



Security Stack

Insight Report





Introduction

Welcome to the 2023 edition of Threater’s annual Security Stack Insight Report! As always in the cybersecurity world, a lot has changed in the year since we released our last report. Threat actors have found new ways into networks along with developing even more malicious, far-reaching, and harder-to-detect attacks, artificial intelligence and machine learning have come into the spotlight, and security teams are stretched thinner than ever.

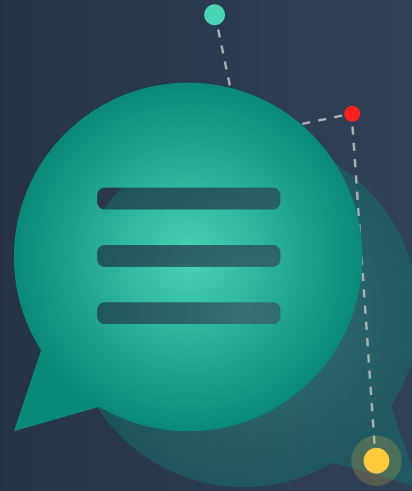
Our goal of the Security Stack Insight Report is to help shed light on why we keep reading devastating headlines about successful cyber attacks daily. This year we decided to approach our survey in a different way and not just ask about the technologies organizations are utilizing to protect their networks but rather recognize that a successful cybersecurity strategy (and stack, for that matter) involves three tried and true components coming and working together: **people, processes, and technology.**



Table of Contents

1. Survey/Audience/Methodology	4
2. The People.....	6
3. The Processes.....	8
4. The Technology.....	12
5. Where do we go from here?.....	16
6. Threater: Your Key to Successful Cybersecurity People, Processes, and Technologies	18

Survey Audience /Overview



Who took our survey?

Our 200+ survey participants represented a real “slice of life” and their organizations spanned across all industries, sectors, and sizes. Their roles included C-Suite executives, VPs, Directors, and Managers. All participants had a focus on cybersecurity or technology within their industries.

Why this audience?

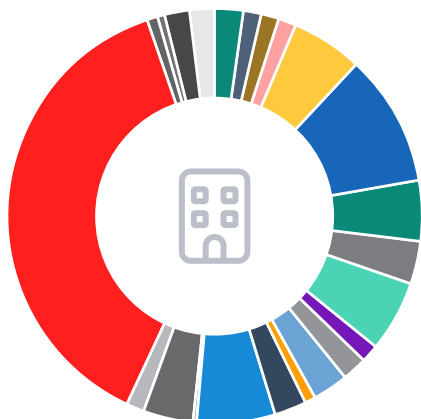
Threat actors don’t just target certain industries or sizes of companies. They cast wide, automated nets, looking for any network with vulnerabilities or access. Some threat actor groups do focus on a specific industry they might see as an “easier” (i.e., less funded and less secure) target.

For instance, the Vice Society ransomware group has repeatedly set their sights on the education sector, targeting K-12 schools and universities, proving once again there is no low too low for these groups.

In order to understand and evaluate the threat landscape and how security professionals are responding to it, we wanted to get a picture of it all. If threat actors are industry-agnostic, our survey needed to be as well.

QUESTION:

Which of the following best describes the principal industry of your organization?



Top Responses:

- Telecommunications, Technology, Internet, & Electronics
- Business Support & Logistics
- Construction, Machinery, & Homes
- Finance & Financial Services
- Manufacturing
- Education

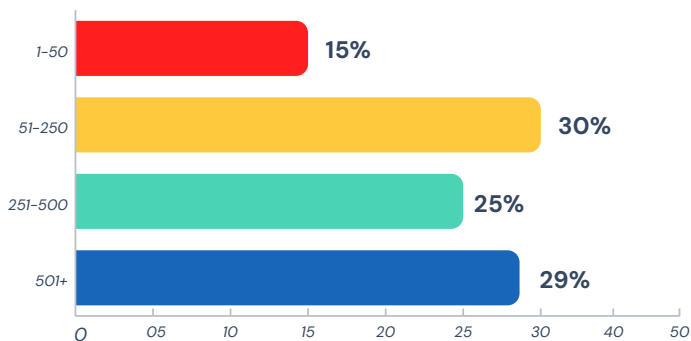
Additional Responses

Retail & Consumer Durables • Entertainment & Leisure • Healthcare & Pharmaceuticals • Advertising & Marketing • Insurance • Government • Agriculture • Airlines & Aerospace (including Defense) • Automotive • Food & Beverages • Real Estate • Health & Fitness • Transportation & Delivery • Nonprofit • Utilities, Energy, and Extraction • Currently not employed • Prefer not to answer

QUESTION:

What is the size of your organization?

ANSWER CHOICES	RESPONSE PERCENT
1-50	14.95%
51-250	30.37%
251-500	25.23%
501+	29.44%



The People



Who's keeping the lights on?

One of the hottest issues in cybersecurity is the chronic industry staffing crisis. Unfortunately, this crisis is only worsening. As budgets tighten, fewer and fewer entry level positions are posted, making it difficult to train up the next generation of professionals. And because the demand for experienced professionals is so high, they are also extremely expensive for companies to hire and retain, further stretching budgets. Those who remain in the industry are reporting high levels of overwhelm and burnout as threat actors quickly advance the techniques, attack vectors, and volume of threats security teams need to manage.

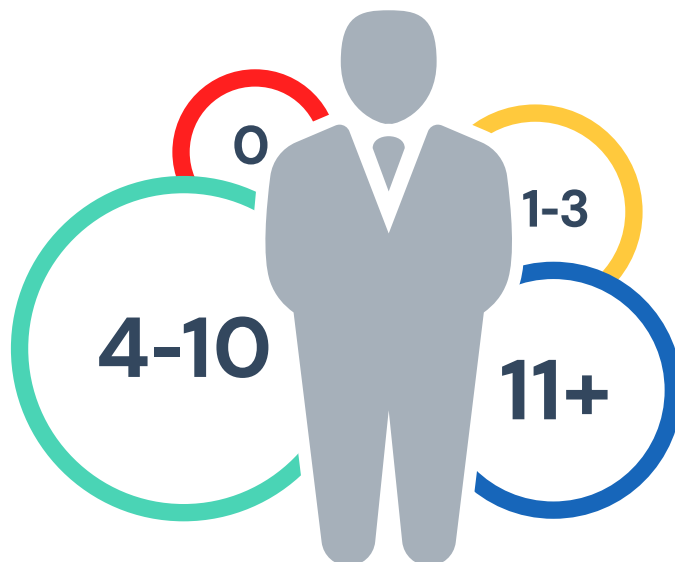
More interesting data points...



QUESTION:

How many full time employees are dedicated solely to network/cybersecurity?

ANSWER CHOICES	RESPONSE PERCENT
0	5.61%
1-3	19.63%
4-10	41.12%
11+	33.64%



Takeaways

The cybersecurity staffing shortage crisis is still in full swing. And while the amount of traffic and threats have increased, security teams are still running extremely lean and overstretched (if they exist at all!), no matter the size of the organization.

As companies look to shore up their security with new tools and technologies, they must also consider what kinds of staffing they'll need for the tool. If a tool is extremely powerful but requires full time staff the organization cannot provide in order to protect the network, nobody wins and the network remains vulnerable.

Many organizations are now turning these staffing needs to Managed Security Service Providers (MSSPs), who can help them manage their security tools reliably. Of course, these are expensive and often charge based on ingest, which of course further strains limited budgets.

Organizations looking to invest in new technologies – which, as you'll find out soon, is almost everyone – must first look at the people who will be responsible for them. When looking for new security solutions, organizations need to find autonomous tools (i.e., solutions that don't require constant monitoring or babysitting) that help the lives of the teams responsible for securing our networks and data.



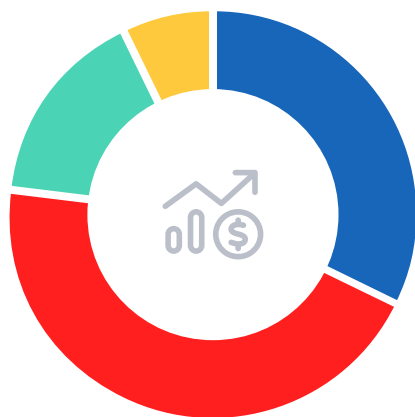
The Processes



Why are we talking about processes?

Processes are where the people and the technology come together. Technology obviously needs the people to run it, but without processes in place to take action if/when something arises, they both are inefficient at best and ineffective at worst.

They say the one constant in life is change, and there might not be an industry where that is more readily provable than in cybersecurity. Understanding how organizations can – and do! – respond to the constantly shifting threat landscape is one of the most important pivotal aspects of any modern security stack. So let's dive into the data.



QUESTION:

How often do you evaluate your security budget?

ANSWER CHOICES	RESPONSE PERCENT
Once a month	32.24%
Once a quarter	44.86%
Once a year	15.89%
Unknown	7.01%

68% of organizations don't evaluate their security budgets on a monthly basis.

Reactive processes still seem to rule

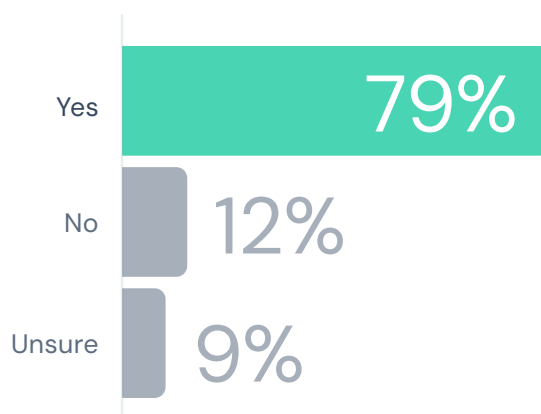
While **almost 80% of organizations report being able to add new tools or technologies** if they fall victim to a cyberattack (which is good news), **only about one-third (32%) evaluate their security budget on a monthly basis** (which is...probably not such good news). In today's threat landscape, where new attacks and attack vectors are appearing almost daily, this might not be quick enough for many organizations to protect themselves.

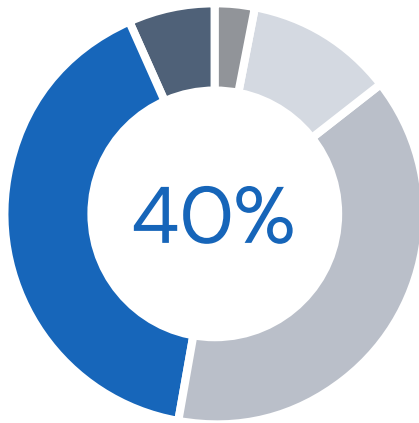
No matter how up-to-date your security team's knowledge might be on the latest attacks, if they don't have the processes in place to add protective technologies, they won't be able to do anything to stop them. And while adding new technologies after a breach to prevent future ones is important, it's also closing the barn door after the horse has bolted. (In other words: too late.)

QUESTION:

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

ANSWER CHOICES	RESPONSE PERCENT
Yes	79.44%
No	11.68%
Unsure	8.88%





QUESTION:

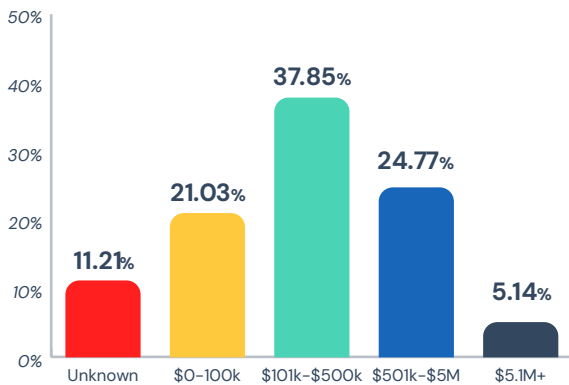
Do you monitor access by critical accounts on a routine basis to look for anomalies in access?

Critical access accounts are defined as accounts that have access to critical corporate or customer data.

ANSWER CHOICES	RESPONSE PERCENT
Never	3.27%
Rarely	11.21%
Sometimes	38.32%
Always/Continuously	40.65%
Unsure	6.54%

QUESTION:

What is your estimated annual spend on your entire security stack?



Unfortunately, one of the most shocking discoveries in this section was that of monitoring access to critical accounts, where we learned almost **60% of organizations do not monitor access to critical accounts** – defined as accounts that have access to critical corporate or customer data – continuously. Verizon’s 2023 Data Breach Investigations Report (DBIR) reported that **74% of all breaches included the human element**, such as stolen credentials (~50%), social engineering, and phishing.

74% of all breaches include the human element.



Almost 60% of organizations do not monitor access to critical accounts continuously



Only 50% of organizations with 500+ employees monitor access continually

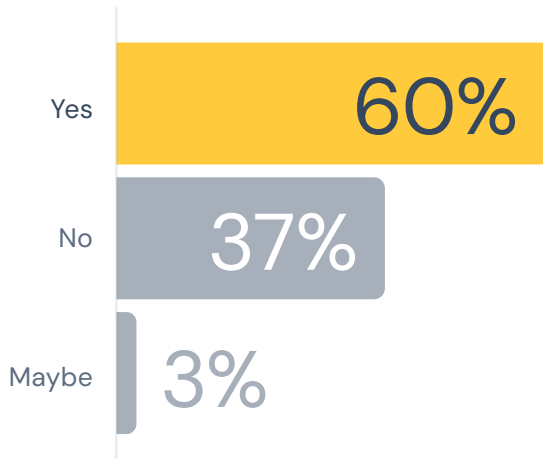


25% of organizations who don’t monitor critical access continually rate their security posture as a 5/5

QUESTION:

Have the new SEC rules on data breach reporting requirements affected cybersecurity decisions in your organization?

ANSWER CHOICES	RESPONSE PERCENT
Yes	60.28%
No	36.92%
Maybe	2.8%



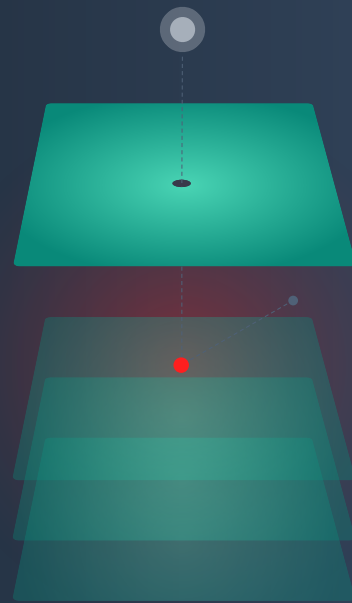
However, it does appear that new reporting requirements handed down this past year by the SEC regarding cyberattacks have made an impact on purchasing decisions. **Approximately 60% of organizations noted they have altered their security decisions** because of them.

These new rules require publicly-held organizations to report cyberattacks within four business days of discovery. While clearly not all organizations are publicly held, this does seem to have shifted the culture around reporting attacks.

Takeaways

Threat actors know the weakest points of any network are the people using them. However, people and their processes are also what save a network after an attack. As much of the security industry has focused on the “right of boom” technologies to minimize the damage of an attack, so too have organizations’ processes. By investing in processes that can enable security teams to evaluate and proactively protect against new threats and protect against the realities of stolen credentials and backdoor access into networks, organizations can truly bring the people and technologies together in meaningful ways.

The Technology



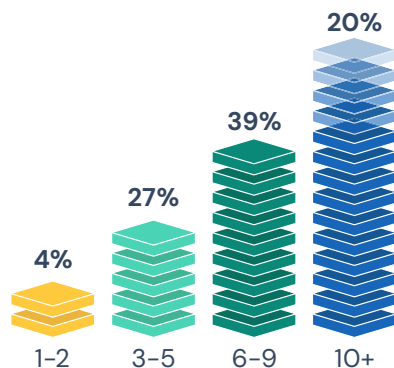
The search for intelligent security is on.

Alright, it's time to get nerdy and talk about the tech. This past year intelligence became the name of the game (and lives in general, for that matter), and our survey data backed this up.

Most organizations' security stacks are composed of some combination of the "usual suspects" such as firewalls, detection systems, endpoint monitoring, antivirus, and more. However, the vast majority still are out there looking for more ways to protect their networks, as demonstrated by almost two thirds responding they had added new cybersecurity technologies in the last year.

We don't see this trend slowing down, either, as artificial intelligence (AI) has exploded into the mainstream. Both threat actors and security professionals have been scrambling to figure out how this changes the game. To name just a few examples, AI allows threat actors access to easier malicious code and convincing phishing content, while it has granted security professionals better access to cyber intelligence and monitoring. In addition, organizations face the unenviable choice of trying to balance the risks of leveraging breakthrough technologies and their unknown potential security gaps while still staying ahead of new attacks.

Clearly the race to make our security technologies more "intelligent" is on. So let's take a look at what the data actually say about the matter.



QUESTION:

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

ANSWER CHOICES	RESPONSE PERCENT
1-2	3.74%
3-5	27.1%
6-9	38.79%
10+	20.56%
Unknown	9.81%

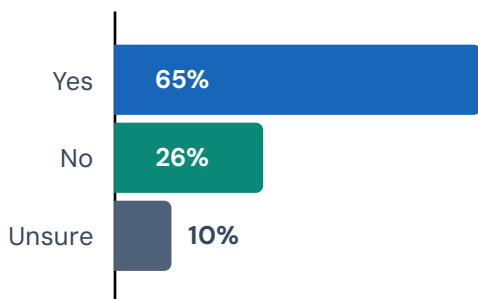
While the number of cybersecurity tools and technologies available to organizations feels almost infinite, organizations clearly have only but so much capacity to add them to their stacks. Luckily our insights from the People and Processes sections before shed light into why.

Limited budgets create overstretched teams that can't manage more high-maintenance tools. Processes that are too slow to prevent breaches and remain mostly reactive hamper the ability to add more technologies as needed. And, of course, tight budgets don't help, either. That probably explains why **65% of organizations report having 9 or fewer tools** in their security stacks.

It's clear organizations have a vested interest in staying ahead of modern threats and threat actors, which is demonstrated by the fact that almost all reported adding new security technologies to their stacks this past year. And it's not just adding one new technology, either. Half of our respondents reported adding three or more new technologies this past year, and a quarter added six or more. And while new technologies and innovations can provide some of the most advanced protections, we also know there might not be the people or processes in place for those technologies to provide as much protection as they should. It will be interesting to see how this "security stack sprawl" starts playing out in the coming year as well.

QUESTION:

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



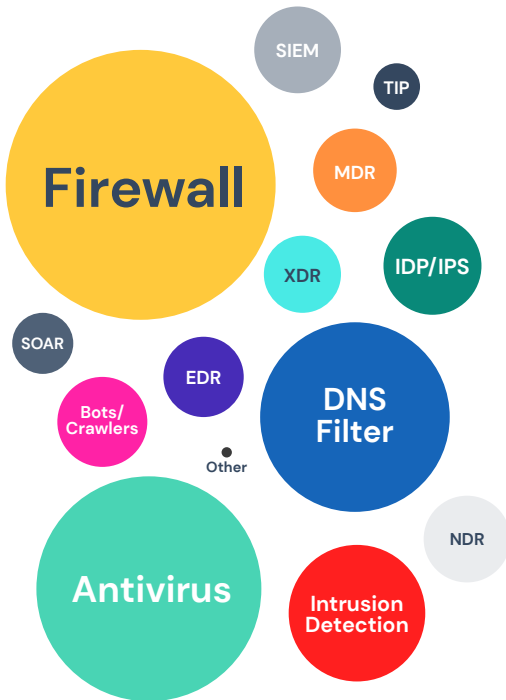
If yes, how many new security technologies have you added in the past year?

ANSWER CHOICES	RESPONSE PERCENT
1-2	21.7%
3-5	27.36%
6-9	18.4%
10+	6.13%
Unknown	10.38%

51% of organizations added 3 or more security technologies to their stack in the past year

QUESTION:

Which of the following tools do you currently have in your stack?



ANSWER CHOICES	RESPONSE PERCENT
Firewall	78.5%
• Antivirus	65.42%
• DNS Filter	55.14%
• Intrusion Detection	39.72%
• IDP/IPS	28.50%
• Bots/Crawlers	26.17%
• SIEM	25.23%
• NDR	25.23%
• MDR	24.30%
• EDR	23.36%
• XDR	22.43%
• SOAR	17.76%
• TIP	13.55%
• Any others?	2.80%

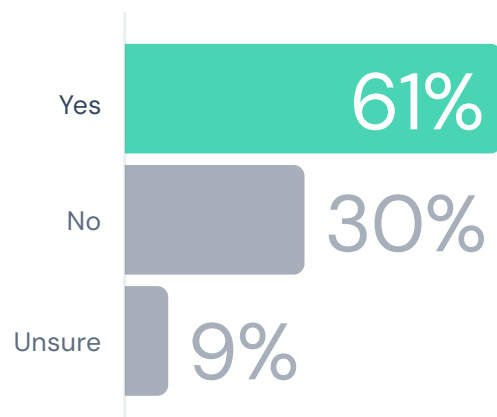
On the preventative side, we were shocked to see that **20% of organizations do not have a firewall** long considered a cornerstone of any security stack. However, it was not surprising that firewalls, along with DNS filters (~55%), are the only two “left of boom” (i.e., preventative, before a breach) technologies the majority of organizations have implemented *en masse*.

Of course, this helps explain why one of the biggest annual conferences in the cybersecurity industry is called “Right of Boom.” This focus on minimizing the damage of a breach instead of preventing the breach from happening is ripe for an overhaul, especially as newer “left of boom” technologies are making some of the biggest strides to protect networks against modern threat actors.

QUESTION:

Are you independently subscribed to any additional cyber intelligence or threat data sources?

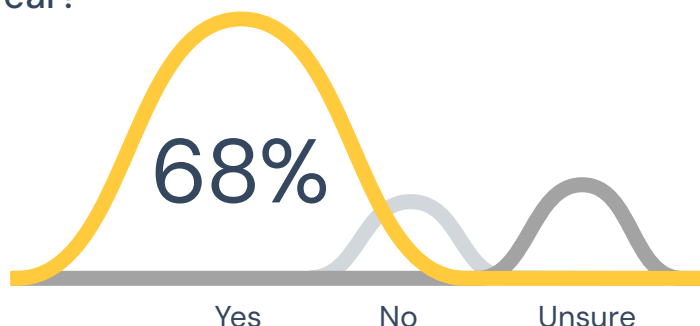
ANSWER CHOICES	RESPONSE PERCENT
Yes	60.5%
No	30.37%
Unsure	8.88%



QUESTION:

Is your organization planning on prioritizing AI tools for your security stack in the coming year?

ANSWER CHOICES	RESPONSE PERCENT
Yes	68.22%
No	14.95%
Unsure	16.82%

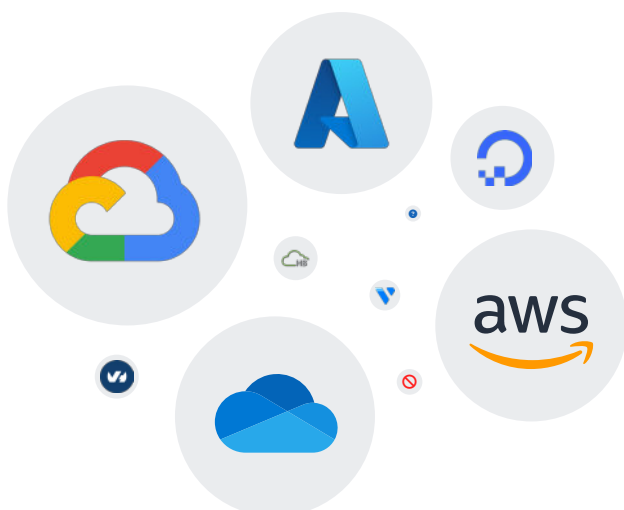


Unless you're reading this after emerging from a rock for the past year, it should be no surprise that **over two thirds (68%) of respondents plan to prioritize AI tools** for their security stack in the coming year. The flip side of the AI/machine learning coin, however, is the fact that threat actors have already begun using AI themselves to produce malicious code, craft convincing social engineering emails, and much, much more.

Unfortunately, sometimes sitting on the cutting edge of a new technology means you can be the one who ends up bleeding. Keeping up with modern threat actors is pivotal, but organizations should also find ways to leverage these technologies in ways that shield them from unknown risks and security holes. Like they say, "You don't know what you don't know," and with the rise of AI in 2023, this idiom feels especially poignant.

QUESTION:

Are you currently using — or do you plan to use in the next 6 months — any of the following Cloud providers?



ANSWER CHOICES	RESPONSE PERCENT
Google Cloud	56.07%
OneDrive	46.73%
AWS	44.86%
Azure	42.52%
DigitalOcean	24.30%
HostedBizz	10.28%
OVH	10.28%
Vultr	7.01%
No, not planning to use Cloud providers in the next 6 months	6.07%
Other	1.87%



Bringing it All Together: Where do we go from here?

Are attacks what happen to the “other guys”?

Despite threat actors deploying attacks with more frequency, complexity, and, frankly, damage, it seems that most respondents don’t seem to think their networks are vulnerable. When asked to rate their own security posture, 75% responded feeling fully or extremely confident. This also makes sense why that same number responded “yes” when asked if their organization could withstand an attack.

We hope all these organizations’ security postures are as strong as they think they are – we’re not monsters, after all! – we also worry there might be some overconfidence as well. The security industry is filled with talented people doing the best they can in near-impossible circumstances, yet we are still reading about breaches every day. While difficult to admit, acknowledging vulnerabilities allows you to address them faster and more efficiently.

QUESTION:

How would you rate your organization’s security posture on a scale of 1–5 (5 being highest)?



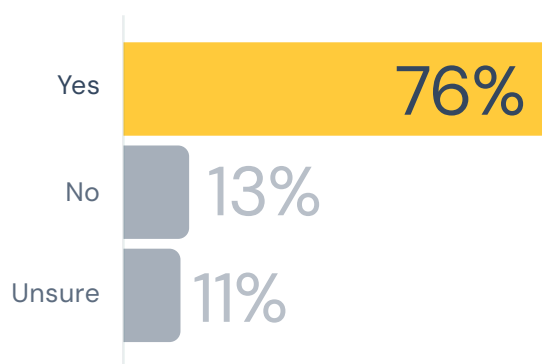
ANSWER CHOICES	RESPONSE PERCENT
1	3.27%
2	4.67%
3	17.76%
4	40.19%
5	34.11%

74% of organizations feel fully or extremely confident in their security posture

QUESTION:

Do you think your organization is equipped to withstand an attack?

ANSWER CHOICES	RESPONSE PERCENT
Yes	75.7%
No	12.62%
Unsure	11.68%



Security professionals work extremely hard not only to learn their craft but stay up-to-date with one of the most rapidly evolving landscapes in the world while also withstanding a literal 24-hour-a-day onslaught of attacks on the networks they are entrusted to protect. It's often a thankless job and sometimes the only time they're noticed is when something goes wrong. Cybersecurity teams should feel proud of what they do and what they accomplish because, simply put, they aren't set up for success.

There is a classic logical fallacy known as the "normalcy bias," which leads people to believe that just because something bad hasn't happened

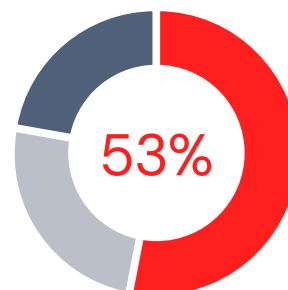
yet, despite the risks, it won't happen to them at all. In cybersecurity this is one of the largest challenges organizations face when asking senior leadership to continue investing in new tools, team members, and organizational processes that create overlapping layers of protection.

We see this in action when over half of respondents said that, if they had an unlimited budget and ability to start their stack over from scratch, they would. Despite being fully confident their networks can withstand an attack, it looks like most security professionals know there are better ways and room for improvement.

QUESTION:

If budget were no concern and you could rip out your entire stack and start over, would you?

ANSWER CHOICES	RESPONSE PERCENT
Yes	53.27%
No	24.77%
Maybe/Unsure	21.96%




Unfortunately, no matter how prepared and well-equipped you are, or how small you think you are that you'll get looked over, threat actors are finding new ways in. Confidence in your work is good, but it has its limits. Or, as Mike Tyson put it: "Everyone has a plan until they get punched in the mouth."



threater™

Helping protect your people,
processes, and technology



The internet is a hostile environment and networks are under constant siege. Threat actors are not only sending large amounts of encrypted traffic but also attempting “back door” entrances to the network such as stolen passwords, phishing, and other means.

In other words: security teams and technologies are bogged down with redundant alerts and unnecessary triaging of known-bad traffic. The people, processes, and technologies are stretched too thin and aren't able to operate at their full potential.

As almost all organizations add technologies and tools to their security stacks while also prioritizing intelligence, Threater is the perfect addition to fill these needs. Best yet: the technology runs fully autonomously, without the need for employees to monitor and act.

By removing traffic going to and from known threat actors, Threater eliminates up to 30–50% of internet traffic hitting the network while also protecting against outbound calls. This allows security teams and technologies to focus on the unknown instead of wasting their time and resources on known-bad traffic, giving the processes in place for unknown traffic to work.

This year's survey gave us fresh insights into the realities of operating security stacks. We are convinced more than ever that investment in autonomous, proactive, intelligence-driven solutions will help every network against this new generation of threat actors.

We want to thank all those who took the time to respond to our survey. We know – because you told us – that your time is extremely limited, and helping us understand your needs means more to us than we can express. We are here with you, and we are here for you.



©Threater 2023

threater.com

sales@threater.com

(855) 765-4925