ARCTIC WOLF

THE LEADER IN **SECURITY OPERATIONS**

2024 Threat Landscape and Emerging Cybercrime Trends

Adam Marrè
Chief Information Security Officer – Arctic Wolf

Background

Video Game Developer

US Army Counterintelligence

FBI Special Agent
Cyber Division
SWAT Team Leader

Global Head of Security,
Qualtrics

CISO
Arctic Wolf

ARCTIC WOLF

2024 Arctic Wolf Labs Threat Report

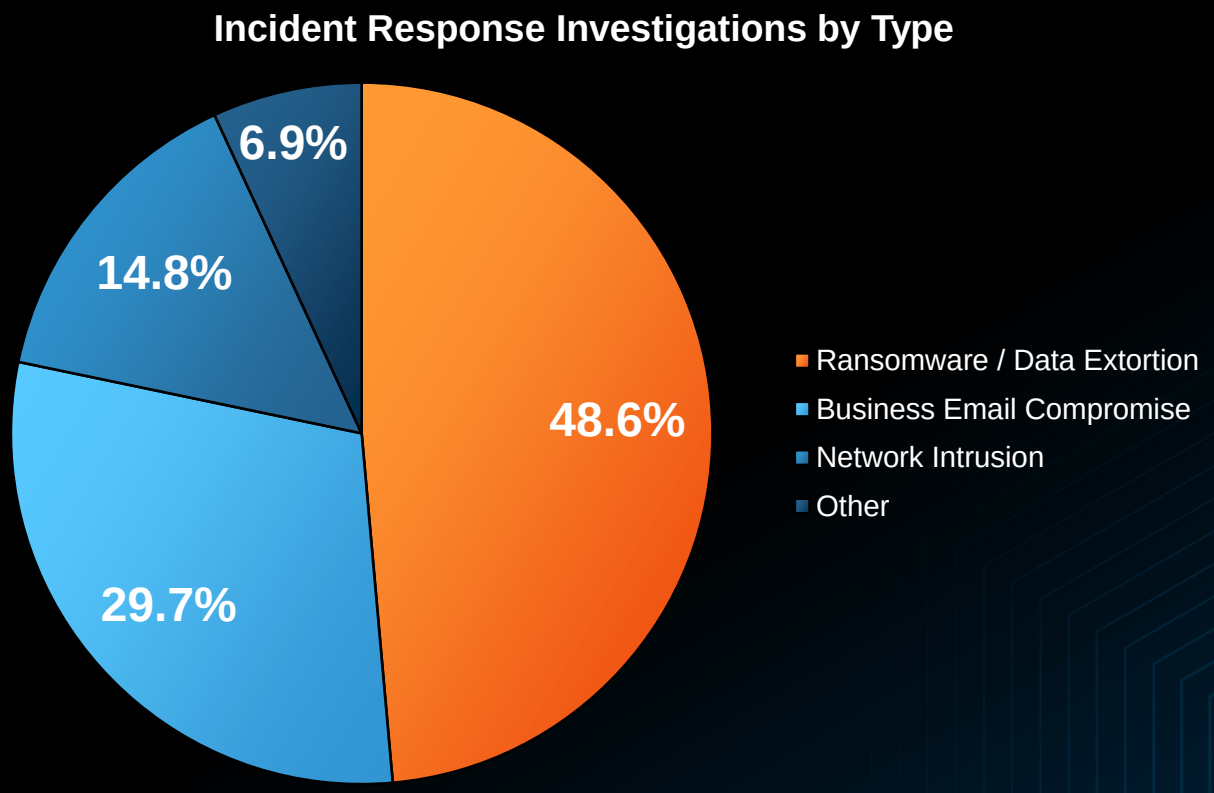
SECURITY OPERATIONS REPORT

PART 1:

Attack Types

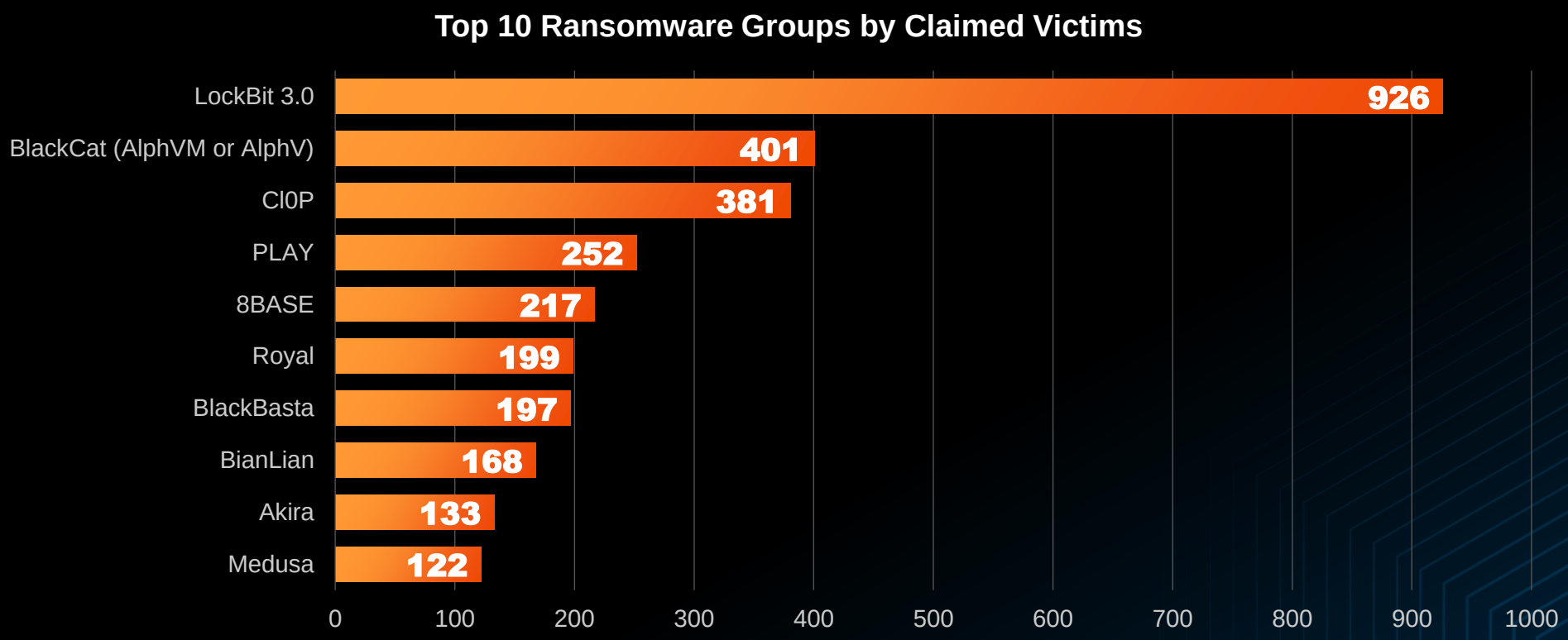
Incident Response Investigations

What did we see?



Ransomware Groups

Repeaters, joiners, and leavers

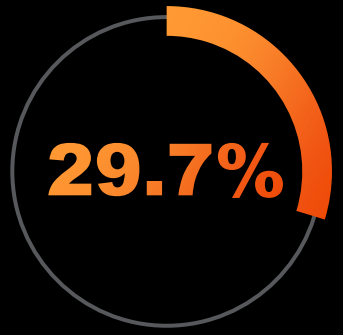


Ransom Demands by Industry

Twenty percent increase overall in 2023

	2022	2023
Healthcare	$275,000	$450,000
Construction	$375,000	$500,000
All Industries	$500,000	$600,000
Finance & Insurance	$500,000	$900,000
Legal & Government	$420,000	$1,000,000
Retail	$627,500	$1,500,000

Business Email Compromise



Business email compromise accounted for over a quarter (29.7%) of incident response cases last year.

Why is Business Email Compromise (BEC) attractive to threat actors?

- BEC is easy to execute
- BEC scams work

Most-Represented Industries

The industries with the most representation in Arctic Wolf Incident Response BEC investigations are:

01 **Finance & Insurance**

02 **Construction**

03 **Education & Non-Profit**

04 **Manufacturing**

05 (TIE) **Legal & Government**
Healthcare

PART 2:

Root Causes

Root Cause

Looking beyond BEC

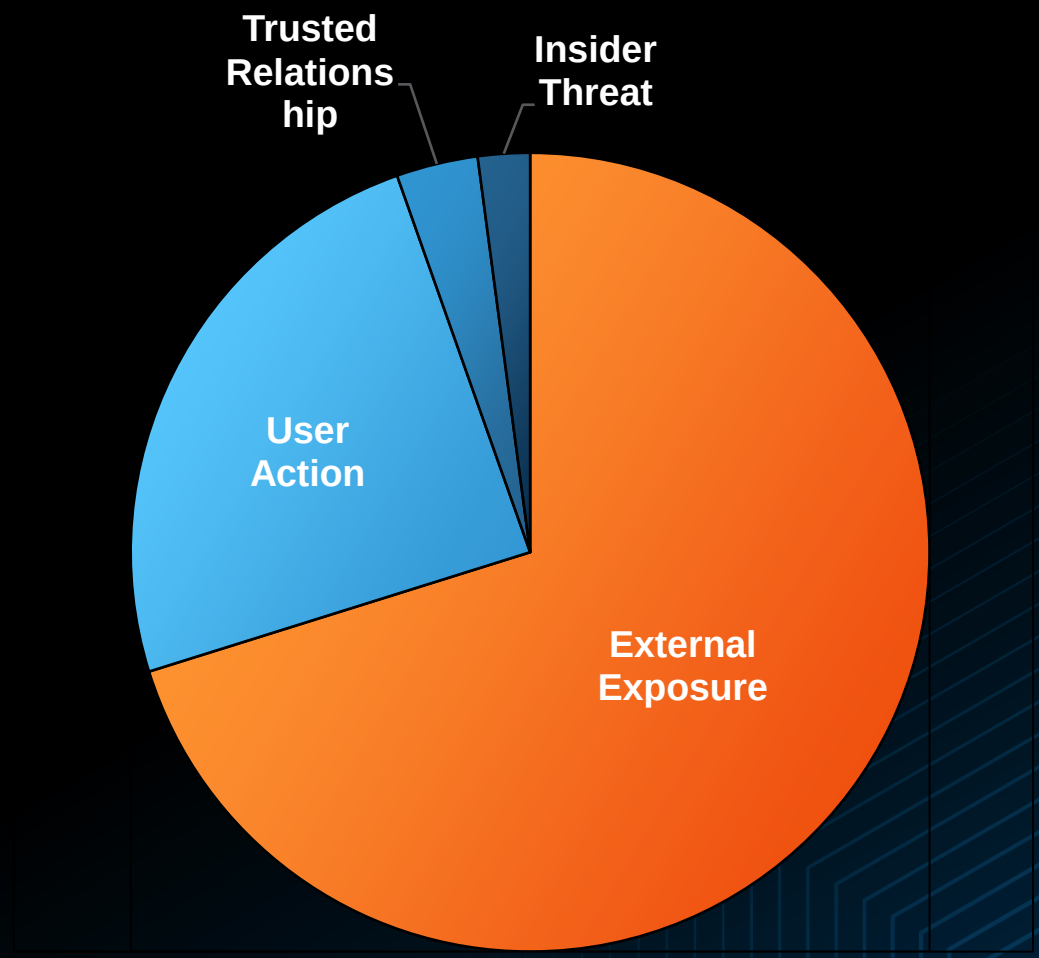
The root cause of incidents fell into one of four top-level categories:

70.1% **External Exposure**

24.4% **User Action**

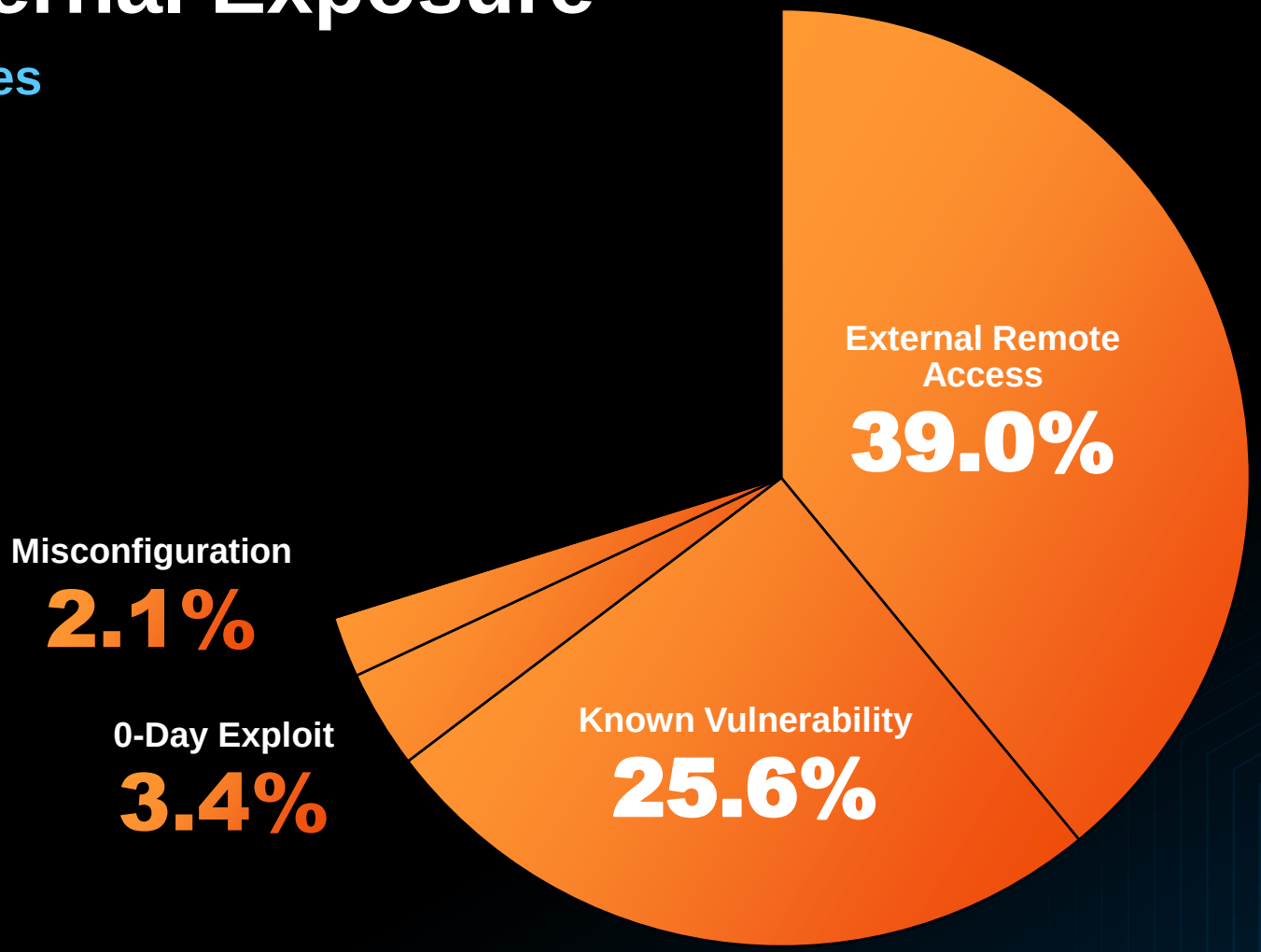
3.3% **Trusted Relationship**

2.1% **Insider Threat**



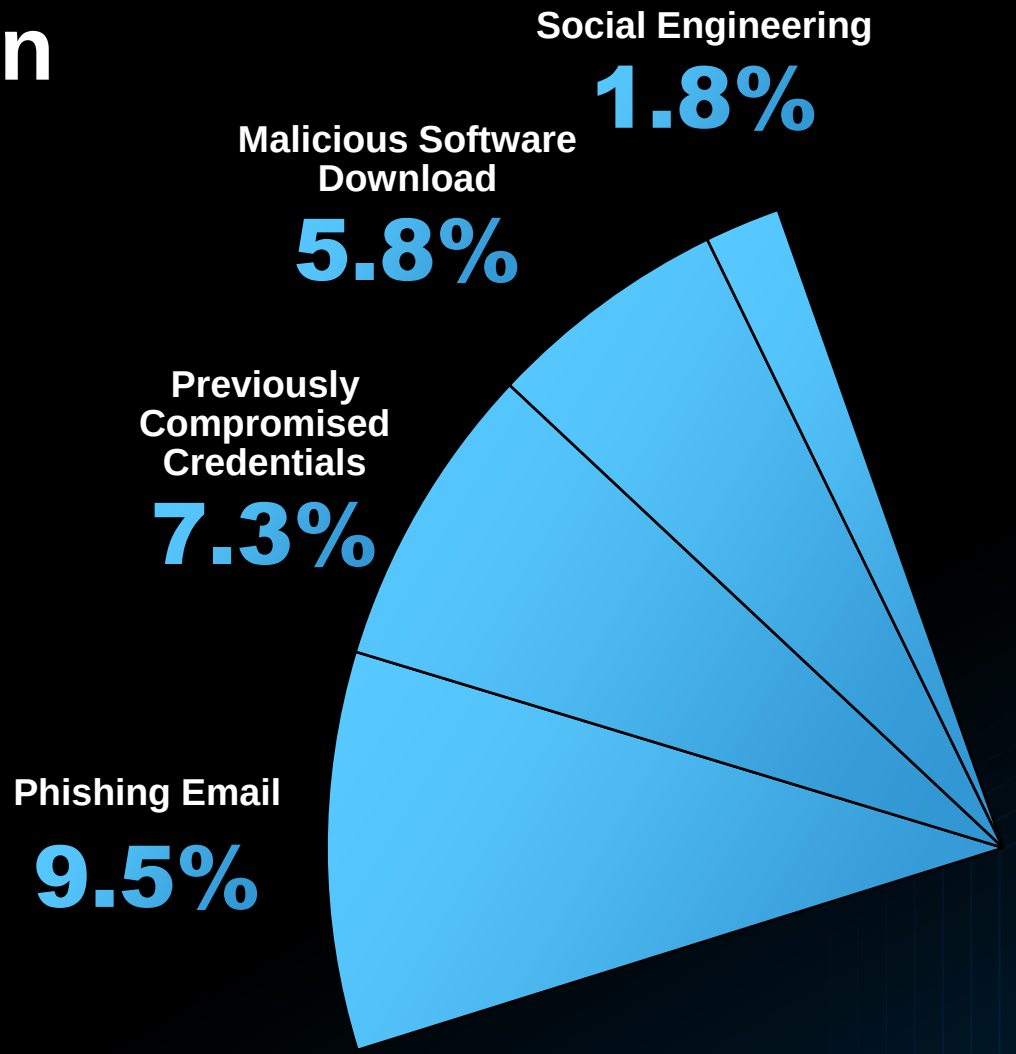
External Exposure

The Categories



User Action

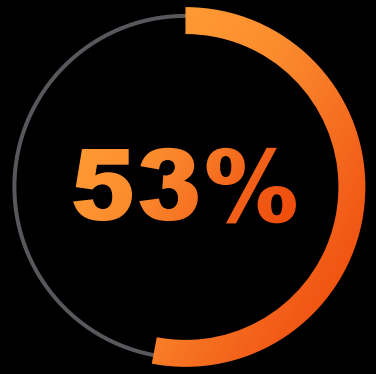
The Categories



PART 3:

Top Vulnerabilities and TTPs

Top Vulnerabilities



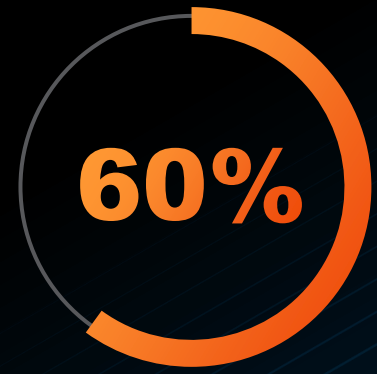
Over half of incidents (53%) involved at least one of **10 specific vulnerabilities**

Three of those 10 vulnerabilities were used in 25% of intrusions

CVE-2023-34362 – MOVEit Transfer

CVE-2022-47966 – ManageEngine

CVE-2022-41080 & 41082 – Microsoft Exchange



60% of incidents leveraged a vulnerability that was **assigned a CVE prior to 2023**

2023 The Most Exploited Vulnerabilities

Top 10

CVE-2023-34362

Vendor: Progress

Product: MOVEit Transfer

Score: 9.8 | Critical

Type: Privilege Escalation

CVE-2023-4666

Vendor: Citrix

Product: NetScaler ADC and NetScaler Gateway

Score: 7.5 | High

Type: Information Disclosure

CVE-2023-20198

Vendor: Cisco

Product: IOS XE Web UI

Score: 10 | Critical

Type: Privilege Escalation

CVE-2023-22518

Vendor: Atlassian

Product: Confluence Data Center and Server

Score: 9.8 | Critical

Type: Improper Authorization

CVE-2023-2868

Vendor: Barracuda

Product: Email Security Gateway (ESG) Appliance

Score: 9.8 | Critical

Type: Remote Code Execution

CVE-2023-20269

Vendor: Cisco

Product: Adaptive Security Appliance and Firepower Threat Defense

Score: 9.1 | Critical

Type: Unauthorized Access

CVE-2023-27350

Vendor: PaperCut

Product: MF/NG

Score: 9.8 | Critical

Type: Remote Code Execution

CVE-2023-22515

Vendor: Atlassian

Product: Confluence Data Center and Server

Score: 9.8 | Critical

Type: Broken Access Control

CVE-2023-46604

Vendor: Apache

Product: ActiveMQ

Score: 9.8 | Critical

Type: Remote Code Execution

CVE-2023-26884

Vendor: Microsoft

Product: Windows

Score: 8.8 | High

Type: Remote Code Execution

ARCTIC WOLF

The State of Cybersecurity: 2024 Trends Report

SECURITY OPERATIONS REPORT

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

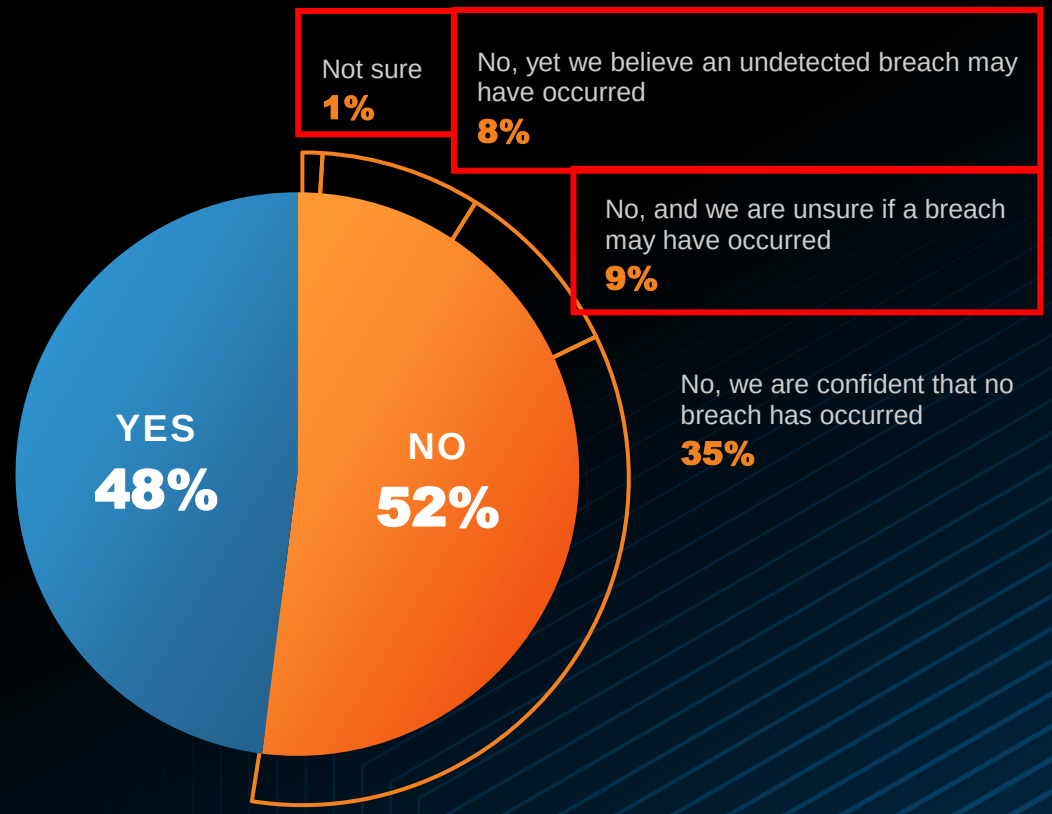
Responses acknowledge **Endpoint Tools** as a foundational element of their security posture, but effectiveness is questioned

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



Data Breaches Persist

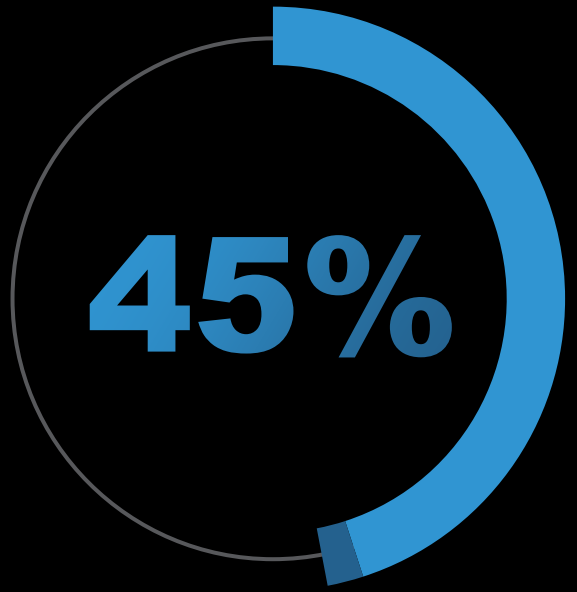
Major business concern...not without merit

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.

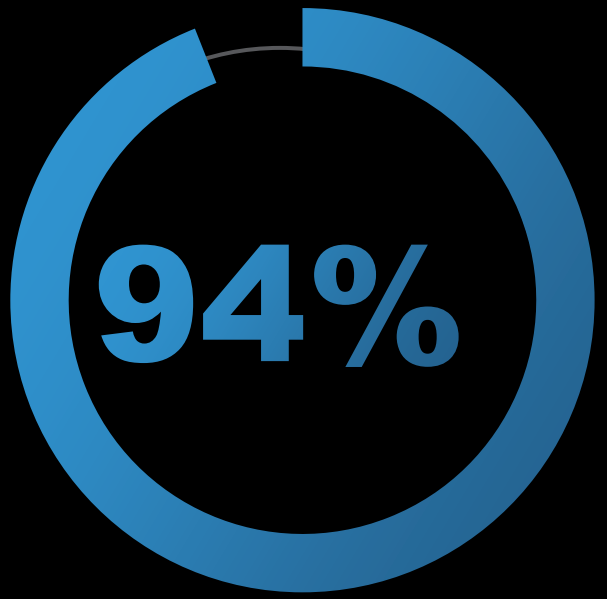
29% Yes, but the attack group did not discuss exfiltrated data

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

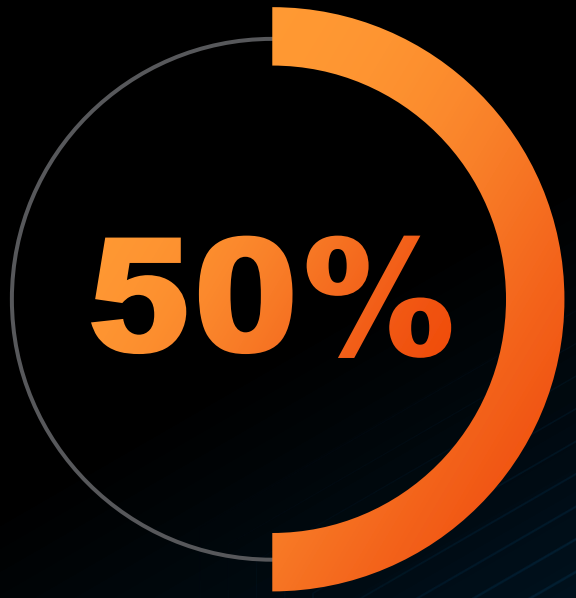
5% No, because we were able to prevent the exfiltration of data

Ransomware Continues to Rise

The ransom isn't the only cost



of victims experienced periods of downtime due to ransomware



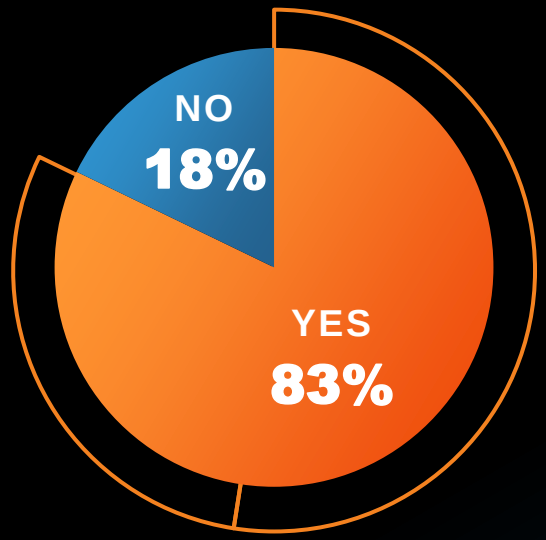
who experienced lost productivity were substantially impacted from 4 months to more than a year

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

Why Is Ransomware Increasing?

And how do we prepare for it?

83% Of victims paid some portion of the ransom

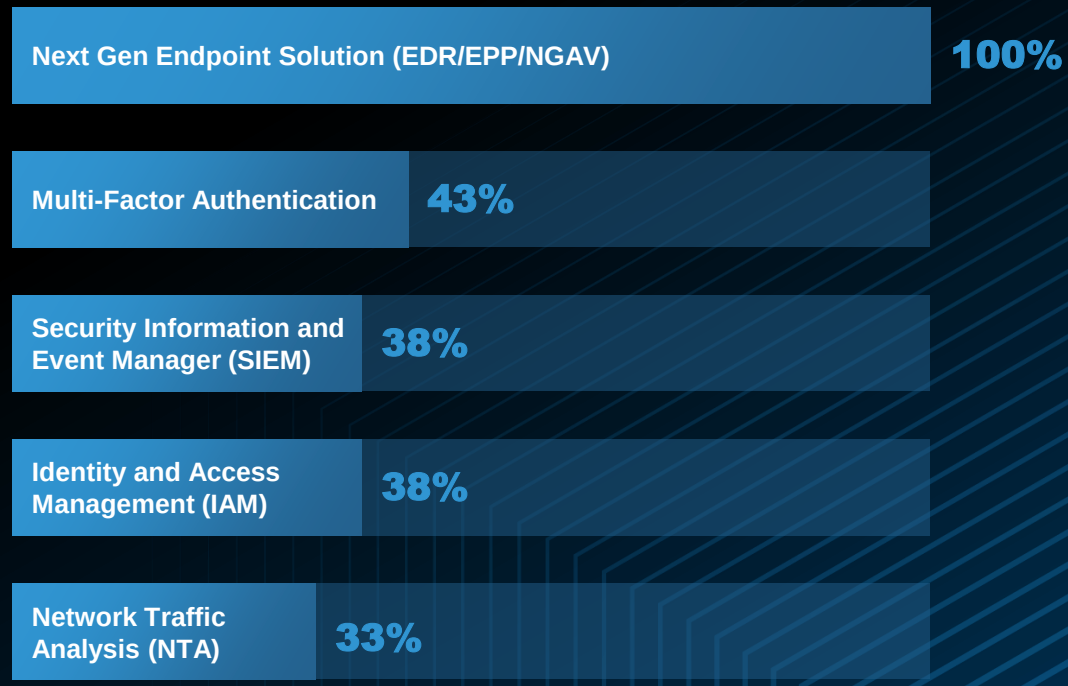


Paid by our organization
53%

Paid by our insurance or outside entity
30%

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

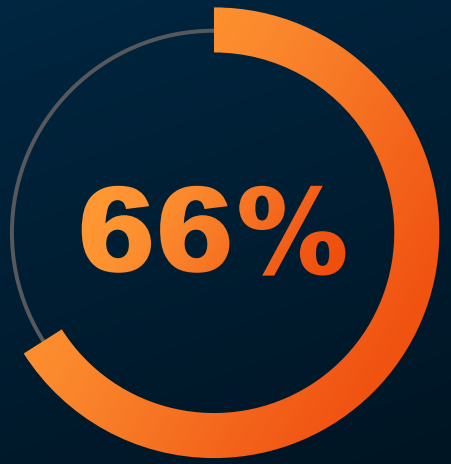
ENVIRONMENTS USING THESE TOOLS PRIOR TO RANSOMWARE ATTACK

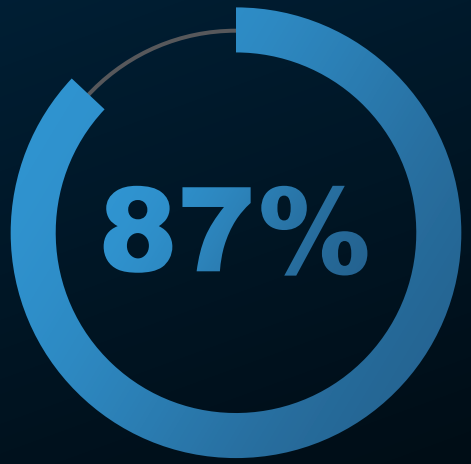


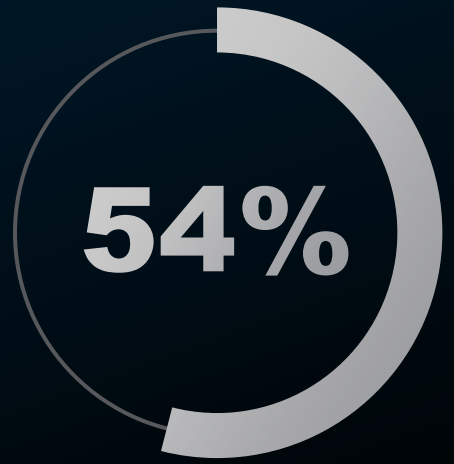
Endpoint Adoption and Footprint

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?

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 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

Tools alone are not sufficient to protect organizations, you must operate the tools to successfully prevent attacks

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

PART 4:

Managing and Mitigating Threats

Safeguard Your Organization

Recommendations

Understand the threat and believe that you are a target

Enforce strong identity controls

Ensure you have broad visibility into your environment and assets

Conduct effective and timely patching

Create and maintain a culture of security

Establish effective security operations

Questions?