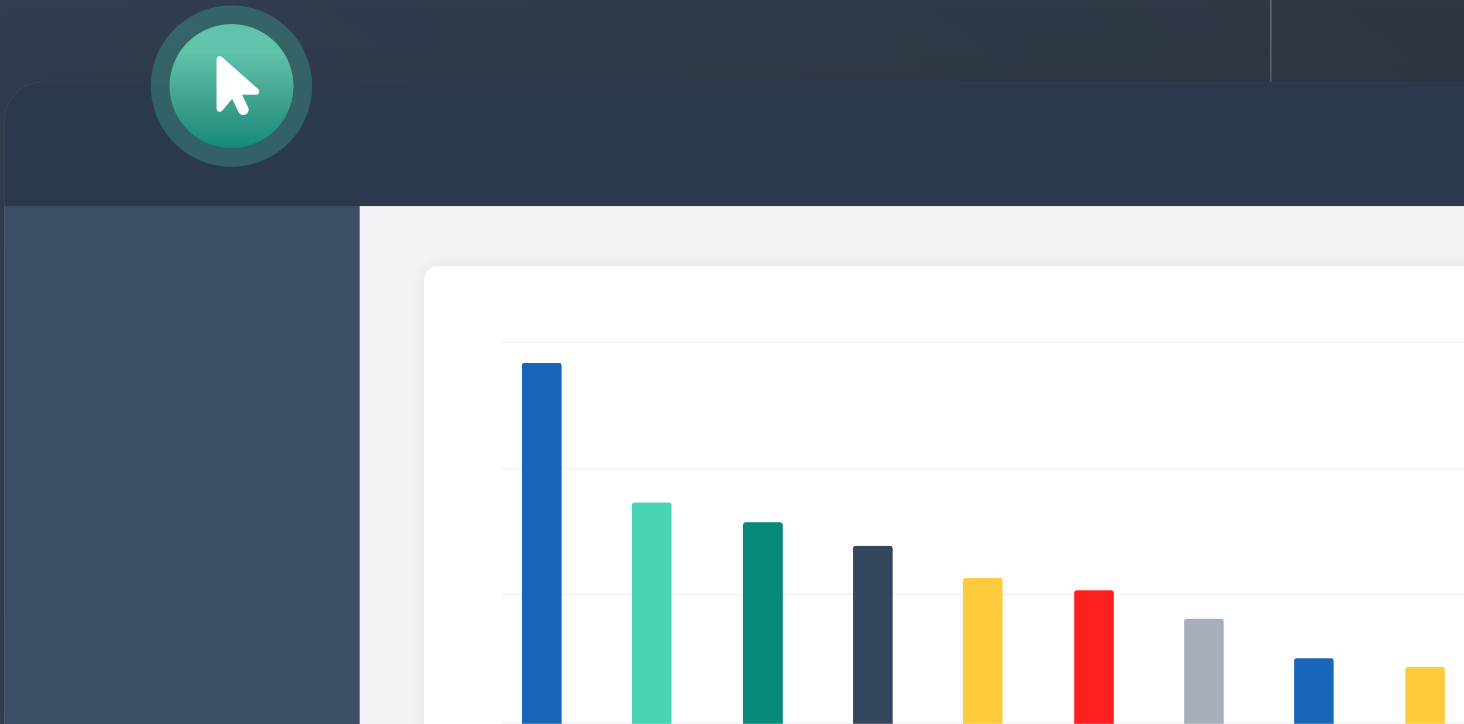
threater

2022

# Security Stack

## Insight Report



# Security Stack Insight Report

## Introduction / Executive Summary

At the Black Hat USA 2022 conference, keynote speaker Chris Krebs discussed his time as the director of the Cybersecurity and Infrastructure Security Agency (CISA) and shared insights into the current state of cybersecurity. He discussed escalating international tensions and the role of cyberwarfare in future clashes, which we're already seeing in the conflict between Russia and Ukraine. In one example, a mass distributed denial of service (DDoS) attack from Russia targeted Ukrainian websites and national banks, forcing the affected agencies and organizations to route traffic elsewhere as cybercriminals flooded networks with illegitimate traffic to impede the normal operations of these services. These types of cyberattacks are the new battleground of modern warfare, and other bad actors may also see a window of opportunity to increase attacks as uncertainty increases across the globe.

When it comes to enterprise security, cybersecurity threats are a ticking time-bomb for many companies, but many have yet to identify cybersecurity as a main budget priority. With cyberattacks increasing in frequency and severity, safeguarding against data breaches, ransomware, and other cyberthreats should be a top concern for businesses of all sizes across every industry. In an ever-changing cyber landscape, companies can no longer protect against real-time data threats with legacy solutions and reactivity. Unfortunately, security-conscious organizations often face the difficult challenge of effectively integrating dozens of threat intelligence tools into their security stack and making sense of the data within their unique context.

As this report reveals, organizations need a more proactive approach to cybersecurity that includes gathering threat intelligence and gaining awareness of vulnerabilities, rather than depending on reactive solutions. Relentless cyberattacks require real-time intelligence that draws from the very best sources and automated protection that actively defends every moment of every day.

# Table of Contents

## Survey Audience/Overview

Threater conducted an online survey of 300+ US-based IT professionals in Summer 2022. Titles included C-Suite Executive, Directors, and Managers in Higher Education, Finance, Computer and Technology, Healthcare, Manufacturing, Pharmaceutical, Telecommunication, and Aerospace in companies with 200+ employees.

> “I’ve been in the industry for a long time, having witnessed many evolutions of cyber threats and defenses created in response—or anticipation. More than ever, it’s crucial for organizations to combine active and reactive cybersecurity strategies to protect their business, their customers, and the industry from sophisticated attackers. By taking lessons learned from the past, we can leverage insights like those within this report to build a more secure future.”

**Ron Gula**
Gula Tech Adventures, *President & Co-founder*
Tenable, *Founder*

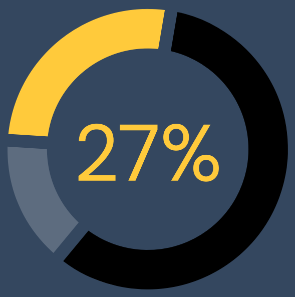
Chapter 1

# Current State of Enterprise Security

## Hope For the Best, Plan For the Worst.

QUESTION

How many tools and services are in your security stack today?

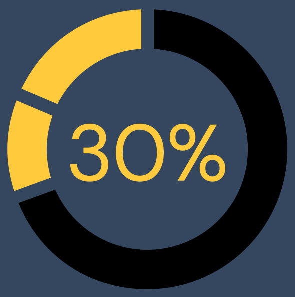


27% of professionals don't know how many tools they have in their security stack, a significant risk for cybersecurity.

| ANSWER CHOICES | RESPONSES |
|---|---|
| 1-9 | 58% |
| 10+ | 15% |
| Unknown | 27% |

QUESTION

Do you think your firewall provides the network protection you need?



30% are not sure if their firewall provides the network protection they need.

| ANSWER CHOICES | RESPONSES |
|---|---|
| Yes | 69.58% |
| No | 11.97% |
| Unsure | 18.45% |

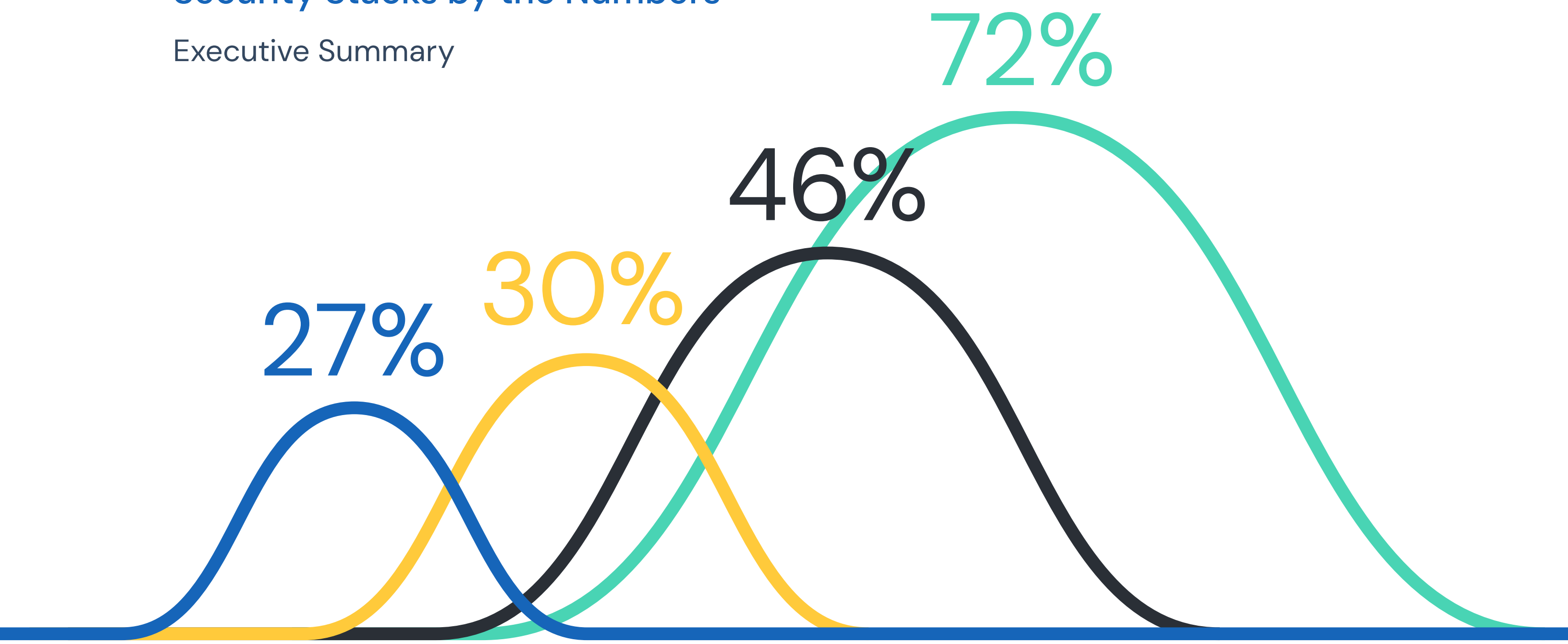
Big Picture Data

You can't protect your technology stack if you don't know what comprises it. The only way to secure your stack is to educate yourself and your team on potential vulnerabilities and ensure your system has all the latest updates and additional security features to protect your company from those threats.

We can't discuss the current state of enterprise cybersecurity without mentioning the ongoing impact of the mass shift to remote work, as well as other workforce changes brought about or accelerated due to the pandemic. It created a perfect storm for enterprise cybersecurity, as threats increased, perimeters grew, and social concerns took precedence – and left individuals vulnerable to cybercriminals who quickly took advantage. With a more dispersed workplace, companies adopted more tools and technologies to support their workforce and continue operations. From a cybersecurity standpoint, this led to an increased attack surface with more potential entry points for cybercriminals to enter an organization.

## Security Stacks by the Numbers

Executive Summary



**27%** of professionals don't know how many tools they have in their security stack, a significant risk for cybersecurity.

**30%** are not sure if their firewall provides the network protection they need.

**Almost half (46%) of professionals have more than six tools and services in their security stack today.**

**Threater allows you to seamlessly integrate into existing security systems, no matter the number of tools you have.**

**72%** of respondents have added new technologies in the past 12 months.

Not all technology professionals know each tech added to the stack. This threat of unknown is risky for the business—allowing for system vulnerabilities.

Too many organizations approach their cybersecurity as an afterthought, believing that instead of developing a well-rounded defense strategy against bad actors, they should invest in one or two defenses like a firewall or antivirus software, then call it a day. Unfortunately, today's threat landscape is too varied and dangerous for this lazy approach to work.

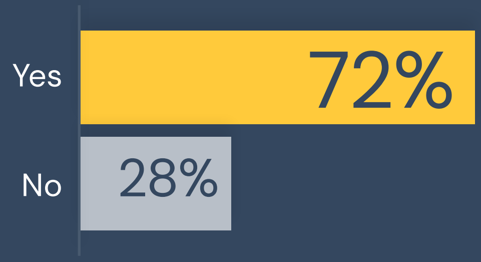
Firewalls in particular aren't designed to, and therefore can't, catch every threat, because the threat intelligence they use represents too narrow a view of the threat landscape in todays era of encrypt everything. Defending against threats is a volume game that requires the use of large volumes of cyber intelligence from multiple sources, deployed intelligently to negate the impact of encryption. Firewalls leave a large gap in cybersecurity for organizations, not to mention the excess manual work and time that must be spent managing or adding threat intelligence in firewalls—and even that is limited. Organizations often think that firewalls protect their attack surface — but they forget that firewalls also comprise a portion of their attack surface itself.

> Organizations often think that their firewalls are protecting their attack surface and they forget that their firewalls are also part of their attack surface.

QUESTION

Have you added any new technologies in the past 12 months?

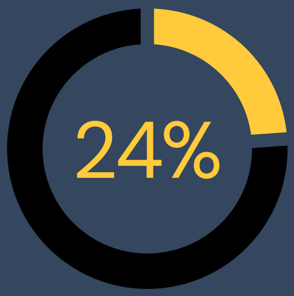
| ANSWER CHOICES | RESPONSES |
|---|---|
| Yes | 71.84% |
| No | 28.16% |



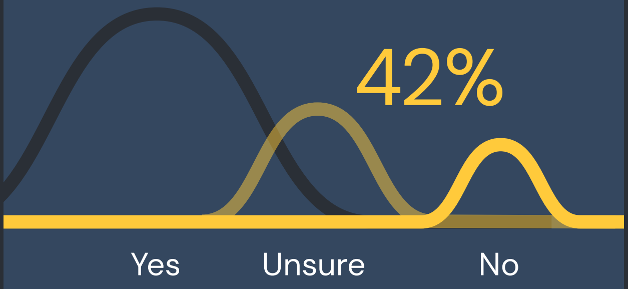
We're continuing to see the longer term impacts of recent workforce shifts and organizations often make the mistake of focusing only on reactive cybersecurity strategies that will detect an attack in progress and hopefully stop it in its tracks. While these defensive approaches are necessary, most organizations should also be considering a more active strategy in addition to these defensive practices.

# Repercussions of a Penetrable Security Stack

## The Best Defense is Both Active and Reactive.



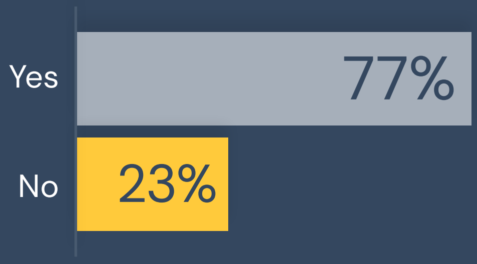
**Almost a quarter of professionals (24%) said their security posture is average or below average, indicating that their security stack is vulnerable to threats.**



QUESTION

Are you using any Cyber Intelligence or threat data sources?

| ANSWER CHOICES | RESPONSES |
|---|---|
| Yes | 57.61% |
| No/Unsure | 42.39% |



QUESTION

Do you have the ability to add new technology or tools if new attacks are demonstrated?

| ANSWER CHOICES | RESPONSES |
|---|---|
| Yes | 77.35% |
| No | 22.65% |

The best defense involves both reactive (such as detection and response solutions) and active (such as threat intelligence) cybersecurity strategies, which combine to form a sophisticated buffer against threat actors who are eager to gain entry into your system and steal valuable data, assets, and more.

A threat intelligence source is an internal or external place where data on cybersecurity threats is collected and analyzed. Unfortunately, the challenge for many organizations is narrowing down which sources they're pulling from, how many can be leveraged at a time, and how they're being integrated into firewalls and other security solutions.

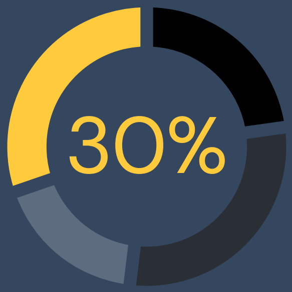
When it comes to firewalls, there is a limited ability to add threat intelligence after the initial setup. These limits include the volume of threat intelligence they can support and the ways you can integrate intelligence into the firewall. Further, updating intelligence in firewalls is too manual and slow. For many organizations, managing external blocklists and allowed lists on firewalls is a manual process. Plus, the threat intelligence volume limits of firewalls adds more work and time, while even more time can be added due to firewall change management processes. This leads to regular management and updates not being done and critical changes not being addressed. If this management slides, other holes get exposed and threat actors can weasel their way in.

As the threats and the threat actors have evolved, so have the methods of identifying them. No one source of threat intelligence or existing security control can cover the entirety of the threat landscape. This means it's critical to use threat intelligence from multiple sources. Sophisticated and security-savvy organizations incorporate a broad-based view of threat intelligence, from multiple cyber threat intelligence sources—commercial providers, open source, government, and industry sources—into their security operations. By leveraging threat intelligence sources from varied perspectives, these organizations gain true visibility into the types of malicious traffic that may affect their networks, improving their ability to protect their networks and organization.

> "There's no denying that cybercrime is growing increasingly sophisticated, and recent headlines are highlighting how challenging it is for organizations to keep up. Despite massive industry innovation and government guidance in recent years, much of the technology we use to protect ourselves remains the same. Firewalls in particular are antiquated when compared to the tools cybercriminals are using, leaving organizations with gaps in their cybersecurity defenses. We need to address these limitations to evolve in tandem with the advancement of cyber threats."
>
> **Pat McGarry**
> Threater, CTO

# Importance of a Security Budget

## Spend a Little Now, Save a Lot Later.



QUESTION

How often do you evaluate your security budget?

| ANSWER CHOICES | RESPONSES |
|---|---|
| Once a month | 22.98% |
| Once a quarter | 29.13% |
| Once a year | 17.80% |
| Unknown | 30.10% |

Staying up-to-date with tools is incredibly important to stay one step ahead of your attackers

Almost one-fifth (19%) of professionals have a limited budget for security (less than $100k).

$
100K
Estimated Annual Security Budget
19%

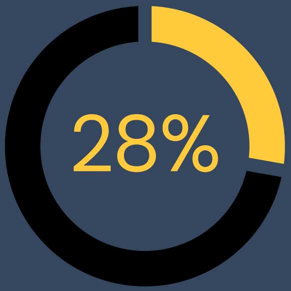
| ANSWER CHOICES | RESPONSES |
|---|---|
| $0- $100,000 | 18.77% |
| $101,000 - $500,000 | 18.77% |
| $501,000 - $5M | 18.45% |
| $5.1M - $20M | 12.62% |
| $20.1M + | 2.91% |
| Unknown | 28.48% |

**With cyber threats rising, prioritizing a security budget and proactively allocating resources to block attacks is critical. As our research shows, most security teams are faced with limited budget and staff constraints. There is a perception that cybersecurity—and threat intelligence in particular—is expensive to acquire and requires significant resources (tools, people, money) to manage and operationalize. But that doesn't have to be the case.**

When it comes to threat intelligence in particular, there are plenty of sources that organizations can access affordably, including open source threat intelligence feeds, and industry and government sourced-intelligence. There are also high quality commercial intelligence feeds that companies can acquire without breaking the bank. Beyond acquiring threat intelligence, managing threat feeds also doesn't have to be difficult or resource intensive. Modern threat intelligence has evolved—you don't need endless money, tools, or staff to manage it. There are great solutions that are easy to deploy, highly automated, and affordable. The most important part to getting the bang for your buck is how you put that threat intelligence to use.

# The Future of Enterprise Security

## Adapt Today to Secure Tomorrow.



QUESTION

Have you added any new technologies in the past 12 months?

28% of professionals haven't updated their security stack in the past 12 months. With attackers becoming more sophisticated, professionals need up-to-date technology to protect their enterprises.

| ANSWER CHOICES | RESPONSES |
|---|---|
| Yes | 71.84 |
| No | 28.16% |

Big Picture Data

In the wake of the pandemic, we've seen cybercrime expand rapidly. In fact, the total global cost of cybercrime is expected to jump to over $10 trillion by 2025. In his Black Hat USA 2022 keynote, Brian Krebs discussed the four factors the cybersecurity community needs to analyze in order to determine the future of the industry: technology, bad actors, government, and people. Looking at the past, present, and future of these factors enables us to efficiently and effectively evolve for a more secure future.

## Four factors shaping the future of the cybersecurity industry

### TECHNOLOGY

In a world where you can connect to nearly anything from almost anywhere, the number of network endpoints has proliferated. From free Wi-Fi networks to unencrypted applications, most people are unaware of how their daily technology use might open them—and their company—up to exploitation by eager bad actors.

### BAD ACTORS

We're not the only ones who have adapted to the new work-from-anywhere world. Cybercriminals are getting smarter and have more resources than ever. Repelling one cyber attack doesn't mean your troubles are over, in fact, it may have just given a bad actor more information they can use to mount the next successful attack.

### GOVERNMENT

The Biden Administration's Executive Order (EO) on Improving the Nation's Cybersecurity highlighted the increasing importance of modernizing cybersecurity infrastructure. Following a string of high-profile cyber attacks, the government has doubled down on modernizing cybersecurity defenses of federal infrastructure, improving collaboration between the public and private sectors, and solidifying the nation's ability to respond to cyberattacks.

### PEOPLE

The volume and speed of remote work opened up a number of vulnerabilities in many organization's cybersecurity infrastructure. Though many companies have now reopened offices, some remain hybrid or entirely remote, leaving IT and security teams with new challenges to boost security for all, regardless of where they are working.

The cyber threat landscape is continually evolving. To secure themselves now and into the future, companies need to invest in cybersecurity infrastructure that can adapt and change with the threats and tactics on the horizon.

> "If we work together to apply lessons learned and advance our knowledge of evolving cyber threats, we can lay the foundation for a more secure future. Collaboration is key if we have any chance of keeping pace with the most agile players in the cybercrime space."
>
> **Stephen Semmelroth**
> Sr. Director of Security, Avant Communications.

# Threater: Your Cybersecurity Partner

## Leading the Intelligence Enforcement Revolution.

Cybercrime has become a profitable business model and launching attacks is now an opportunity for revenue. Every successful attack has breached the security stack. Once the foundation of good cybersecurity, firewalls and other security products are not enough to block all of the sophisticated attacks that are being used by today's hackers. Enterprise defenders need a way to block modern threats that get through their security stack.

While most cyber products are reactive, identifying threats that have already entered a network and alerting a human of the threat, Threater takes a different approach by blocking known bad traffic before it hits the network, and by blocking both inbound and outbound actions. Using more than 50 world-class cyber intelligence feeds to inspect, block, and log every known threat from hitting your network while reducing alerts and allowing your existing security controls do function better. Threater provides instant network protection without expensive upgrades and without overcomplicating the technology stack.

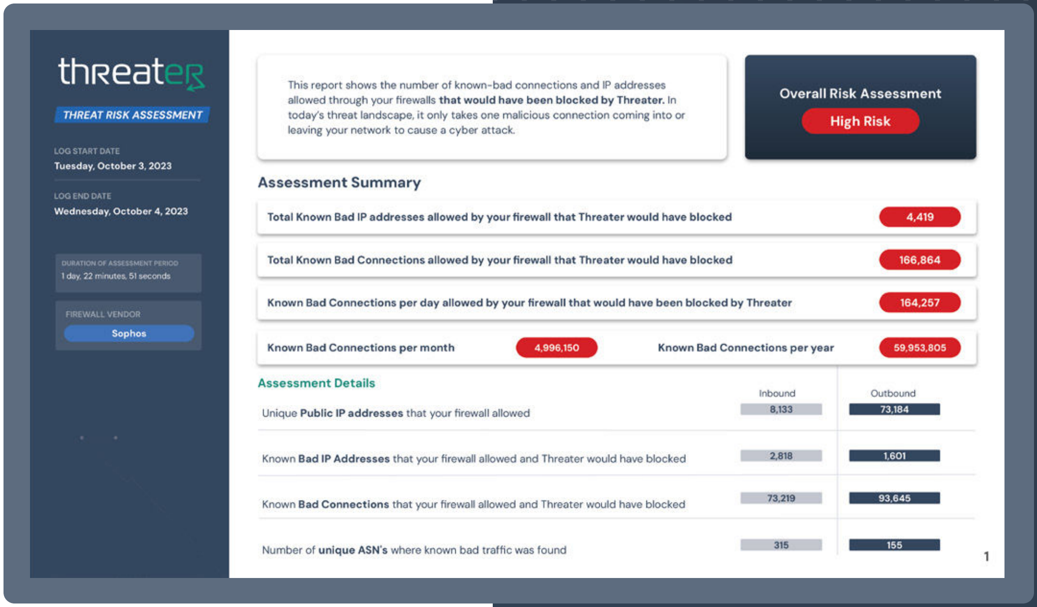
With cybersecurity threats on the rise, and exacerbated by a more vulnerable dispersed workforce, attacks for many companies aren't so much a case of 'if', but 'when.' And, in fact, data shows that in many cases, the attackers are already there we have to assume attacks are a foregone conclusion. Preparing and raising digital defenses can deflect a lot of these attacks, but companies that don't invest in active security now are likely to pay a much higher price in the long run.

### Run a Full Threat Scan

- → Understand your overall security threat positioning
- → Identify assets within the organization
- → Understand vulnerable and compromised areas such as:
  - ✓ Total known bad connections allowed by firewall
  - ✓ Known bad traffic by country that was allowed by your firewall
  - ✓ Known threat categories and potential types of attack breaches

Want to know what it looks like?
Check out the next page to learn more!

Risk Assessment



*THREAT RISK ASSESSMENT*

LOG START DATE
Tuesday, October 3, 2023

LOG END DATE
Wednesday, October 4, 2023

DURATION OF ASSESSMENT PERIOD
1 day, 22 minutes, 51 seconds

FIREWALL VENDOR
Sophos

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

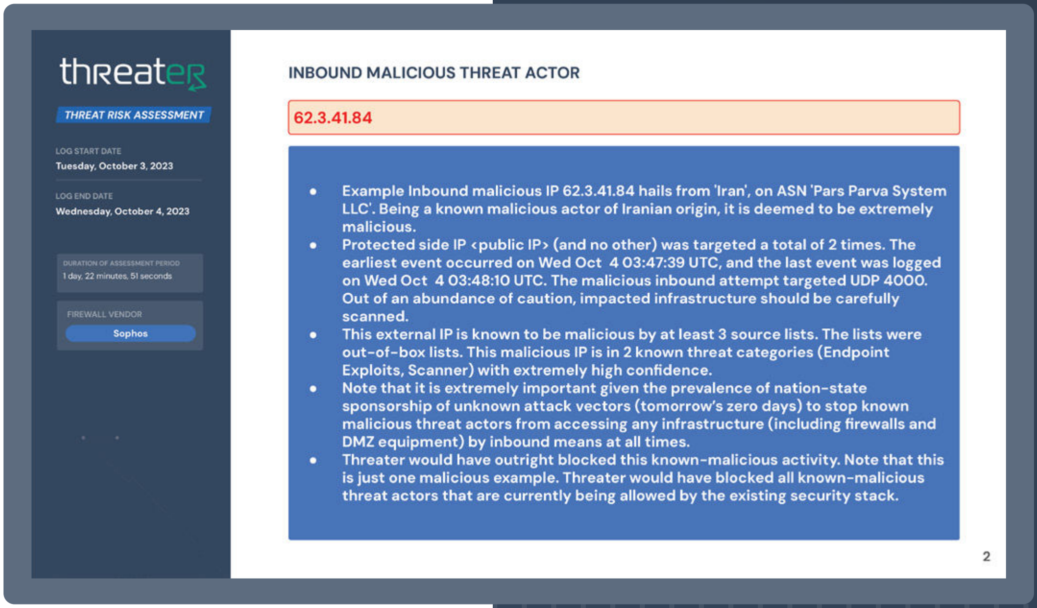
Overall Risk Assessment
High Risk

Assessment Summary

| | |
|---|---|
| Total Known Bad IP addresses allowed by your firewall that Threater would have blocked | 4,419 |
| Total Known Bad Connections allowed by your firewall that Threater would have blocked | 166,864 |
| Known Bad Connections per day allowed by your firewall that would have been blocked by Threater | 164,257 |
| Known Bad Connections per month | 4,996,150 |
| Known Bad Connections per year | 59,953,805 |

Assessment Details

| | Inbound | Outbound |
|---|---|---|
| Unique **Public IP addresses** that your firewall allowed | 8,133 | 73,184 |
| Known **Bad IP Addresses** that your firewall allowed and Threater would have blocked | 2,818 | 1,601 |
| Known **Bad Connections** that your firewall allowed and Threater would have blocked | 73,219 | 93,645 |
| Number of **unique ASN's** where known bad traffic was found | 315 | 155 |



*THREAT RISK ASSESSMENT*

LOG START DATE
Tuesday, October 3, 2023

LOG END DATE
Wednesday, October 4, 2023

DURATION OF ASSESSMENT PERIOD
1 day, 22 minutes, 51 seconds

FIREWALL VENDOR
Sophos

INBOUND MALICIOUS THREAT ACTOR

62.3.41.84

- Example Inbound malicious IP 62.3.41.84 hails from 'Iran', on ASN 'Pars Parva System LLC'. Being a known malicious actor of Iranian origin, it is deemed to be extremely malicious.
- Protected side IP <public IP> (and no other) was targeted a total of 2 times. The earliest event occurred on Wed Oct 4 03:47:39 UTC, and the last event was logged on Wed Oct 4 03:48:10 UTC. The malicious inbound attempt targeted UDP 4000. Out of an abundance of caution, impacted infrastructure should be carefully scanned.
- This external IP is known to be malicious by at least 3 source lists. The lists were out-of-box lists. This malicious IP is in 2 known threat categories (Endpoint Exploits, Scanner) with extremely high confidence.
- Note that it is extremely important given the prevalence of nation-state sponsorship of unknown attack vectors (tomorrow's zero days) to stop known malicious threat actors from accessing any infrastructure (including firewalls and DMZ equipment) by inbound means at all times.
- Threater would have outright blocked this known-malicious activity. Note that this is just one malicious example. Threater would have blocked all known-malicious threat actors that are currently being allowed by the existing security stack.

Get a free custom
threat assessment today

Threater.com
sales@threater.com
(855) 765-4925