SONICWALL®

2022 SonicWall Threat Mindset Survey

Data and Findings

The Human Element of Cybersecurity

Twice a year, the SonicWall Cyber Threat Report serves as a comprehensive resource that covers a wide variety of data points across at least 10 different threat types, collected from a wide cross-section of industries located around the globe. Each section is accompanied by in-depth news and analysis of current trends.

The state of cybersecurity, however, is determined by more than just quantitative data. It's also shaped by the sentiments of those who have made a career defending their companies, their customers or their country from ruthless cybercriminals.

To capture these perspectives, we've developed the SonicWall Threat Mindset Survey. For this inaugural report, we've polled customers to find out what they've experienced and what they anticipate as the future of cybersecurity.

As a companion piece to the bi-annual SonicWall Cyber Threat Report, the Threat Mindset Survey serves as a valuable tool to illustrate the current state of both cybersecurity and the cyber threat landscape — where they are, and where they're likely to be headed.

Methodology

For the inaugural SonicWall Threat Mindset Survey, we created a list of 12 questions — 10 multiple-choice, two open-ended — on a wide variety of cybersecurity topics. The resulting survey was sent to SonicWall customers around the globe. To ensure the objectivity of responses, SonicWall partnered with TechValidate, which ensures anonymity as a default, and made each question optional.

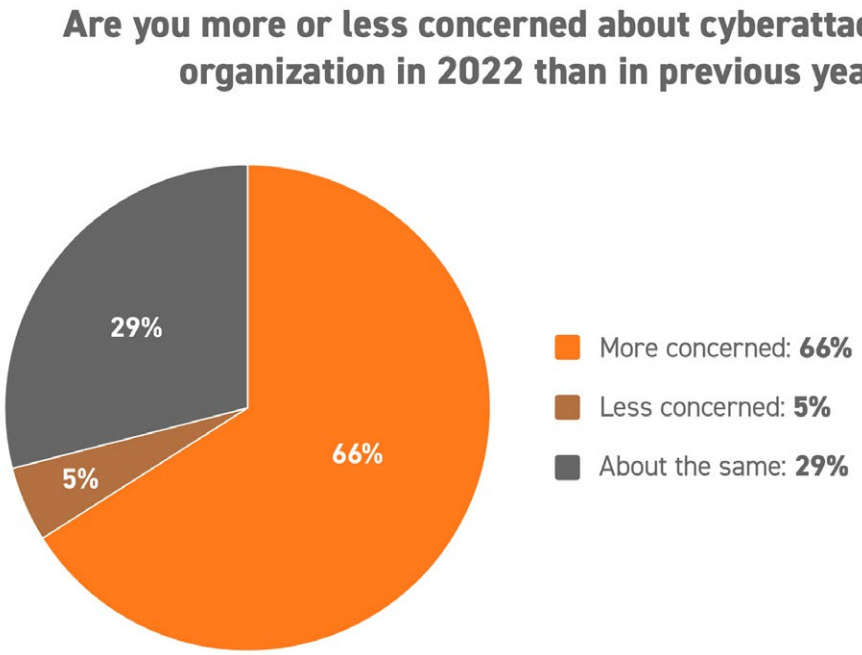
Of the responses we received, 80% were from the U.S., 4.8% were from the U.K., and the remaining 15.2% were from other countries across the world.

Concern About Cyberattacks Remains in 2022

Are you more or less concerned about cyberattacks in your organization in 2022 than in previous years?

In the mid-year update to the 2022 SonicWall Cyber Threat Report, we noted that malware rose 11% year-to-date over the first half of 2021. And while we recorded a slight drop in ransomware for the first half of 2022, attack volume remains at near-historic highs.

Combined with record-setting attack volume for cryptojacking and IoT attacks, it's no surprise that a majority of respondents are more concerned about cyberattacks now than ever before.



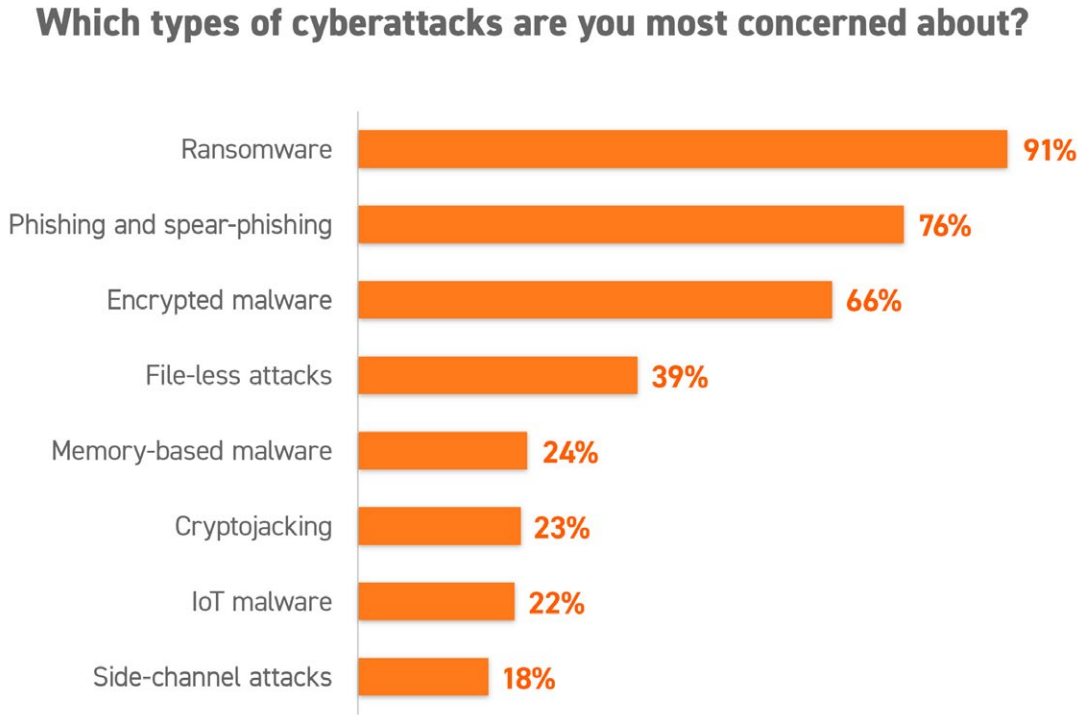
Ransomware Still Top of Mind in 2022

Which types of cyberattacks are you most concerned about?

Ransomware attacks haven't just become more pervasive over the past few years. They've also become more ruthless.

Attacks on hospitals have increased dramatically, and critical infrastructure is now a common target. But even more than who they're attacking is how they're attacking: Ransomware gangs have increased their propensity to steal data in hopes of an additional, extortion-based payday, and some are even harassing customers, partners and investors.

And while a spate of high-profile arrests resulted in some ransomware groups laying low or breaking up entirely, these wins also kept ransomware in the headlines as a top-of-mind threat.

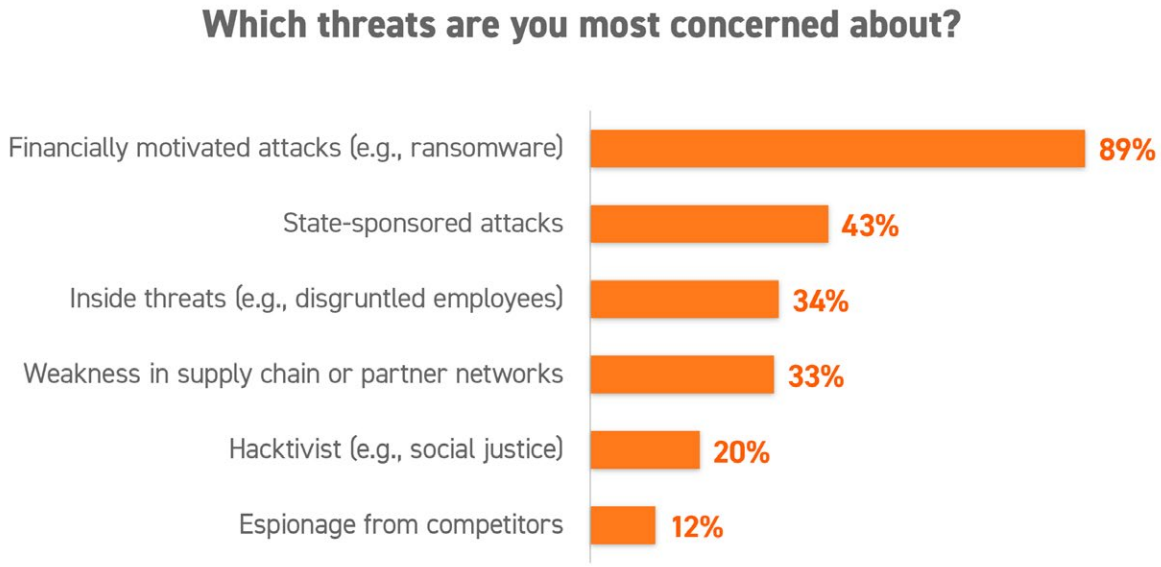


Financially Motivated Attacks Biggest Concern

Which threats are you most concerned about?

Cybercrime isn't just a scourge, it's also an occupation — and reports repeatedly show that most cybercriminals are still in it primarily to make a buck. While some attacks have political or even personal motivations, odds are any given cyberattack that could devastate a business is just another day at work for the attacker.

Unsurprisingly, 89% of respondents named financially motivated threats as their top concern. State-sponsored attacks were a (distant) second, likely bolstered by alerts from CISA and other government entities regarding an uptick in such attacks as a result of the Russia-Ukraine conflict.

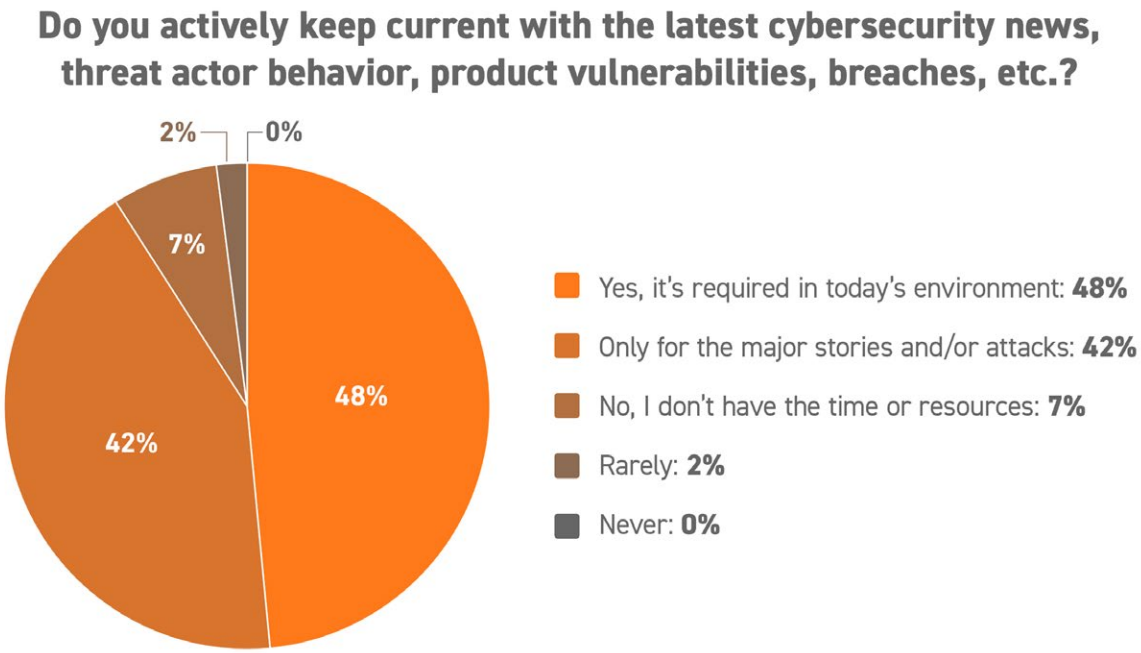


Cyber Threats are Must-Read News … or Are They?

Do you actively keep current with the latest cybersecurity news, threat actor behavior, product vulnerabilities, breaches, etc.?

Chinese general Sun Tsu is frequently quoted in cybersecurity circles for a reason: passages such as "If you know the enemy and know yourself, you need not fear the result of a hundred battles" hold just as true for cyberwarfare as they do for military operations.

A majority of respondents expressed a desire to use every relevant piece of knowledge at their disposal in order to level the playing field between them and their adversaries, such as news articles, threat data, vulnerability reports and more.



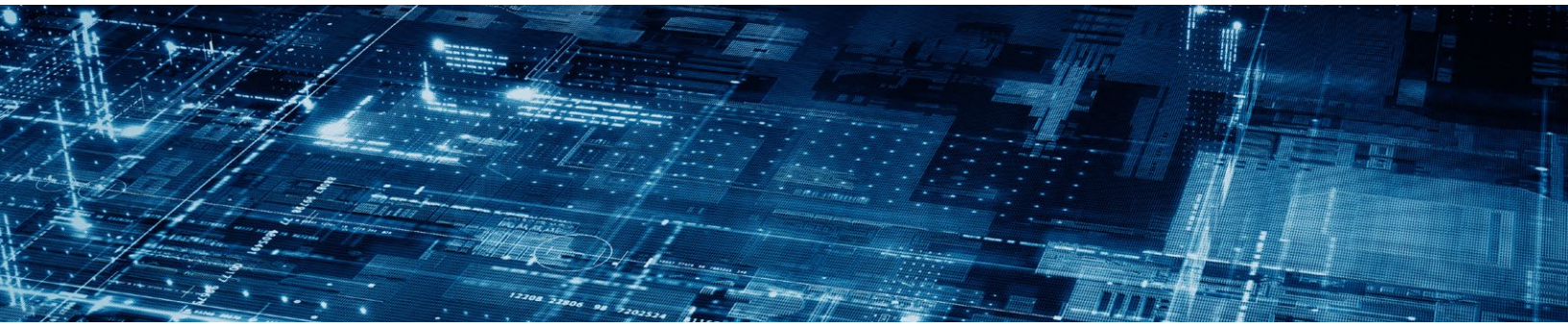
Never Stop Patching

How does your organization prioritize deploying critical patches?

Patching is one of the lowest-cost, highest-impact cybersecurity practices an organization can undertake. Application vulnerabilities continue to be the most common method of external attack, and patching is frequently what separates targets from victims.

According to Ponemon Institute research, 57% of cyberattack victims say their breach could have been prevented by installing an available patch, and 34% of those victims said they knew about the vulnerability, but hadn't acted to stop it.

Worryingly, 78% of organizations surveyed reported they don't patch critical vulnerabilities within 24 hours of patch availability, and another 12% only apply critical patches when they get around to it.

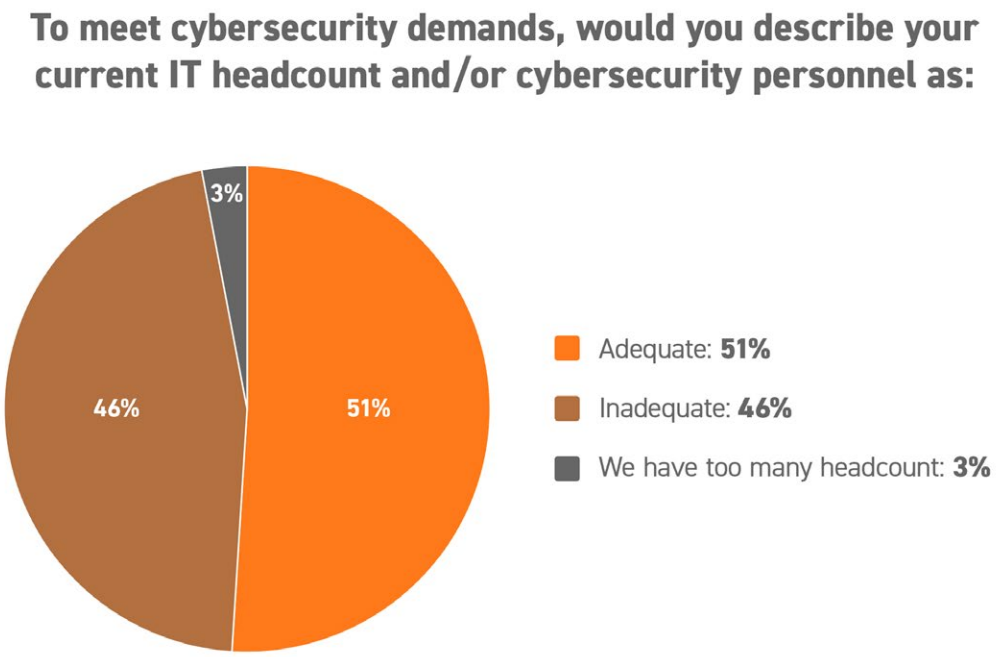


Industry Split on Cybersecurity Headcount Needs

To meet cybersecurity demands, how would you describe the state of your current IT headcount and/or cybersecurity personnel?

According to the National Institute of Standards and Technology, there are more than 700,000 total open cybersecurity jobs — compared with just under 1.1 million total employees working in cybersecurity. In other words, for every three people you know working in cybersecurity today, there are two unfilled positions.

This ongoing labor shortage, combined with the exponential expansion of the attack surface, makes it unsurprising that the number of respondents saying their current staffing is insufficient is 15 times greater than the number of respondents reporting their headcount is excessive. (Fortunately, however, a majority say that they're adequately staffed to meet their current needs.)



A Cyberwar of Revenue

To meet growing cybersecurity demands, how would you describe the state of your current IT/cybersecurity budget?

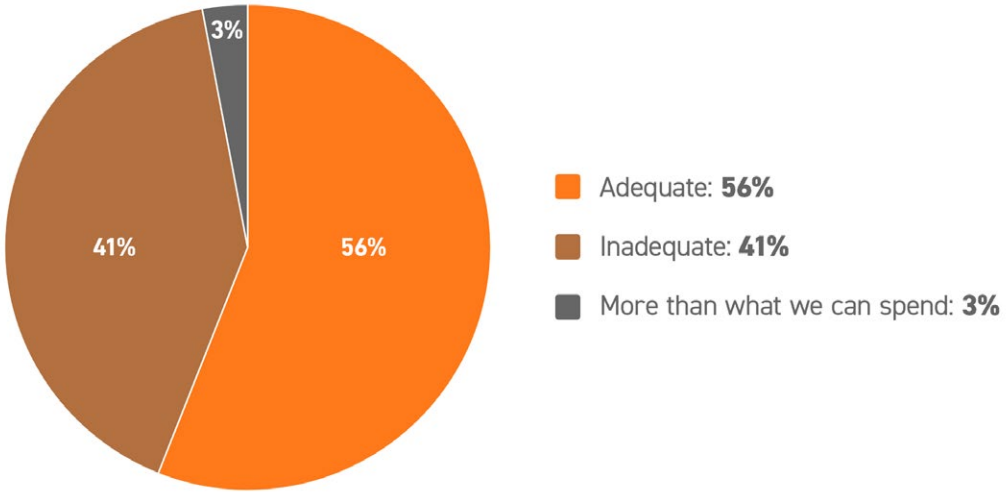
Spending on risk management and information security is estimated to reach $172.5 billion in 2022, an almost 11% increase over 2021. And a survey from PwC showed that 69% of respondents predicted an increase in their cybersecurity spending in 2022.

However, according to survey results, this still may not be enough: A full 41% of respondents said that their current IT/cybersecurity budget was not adequate to meet growing cybersecurity demands.

It's alarming to know that cybercriminals will be outspending cybersecurity investments by an estimated 40-1 by 2025.[1] In fact, some estimate that by 2025 cybercrime will be the third-largest global economy behind the U.S. and China.

[1]Figure based on estimated average of 2025 market values for cybersecurity ($250 billion) and cybercrime ($10 trillion), and average CAGR for cybersecurity (11%) and cybercrime (15%). ($250 Billion x 40 = $10 Trillion (2025 Market Value Estimates).

To meet growing cybersecurity demands, would you describe your current IT/cybersecurity budget as:



Trying to Keep Up

If you manage your own cybersecurity strategy, what are your major issues to address the growing cybersecurity demands?

Predictions for the future of cybersecurity include everything from the evaporation of the cloud to the potential for quantum computing to break the RSA algorithm.

But seismic shifts in cybersecurity don't require these sorts of extreme prognostications coming to pass — they're happening right now, as the world continues to reel from the twin revolutions of hybrid and remote work and the rapid adoption of cloud services.

Given today's extremely volatile climate, it's unsurprising that roughly three out of four respondents ranked "keeping up with the changing security landscape" as their biggest issue to tackle in the near term.

If you manage your own cybersecurity strategy, what are your major issues to address the growing cybersecurity demands?

What Our Customers Are Saying

In your own words, how has the evolving cyber threat landscape impacted your organization's ability to operate normally?

In the first half of 2022, malware rose 11%, cryptojacking spiked 30% and IoT malware was up 77%. In addition, 2021 set a new record for number of data breaches, jumping 68% to 1,862 — and so far, 2022 is looking even worse.

But while the evolving cyber threat landscape affects all organizations, it doesn't affect all of them in the same way. Here's how a few respondents said they were dealing with the growing risk and complexity:

More Risks Demand Greater Security

"We really have to put resources — people and money — in areas that previously we did not. (I am talking years ago.)"
— IT Manager, Electric Utility Provider

Bombarded with Requirements

"Operationally (to the end user) we have not been impacted [by a changing cyber threat landscape]. On the back end, we have been increasingly bombarded by new requirements from existing and new clients. Keeping up has been a challenge." ***— Director, Medium Enterprise Engineering Company***

A Foundation of Sound Cybersecurity

"As a startup, it's important for us to implement good security from the beginning. What we have made normal for us from the start would be a major change for most established companies. We have the flexibility to enact changes to policy as issues arise." ***— Chief Technology Officer, Small Business Computer Services Company***

An Evolution of Threats

"The evolution of cyberattacks hit over the years due to technological progress where, day by day, we must be more aware and apply new solutions for our clients."
— IT Specialist, State Government Agency

Defining 'Normal' Changes Every Day

"Mainly in training end users — taking time away from productive work. [Changing cyber threats] create hurdles for internal users to get to the information they need to work and also lead to pushback and lost productivity. 'Normal' changes every day with each new vulnerability discovered."
— IT Manager, Medium Enterprise Engineering Company

The Terror of Attack

"Frankly, I live in terror of a ransomware attack and state-sponsored intrusions. On my logs, I have seen massive increases in probes from Russia, China and a handful of other (what I would call) enemy nations." ***— Business Professional, Small Business Healthcare Company***

Just Takes a 'Click'

"[The evolving cyber threat landscape] has made us train users a lot more. It's made us spend more on cybersecurity. It scares the hell out of me that an end user can click on something and bring our systems down — even though we are WELL protected."
— IT Director, Financial Services Business

SONICWALL®

What Our Customers Are Saying

In your own words, how has a proven cybersecurity product, solution or strategy positively impacted your organization's ability to operate successfully?

Cybersecurity is often referred to as an investment — and just like with more traditional investments, some bets are better than others. Here are some of the ways survey respondents said their cybersecurity investments paid major dividends:

Significant Cybersecurity

"The deployment of SonicWall solutions has significantly increased the security of the corporate environment."
— IT Manager, Medium Enterprise Engineering Company

Less Fear, More Productivity

"Proven cybersecurity products, solutions and strategies reduce anxiety and fear amongst the user base. That reduction helps to maintain productivity and the ability to work without too much continuous worry, which makes us much more successful." **— Director, Non-Profit Agency**

Maintaining Business-Critical Uptime

"By both protecting and preventing a breach or compromise, we maintain uptime to our customers and productivity from our staff."
— IT Specialist, Medium Enterprise Wholesale Distribution Company

Valuable Visibility

"Any product that brings about the visibility of the behavior of our digital assets and also captures historical data is very much appreciated."
— Network Administrator, Medium Enterprise Energy & Utilities Company

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper distributed era and a working reality where everyone is remote, mobile, and unsecured. SonicWall closes the cybersecurity business gap for hospitals, clinics and providers worldwide by knowing the unknown, providing real-time visibility, and enabling breakthrough economics. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®

ExecBrief-2022CyberThreatSurvey-JK-7207