The State of Cybersecurity:
2024 Security Trends and Threat Predictions

Christopher Fielder, Field CTO

THE LEADER IN SECURITY OPERATIONS

SPEAKERS

Speaker

Title

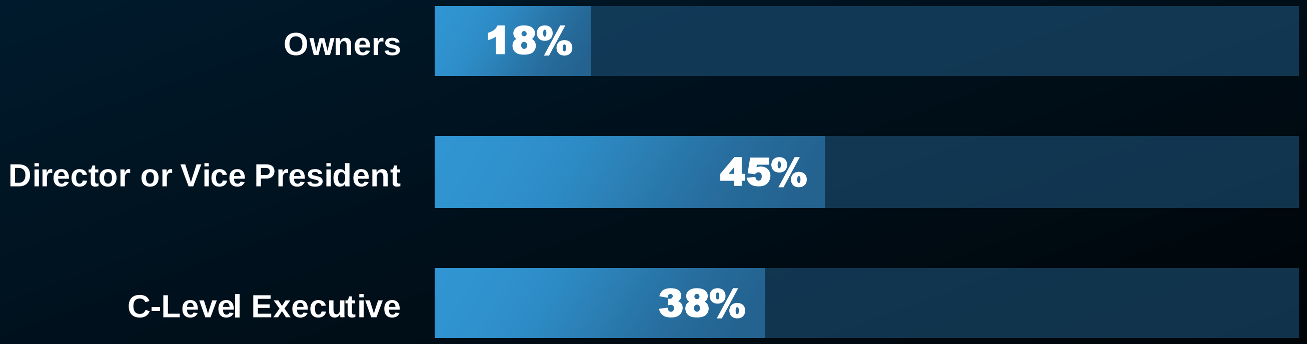
Our Research Methodology

Arctic Wolf surveyed over **1,000 security and IT professionals across the globe** to better understand their top priorities and objectives and gain first-hand perspective on current challenges and future concerns. Our goal was to understand their security roadmaps for the next 12 months, and to understand what's changed since last year.

INSIGHTS FROM AROUND THE GLOBE

SURVEY RESPONDENTS

Our 2024 survey respondents included Owners, Directors & Vice Presidents, and C-Level Executives from all 9 regions.



Turning Security Concerns into Action

After compiling the results, we found some common themes persisted across organizations.

The majority of our findings showed global themes, not isolated to geographic regions or countries

Many organizations have implemented **Incident Response Planning** strategies to actively prepare if an incident is declared

Ransomware is still the ultimate area of concern, with devastating impacts in demands, data theft, and lost productivity

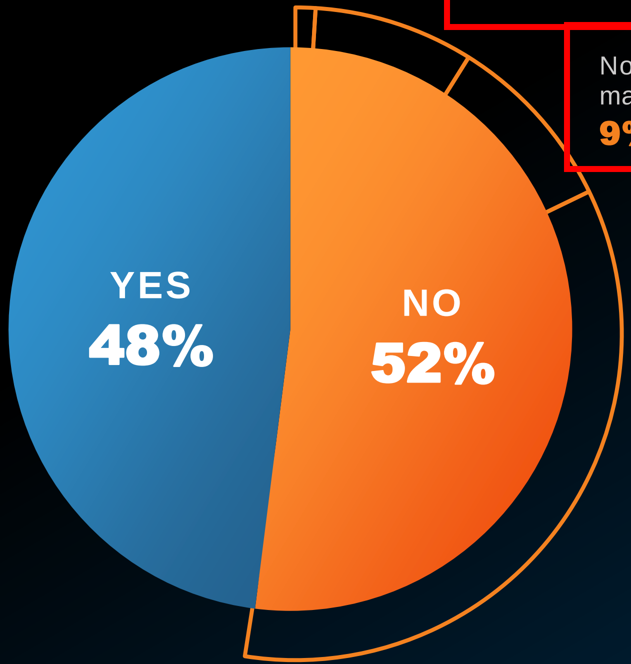
Responses acknowledge **Endpoint Tools** as a foundational element of their security posture, but effectiveness is questioned

A global shift in the acceptance of **Staffing Shortages as most business** embrace alternative coverage solutions

Data Breaches Persist

Major business concern...not without merit

48% of organizations identified a breach in the last 12 months



Not sure
1%

No, yet we believe an undetected breach may have occurred
8%

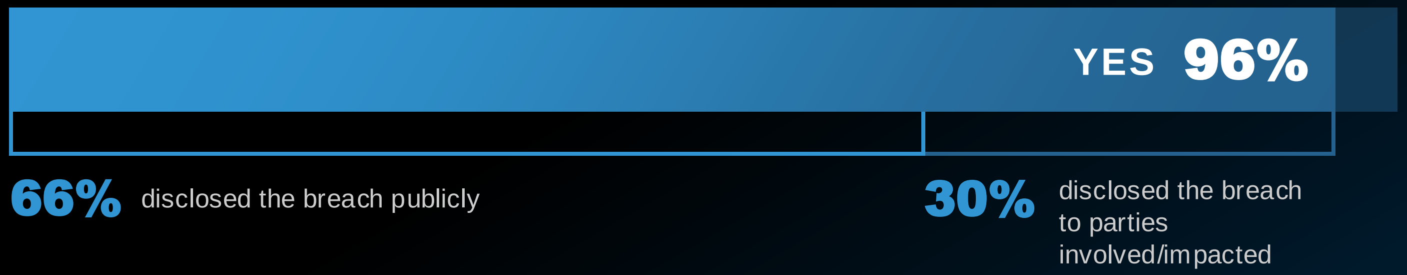
No, and we are unsure if a breach may have occurred
9%

No, we are confident that no breach has occurred
35%

Data Breaches Persist

Major business concern...not without merit

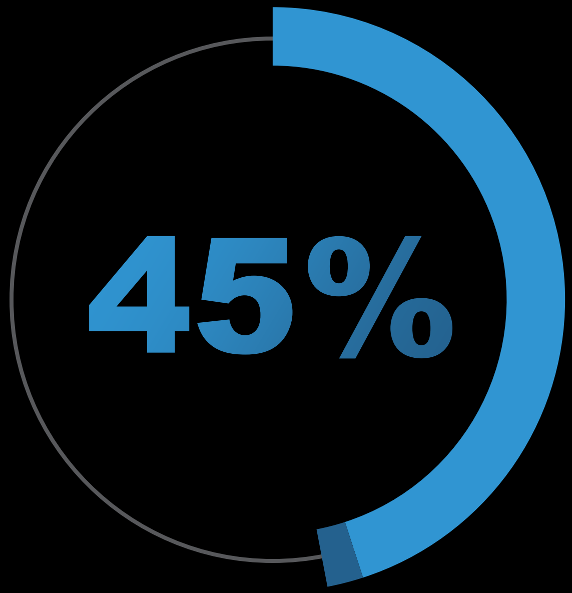
96% Disclosed some aspect of the breach



THIS REPRESENTS A **68% INCREASE** FROM LAST YEAR

Ransomware Continues to Rise

An increasingly dangerous threat

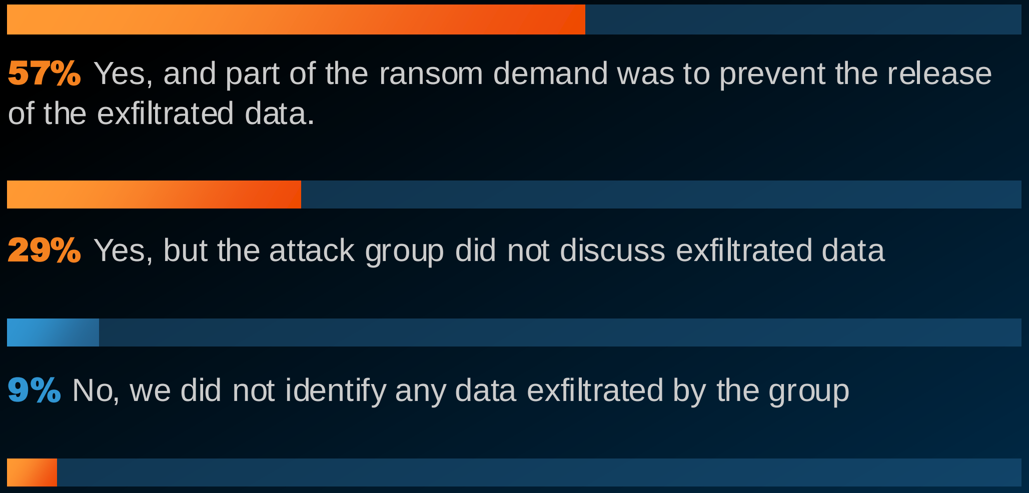


of organizations surveyed suffered a ransomware attack in the last 12 months

An additional 2% claiming to be unsure if they were victims

91% of these attacks included **data exfiltration**

WAS ANY DATA SUCCESSFULLY EXFILTRATED BY THE ATTACK GROUP?



57% Yes, and part of the ransom demand was to prevent the release of the exfiltrated data.

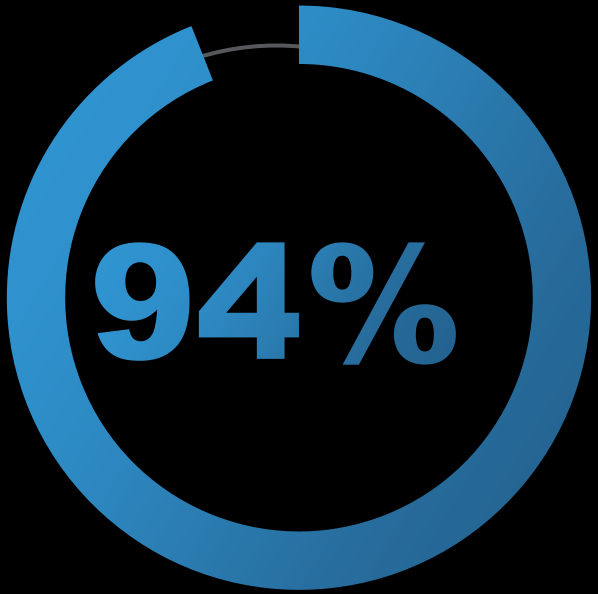
29% Yes, but the attack group did not discuss exfiltrated data

9% No, we did not identify any data exfiltrated by the group

5% No, because we were able to prevent the exfiltration of data

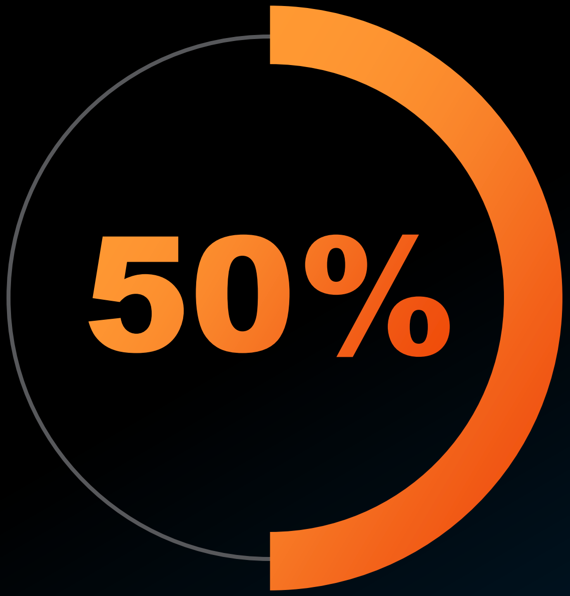
Ransomware Continues to Rise

The ransom isn't the only cost



of victims experienced periods of downtime due to ransomware

40% of ransomware victims experienced a period of total work stoppage and complete loss of productivity

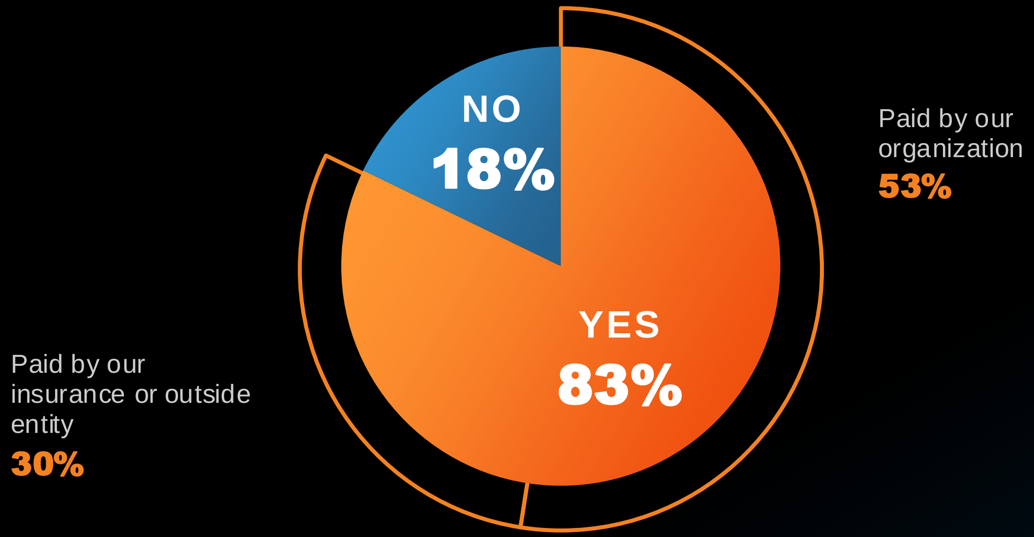


who experienced lost productivity were substantially impacted from 4 months to more than a year

Why Is Ransomware Increasing?

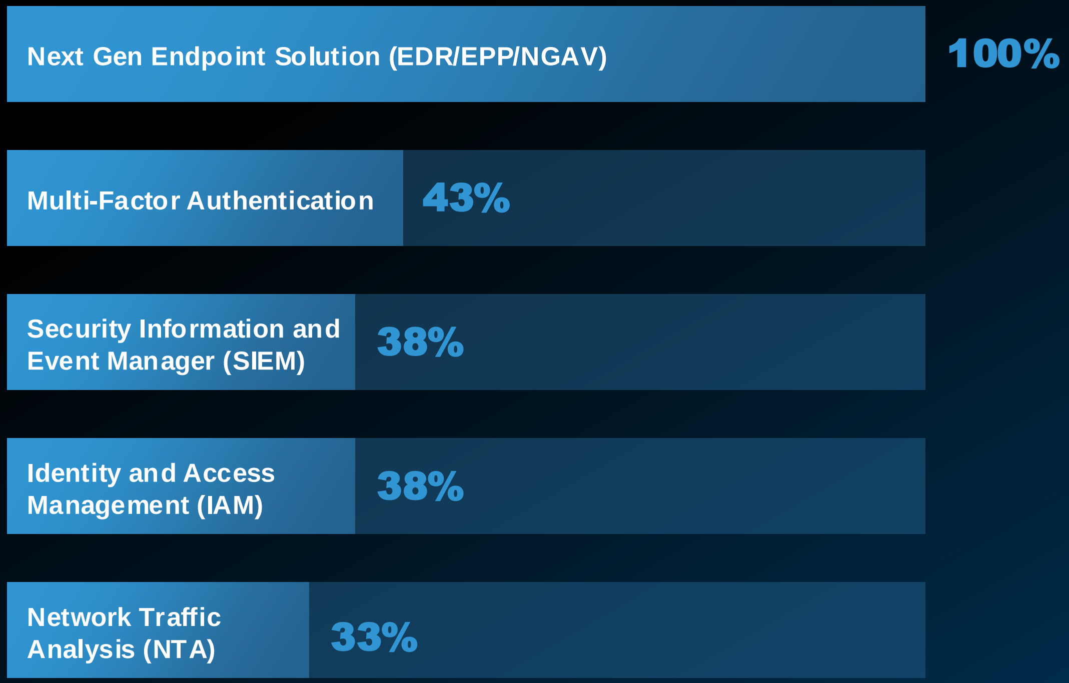
And how do we prepare for it?

83% Of victims paid some portion of the ransom



Increased visibility shows a direct correlation to a decrease in ransomware effectiveness

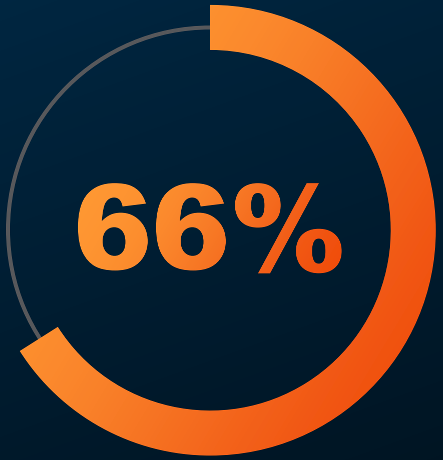
ENVIRONMENTS USING THESE TOOLS PRIOR TO RANSOMWARE ATTACK

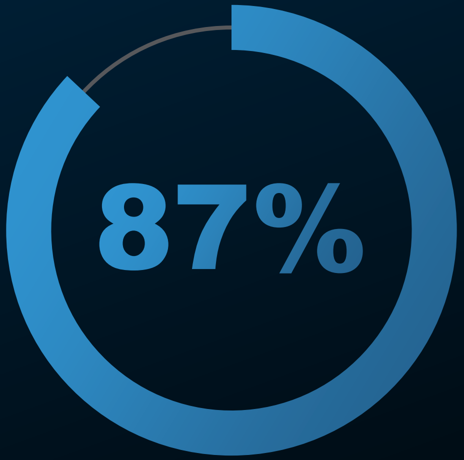


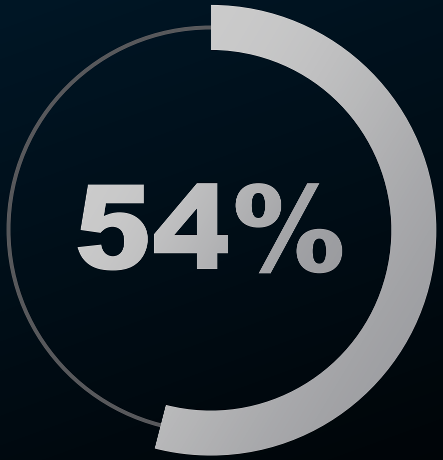
Endpoint Adoption and Footprint

Are organizations using one or more Next Generation endpoint security solutions?

[EDR, EPP, XDR]







Tool Usage

66% of organizations are currently using one or more next generation endpoint security tools

Vendor Prevalence

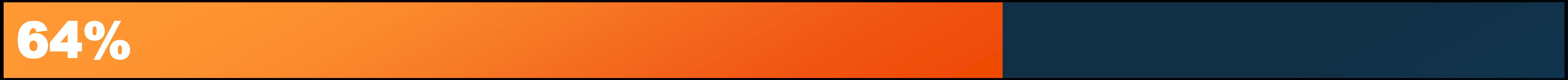
Of the 66% of organizations currently using one or more**,** **87% are using two or more**

Deployment Rates

54% of environments have been unable to reach a complete deployment rate of the agent to all endpoints within their environment

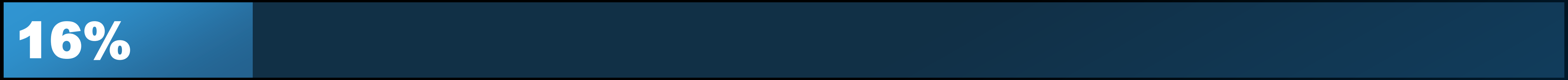
Acceptance of the Skills Shortage

Last Year



of organizations felt hiring and recruiting of security staff was their primary areas of concern

This Year



of organizations feel hiring and recruiting of security staff is their primary areas of concern

WHAT'S CHANGED?

- ? Talent surge?
- ? Accepting the skills shortage?
- ? Implementing alternative solutions?

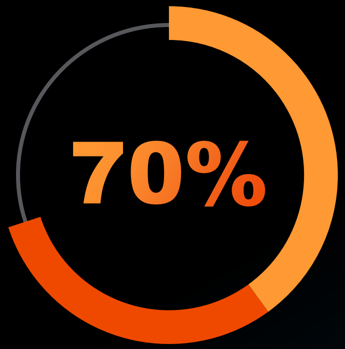
Incident Readiness + Response

Preparing for the worst is a good idea

76% of organizations maintain a formal IR plan

64% have purchased an active IR retainer

Retainers and Plans pay off



have utilized their incident response retainer in the last
12 months.

30% of those who what used their retainer have used it multiple times within 12 months.

Artificial Intelligence Adoption and Usage

Balancing benefits against potential security and privacy risks

How are companies and policy makers approaching the subject of generative AI and Large Language Models?

94%

Percentage of organizations either currently have or plan to implement adoption and usage policies within the coming 12 months

49%

[OF THE 94%]

49% currently have developed and implemented policies that outline the proper usage of LLMs and generative AI

34%

[OF THE 94%]

34% have implemented policies which strictly forbid the use of these technologies in their environments

KEY PREDICTIONS

#1 Increased Cyber Activity Around 2024 Elections Worldwide

#2 RaaS and Data Exfiltration Ecosystem Will Continue to Evolve

#3 AD Security Config Will Continue to Represent a Significant Threat

ARCTIC WOLF LABS

KEY PREDICTIONS

#4 Industrial Espionage and IP Theft will be Aggressively Pursued via CCP Cyber Operations

#5 AI Generated Code will Introduce Security Vulnerabilities into the Development Process

Key Takeaways

Data breaches show no signs of slowing, but organizations are doing more to prepare

The total cost of Ransomware must factor in loss of productivity and the cost of stolen data

IR Retainers are a smart investment and often a safety net during an attack

AI is a hot topic, and most leaders are taking steps to address it before it's too late

Questions?