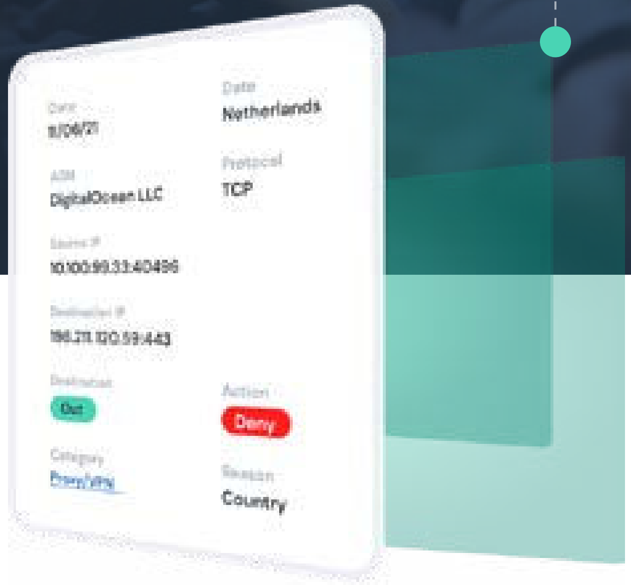
threater™

An MSP's Guide to Building a Successful Security Practice

Threater.com

Global cybercrime costs are expected to reach **$10.5 trillion USD annually by 2025**, an estimation based on recent year-over-year growth, the dramatic increase in nation-state sponsored and organized crime activities, and a threat surface that continues to expand each day. From damage and destruction of data, stolen money, intellectual property theft, to organizational downtime, lost productivity, and reputational harm, it's clear that more than money is at stake as cyber threats continue to increase. Unfortunately, many cybersecurity measures being used by businesses, governments, and individuals are **increasingly futile in comparison** to the growing sophistication of cybercriminals. It is more important than ever that MSPs evaluate their cybersecurity programs to ensure they are protected in the event of an attack.



Date
11/06/21

ASN
DigitalOcean LLC

Source IP
10.100.99.33:40496

Destination IP
198.211.120.59:443

Direction
Out

Category
Proxy/VPN

Geo
Netherlands

Protocol
TCP

Action
Deny

Reason
Country

01

Protect Yourself to Protect Others

As MSPs increasingly become cybercriminals' prime targets, their ability to protect themselves is a top priority.

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.

Protecting your network requires a three-pronged approach:

Build concentric rings of security around your data:
If for some reason your endpoint security system or firewall misses something, what do you have in place to pick it up? Your security suite should include tools that can scan for vulnerabilities, detect instructions, isolate attackers before they can move through a network, and mitigate damage.

Visibility is key – enable real-time monitoring:
You need to know if you have a problem – that's why monitoring your environment is basically essential. Best-of-breed security operations centers monitor and detect cyber incidents 24x7 to help keep MSPs ahead of potential threats in their networks and within client networks.

Standardize on accepted frameworks for cybersecurity:
A framework – such as the NIST Cybersecurity Framework – is not a solution in and of itself, but will provide a way for MSPs and their clients to measure performance against those best practices and continually improve.

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.

02

Collaborate and Consolidate

Defending against today's threats is a volume game that requires the use of threat intelligence from multiple sources.

Cyber attacks are big business, with threat actors ranging from individual attackers to well funded, coordinated cyber threat organizations, to state sponsored attacks. Therefore, one vendor or threat intelligence provider's view of the threat landscape is simply not enough to protect from the constantly evolving and sophisticated threat actors that are attacking. This is proven not only in the volume of threat intelligence available, but also the fact that when comparing various threat intelligence from multiple vendors, the overlap is negligible.

Let's face it, we're spoiled for choice when it comes to security solutions. The market is heavily saturated, particularly post-pandemic as many organizations made the move toward remote or hybrid working. Despite organizations needing more robust security measures than ever before, budgets are tight and leadership may feel pressured to only focus on the specific problem they face today, rather than thinking bigger picture to protect against the threats of the future. That said, a piecemeal approach to security poses significant challenges for IT and security teams, from performance issues and delayed incident response time, to unnecessary complexity and siloed information. Siloed information leads to a lack of visibility across environments, which could ultimately force security teams to make critical decisions based on inaccurate or incomplete data. Further, without the proper context, information can't be appropriately prioritized and business-critical data could be lost or held for ransom.

A multi-vendor approach might offer a fix for short-term problems, but it puts a great deal of strain on security teams who might not have the resources to adequately vet every product or vendor. CISOs might have a good idea of what's best for their own organization, but it's difficult to apply that knowledge to an ever-expanding list of disparate vendors that are pulled together under one umbrella.

Siloed information leads to a lack of visibility across environments.

03

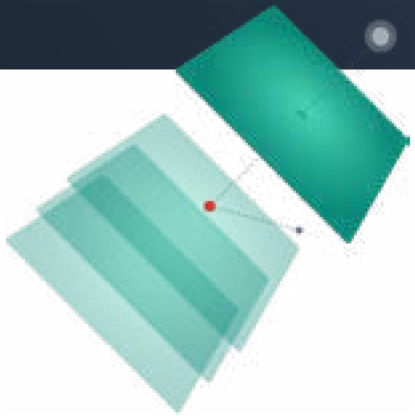
Assess Your Cyber Portfolio

Organizations might fall into the trap of thinking cybersecurity is a one-and-done type of deal.

They implement a patchwork of solutions for known problems, assume they are “good to go” or “set it and forget it,” and are unfortunately surprised when their organization remains at risk. As with most areas of business, it’s important to take a critical look at each solution that your organization relies on for security.

A few questions that security teams should be asking about to get a more accurate view into their organization’s network defense posture:

- ✓ What does your team’s cybersecurity knowledge look like?
- ✓ Does your security team spend time understanding the “other side?”
- ✓ Which challenges are facing your organization today?
- ✓ Which challenges might your organization face in the future?
- ✓ What are your organization’s – wwand its customers’– most important assets?



04

Offer a Comprehensive Solution

To stay safe in today’s increasingly dangerous threat landscape, cybersecurity requires an integrated and consolidated approach that covers all the bases, from endpoint to data center to cloud.

Unfortunately, many vendors offer “next-generation” security solutions and, while this is technically achievable with a multi-vendor approach, it’s simply not viable for organizations that want to take a long-term, streamlined and cost-effective approach to security. Now, more than ever, organizations need to consolidate solutions and go back to basics with a comprehensive cybersecurity solution.

Building security awareness and providing training is essential. Protecting against cyber threats is easier when everyone in an organization is informed about the risks and common tactics that may be used against them. Further, keeping backups, maintaining systems, and implementing the right combination of technology can help build your organization’s cyber defenses.

05

Gain Efficiency with Threater

This is where Threater comes in!

The Threater platform blocks known bad traffic at scale using large volumes of threat intelligence from best-in-class providers and sources.

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. Threater appliances handle policy enforcement and blocking, with the capability of blocking up to 150 million threat indicators in real-time with no latency. As data flows through Threater appliances, the Threater platform generates data that lets MSPs analyze customers’ security posture, identify and remediate threats in real time, and easily solve for false positives.

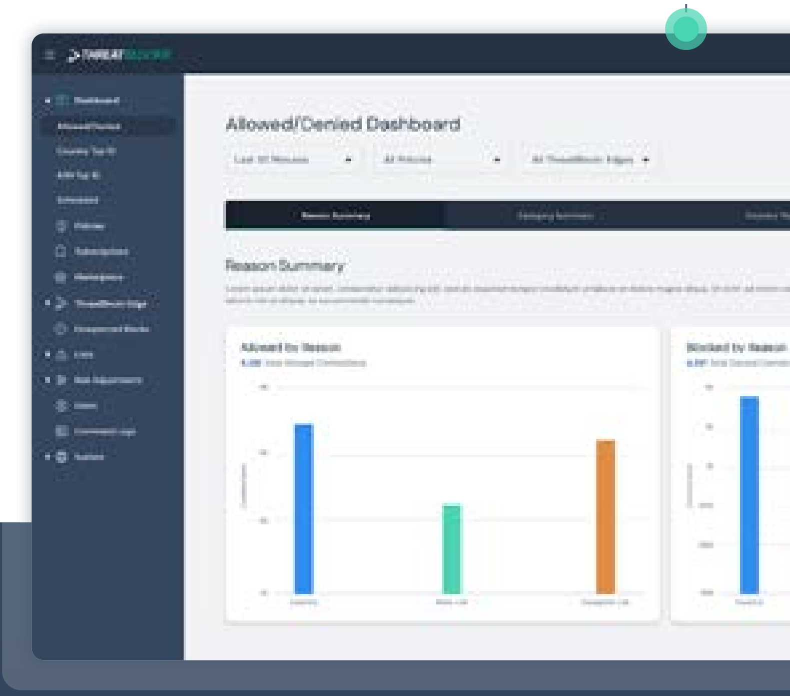
150 MILLION

THREAT INDICATORS IN REAL-TIME

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. Threater appliances handle policy enforcement and blocking, with the capability of blocking up to 150 million threat indicators in real-time with no latency. As data flows through Threater appliances, the Threater platform generates data that lets MSPs analyze customers’ security posture, identify and remediate threats in real time, and easily solve for false positives.

When it comes to cloud and remote user protection, Threater has your back. Threater Cloud enables MSPs to strengthen cloud security offerings. Threater Cloud protects customers’ cloud networks in AWS, Azure (forthcoming), and in the future Google Cloud. Threater Anywhere is a cloud-based service that MSPs can use to protect customers’ remote and mobile users. Threater Anywhere can be consumed as a hosted service or MSPs can operate their own Threater Anywhere service using Threater Cloud for AWS in combination with Threater Anywhere Server.

MSPs use Threater to provide a next-generation network protection service powered by threat intelligence. Threater not only provides another layer of network protection but also improves the effectiveness and efficiency of firewalls, complementing existing network security capabilities and services. With Threater, 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.



06

Offer a Comprehensive Solution

When it comes to cybersecurity, performance is key.

With Threater, MSPs and their customers don't have to choose between performance and security - they can have both!

Deploying Threater is quick and easy with most deployments happening in 30 minutes or less. Not to mention, installing Threater in customer environments is simple, requiring no significant network configuration changes. Out of the box, Threater provides tens of millions of threat indicators from best-in-class providers and leverages over 50 connectors and integrations to easily add IP and domain threat intelligence. Highly automated and low touch, Threater's threat intelligence data is automatically updated and policies applied in real time, scaling to your needs.

MSPs can achieve clear visibility into customer activity through easy to read, high level dashboards that show network connections, threats, countries, and networks being allowed or denied. With multi-tenant management, Threater makes it easy for MSPs to configure and manage the platform for multiple customers. High value log data provides detailed information on connections being allowed or denied, as well as threats targeting customers’ networks.

Lastly, Threater is affordable and easy to use, enabling MSPs to protect applications, data, and users wherever they are on premises, in the cloud, and/or remote networks. With Threater, MSPs can expand revenue opportunities, increase the value of existing services, increase differentiation, and improve customers’ security.

Interested in learning more? Run a full threat scan in minutes with **Threater’s Free Firewall Risk Assessment.**