ARCTIC WOLF

Threat Report

2026

TABLE OF CONTENTS

Foreword

The past year has reinforced a lesson defenders often learn the hard way: Attackers don't need new tricks when the old ones still work.

Whether it's ransomware crews abusing remote access, social engineers weaponizing trust and timing, or affiliates pivoting to pure data theft when encryption loses its edge, the pattern is the same. Attackers follow the path of least resistance — and they follow it at scale.

From the vantage point of Arctic Wolf® Labs, where we analyze thousands of real-world intrusions, three signals stand out:

- Attackers are compressing the kill chain through automation
- They are bypassing controls by logging in, not breaking in
- They are exploiting identity, remote access, and trusted platforms long before they need an exploit

Most modern intrusions, in other words, are not technical surprises. They are architectural consequences.

This year, organizations that hardened remote access, segmented their environments, and invested in strong identity controls consistently stopped attacks that would have become headline-level incidents elsewhere. At the same time, threat actors continued to adapt — shifting toward data-only extortion, abusing trusted platforms and developer ecosystems, and operating with increasing speed and specialization.

That's why this report matters. Its insights come not from hypothetical trends, but from the most disruptive incidents our teams were called in to contain and investigate — revealing how attackers actually behave under pressure, and which controls consistently buy defenders time.

If there's one takeaway, it's this: **Defensibility beats novelty.** Organizations that invested in the fundamentals — identity, segmentation, logging, disciplined remote access, and monitoring of trusted platforms — fared dramatically better, regardless of size or industry.

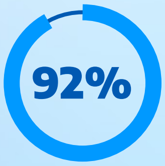
This report is designed to give you two advantages: better decisions and more time. You don't need perfect security — you need defenses built for how attacks really unfold.

Think Red. Act Blue.

ISMAEL VALENZUELA
Vice President of Labs,
Threat Research & Intelligence
Arctic Wolf

Key Takeaways

We understand that your time is in high demand, so for those readers in a rush, here's a summary of this report's major takeaways and predictions.

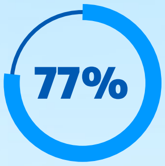


Three common cyber incident types account for 92% of Arctic Wolf IR cases

Organizations typically reserve third-party IR engagements for only the most disruptive and damaging incidents, so it's telling that our cases are dominated by ransomware (44% of cases), business email compromise (BEC) (26%), and data incidents (22%). While the relative contribution of ransomware and BEC to our caseload remained essentially consistent, data incidents surged 20% from our prior report, as cybercriminals adapt to improved organizational resilience and recovery capabilities by focusing solely on exfiltrating sensitive data and extorting victims to prevent publication.

Improved defenses are stopping ransomware before detonation

Pre-ransomware incidents accounted for 5% of Arctic Wolf IR cases (in these incidents, an intrusion was detected and contained prior to detonation of what was later confirmed to be an attempted ransomware attack). In particular, behavioral analytics and endpoint telemetry allowed defenders to identify reconnaissance and privilege escalation attempts, and timely and effective response prevented ransomware detonation.



Professional incident response pays off

Engaging with a ransomware actor is best left to the experts, as they generally have a great deal more experience with handling these events than any in-house personnel. In 77% of ransomware IR cases handled by Arctic Wolf, the impacted organization elected not to pay a ransom. In the 23% of ransomware IR cases in which the victim made the business decision to pay a ransom, Arctic Wolf's IR team secured an average reduction (compared to the initial demand) of 67%. For larger organizations, this represents an important savings; for smaller organizations, it can be the difference between survival and insolvency.

Blurred lines and shifting allegiances define the modern ransomware landscape

Ransomware groups continue to operate like profit-driven business enterprises, offering structured affiliate programs, tiered revenue models, and operational support to attract and retain a broader pool of cybercriminals. These developments have contributed to a more competitive and interconnected ecosystem, where the boundaries between distinct ransomware groups and brands are becoming increasingly difficult to delineate.

65%

Attackers are abusing common remote access tools to gain initial access

Nearly two-thirds of our non-BEC IR cases (65%) are attributable to abuse of external remote access products and services including remote desktop protocol (RDP), virtual private networks (VPN), and remote monitoring and management (RMM) tools. This dramatic surge from 24% just two years ago underscores a broader trend: Threat actors are increasingly prioritizing accessible and low-complexity entry points, rather than investing in sophisticated exploits.

85%

To stop BEC fraud, invest in phishing defenses

A whopping 85% of BEC fraud incidents were traced to email phishing, an 11% jump from last year's report. As AI empowers threat actors to build efficient workflows and craft more convincing lures, robust phishing defenses — including security awareness training — are necessary for combating BEC.

Prioritized patching remains effective, but don't forget to rotate credentials

Each of the 10 CVEs we encountered in the majority of non-BEC IR cases date to 2024 or earlier, indicating that patching even just the most-exploited vulnerabilities can significantly improve an organization's security posture. However, organizations must rotate credentials following any known vulnerability exposure, otherwise cybercriminals can simply return later and log in using stolen credentials.

180+

Threat actors are targeting key roles by abusing trusted channels

A number of campaigns (notably GPUGate, Oyster/Broomstick, and the compromise of 180+ npm packages) specifically targeted IT personnel and developers to gain initial access into organizations' environments. Particularly in the second half 2025, threat actors employed SEO poisoning and trojanized tooling, and in 2026 they will likely explore generative engine optimization (GEO) and large language model (LLM) poisoning to directly surface malicious links in search engines' AI summaries.

2026 Predictions Preview

Below, you'll find summaries of our predictions for the near future (see "2026 Predictions" for full explanations):

1. Ransomware will remain the most significant threat, but data incidents may overtake BEC
2. Social engineers will increasingly incorporate real-time voice and video manipulation
3. AI will become less of a novelty tool for threat actors and more of an everyday utility
4. Information warfare will reach new heights
5. Threat actors will take advantage of major global events

Data Sourcing & Methodology

The insights and data presented herein are drawn from 12 months of active global digital forensics and incident response (DFIR) engagements conducted by the Arctic Wolf Incident Response (IR) team. To enable the holistic analysis within this report, all data is aggregated without any identifying characteristics or attributes.

The IR case data is supplemented with telemetry from the Arctic Wolf Aurora Platform and insights from Arctic Wolf Labs: a cross-functional set of industry-leading professionals in threat intelligence, digital forensics, incident response, and experts in ransomware tactics and negotiations. Additionally, we have incorporated analysis using leak site data from third-party sources, including eCrime, to provide deeper insights into the cyber threat landscape.

Unless otherwise stated, all data (e.g., from IR cases, leak site research, or other sources) pertains to the 12-month period running from November 1st, 2024, through November 1, 2025 (which we refer to as "this reporting period" or by similar language).

Any mention of "last year's threat report" (or similar) is in reference to the Arctic Wolf 2025 Threat Report. Accordingly, analysis and explanations invoking a "report-over-report" change compare this 2026 Threat Report to the 2025 Threat Report.

Case Classification

We classify cases by the focal point of the incident, or the best answer to the question, "What is the most impactful aspect of the attack?" This year's report divides IR cases into six categories:

Ransomware

Malware intended to render systems, services, data, and other assets unusable, usually via encryption.

Business email compromise (BEC)

Email-borne phishing fraud in which a threat actor attempts to trick members of an organization into transferring funds, sensitive data, or something else of value.

Data incident

A cyber incident involving unauthorized access to and/or exfiltration of potentially sensitive data, but without the use of ransomware or attribution to an insider threat.

Pre-ransomware

Unauthorized activity/access that has not yet led to ransomware detonation, but which — via behavior; tactics, techniques, and procedures (TTPs); indicators of compromise (IOCs); or some other factor — is assessed with confidence to be part of a ransomware attack.

Malware

Malicious software not directly associated with a ransomware or data incident. Examples include cryptocurrency miners, infostealers, and remote access trojans (RATs).

Other

A catchall for incidents not attributable to one of the causes listed above. Examples include insider threats and distributed denial of service (DDoS) attacks originating from an external network (i.e., as opposed to denying service via ransomware encryption).

FROM BREACH TO INSIGHT:

Regional Data Trends in EMEA

HIGHLIGHTS

A **high concentration of ransomware activity across Western Europe,** as observed in multiple critical business verticals

The **growing trend of data extortion without encryption** and pure data theft in EMEA, especially among smaller businesses and municipalities

Supply-chain exposures increase as many EMEA leaks trace back to third-party service providers

Regulatory pressure driving attacker behavior as GDPR requirements make EMEA victims more likely to appear on leak sites

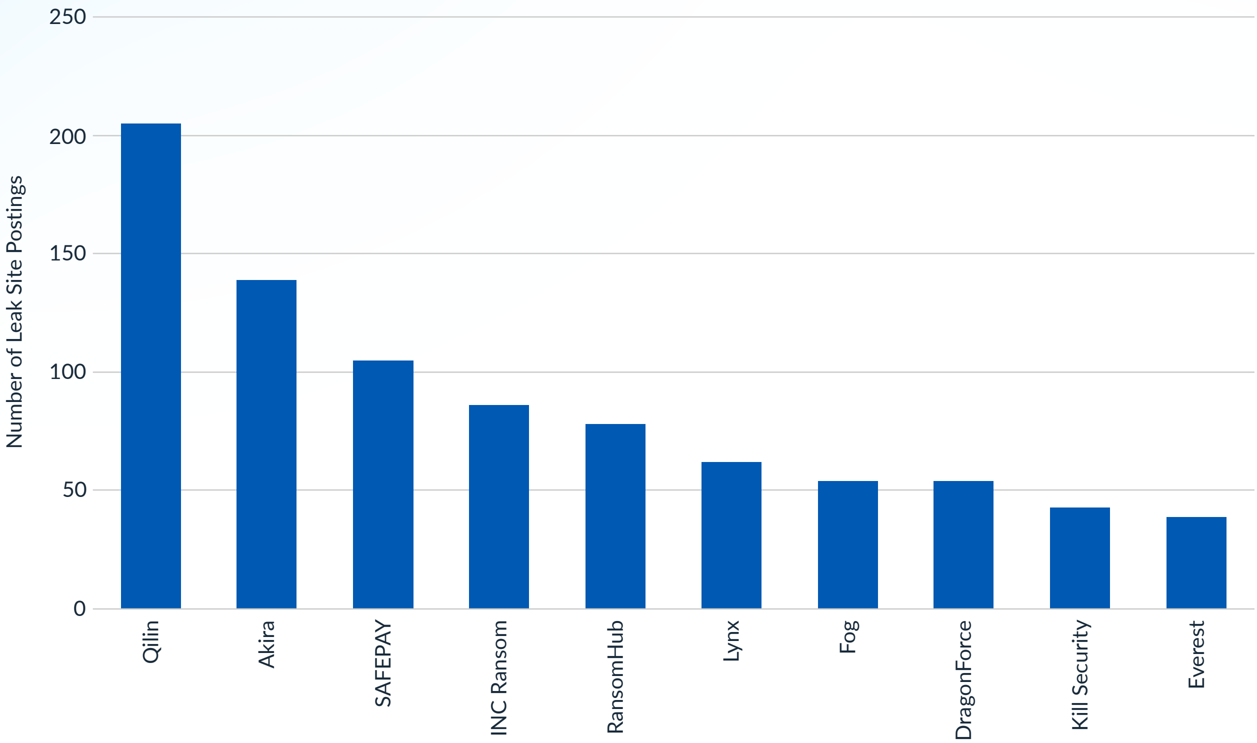
Regional Observations

Europe remains a focal point for ransomware-driven data leaks, with Western Europe accounting for the highest activity. France, Germany, and the UK consistently lead victim volumes, particularly across construction, IT services, retail, and financial services. While large enterprises in logistics and aviation remain attractive due to operational leverage, leak-site disclosures across the E.U. skew toward midsize organizations, reflecting persistent gaps in cybersecurity resources. The region exhibits a dual pattern: sustained ransomware pressure in mature economies and more opportunistic activity in markets undergoing digital transformation.

Ransomware and multi-extortion continue to drive disruption across EMEA. E.U. analysis and multiagency advisories describe a professionalized, decentralized ecosystem that rapidly weaponizes newly disclosed vulnerabilities. Initial access commonly occurs through internet-facing applications, VPN and edge infrastructure, and backup platforms, followed by fast data exfiltration and coordinated leak-site publication across Windows, Linux, and virtualized environments. Activity frequently spikes after exploitation campaigns, as seen during the Cleo managed file transfer vulnerability (CVE-2024-50623), which triggered short, high-impact disclosure waves across regions and supply chains. Outside these surges, groups such as Akira and PLAY maintain steadier, exfiltration-first publication patterns tailored by victim size and geography.

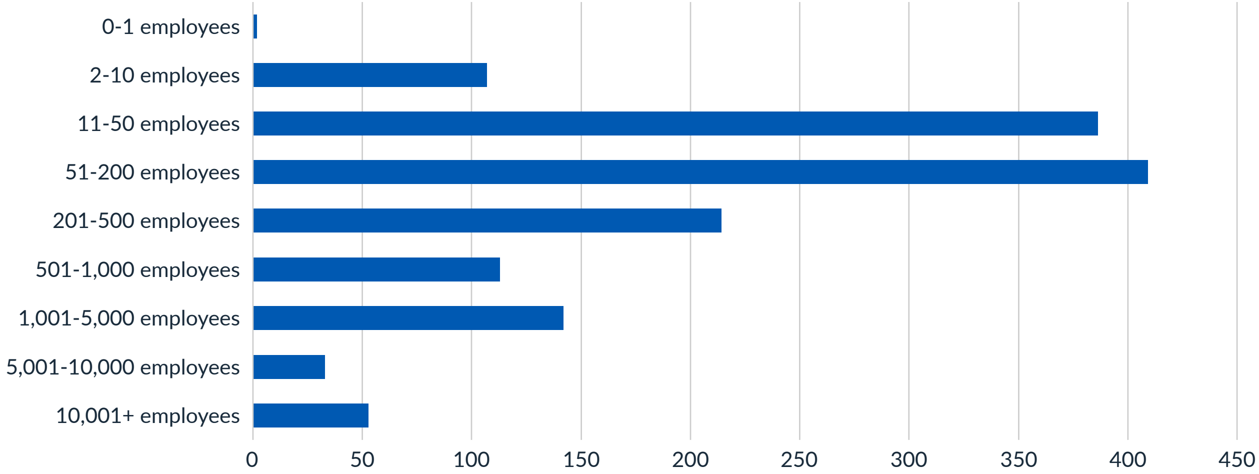
Sector exposure remains broad, spanning manufacturing, professional and technology services, public administration, retail, and healthcare. ENISA's 2025 assessment identifies ransomware as the most disruptive threat across critical sectors, with healthcare incidents increasingly reflecting exfiltration-only extortion and third-party exposure. While leak-site activity skews toward small and midmarket organizations, enterprise incidents remain lower in volume but higher in operational impact.

Top Ten Threat Actors Targeting Europe



Note: this is according to publicly available leak site information.

Leak Site Postings by Business Size in EMEA

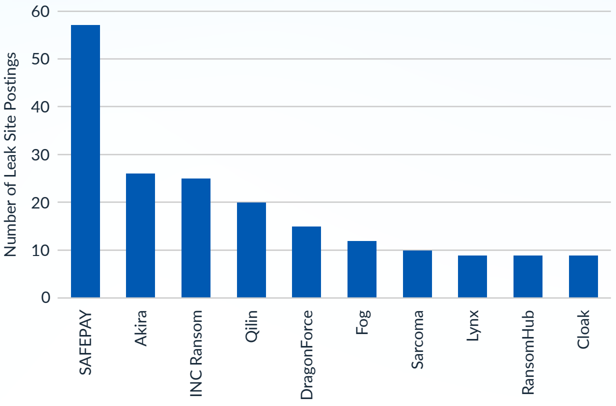


Note: this is according to publicly available leak site information.

Germany

Germany's leak-site activity reflects a consistent actor mix, including SAFEPAY, Akira, INC Ransom, and Qilin, with disclosures clustering in construction, IT services, and wholesale. Activity is dominated by small and medium-sized organizations, aligning with 2025 reporting that identifies ransomware and data leaks as the most significant criminal risks. BSI analysis highlights coercion methods such as zero-day exploitation and leak-site publication without encryption, patterns observed during the Cleo campaign window. Germany's prominence reflects its role as an industrial hub, where operational complexity, vendor reliance, and GDPR-driven disclosure pressures amplify extortion leverage.

Top Ten Threat Actors Targeting Germany

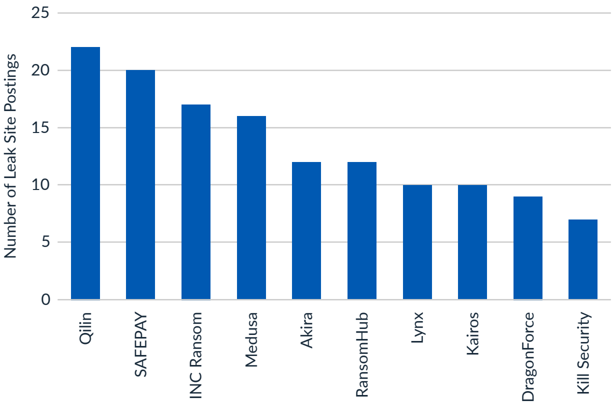


Note: this is according to publicly available leak site information.

United Kingdom

U.K. postings show a stable actor set, including Qilin, SAFEPAY, INC Ransom, Medusa, and Akira, with exposure concentrated in construction, financial services, retail, and healthcare. Victim size skews toward small and midsize organizations, with steady representation from larger firms. The NCSC Annual Review 2025 identifies ransomware as the most pressing national cyber threat and notes an increase in nationally significant incidents. Policy continues to shape response posture, including restrictions on ransom payments and proposals to mandate incident reporting. High-profile retail breaches involving Harrods and the Co-operative Group highlight the sector's vulnerability to ransomware and supply-chain compromise. Legislative expansion under the Cyber Security and Resilience Bill further reinforces a shift toward rapid disclosure and regulatory oversight.

Top Ten Threat Actors Targeting the UK

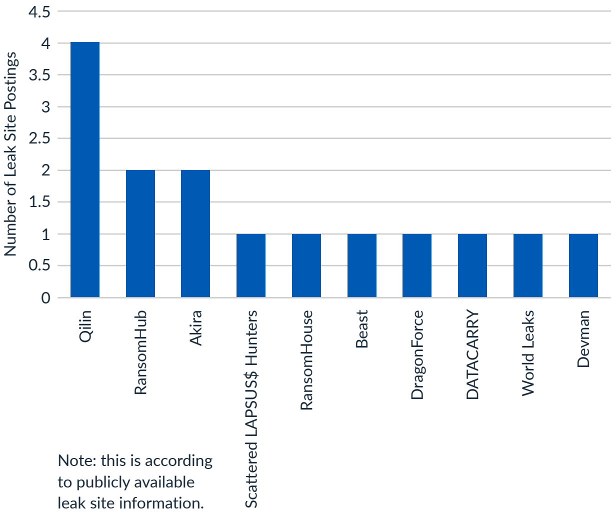


Note: this is according to publicly available leak site information.

Denmark

Denmark's leak-site volume is lower than Germany and the U.K. but follows similar patterns. Actor activity includes Qilin, Akira, and RansomHub, with cases concentrated in small and midsize organizations across construction, retail, aviation, wholesale, education, and telecom-linked services. This distribution suggests opportunistic targeting tied to reliance on externally operated platforms. Broader threat activity in 2025, including coordinated DDoS attacks against municipalities and public services ahead of elections, reinforces national assessments that rate cybercrime and cyber espionage as persistent operational risks. These dynamics align with Denmark's leak-site trends, where vendor spillover and widely used platforms can drive short but concentrated disclosure bursts.

Top Ten Threat Actors Targeting Denmark



Note: this is according to publicly available leak site information.

The Threat Landscape in 2025

HIGHLIGHTS

44% — **Ransomware continues its reign as the most common cause of IR cases:** 44% of Arctic Wolf IR cases during this reporting period pertained to deployed/detonated ransomware, the fourth consecutive threat report where ransomware topped the list.

26% — **Business email compromise remains an all-too-common and impactful threat:** BEC incidents represented 26% of Arctic Wolf IR cases this period, underscoring the staying power and costly impact of this often-misunderstood threat.

22% — **In lieu of operational disruption, some cybercriminals are specializing in data theft and extortion:** Data incidents surged from 2% of IR cases in our prior report to 22% in this reporting period, as cybercriminals adapt to improved organizational resilience and recovery capabilities by focusing solely on exfiltrating sensitive data and extorting victims to prevent publication.

Improved detection capabilities are thwarting ransomware attacks before detonation: In 5% of Arctic Wolf IR cases, ransomware attacks were contained before the payload could be detonated, thereby preventing greater impact.

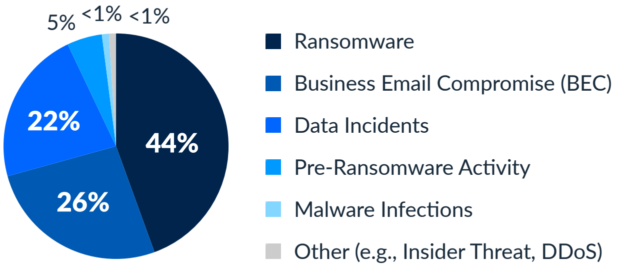
As we revealed in the Arctic Wolf 2025 Human Risk Report — which was based on a survey of more than 1,700 IT leaders and end users worldwide — 68% of IT leaders indicated that their organization "suffered a breach in the past year."

However, not every breach is severe enough to require a full-scale incident response engagement, as mitigation strategies such as 24x7 managed detection and response (MDR) can quickly contain threats before they reach an enterprise-critical level.

This is why the majority of our IR engagements originate through our insurance provider relationships and privacy law practitioners, who are called in when incidents are so damaging and disruptive that they lead to insurance claims. Consequently, studying IR cases is an effective way to better understand the most dangerous threats.

Arctic Wolf Incident Response Cases by Category

(November 1, 2024 through November 1, 2025)



> "We're seeing a clear pivot in attacker behavior. As organizations improve their ability to recover from encryption events, some threat actors are skipping ransomware altogether and moving straight to data theft and extortion. From an incident response perspective, this shift fundamentally changes how impact is assessed and managed."
>
> KERRI SHAFER-PAGE, VP OF INCIDENT RESPONSE AT ARCTIC WOLF

Ransomware and BEC remain the most common incidents

Although the threat landscape is shaped by a broad mix of actors, financially motivated cybercriminals are behind the majority of attacks severe enough to require help from an IR team. In this reporting period, ransomware (excluding pre-ransomware incidents, discussed below) and BEC incidents combined to account for 70% of our IR cases. For context, in the prior reporting period this figure stood at 71%, and two reports ago it was 78%.

Against headwinds, ransomware groups continue to wreak havoc

Ransomware accounted for 44% of our IR incidents — exactly the same portion as in our 2025 Threat Report. This dominance reflects the continued profitability and operational impact of ransomware attacks, which often force organizations into urgent response scenarios.

Notably, this is our third consecutive threat report in which ransomware has topped our IR charts, a streak that continues despite organizations' improved ability to detect ransomware, a number of significant law enforcement takedowns, and a shifting ransomware ecosystem (see **Ransomware Ecosystem Shifts**).

Ransomware groups and their affiliates consistently target organizations that are extremely sensitive to downtime and/or are severely impacted by the theft and unauthorized release of sensitive data. Accordingly, the sectors with the most representation in our ransomware IR cases are:

1. **Manufacturing**
2. **Legal**
3. **Education & Nonprofit**
4. **Finance & Insurance**
5. **Healthcare**

BEC groups might not steal headlines, but they're still stealing funds

Business email compromise also showed impressive year-over-year consistency, falling by only a single percentage point to 26% of cases. Again, this persistence comes despite BEC headwinds, including increased awareness and improved detection of email-borne threats.

Based on case investigations, Arctic Wolf IR experts believe some of the staying power of BEC can be attributed to the use of artificial intelligence (AI) to increase both the efficiency of an attack campaign (driving scale) and its effectiveness (i.e., through improved impersonation).

Threat actors who favor BEC tend to target prospects who have a high volume of valuable transactions, evident in the most represented sectors within our BEC IR case catalog:

1. **Finance & Insurance**
2. **Legal**
3. **Education & Nonprofit**
4. **Manufacturing**
5. **Business Services**

BEC activity throughout the reporting period showed a fairly steady flow of cases, with a dip in May followed by a surge in June and July. These fluctuations suggest that threat actors time campaigns strategically to align with organizations' financial cycles, world and cultural events, or high-volume transaction periods (such as holidays) when oversight may be reduced.

BEC: An underestimated and misunderstood risk

In April 2025, the FBI released their annual **Internet Crime Report**, which tallied losses due to BEC conducted in 2024 at more than $2.7 billion (USD) — yes, with a "b."

Yet, this threat remains both underestimated and misunderstood.

Part of the reason is the name itself:

- First, the name "business email compromise" describes only an intermediate step in a larger attack chain, diluting the actual threat and consequence.
- Second (and confusingly), modern BEC attacks don't necessarily involve an account compromise, as threat actors can achieve the same desired outcomes simply by impersonating a trusted email account. A simple example would be creating a false Gmail account in the name of your organization's CEO and emailing unsuspecting employees with an urgent request to transfer funds.

Plus, although most BEC attacks attempt to trick a target into transferring funds, that isn't the only goal. Today's BEC attacks come in a variety of forms, most prominently:

Account Compromise

In this classic form, rather than simply masquerading as a trusted email account, an attacker succeeds in gaining access to a legitimate email account and uses it to execute the scam by sending and replying to emails from the hijacked account, sometimes using filtering tools and other techniques to prevent the real account holder from noticing the activity.

Data Theft

An attacker targets HR and finance employees to obtain personal or sensitive information about individuals within the company, such as CEOs and executives. This data can then be leveraged to enable future cyber attacks.

In rarer instances, an attacker masquerading as a customer or vendor may ask a recipient (e.g., someone in a legal or technical role) to send intellectual property or other sensitive or proprietary information.

CEO/Executive Fraud

An attacker masquerading as the CEO or other senior executive within an organization emails an individual with the authority to transfer funds, requesting a transfer to an account controlled by the attacker.

False-Invoice Scheme

An attacker posing as a known vendor or supplier emails an individual with the authority to transfer funds to an account controlled by the attacker.

Product Theft

A relatively new twist, in which an attacker imitating a customer tricks an organization into selling (and shipping) a large quantity of product on credit.

Attorney Impersonation

An attacker impersonates a lawyer or legal representative for the company and emails an employee requesting funds or sensitive data. Lower-level employees are commonly targeted through these types of BEC attacks.

Data incidents surged to 22% of IR cases — an 11x increase

Data incidents (defined in **Data Sourcing & Methodology**) accounted for 22% of our IR cases in this reporting period, a remarkable 11x increase over the prior period (2%). This increase shows that threat actors are willing and able to adapt when needed. Our IR experts believe this adaptation is a direct response to organizations' increased ability to recover from traditional ransomware attacks.

Signs of this shift began with the rise of double-extortion ransomware, and it now appears that some threat actors (e.g., Silent Ransom) have begun abandoning encryption altogether to focus purely on data exfiltration and extortion in hopes of better net returns.

LOOKING AHEAD

Our Arctic Wolf 2025 Human Risk Report revealed that 80% of IT leaders and 63% of employees are using generative AI tools for work — and 60% of leaders and 41% of staff admit to feeding these tools confidential data.

With the breakneck pace at which companies are rolling out large language models (LLMs) and making data accessible through AI agents, we anticipate a growing number of data incidents related to insecure AI implementations.

Pre-ransomware detection is improving

In previous threat reports, the minimal number of pre-ransomware incidents didn't warrant their own category. Yet in this period, they accounted for 5% of total Arctic Wolf IR cases.

This year-over-year change is likely driven by a combination of:

1. **Improved detection capabilities,** including behavioral analytics and endpoint telemetry, that identify the intrusion before the threat actor can detonate the encryption malware.
2. **Timely and effective response** to the alerts generated by these improved detection capabilities.

However, despite these positive developments, we must stress continued investment in an organization's defense-in-depth approach. While it seems that many organizations are now better able to detect the early signs of an intrusion, threat actors don't simply walk away. Continued vigilance and continuous improvements remain necessary.

> **"Earlier detection is one of the most encouraging trends in our IR data. In cases where defenders interrupt the attack before detonation, the difference in cost, downtime, and recovery complexity is dramatic. These are the outcomes that justify sustained investment in detection and response."**
>
> **KERRI SHAFER-PAGE, VP OF INCIDENT RESPONSE AT ARCTIC WOLF**

Ransomware Ecosystem Shifts

HIGHLIGHTS

Ransomware groups are continually experimenting with operational optimizations, affiliate relationships, and monetization strategies: This reporting period saw shared infrastructure, refined affiliate programs, threat diversification, and other experiments as ransomware groups chase partners, prominence, and — ultimately — profits.

31.4%

Akira, Fog, and Play continued as leaders: These three groups are the only holdovers from our previous threat report leaderboard, and collectively accounted for 31.4% of Arctic Wolf ransomware IR cases where confident attribution was possible.

Six ransomware groups climbed onto the leaderboard: Underscoring the dynamism of the ransomware ecosystem, six groups (Qilin, RansomHub/DragonForce, INC, Silent Ransom, Lynx, and Rhysida) enjoyed enough success to emerge among the leaders.

Law enforcement takedowns made an impact: LockBit, ALPHV/BlackCat, and BlackSuit were among the most successful ransomware groups in our previous threat report; but have fallen off the leaderboard in this reporting period.

Attribution is a growing challenge: Between affiliate migrations, shifting partnerships, overlapping TTPs, frequent rebrands, and ongoing mergers and acquisitions, the shifting ransomware ecosystem is making firm attribution increasingly difficult.

A maturing affiliate ecosystem

During this reporting period, we observed that ransomware groups are increasingly operating like business enterprises, offering structured affiliate programs, tiered revenue models, and operational support to attract and retain a broader pool of cybercriminals.

These developments have contributed to a more competitive and interconnected ecosystem, where the boundaries between distinct groups and brands are becoming increasingly difficult to delineate. This is especially true as individual groups may operate more than one brand, or even rebrand when necessary (e.g., Hunters International rebranded to World Leaks).

Affiliate diversification

A prominent trend is the diversification of affiliate offerings. Ransomware-as-a-Service (RaaS) model — which typically offers affiliates up to 80% of ransom proceeds — remains foundational, many groups have expanded their services to include data extortion and access monetization.

These models allow affiliates to profit from stolen data or compromised credentials without necessarily deploying ransomware. Some groups now assist affiliates in publishing exposés of victim data or provide intelligence packages to help increase pressure during extortion. As with enterprise partner programs, these services often impose specific requirements, such as geographic restrictions or sector exclusions (e.g., healthcare), reflecting a more segmented and disciplined approach to operations.

However, despite these innovations, we have yet to observe a noteworthy increase in activity from all groups employing these expanded models. For example, groups like Anubis and DragonForce have introduced flexible monetization paths and infrastructure consolidation strategies, but their overall activity levels have remained relatively stable (or even decreased). Whether this is designed to be a strategic pace of operation or a limitation in their ability to expand, we are not entirely sure, but time will tell if these new offerings will lead to long-term growth and affiliate loyalty.

By contrast, other groups, such as those that absorbed affiliates from dissolved operations, have seen more immediate impact. Qilin, for instance, experienced upticks in activity after reportedly onboarding affiliates from groups like RansomHub. This indicates that affiliate migration may be a more immediate driver of operational scale than service innovation alone. Should that turn out to be the case, we can expect more groups to focus growth efforts on affiliate recruitment.

Blurring lines

Another noteworthy development is the increasing overlap between affiliates, infrastructure, and tactics across different ransomware brands. We have observed a number of cases in which threat actors seemingly operate across group boundaries, deploying one group's ransomware while leveraging another's infrastructure or negotiation channels.

This affiliate fluidity is further complicated by the evolution of community-driven collectives, such as The Com, also known as The Community. According to the FBI, The Com is an expansive global affiliation composed of several overlapping networks of criminals (primarily hackers, SIM swappers, and extortionists). Existing as a collective extends this group's activities beyond the digital world and into areas such as violent crime as a service (e.g., shootings, robbery, assault, SWATing, crypto-related kidnappings, etc.).

These groups emphasize peer vetting, insider recruitment, and technical collaboration, often blending social engineering with traditional ransomware tactics. As a result, attribution has become more challenging, with a threat landscape that is increasingly modular, decentralized, and agile.

LOOKING AHEAD

In 2026, we expect to see continued emphasis on agility as well as frequent rebrands.

For example, BlackSuit — which accounted for nearly 6% of Arctic Wolf IR cases in our previous Threat Report — disappeared from the 2025 landscape.

However, similarities in tactics, tooling, and ransom notes hint at a possible rebrand as "Chaos."

Competition among ransomware groups is fierce

In addition to the evolving RaaS ecosystem outlined above, law enforcement agencies have made significant inroads in disrupting, and on occasion, entirely shutting down ransomware groups, including LockBit, ALPHV, and BlackSuit.

All these factors combine to create a very dynamic ecosystem in which:

△

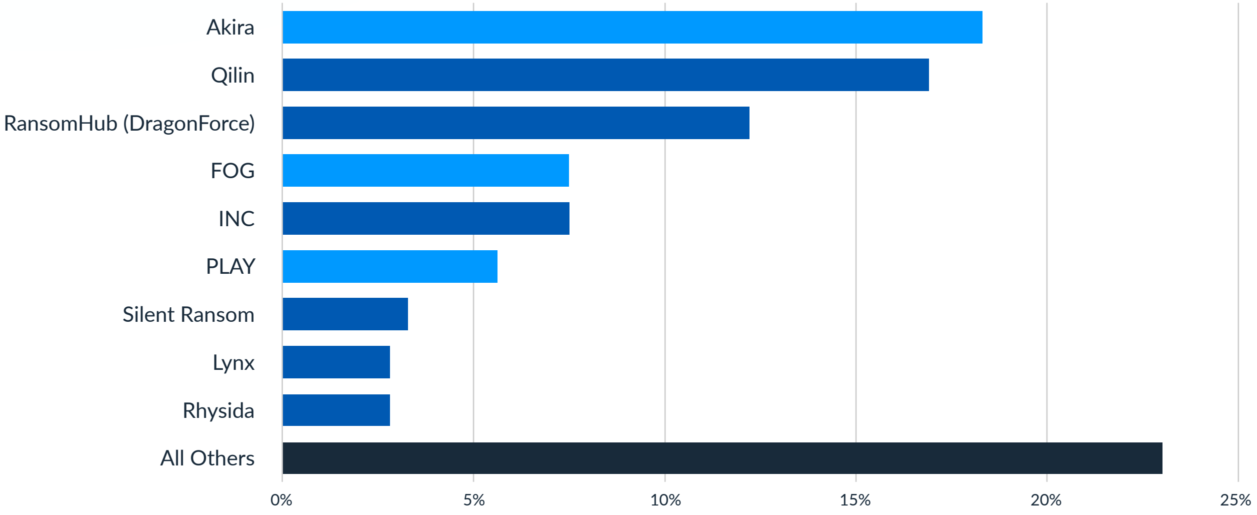
A small number of groups dominate at any point in time: Akira, Qilin, and RansomHub (which has been taken over by DragonForce) account for more than 47% of the IR cases for which we can confidently attribute a perpetrator.

▽

Time at or near the top can be fleeting: Only three of the most represented groups from our previous threat report maintained their status (Akira, FOG, and PLAY), while six groups climbed the ranks (Qilin, RansomHub, INC, Silent Ransom, Lynx, and Rhysida).

Ransomware Groups by Share of Attributed Cases

(sourced from Arctic Wolf IR cases)



Initial Access Trends

HIGHLIGHTS

65%

Attackers are maliciously leveraging the very tools organizations deploy to secure remote access: 65% of this report's non-BEC IR cases are attributable to abuse of external remote access products and services, including RDP, VPN, and RMM tools — a steady climb from just 24% three years ago.

11%

External exploits remain a dangerous threat but are behind comparatively fewer cases: Perhaps due to improved patching programs, external exploits of known vulnerabilities for which patches were already available drove 11% of non-BEC IR cases, a sharp decline from 29% in the previous threat report.

85%

BEC threat actors continue to have success with low-cost, low-complexity attack vectors: Among Arctic Wolf BEC IR cases with a confirmed root case, email phishing accounted for a whopping 85% of cases and previously compromised accounts or credentials drove 10%.

Where the root cause of an IR case can be determined, two conclusions stand out:

- **Non-BEC incidents** (e.g., ransomware, data incidents, pre-ransomware, and malware attacks) are mostly due to external remote access.
- **BEC incidents** are largely caused by phishing emails.

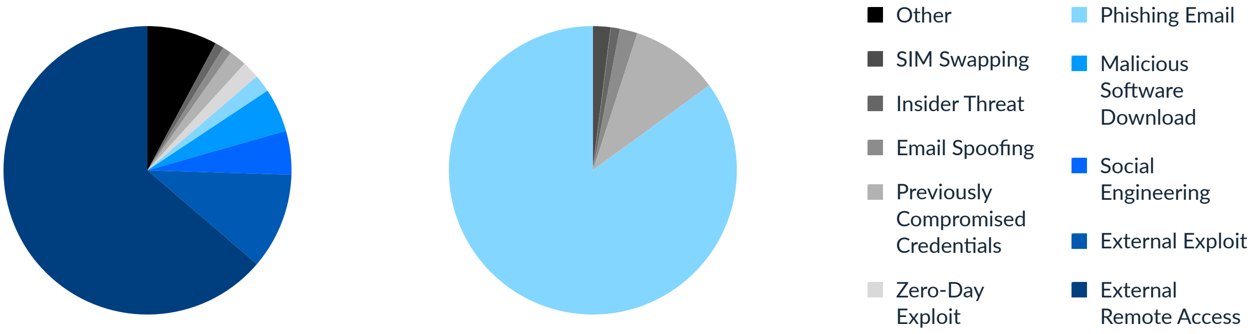
However, it's worth taking a deeper dive into each overall category to explore other root causes and to project into 2026.

Root Cause of Non-BEC Incidents

(sourced from Arctic Wolf IR cases)

Root Case of BEC Incidents

(sourced from Arctic Wolf IR cases)



> "Group names change but attacker tradecraft remains consistent. Defenders who focus on behaviors rather than chasing names and labels make far better decisions under pressure."

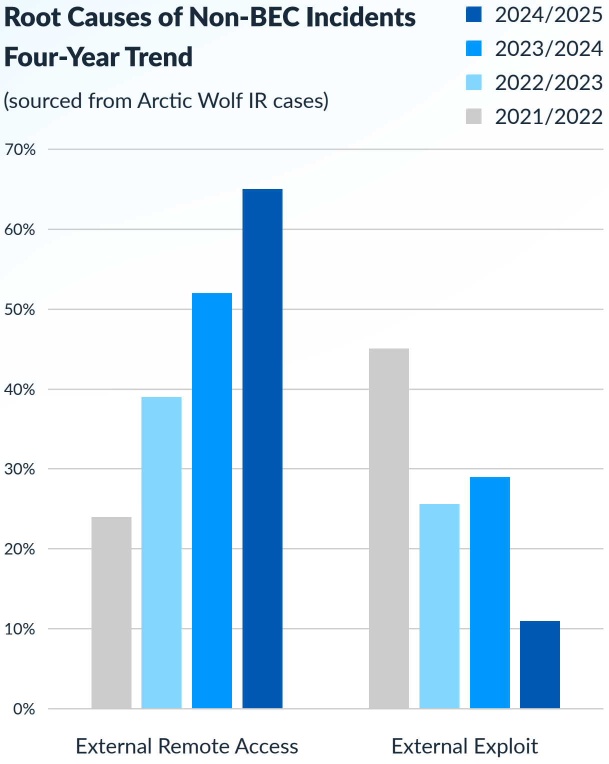
ISMAEL VALENZUELA, VP OF LABS, THREAT INTELLIGENCE AT ARCTIC WOLF

External remote access is the leading cause of non-BEC IR cases

As noted above, the leading determined cause of non-BEC IR cases is the malicious leveraging of **external remote access,** which is behind 65% of incidents. This group includes RDP, VPN, and RMM tools, which remain common attack surfaces. To put this in perspective, attackers are abusing the very tools organizations have implemented to enable and secure their remote offices and workforces, often by simply logging in to unprotected services.

Root Causes of Non-BEC Incidents Four-Year Trend

(sourced from Arctic Wolf IR cases)



The second-leading cause was **external exploits** at 11%. It's important to note that in these incidents our teams found that the threat actors exploited common vulnerabilities with existing patches, not zero-days.

Although these may be common root points of compromise (RPOCs), we have observed a shift with external remote access growing in prominence (rising from 39% two reports ago) while external exploits become less frequent (falling from 26% two reports ago). The move away from external exploits could be an indicator that adversaries are prioritizing easier targets over exploit development.

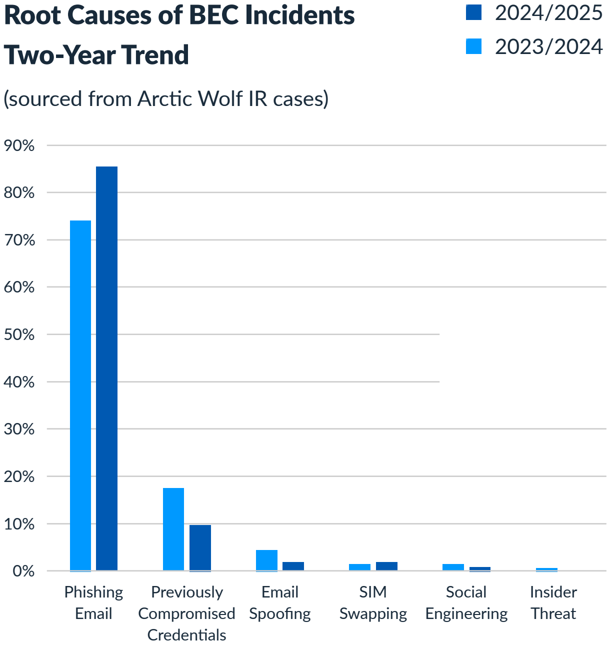
Accounting for less than 1% of cases last year, the combination of **trusted relationships and misconfigurations** surged to 8% in this reporting period, indicating that supply chain dependencies and configuration errors are potentially becoming more attractive attack vectors.

This shift underscores a broader trend: threat actors are increasingly prioritizing accessible and low-complexity entry points, rather than investing in sophisticated exploits.

Email phishing drives BEC cases

Root Causes of BEC Incidents Two-Year Trend

(sourced from Arctic Wolf IR cases)



Among BEC IR incidents with a confirmed root cause, **email phishing** dominated, at 85% of cases (a significant jump over the 74% in last year's report).

Previously compromised accounts or credentials accounted for 10% of BEC cases, an eight-percentage point decline over the 18% shown in last year's threat report.

The ongoing dominance of phishing and credential use demonstrates that threat actors continue to favor scalable, low-cost phishing campaigns as their primary entry point for BEC attacks, exploiting trust rather than technical flaws.

Edge Device Abuse & Infrastructure Exploitation

HIGHLIGHTS

Edge devices remain prime targets: Owing to their exposure, inconsistent patching, and often weak credential hygiene, edge devices can provide an effective and stealthy means for attackers to gain access.

Skilled attackers can achieve full domain compromise in minutes: Automation and operational maturity on the part of cybercriminals underscores the importance of highly effective detection, containment, and response capabilities.

Patching pays off: While new exploits rightfully deserve attention, every single one of the CVEs we encountered the most in this report's non-BEC IR cases dates from 2024 or earlier.

...But patching alone is insufficient if compromised credentials aren't rotated: Organizations must rotate credentials and audit access logs following any known vulnerability exposure, especially for edge devices that serve as entry points into the network, otherwise criminals can simply return later and log in using stolen credentials.

Edge devices remain under attack

During this reporting period (and fulfilling a forecast made in our 2025 Predictions Report) threat actors relentlessly attacked edge devices and other privileged pieces of infrastructure.

The consistent targeting of VPNs, firewalls, and RMM utilities, as well as internal software ecosystems, demonstrates not just opportunism, but a strategic understanding by threat actors of how these systems can meaningfully accelerate attacks. In our case reviews we have found that edge devices remain high-value targets due to their exposure, inconsistent patching, and often weak credential hygiene.

Whether through rampant credential reuse or potentially devastating exploitation, threat actors are demonstrating a high level of automation and operational maturity, at times achieving full domain compromise within minutes of gaining access.

> "In multiple investigations this year, we observed attackers achieve domain-level control in minutes. That speed leaves little room for manual intervention and underscores why continuous monitoring and rapid response are no longer optional."
>
> KERRI SHAFER-PAGE, VP OF INCIDENT RESPONSE AT ARCTIC WOLF

Exploitation of familiar CVEs underscores the importance of patching

The CVEs that show up the most in our non-BEC incident response cases skew heavily towards high-value edge devices, as they enable adversaries to bypass initial access defenses and establish persistence early in the kill chain.

NON-BEC CVES

01	CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability
02	CVE-2023-4966	Citrix NetScaler ADC & Gateway Buffer Overflow Vulnerability
04 (TIE)	CVE-2024-1709, CVE-2024-1708	ConnectWise ScreenConnect Authentication Bypass Vulnerability
04 (TIE)	CVE-2023-3519	Citrix ADC, Citrix Gateway/ Citrix Bleed Remote Code Execution Vulnerability
06 (TIE)	CVE-2023-20269	Cisco ASA Firewall VPN Authentication Vulnerability
06 (TIE)	CVE-2024-55591	FortiOS and FortiProxy Authentication Bypass Vulnerability
07	CVE-2023-48788	FortiClientEMS Remote Code Execution Vulnerability
08	CVE-2021-34473, CVE-2021-34523, CVE-2021-31207	ProxyToken: On-Premises Microsoft Exchange Authentication Bypass Vulnerability
09	CVE-2024-55956	Cleo LexiCom, VLTransfer, and Harmony Unauthenticated Remote Code Execution
10	CVE-2024-53704	SonicOS Authentication Bypass Vulnerability

Beyond initial access

Importantly, these vulnerabilities were not only exploited for entry, they also accelerated adversary progression through the kill chain, often skipping privilege escalation phases due to the elevated access that edge devices inherently provide.

These flaws enabled unauthenticated attackers to gain administrative access and conduct lateral movement, directly impacting the exploitation and command-and-control phases of the kill chain.

In some cases, exploitation occurred before CVEs were formally assigned, as seen in **this analysis of a campaign targeting Palo Alto firewalls**. Absent a CVE (which describes a vulnerability in detail) and a patch, organizations impacted by a vulnerability are often forced to enact coarse defensive measures, as shown in the example above, where "PAN strongly advises customers to secure their management interfaces by restricting access to trusted internal IP addresses and ensuring they are not exposed to the internet."

As edge infrastructure continues to grow in complexity and exposure, proactive vulnerability management, segmentation, and continuous monitoring of externally facing assets are essential to reducing exposure and mitigating the growing risk posed by edge-focused exploitation.

Trusted Platform & Supply Chain Abuse

HIGHLIGHTS

Threat actors are targeting high-value demographics by abusing trusted channels: Compromising a developer or IT account or device can allow an attacker to bypass perimeter defenses and endpoint detection systems, and threat actors target these users through code repositories, SEO poisoning, and other trusted channels.

180+

Self-replication is back: In a throwback to the early 2000s, a self-replicating malware campaign compromised over 180 npm packages, many of which were widely used in developer environments

As we noted in **Initial Access Trends**, threat actors are increasingly abusing trusted platforms and services as a means to gain initial access into IT environments. In particular, the second half of 2025 saw a significant number of such campaigns, with many targeting sites and services used by developers and IT professionals.

These campaigns are key drivers behind an emerging trend in which threat actors reach particular demographic targets by abusing platforms those users inherently trust. This approach can be an effective way to bypass traditional perimeter defenses and endpoint detection systems.

Platform abuse with GPUGate

The GPUGate campaign, uncovered in September 2025, showcased a novel malware delivery method using GitHub Desktop installers embedded with GPU-gated decryption routines. This ensured the malware only decrypted on systems with real GPUs to target high-value users like developers, gamers, and crypto miners, while simultaneously evading sandbox analysis (see **this Arctic Wolf blog** for full details).

Oyster/Broomstick SEO poisoning

The **Oyster/Broomstick** campaign used SEO poisoning and trojanized IT tools like PuTTY and WinSCP to deliver backdoors. These tools were hosted on malicious domains and promoted via sponsored search ads.

After landing on the malicious domain, the user may download and execute a trojanized installer. Upon execution, the Oyster/Broomstick backdoor is installed, establishing persistence via scheduled tasks and DLL registration routines.

Compromise of 180+ npm packages

Arctic Wolf also tracked a **wormable malware campaign** that compromised over 180 npm packages, many of which were widely used in developer environments.

The malware harvested credentials and cloud tokens, then exfiltrated them via public GitHub repositories. Harkening back to the days of SQL Slammer, MyDoom, Zotob, and other worms, this malware propagated by injecting itself into additional packages, thereby creating a self-replicating supply chain compromise across the npm ecosystem.

Ransomware Impact Analysis

HIGHLIGHTS

Manufacturers beware: The manufacturing sector suffered, by far, the highest number of successful ransomware attacks (nearly 70% more than the second-place sector, construction).

Cybercriminals follow the money: The top six countries represented on leak sites are all G7 nations, and are joined by other economic powers like Brazil, Spain, Australia, and India. Suspiciously absent? Russia and the CIS nations.

Provided the findings are taken with a dusting of salt (some groups have been known to exaggerate their successes), studying leak sites can provide a big-picture view of the activity of ransomware groups.

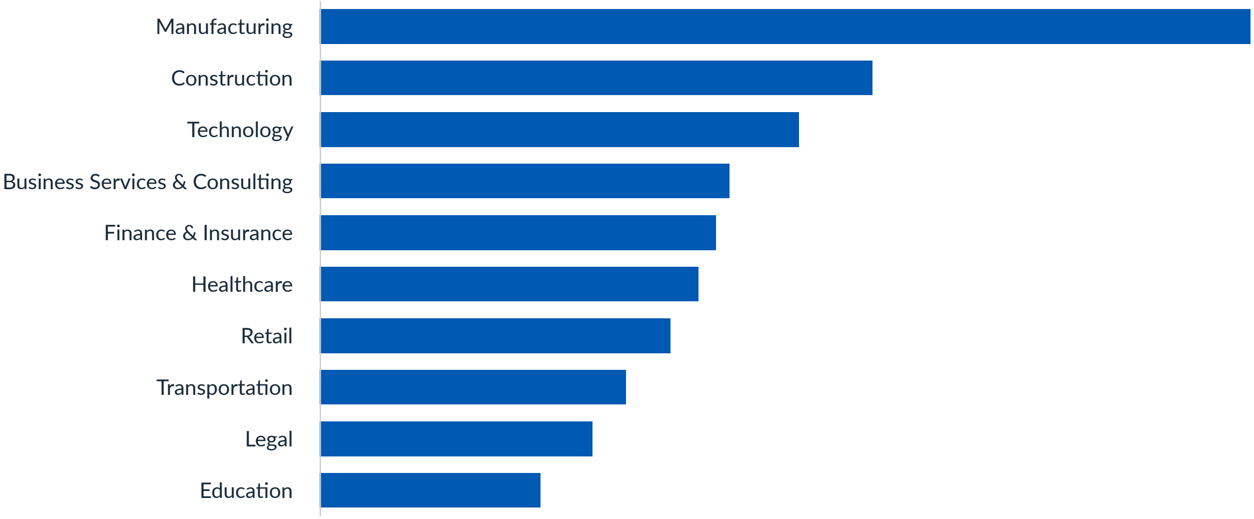
Manufacturing and construction companies are under siege

Looking at individual sectors, we can see that ransomware groups continue to set their sights firmly on manufacturers, with the **manufacturing** sector as a whole standing out with, by far, the highest victim count during this reporting period.

Manufacturers are historically a favored target of threat actors, as any operational disruption threatens to derail production, risk contractual penalties, create backlogs, and damage the manufacturer's reputation. Plus, manufacturers often hold valuable information about industrial processes and customers, making them similarly susceptible to the data extortion aspect of modern ransomware.

Ransomware Victims by Sector

(sourced from leak sites)



Like manufacturers, **construction** companies are especially susceptible to the pressures of downtime. Plus, while manufacturers have been under focused threat for years now (giving them time to boost their defenses) it may take some time for the construction sector to collectively recognize the increased threat. Should they be slow to take action, the lesson of the manufacturing sector is clear: Ransomware operators will take note, and they will relentlessly attack.

Despite a series of high-profile attacks targeting major retailers (perhaps, most notably **Marks and Spencer** in the U.K.), the **retail** sector placed seventh in terms of victim count.

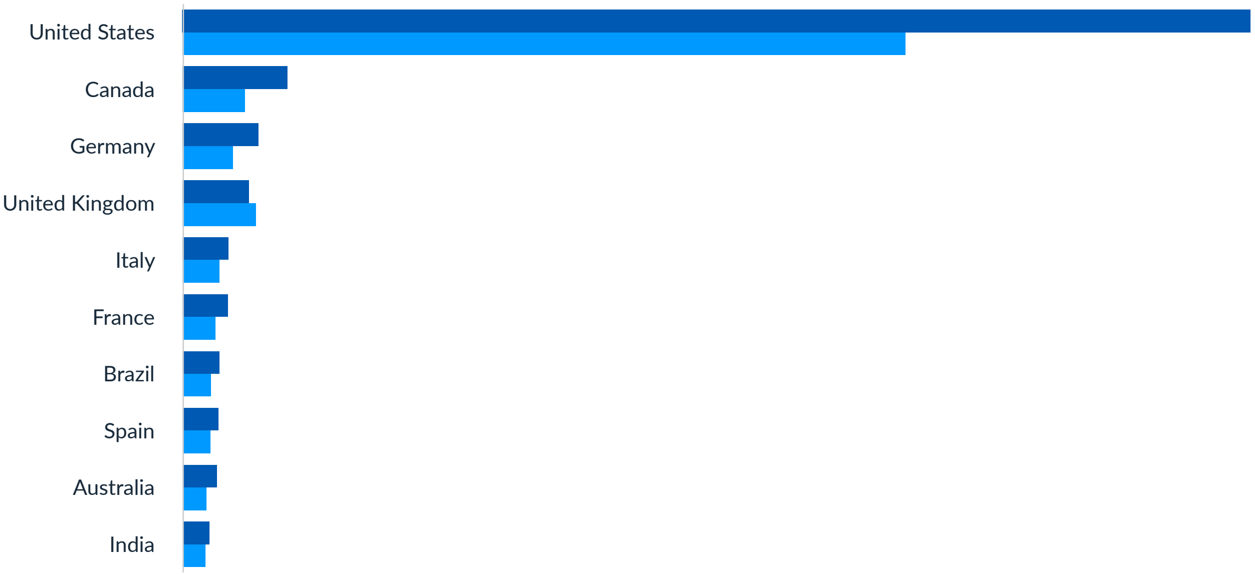
Healthcare organizations are highly sensitive and very visible targets. Some ransomware groups regard attacking healthcare organizations as not worth the potential backlash, as public outcry and law enforcement responses can be fierce. For others, perhaps somewhat protected from the reach of international law enforcement, the visibility and sensitivity make for the perfect targets, as successful attacks garner headlines and increase brand recognition.

G7 nations continue to be targeted

Shifting our attention to the countries with the highest number of victims, we can see that this reporting period's list looks very similar to last year's: G7 members continue to occupy the top six spots on the list, with Japan the only G7 member absent.

Ransomware Victims by Country

(sourced from leak sites)



The **United States** continued to have, by far, the most representation, accounting for nearly 70% of the attacks on this top 10 list and very slightly outpacing the 42.5% growth of the rest of the countries on the list year-over-year.

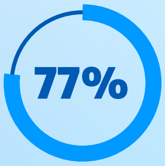
Canada, **Germany**, and **Australia** also saw their proportional representation grow year-over-year, with Canada suffering the largest increase.

Despite several extraordinarily high-profile attacks (e.g., **Jaguar Land Rover**, **Marks and Spencer**), the **United Kingdom** was the only country on this list to see a decline in raw victim count, which means the number of victims posted on leak sites. Coupled with the higher numbers for Canada and Germany, this drop was sufficient to see the U.K. fall from second to fourth.

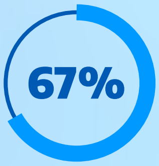
Ransomware Economics & Extortion Trends

HIGHLIGHTS

For the first time in the history of our threat report, the median initial ransom demand declined: After steadily growing for years and then staying flat for two reporting periods, the median initial ransom demand (across all industries) fell by 20% to $414,000 (USD), perhaps in an attempt to increase the overall rate of payouts.



Professional incident response should be a no-brainer: In 77% of ransomware IR cases handled by Arctic Wolf, the impacted organization elected not to pay a ransom.



Expertise in ransomware tactics and negotiation is invaluable: In the 23% of ransomware IR cases in which the victim made the business decision to pay a ransom, Arctic Wolf's IR team secured an average reduction (compared to the initial demand) of 67%.

From an outside perspective, ransomware incidents can seem like fairly simple transactions: An attacker severely disrupts an organization and threatens to publicly release confidential data, the attacker states a ransom amount, the organization pays to expedite recovery or refuses to pay.

Behind the scenes, though, things are considerably more complicated. For example:

- Across all the ransomware IR cases to which Arctic Wolf responded during this reporting period, cybercriminals demanded a total of $302,155,615 in ransoms.
- Ultimately, by following a process similar to the generalized one shown below, the victimized organizations collectively paid a total of $16,481,559.

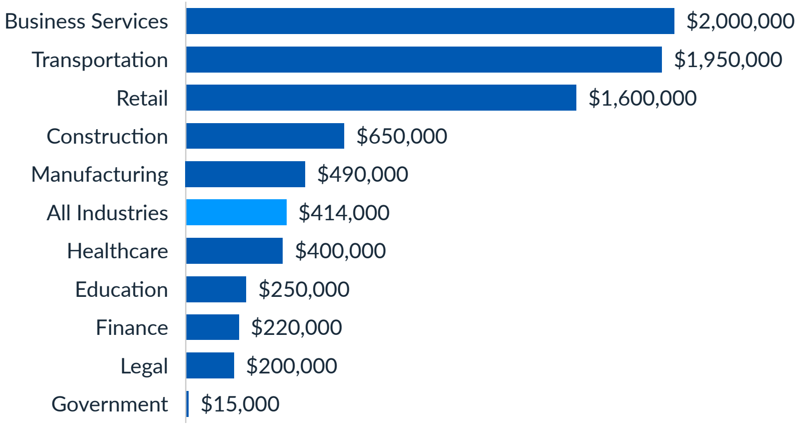
While this is more than the zero dollars we would all like to see, it still represents a reduction of 94.6%.

For this reporting period, the median initial ransom demand for Arctic Wolf IR cases was $414,000. This figure represents a noteworthy decrease, as the initial demand had stayed at $600,000 for the last two reports.

We speculate that this overall decline is an attempt to increase payout rates, in response to improved organizational resilience and recognition that spectacularly high ransom demands may cause victims to not even consider payment as an option.

Median Initial Ransom Demand by Industry

(sourced from Arctic Wolf IR cases)



Success emboldens ransomware groups to increase their demands

The disciplined approach to ransoms described above reflects a shift from opportunistic attacks to more calculated operations, where ransom pricing is part of a broader strategy to maximize return on investment.

However, at the same time as the median initial ransom demand has dropped, some threat actors have done the opposite.

When threat actors achieve success in disrupting business operations (especially when victims pay the ransom), they gain additional assurance that future victims will also pay quickly to restore functionality. This success amplifies their perceived bargaining power, allowing them to increase initial ransom demands.

Moreover, public reporting of high ransom payouts exerts a 'rising-tide' effect that further fuels this escalation. Threat actors monitor headlines and regulatory disclosures closely, and when they see peers successfully extorting large sums, it emboldens them to raise their own demands. This creates a feedback loop where each high-profile payment sets a new benchmark.

For example, in **the indictment related to the Scattered Spider threat actor group** (U.S. Department of Justice, 2023), one victim paid $26 million and another paid $36.2 million. These astronomical sums almost certainly influenced the expectations of other actors in the ecosystem. These figures not only 'validate' the profitability of ransomware but also serve as aspirational targets for other groups seeking similar returns.

Arctic Wolf Incident Response observed this pattern with a prolific threat actor group. Historically, this group's initial average demand was close to $1,000,000, with seven-figure demands occurring every few months. While the overall mean demand has remained the same, we observed a marked increase in the frequency of seven-figure demands, with 13 such demands in a roughly four-month period.

To pay or not to pay: the negotiation phase

At Arctic Wolf, our position aligns with the general recommendations of the FBI, other law enforcement agencies, and governments: If possible, ransom demands should not be paid, as starving the perpetrators is the only way we can collectively hope to eliminate these attacks.

Nevertheless, the decision on whether to pay is one that must be made by stakeholders within the victim organization once presented with all possible information and options.

Calling in the experts

Engaging with a ransomware actor is best left to the experts, who generally have much, much more experience with doing so than any in-house personnel. A professional ransomware negotiator will work on the victim's behalf to communicate with the threat actor, to better understand the situation, and to try to reduce the amount demanded.

Employing the services of a professional IR organization can have many benefits, including:

Preventing further problems: In some circumstances, the threat actor demanding a payment could be a sanctioned entity or have ties to a terrorist organization. In these cases, any payment to such a group constitutes a crime on behalf of the payee.

Insight into the situation and explanation of what options are available: This can include if a payment is even necessary (sometimes decryption keys are already known) and the reputation of the threat actor. Professional negotiators can sometimes get information from the threat actors (e.g., what data was stolen) that can lead to better-informed decisions.

Smaller payments: While every ransomware affiliate and group is different, professionals know who is more likely to lower their demands, and by how much.

In 77% of ransomware incidents, Arctic Wolf clients did not pay a ransom

The best outcome for an organization victimized by ransomware is simply to not pay the ransom. While occasionally this is due to a matter of principle or the illegality of paying a ransom, the ideal reason for not paying is because any disrupted operations can be restored without 'aid' from the cybercriminals responsible for inflicting it.

Indeed, in 77% of the Arctic Wolf ransomware IR cases, our clients elected not to pay. Typically, this outcome is the result of:

- Effective containment that limited the scope of the attack
- Robust backup and restoration capabilities that allowed the organization to recover quickly and effectively
- An assumption that cybercriminals cannot be trusted to delete sensitive data they stole, even if a ransom was paid (more on this in a moment)

Occasionally, our IR team might know of a flaw in the encryption algorithm that renders decryption without a key possible or already has decryption keys from prior incidents. Plus, some law enforcement actions recover decryption keys and make them available to organizations that reach out.

> "The strongest negotiating position is resilience. When recovery does not depend on an attacker, the economics of extortion shift in favor of the defender."
>
> ISMAEL VALENZUELA, VP OF LABS, THREAT INTELLIGENCE AT ARCTIC WOLF

When ransoms ultimately were paid, Arctic Wolf negotiators secured an aggregate 67% reduction

It's important to recognize that the worst outcome for a ransomware threat actor is not getting paid. Excessively high demands or outright refusals to negotiate increase the likelihood of that outcome, which gives attackers strong incentives to engage in negotiations.

Many victims, particularly those responding without professional support, may not realize that the initial ransom demand is typically a starting point rather than a fixed price, and that negotiations often result in significantly lower demands.

As attackers adopt more aggressive extortion tactics, including employee harassment and outreach to business partners or executives' families, negotiations are best handled by experienced professionals who have encountered these tactics before.

In Arctic Wolf ransomware IR cases conducted during this reporting period, only 23% of organizations ultimately chose to pay a ransom. In those cases, Arctic Wolf negotiators secured an average reduction of 67% from the initial demand, representing meaningful savings for larger organizations and, for smaller ones, potentially the difference between recovery and insolvency.

2026 Predictions

The predictions below highlight areas of concern, but please note that they're not presented in a ranked or hierarchical order. We suggest determining the priority of each topic based on the specifics of your environment.

Ransomware will remain the most significant threat, but data incidents may overtake BEC

As we noted in earlier in this report, ransomware continues to be the leading cause of our IR cases.

Unfortunately, we see no reason why this will change in the short term. However, we do expect to see:

- **Longer negotiation cycles** as attackers dig in their heels, knowing that time is on their side; some may even largely automate these exchanges, leveraging LLMs instructed to be tough negotiators
- **Larger initial ransom demands** as threat actors push for higher payouts or seek to 'anchor' stronger positions to negotiate from
- **More public shaming** as groups leverage the fear caused by high-profile incidents (e.g., Jaguar Land Rover) to apply pressure and deter others from nonpayment

We also anticipate that more ransomware groups and affiliates, and perhaps some emerging threat actors, will favor data theft and extortion over system encryption. Even a small shift in this direction will see data incidents overtake business email compromise in our IR case catalog.

Social engineers will increasingly incorporate real-time voice and video manipulation

For as long as there have been security measures, there have been people skilled at bypassing them by manipulating and deceiving others. To pick just two examples from the last year, the groups designated UNC6040 (aka ShinyHunters) and UNC3944 (aka Scattered Spider or Octo Tempest) both enjoyed tremendous success employing complex pretexting and spear phishing.

As security technologies — especially identity controls and AI capabilities — continue to improve, we expect to see threat actors doubling down on AI-powered:

- **Email phishing,** backed by convincing lures leveraging open-source intelligence (OSINT)
- **Voice phishing (vishing),** with attackers manipulating their voices in real time to masquerade as executives and other positions of influence
- **Video deepfakes,** using real-time face and voice swapping

While we don't expect vishing and video deepfakes to be present in the bulk of social engineering cases, attackers have shown time and again their willingness to adopt new technologies and to refine their approaches to make the best use of new tools.

For threat actors, AI will become less of a novelty tool and more of an everyday utility

Already, researchers and threat actors have demonstrated some success weaponizing AI to gain initial access, but this is only the beginning.

In 2026, we expect that threat actors will:

- **Introduce specialty AI functions and services,** further extending the cybercrime-as-a-service ecosystem
- **Generate malicious code "on the fly,"** such that no two samples have the same signature
- **Experiment with AI's application throughout the attack chain,** extending beyond initial access

Information warfare will reach new heights

Two related side effects of our information age are that global, regional, national, and even local politics have never before been so fractious or so vulnerable to manipulation.

A quick look ahead shows that 2026 will deliver plenty of opportunities for bad actors, including:

- General elections in Brazil, Quebec (Canada), Sweden, and New Zealand
- Midterm elections in the United States
- Legislative elections in Israel, India, and Russia
- Other types of elections in the United Kingdom, Germany, Taiwan, and more

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

Threat actors will take advantage of major global events

For threat actors, a pop-culture subject or newsworthy phenomenon that everyone is talking about provides both opportunity and efficiency.

And 2026 has much on offer, including:

- The elections noted above
- The 2026 FIFA World Cup, which is being co-hosted by the United States, Canada, and Mexico
- The 2026 Winter Olympics in Milan, Italy
- The 2026 Commonwealth Games in Glasgow, Scotland

We expect to see experimentation with social engineering lures leveraging these events, plus the usual plethora of ticket scams, malware delivery infrastructure masquerading as cheap streaming services, and dodgy VPN services (e.g., to bypass streaming restrictions on work devices).

It's also entirely possible that threat actors may seek jackpot-level payouts by attacking and disrupting organizations or services that are critical to the success of these very public events.

12 Recommendations for 2026

As we've seen, the threat landscape continued to evolve during the timeline of this report, with attackers leveraging both traditional and modern techniques across hybrid environments. Consequently, these 12 recommendations are designed to help organizations reduce risk and improve resilience, while retaining the ability to adapt in response to ever-changing threats.

1 Minimize internet exposure

Organizational changes due to growth, merger and acquisition activity, transformation initiatives, or other motivations can cause network perimeters to become cluttered with outdated or redundant systems, creating easy entry points for attackers.

- **Decommission unused systems:** Remove temporary, duplicate, or end-of-life infrastructure
- **Disable unnecessary services:** Turn off legacy protocols, unused VPN types, and features not essential to operations

2 Prioritize patching in general, and vulnerability management specifically

As we've seen, edge devices such as firewalls and VPNs are high-value targets due to their privileged access and limited visibility (e.g., gaps in monitoring, opaque proprietary systems, excessive noise).

- **Patch known exploited vulnerabilities:** Focus on flaws actively used in attacks, as most already have fixes available
- **Maintain a complete asset inventory:** Visibility is key to prioritizing patching and reducing risk
- **Secure management interfaces:** Ensure they are isolated from public access and properly configured
- **Subscribe to advisories:** Use vendor updates and CISA's Known Exploited Vulnerabilities (KEV) catalog to stay ahead of emerging threats
- **Reset credentials after patching:** Rotate passwords and keys if a vulnerability may have exposed them
- **Keep firmware updated:** Firmware updates often include critical security improvements not covered by standard patches

3 Harden infrastructure

Strengthen infrastructure to increase resilience and improve defense-in-depth.

- **Restrict admin access:** Block internet-facing management interfaces and limit access to trusted internal networks
- **Apply IP-based filtering:** Allow access only from known safe regions and IP ranges
- **Filter botnet traffic:** Use vendor-provided rules to block known, malicious sources
- **Enforce strong encryption:** Use secure standards like AES-256 and disable outdated cipher suites

4 Strengthen authentication controls

Credential-based attacks remain a favorite tactic of threat actors, but correctly implementing strong authentication controls reduces the risk of unauthorized access.

- **Centralize authentication:** Use SSO and SAML to manage access through trusted identity providers (IdPs)
- **Audit VPN accounts:** Regularly review user lists and remove access for inactive users and third parties
- **Require strong multi-factor authentication (MFA):** Use phishing-resistant methods (e.g., hardware tokens) backed by modern WebAuthn standards
- **Promote credential hygiene:** Enforce strong passwords (i.e., long and not guessable), password rotation, and password manager usage

5 Monitor and log strategically

Visibility into edge devices and user activity is essential for detecting and responding to threats.

- **Log as much as is possible (or practical):** If you're working with a solution or solution provider that can accommodate high data volume without incurring/imposing punitive costs, then log everything — otherwise, prioritize logs that provide visibility not available from other systems
- **Centralize log collection:** Send logs to external systems to prevent tampering and to support investigations
- **Deploy behavioral analytics:** Detect lateral movement and persistence techniques that bypass traditional controls

6 Promote safe software practices

User behavior can introduce risk, especially when downloading tools from unverified sources (or simply by being tricked).

- **Educate users:** Raise awareness about the risks of downloading software from search engines or unofficial sites, and teach users to be vigilant of watering hole-style attacks (e.g., malvertising, typo squatting)
- **Enforce acquisition policies:** Require software to be sourced through approved internal or vendor channels

7 Monitor trusted platform abuse

Attackers increasingly use legitimate platforms to distribute malicious content or to hide malicious activity.

- **Watch for misuse of platforms:** Monitor traffic and usage patterns involving GitHub, Google Ads, and IT tool repositories
- **Understand your own dependencies:** A supply chain compromise might affect your organization via a dependency chain

8 Manage third-party risk

Third-party vendors and service providers often have access to sensitive systems and data, making them attractive targets.

- **Assess vendor security posture:** Include security requirements in contracts and conduct regular reviews
- **Limit and monitor access:** Apply least-privilege access principles and segment external connections to reduce risk

9 Implement network segmentation and zero trust principles

Flat networks make it easier for attackers to move laterally once inside.

- **Segment critical systems:** Isolate sensitive environments from general user networks
- **Adopt zero trust:** continuously verify access requests and monitor trust levels

10 Prepare for incident response and recovery

Being prepared for incidents reduces impact and recovery time.

- **Maintain and test IR plans:** Ensure playbooks are current and exercised regularly
- **Protect and test backups:** Ensure backups are secure, reliable, and recoverable
- **Define communication protocols:** Include internal teams, legal counsel, and external stakeholders in planning

11 Leverage threat intelligence

Timely, relevant intelligence helps security teams anticipate and respond to threats more effectively.

- **Operationalize threat intelligence:** Integrate feeds into SIEM, SOAR, and detection workflows
- **Use contextual enrichment:** Apply intelligence to prioritize alerts and guide investigations
- **Collaborate with trusted sources:** Participate in Information Sharing and Analysis Centers (ISACs) or similar industry-specific sharing groups

12 Continually foster a security-aware culture

Technology alone isn't enough: people play a critical role in defense.

- **Run regular awareness campaigns:** Focus on phishing, social engineering, and secure behaviors
- **Tailor training to roles:** Provide specialized guidance for high-risk groups like IT admins or finance teams
- **Encourage reporting:** Make it easy and safe for employees to report suspicious activity

Conclusion

Most threat actor groups are financially motivated operations, and changing their ROI calculations is essential for protecting your organization.

One problem we encounter when preparing our annual threat report is trying to avoid restating the phrase "threat actors continue…" in one form or another dozens of times.

The reason for this problem? Threat actors continue to stick with what works. Finding vulnerabilities, crafting exploits, and weaponizing them at production scale is time-consuming, expert-driven, and expensive work. That means it's much cheaper to stick with tried-and-true TTPs. Only when these offer scarce returns will a group be motivated to build or buy some hot new exploit or develop a new attack chain.

For cyber defenders, this means that protecting against known TTPs (including CVEs that have been exploited for literally years) can make your organization a much more challenging target.

Nevertheless, preventative measures are what engineers call "necessary but insufficient."

Yes, defenders must build and maintain a foundation of fundamentals and continually adapt and evolve their security posture such that, over time, those novel defenses are integrated into the new normal.

But defenders must also augment these proactive measures with:

- Reactive capabilities designed to quickly and effectively detect and respond to attacks that break through outer defenses.
- Robust and reliable backup and restoration capabilities to enable fast and full recovery (and to help avoid paying ransoms).
- Risk transfer measures, including leveraging warranties and insurance, in response to the reality that incidents do happen (even to well-prepared organizations).

It can all seem overwhelming — but you're not alone.

An entire cybersecurity community stands with you and is committed to sharing and learning, lifting and helping, and working together to withstand attacks and intrusions.

If you'd like to augment your internal capabilities with external expertise, we're ready for you to join the Pack.

How Arctic Wolf Can Help

The outcomes you need, the convenience you'll love.

When we speak with organizations around the world, we're often asked for three things:

1. **An effective cybersecurity solution that will provide end-to-end protection against cyber threats, that will be easy to manage, and that will integrate with the security products they've already deployed.**
2. **A way to financially offset the remaining risk.**
3. **Expert assistance to help evolve their security posture over time, aligned with their specific priorities and operating context.**

In response, we've created the Arctic Wolf Security Operations Bundles.

These bundles provide the full suite of technology, security expertise, and risk transfer options to help you End Cyber Risk®.

Whether it's proactive security offerings like security awareness training, vulnerability scanning, and incident readiness planning; or reactive detection, remediation, and active response capabilities to minimize the severity of an incident, the Security Operations Bundles provide full coverage across all your attack surfaces.

Best of all, some of the remaining risk may be financially transferred to Arctic Wolf through our industry-leading Security Operations Warranty. With up to $3 million (USD) in financial coverage and the ability to fund your cyber insurance deductible, your out-of-pocket costs after a severe cyber attack may be mitigated.

If you aren't getting the outcomes you're looking for from the solutions you have today — or if you just need some support in putting your existing investments to work — we would love to help.

For more information about Arctic Wolf, visit **arcticwolf.com/uk**

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Built on open XDR architecture, the Arctic Wolf Aurora™ Platform operates at a massive scale and combines the power of artificial intelligence with world-class security experts to provide 24x7 monitoring, detection, response, and risk management. We make security work.

Arctic Wolf and its employees are not licensed producers and therefore are not engaging in the sale, solicitation or negotiation of insurance and are NOT offering advice regarding insurance terms, conditions, premium rates or claims. Customers interested in purchasing Cyber Insurance coverage should consult with an appropriately licensed insurance broker.

Informational Use Only. This content is for general information and does not constitute legal, accounting, or other professional advice.

No Warranty/No Reliance. It is provided "as is" without warranties of any kind; do not place undue reliance on a single metric or example.

Methodology & Scope. Statistics reflect Arctic Wolf engagements and telemetry for the period [November 1, 2024–November 1, 2025], may be influenced by case mix (e.g., insurer/counsel referrals), and may differ from broader market experience. Sanctions/Payments. Any engagement with threat actors may implicate sanctions or other laws. Arctic Wolf does not advise paying ransoms; decisions rest with the customer in consultation with counsel and relevant authorities.

The predictions and outlooks in this publication reflect Arctic Wolf's observations and analyst judgment as of January 2026. They are inherently uncertain and involve assumptions about attacker behavior, technology adoption, regulation, and macro conditions. They are not guarantees of future events, may change without notice, and we undertake no obligation to update them. Readers should not rely on any single prediction and should consider alternative scenarios and local legal constraints.

AW_RP_2026 THREAT REPORT_EMEA_0226