ARCTIC WOLF

2026 Arctic Wolf Threat Report

Cybersecurity never sleeps.
Neither do threat actors.

AGENDA

01 Introduction and Methodology

02 The Threat Landscape in 2025

03 The Big Business of Ransomware

04 Business Email Compromise

05 Predictions for 2026

06 Key Takeaways and Questions

Introduction and Methodology

We Are Arctic Wolf

OUR MISSION: END CYBER RISK

10,000+
Customers

1,000+
Security Engineers

8+
Trillion Events per Week

1,000+
IR Engagements per Year

100+
Countries

2,250+
Partners Globally

TRIED, TESTED, & PROVEN

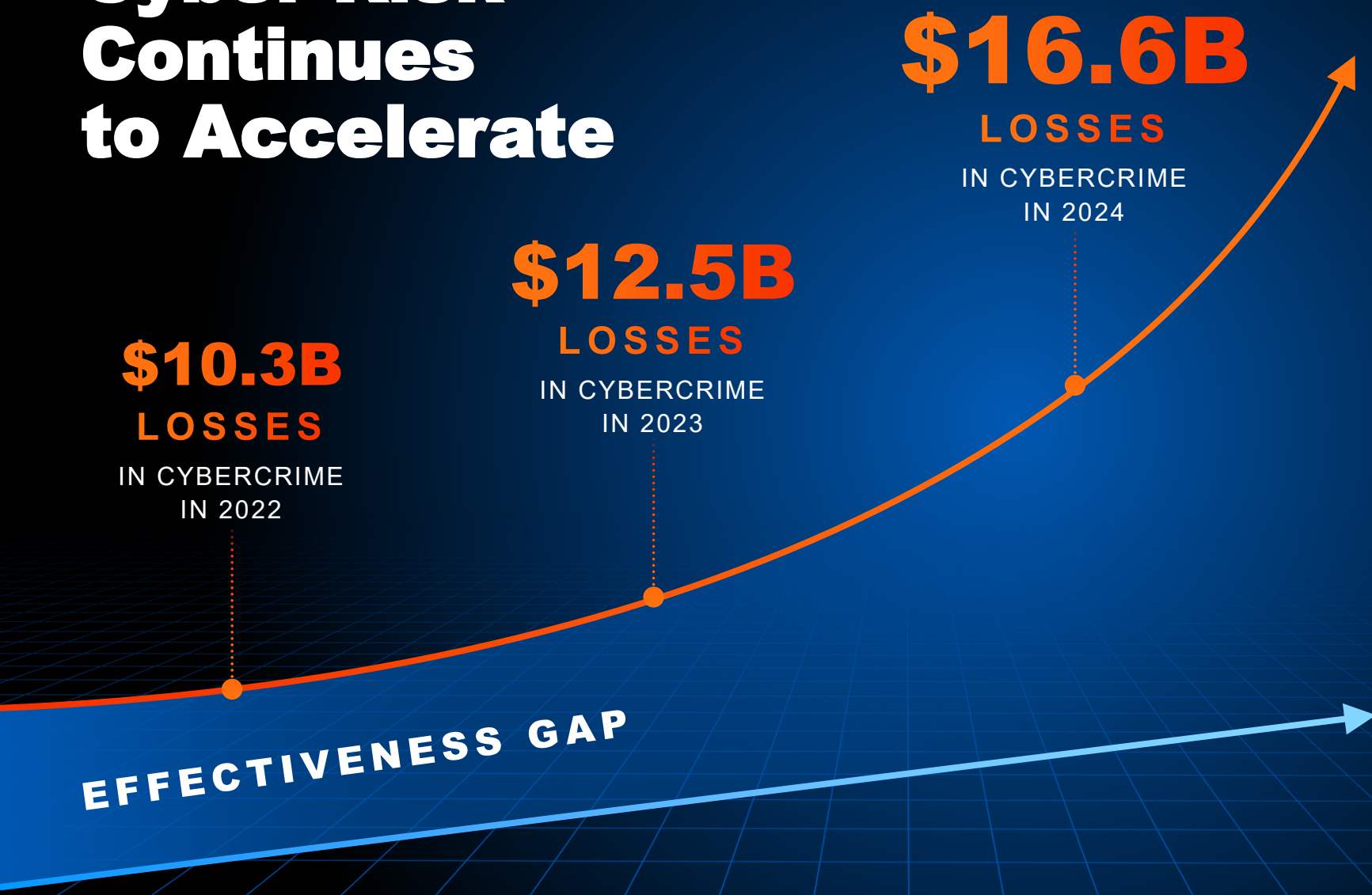
IDC
2X LEADER
MDR MarketScape

Gartner Peer Insights™
MOST RECOMMENDED
MDR, Vulnerability Assessment, and Security Awareness

CNBC DISRUPTOR 50
3X WINNER
Only Cybersecurity Company Ever

bsi ISO/IEC 27001 Information Security Management CERTIFIED
AICPA SOC
CERTIFIED
Ongoing Validation

Cyber Risk Continues to Accelerate



2022 → 2023
21% Increase

2023 → 2024
33% Increase

TOTAL SECURITY COMPANIES IN 2024:
4,000+

TOTAL SECURITY SPEND:
183B

YOY SPEND INCREASE:
13%

Sources: IC3, Gartner, It-Harvest

Introduction and Methodology

Our annual Threat Report sources data from threats that escalated to the point of requiring a full Arctic Wolf Incident Response (IR) investigation.
By focusing on this level of threat, we aim to:

Identify Most Popular Attack Types

Highlight the most common attack types and those that are responsible for high severity incidents

Uncover Threats Hiding in Plain Sight

Spotlight the tactics, techniques, and procedures (TTPs) that allowed threat actors to evade detection long enough to pursue their objectives

(i.e. deploying ransomware, exfiltration of data, establishment of persistence, etc.)

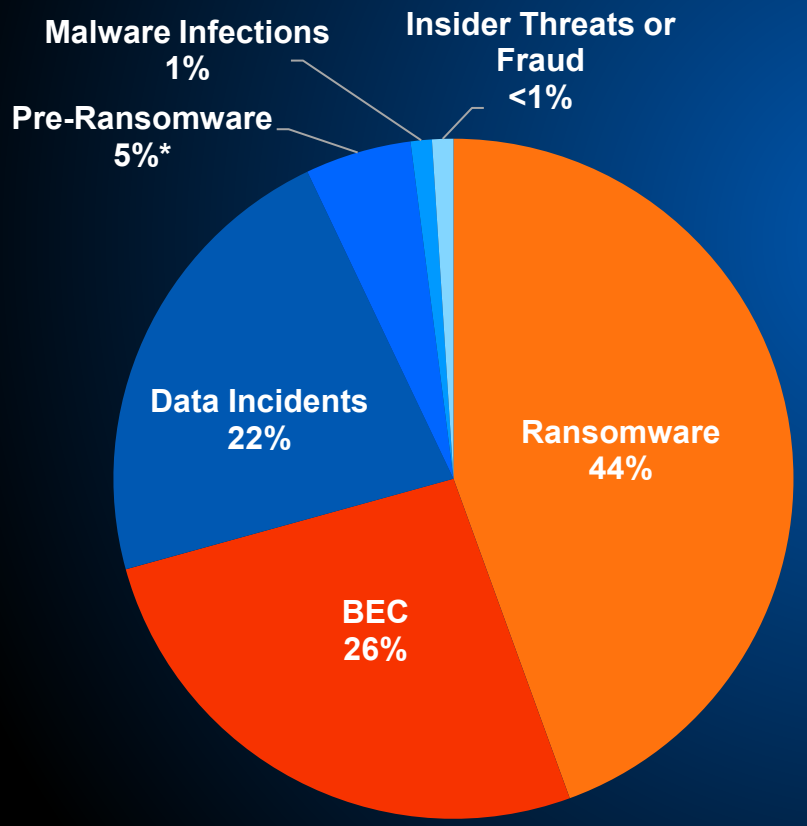
Take A Holistic Approach

Raise awareness of the full threat lifecycle and the necessary practices needed to prevent, detect, and recover from such incidents

The Threat Landscape in 2025

Top 6 Cyber Incident Types

During the reporting period, our IR team identified these top six types of cyber incidents – with 3 collectively accounted for 92% of all IR cases



We will examine these incidents in detail to provide an overview of the threat, including:

- Which industries are most impacted
- What are the primary root causes
- Expand into related topics associated with each threat

*New category for IR data

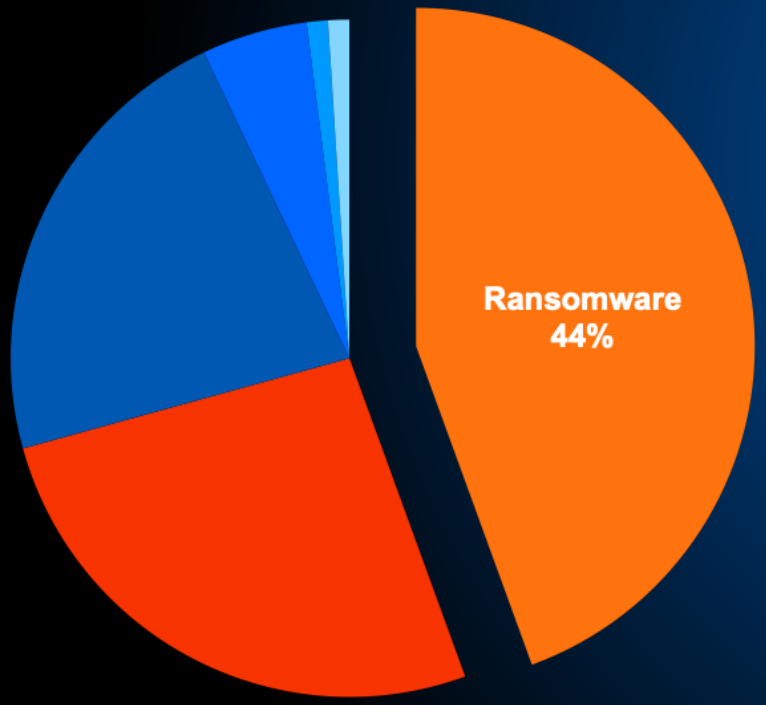
The Big Business of Ransomware

Ecosystem Shifts, Impacts and Economics

Ransomware Reigns Supreme

Despite headwinds and improved detection methods, Ransomware remains the top threat

Our 3rd annual Threat Report again ranks Ransomware as the #1 threat



Holding at 44% of IR cases highlights a lack of sustained growth, attributed to multiple factors

Increased early detection capabilities preventing execution

Law enforcement disruption and increased competition between affiliates

Operational refinement and modification of tactics

The illusion of “Business as Usual”

Stead ransomware cases deceptively covers a changing ecosystem

Improvements in Detection

- Increased ability to detect threats before they reach the detonation phase
- Timely and effective response processes from high fidelity alerting
- The results are 5% of IR cases focused on recovery of “Pre-Ransomware” threats
- Preventing detonation does not eliminate the overall threat

Takedowns and Competition

- Law enforcement actions shifted LockBit, ALPHV/BlackCat, and BlackSuit from leaders to minimal impact on our data
- Only three groups remained in the top 10 between last year and current data (FOG, Akira, and PLAY)
- New groups emerge while others absorb their peers (Qilin/Ransomhub/Dragonforce)

Refining their tactics to increase their effectiveness

- Groups like Silent pivot their focus to data theft and forgo traditional encryption methods
- This is partially responsible for the 11x increase in “Data Incidents” to 22% of IR cases
- Community driven collectives like The Com increase their effectiveness by expanding beyond the digital world with sometimes violent crime

The Motivation is Clear : Money

Financial motivation is the primary force behind most attacks

TOP INDUSTRIES (NON-BEC CASES)	2024	2025
Manufacturing	22%	**21.6%**
Legal & Government	16.8%	**21.3%**
Education & Non-Profit	17.2%	**20.2%**
Healthcare	16.5%	**13.2%**
Finance & Insurance	12.9%	**12.7%**
Construction	14.6%	**11%**

TOP INDUSTRIES (BEC CASES)	2024	2025
Finance & Insurance	34.1%	**30.9%**
Legal & Government	17.5%	**22.3%**
Education & Non-Profit	10.4%	**16.1%**
Manufacturing	15%	**11%**
Business Services	8%	**10.1%**
Construction	15%	**9.6%**

Ransomware 2026, by the numbers

Ransom Demand Insights

MEDIAN INITIAL RANSOM DEMAND ‘24:

$600,000

MEDIAN INITIAL RANSOM DEMAND ‘25:

$414,000

TOTAL DEMANDED RANSOMS:

$302,155,615

TOTAL RANSOMS PAID:

$16,481,559

INITIAL MEDIAN DEMAND DECREASE

31%

TOTAL RANSOM PAYMENT REDUCTION

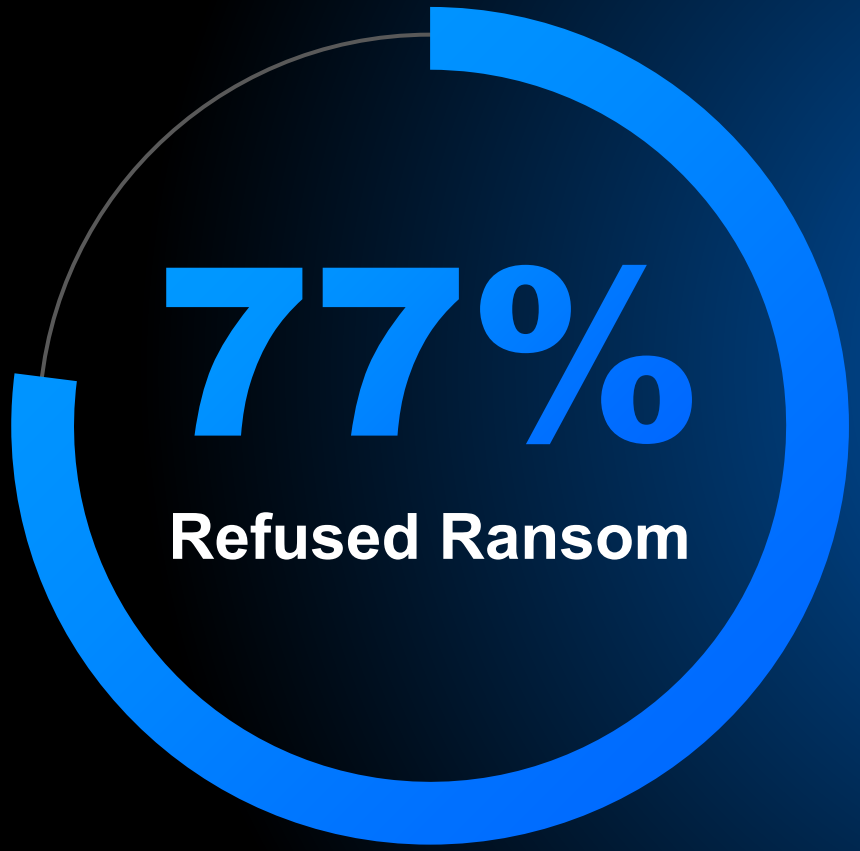
+94%

Ransom Demands by Industry

Initial Ransom Demand Made by Threat Actors

	2022	2023	2024	2025
Construction	$375,000	$500,000	$775,000	**$650,000**
Finance	$500,000	$900,000	$325,000	**$220,000**
Healthcare	$275,000	$450,000	$400,000	**$400,000**
Legal & Government	$420,000	$1,000,000	$600,000	**$200,000**
Retail	$627,500	$1,500,000	$800,000	**$1,600,000**

Expert Negotiation Pays Off

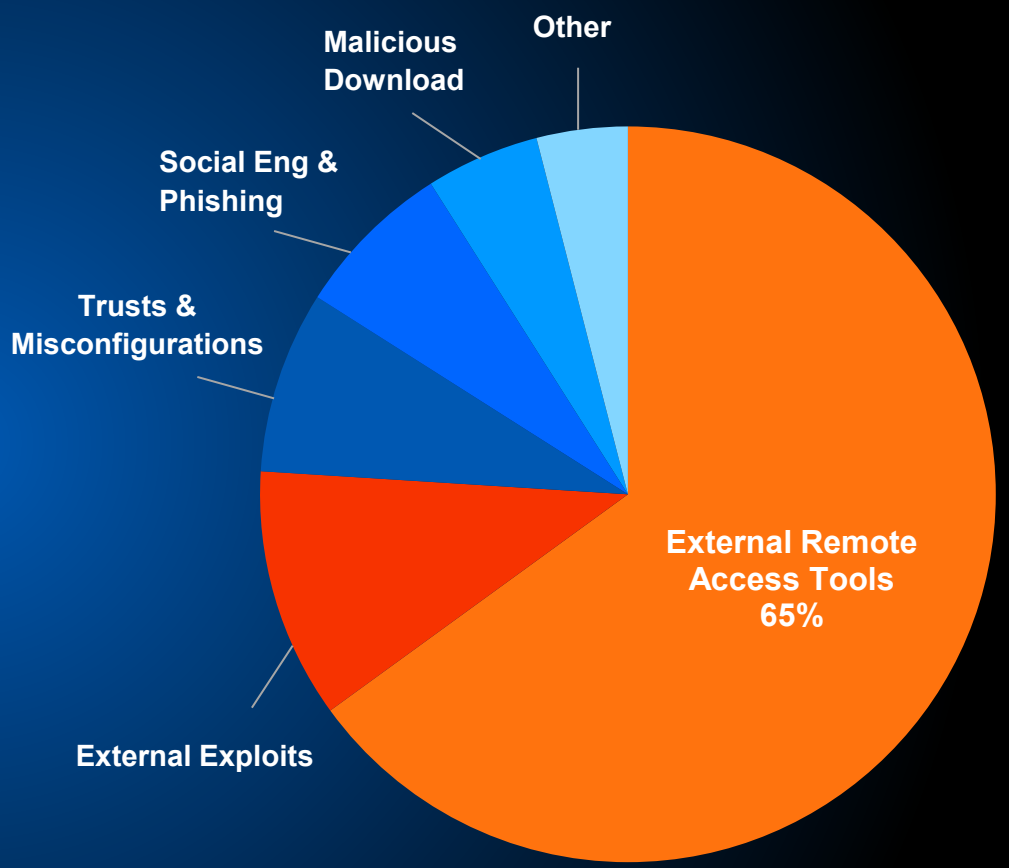


"Strong backups empower you to reject ransom demands, because resilience beats extortion. Even insurers are urging companies not to pay, proving that preparation is the smartest path to recovery, and helped **77% of clients refused ransoms entirely."**

Root Point of Compromise

The simplest methods remain the most effective

- **External Remote Access Tool account for 65% of all non-BEC Incident Response cases**
  - This includes RDP, VPN, and RMM tools
- **External Exploits dropped to 11% of IR cases in 12 months**
  - This does not account for 0-day exploits which were >2% of all IR cases
- **Trust Relationships and Misconfigurations were 8% of non-BEC case RPOC**
  - Code repositories and SEO poisoning proved effective
- **Social Engineering and Phishing made up 7% of cases**
  - Attackers will use low tech manipulation when seen as easier than high tech methods



Root Point Of Compromise (Non-BEC)

Business Email Compromise

Business Email Compromise

The underestimated and misunderstood threat costing companies Billions

BEC was the second most common threat for the 3rd consecutive year, accounting for 26% of cases

- FBI estimates yearly BEC loses over $2.7B USD
- The RPOC was phishing in 85% of BEC cases, with previously compromised credentials used in an additional 10%
- The threat of a BEC is not the compromised e-mail account, but the result of access to the account
- Many successful BEC attacks do not even require a compromise email account, using impersonation instead

Methods of Business Email Compromise

CEO / Executive Fraud

False Invoice

Product Theft / Shipping Fraud

Attorney Impersonation

Data Theft

Regional Spotlights

Beyond the global perspective

EMEA

- European countries are a hotspot for data theft without encryption
  - EMEA is the leading region for attackers that are streamlining their tradecraft and forgoing encryption in favor of data theft and extortion
  - Primary targets for this method are smaller businesses and municipalities
- Attackers are leveraging regional regulatory requirements to add additional pressure on their victims
  - GDPR fines and disclosure requirements are adding additional dynamics to victims of ransomware
  - EMEA victims are more likely to appear on leak site, with attackers moving quickly to post data

APAC

- Threat Campaigns in region show pronounced waves March and September/October timeframes
  - Aligning with Japanese FY end and end of Australian Q3 end and may be timed to use this as an advantage
  - Alternatively, threat actor Qilin lead multiple months; showing sustained yearly activity rather than singular campaigns
- SMBs constitute ~71% of APAC victims with enterprise just over 29%.
  - Interestingly, there is an inverse split between countries in this region
  - Australian and New Zealand victims are primarily comprised of SMB organizations
  - China and Japan sees a higher percentage of enterprise level organizations being targeted as victims

2026 Predictions

From Arctic Wolf Labs Experts

2026 Predictions

From AW Labs

PREDICTION 1

Information warfare will reach new heights

We expect to see a sharp rise in misinformation, disinformation, and malicious campaigns attempting to influence world politics or simply sow discontent and drive wedges into population groups.

PREDICTION 2

Threat actors will take advantage of major global events

Attackers will use the opportunity surrounding global elections along with notable worldwide sporting events to craft social engineering lures, along with ticket scams and malware delivery via fake streaming services.

Key Takeaways

Three well known threat types accounted for 92% of all IR cases

Improved defense and response strategies have resulted in decreased ransomware detonation

Attackers are finding success in abusing remote access tools

Global events are increasingly being leveraged by threat actors

Thank You