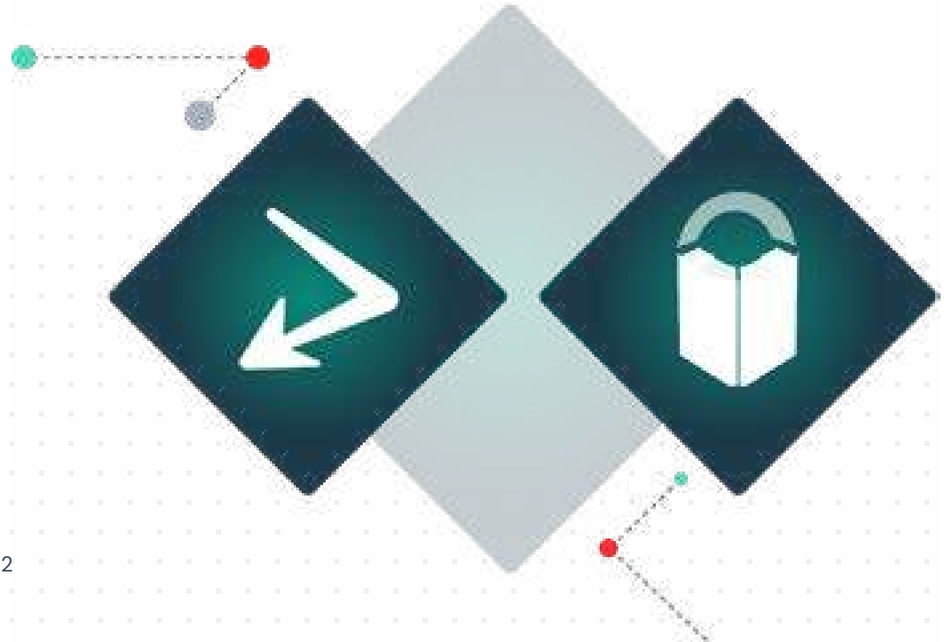
With ThreatBlockr, MSPs can expand revenue opportunities, increase the value of existing services, increase differentiation, and improve customers' security.

The Need For Stronger More Intelligent Network Protection

When it comes to network security, many MSPs continue to rely on traditional network security controls like firewalls to protect customers' networks. However, while firewalls provide a foundational level of network protection, they're having a tough time keeping up with today's advanced threats.

One of the key challenges with firewalls is they rely on proprietary threat intelligence to detect and block threats. This threat intelligence has value but alone is insufficient because it provides too narrow a view of the threat landscape—a single vendor's view. Defending against today's threats requires the use of threat intelligence from multiple sources, including commercial threat intel providers, open source, industry, and government sources. This is why more MSPs are adding threat intelligence into their security offerings to increase visibility into threats and improve protection for customers.

While threat intelligence provides significant benefits, it can bring its own challenges. It can be resource intensive and hard to deploy. Another significant challenge is the inability to integrate third-party threat intelligence data into existing security controls like firewalls. Firewalls don't play nicely with third-party threat intelligence and have significant limits on the amount of third-party threat intel data they can integrate.



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. The platform provides tens of millions of "out of the box" threat indicators from the world's best sources and offers over 50 point-and-click integrations and connectors: ISACs, ISAOs, Threat Intelligence Platforms (TIPs), SIEMs, SOARs, or any other IP or domain-based source.

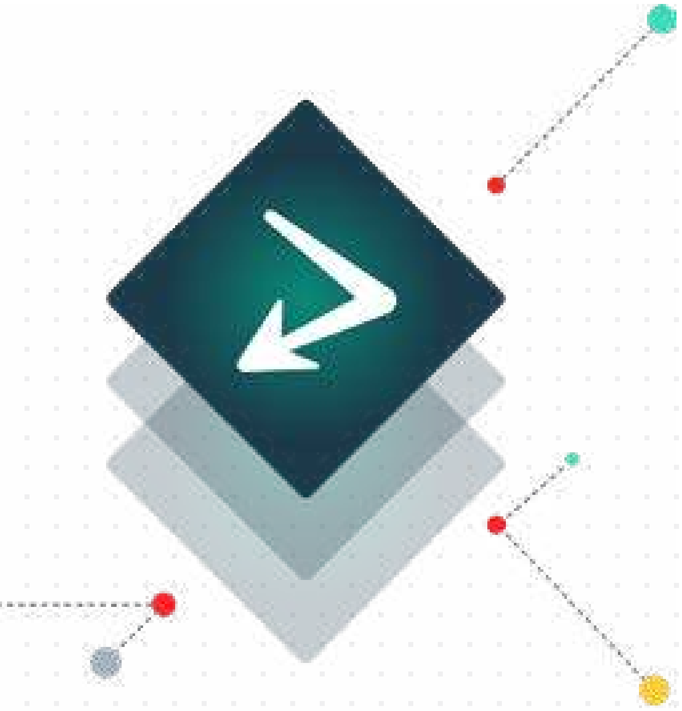
Policy enforcement and blocking is handled by ThreatBlockr, which can block up to 150M threat indicators in real-time with no latency. ThreatBlockr inspects inbound and outbound traffic and makes simple, policy-based allow or deny decisions based on threat intelligence (IP reputation, block lists, allow 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, MSPs can protect users and networks everywhere and our cloud-based, multi-tenant management portal gives MSPs a central point of visibility and control for all customers.

As data flows through ThreatBlockr, the ThreatBlockr platform generates a significant amount of data that lets MSPs analyze customers' security posture, identify and remediate threats in real time, and easily solve for false positives. Non-PII metadata is sent to the cloud-based management portal to allow quick analysis of customers' security posture and detailed data can be sent to any SIEM, Syslog server or security analytics tool for further detailed analysis.

Policy enforcement and blocking is handled by ThreatBlockr, which can block up to 150M threat indicators in real-time with no latency.

How MSPs Are Using ThreatBlockr

MSPs are using ThreatBlockr to expand service offerings across network security, threat intelligence, cloud security, and security-as-a-service for remote user protection.



Managed Network Protection Service Powered by Threat Intelligence

MSPs are using ThreatBlockr to provide a next-generation network protection service that is powered by threat intelligence. Using ThreatBlockr, MSPs are able to improve customers' network security by proactively using threat intelligence to prevent threats while also having the ability to provide rapid and automated threat response. Importantly, this network protection service complements existing network security capabilities and services provided by next-generation firewalls. ThreatBlockr not only provides another layer of network protection but also improves the effectiveness and efficiency of firewalls.

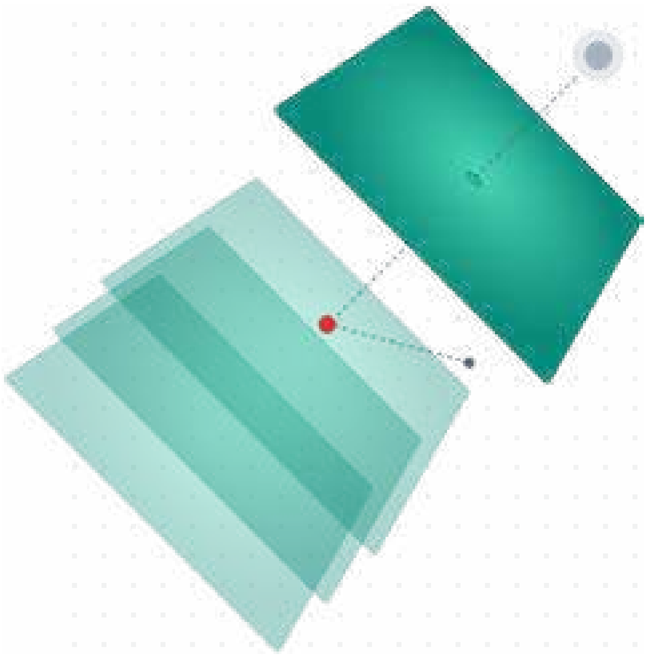
Managed Threat Intelligence Service

MSPs are also using ThreatBlockr as a platform to provide managed threat intelligence services to customers. With ThreatBlockr, MSPs can quickly deploy actionable threat intelligence to protect customer networks. ThreatBlockr also provides MSPs with insights and data into threat activity occurring at customers. By aggregating this data, MSPs can generate their own threat actionable intelligence that can be used to increase protection for customers, increase differentiation and expand revenue opportunities.

Cloud Protection

ThreatBlockr Cloud enables MSPs to strengthen cloud security offerings. ThreatBlockr Cloud protects customers' cloud networks in AWS, Azure (forthcoming), and in the future Google Cloud.

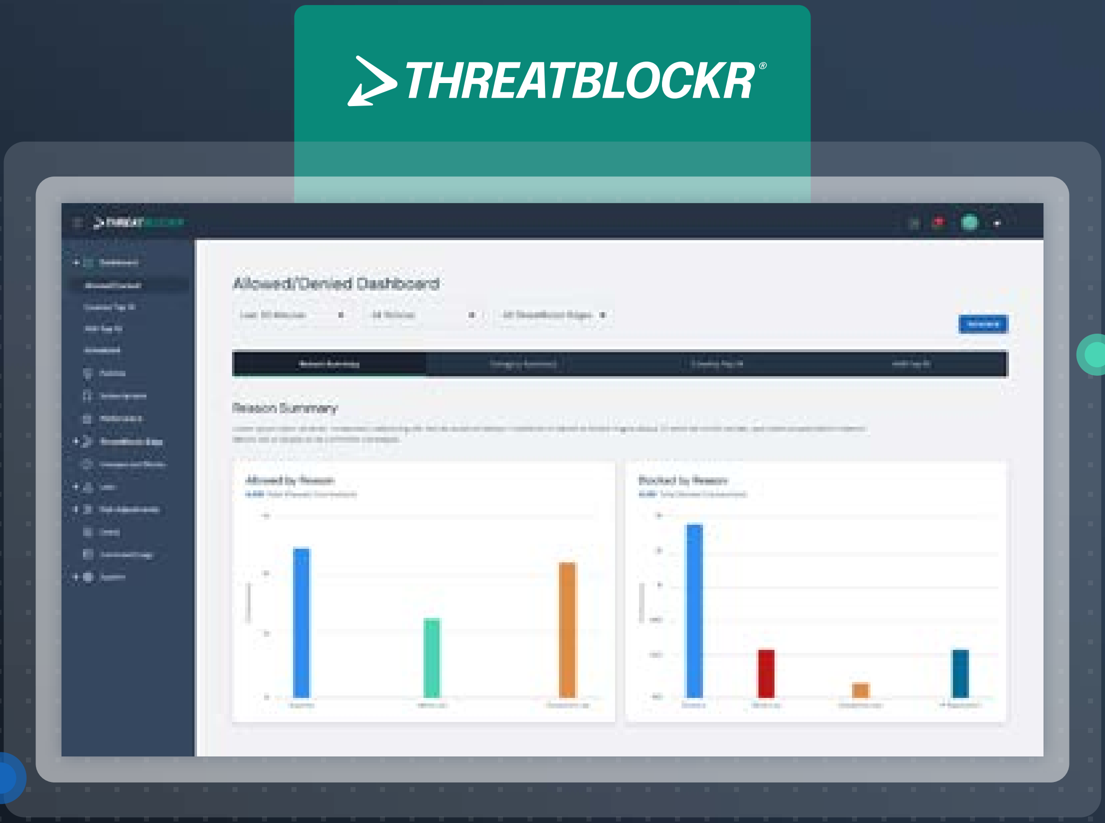
ThreatBlockr Everywhere… All With Centralized, Multi-Tenant Management



With ThreatBlockr, MSPs have the flexibility to expand managed security service offerings in multiple ways and to protect applications, data, and users wherever they are—on prem, cloud, and remote. Importantly, cloud-based multi-tenant management capabilities make it easy for MSPs to manage ThreatBlockr across their customer base and across hybrid, multi-cloud environments.

ThreatBlockr Platform Key Features

- **Block up to 150 Million IP and Domain Indicators:** ThreatBlockr can detect and block up to 150 Million threat indicators at line speed. This far exceeds the capabilities of any next-gen firewall.
- **Out of the Box" Threat Feeds:** ThreatBlockr provides tens of millions of "out of the box" threat indicators from best-in-class providers including leading commercial threat intel providers, open source, and government sources.
- **Easily Integrate IP and Domain Threat Intelligence From Any Source in Real Time:** Using over 50 out of the box connectors and integrations, MSPs can easily add additional IP and domain threat intelligence into the platform. Easily add customer-specific threat intelligence or threat intelligence for all customers.
- **Highly Automated & Low Touch:** Threat intelligence data is automatically updated and policies applied in real time. The ThreatBlockr platform scales to the needs of the MSP from the low touch "set and forget" crowd to those that want to take a deeper, more "hands on" approach.
- **Quick and Easy to Deploy:** Deploying ThreatBlockr is quick and easy with most deployments happening in 30 minutes or less. Installing ThreatBlockr in customer environments is simple requiring no significant network configuration changes. ThreatBlockr is deployed as a layer 2, "bump in the wire" either in front of or behind the firewall.
- **Simple Policy Management:** Policy management with ThreatBlockr is simple. Activate the threat intelligence sources you want to use, set risk score thresholds for blocking threat categories, and set any country blocking policies. Boom! That's it! You're off and running!



- **Clear Visibility into Activity with Dashboards:** Quickly see activity and the security posture of customers through easy to read, high level dashboards that show network connections, threats, countries, and networks being allowed or denied.
- **Multi-tenant Management:** Multi-tenant, cloud-based management capabilities make it easy for MSPs to configure and manage the ThreatBlockr platform for multiple customers.

- **High Value Log Data:** ThreatBlockr logs every network connection and provided detailed information on connections being allowed and denied and threats targeting customers' networks. MSPs can use log data for deeper analysis and investigations. Robust syslog export capabilities enable easy export of log data to log management and SIEM solutions for long-term log storage and analysis and correlation with other security and system logs. By aggregating log data across all customers, MSPs can identify trends in threat activity and generate MSP-specific threat intelligence.
- **Affordable:** Along with simplicity and ease use, affordability is a key value proposition consistently highlighted by ThreatBlockr customers.
- **Everywhere:** The ThreatBlockr platform allows MSPs to protect applications, data, and users wherever they are on premises, in the cloud, and/or remote networks.