ARCTIC WOLF

2023 TRENDS

RANSOMWARE, CLOUD SECURITY CHANGES, AND MORE

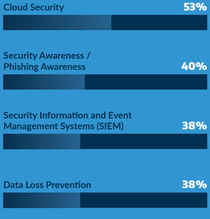
The State of Cybersecurity: 2023 Trends report pulls data and insights from over 700 IT professionals across the globe to understand where organizations are heading when it comes to cybersecurity. These concerns, obstacles, and objectives highlight that while old problems still persist, organizations are making moves to increase their security posture and tackle future threats.

COMPANIES ARE ACTING ON CLOUD SECURITY CONCERNS

As organizations digitize and remote work transitions to a state of permanence, the cloud is top of mind for major organizations.

This concern is not a new one, but this year, our survey showed that organizations are not only understanding the concern but taking actionable steps to fill their cloud security gaps. They see their current cloud security as offering the least amount of value and are actively seeking to learn more and improve their cloud operations.

Security Solutions Expected to be Implemented or Updated in 2023



46%

46% of respondents are most interested in learning about cloud security and the evolving infrastructure

42%

42% of respondents stated that cloud security gaps are their primary area of worry

SKILLS SHORTAGE IS A MAJOR ORGANIZATIONAL OBSTACLE

The "security skills gap" has been known for a while, and this year's survey data highlights how much it's impacting organizations' security objectives.

Even as security budgets increase, businesses are struggling to hire and retain the talent needed to operate solutions, run security operations centers, and manage an ever-growing security environment. Not only are organizations struggling to add to the head count, but the employees they do hire tend to lack the security expertise needed to get the job done.

The Top Obstacles to Achieving Cybersecurity Objectives

The survey found that **68% of organizations identified staffing related issues** as their number one threat to achieving their objectives.

THIS IS BROKEN DOWN INTO:

- 32% of organizations are having difficulty with hiring and retaining staff
- 36% of organizations feel their current staff lacks the necessary expertise needed for their goals

5+

56% of Respondents believed they would need to hire 5 or more full-time staff members

48% of Respondents have increased that to 10 or more full-time staff members

10+

EVEN IN UNCERTAIN TIMES, ORGANIZATIONS ARE UPPING THEIR BUDGETS

Doing more with less doesn't look like it will apply to cybersecurity budgets in 2023.

As businesses look to fill their skills shortage, revamp their cloud security, and stay on top of emerging threats, they're putting dollars down and increasing their security budgets.

57% of organizations we spoke with are already planning for their cybersecurity budget to increase in 2023.

- Of this group, 15% acknowledge that they are expecting a dramatic increase in this area, at a rate of over 50% in comparison to the previous year.

RANSOMWARE IS INFLUENCING ORGANIZATIONS' SECURITY DECISIONS

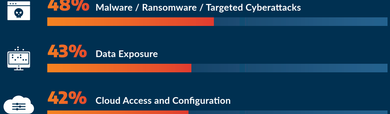
Ransomware continues to make headlines and top concerns, and for good reason.

While this year saw a dip in the total number of ransomware attacks, the cybercrime method is still widely used and thoroughly effective — and it's showing no signs of slowing down.

42% of organizations experienced a ransomware attack in 2022

63% of attacked organizations paid the full or partial ransom

Ransomware Remains a Top Concern for Organizations



JUST RELEASED!

An In-Depth Exploration: 2023 Cyber Security Trends

Review the concerns, objectives, and obstacles that are top of mind for industry leaders.

LEARN MORE