ARCTIC WOLF

Security Operations Report

2025

Table of Contents

Foreword

CYBERSECURITY IS A WHIRLWIND OF CONSTANT CHANGE.

Practitioners understand that no two days are the same, and each brings new insights and lessons. It's also true for us at Arctic Wolf, but on an exponential level: the scale at which we operate and the vast amount of security telemetry we see grant us unique insight into the current state of security operations, and what's coming next.

Entering the third year of the Arctic Wolf Security Operations Report, our annual review highlights that cyber threats are not just persistent, they are steadily getting worse. Despite record-breaking budgets and continued innovation, cyber losses are not merely continuing, they are accelerating.

This concern is echoed in the FBI's 2024 Internet Crime Report, which reveals a staggering **28%** increase in reported losses year-over-year, reaching **$16 billion (USD)**, up from **$12.5 billion** the year prior. This increase is ultimately a flashing siren, directing our attention towards the disconnect between investment and security outcomes.

Our analysis suggests that the gap between effort and effectiveness is driven by compounding operational failures, which history has proven cannot be solved with more money and tools. Instead, we must address the core factors driving this "effectiveness gap," including a focus on security checklists over security operations, legacy platforms ill-equipped for modern IT environments, the one-size-fits-all models that ignore unique organizational context, and legacy attitudes that presume outdated adversarial tactics rather than the adaptive, autonomous techniques reshaping today's threat landscape.

Identifying the problem is only the first step. That is why this has been a year of evolution for Arctic Wolf. Our introduction of Alpha AI, Arctic Wolf's suite of unique, cutting-edge machine learning and artificial intelligence technologies, is designed to improve security operations efficacy by increasing speed, accuracy, and efficiency. This is supported by investments in threat intelligence, a refined Security Journey® process, and a new suite of endpoint technologies — all while reaffirming our commitment to a vendor-neutral platform that maximizes a customer's existing investments. It is through this evolution that we are prepared to face the next generation of cyber threats.

This year's report shows how these threats also continue to evolve in both scale and sophistication. Adversaries are taking advantage of "off-business hours" to launch attacks as **51%** of all alerts are now generated **outside of traditional working hours,** underscoring how non-negotiable 24x7 monitoring is. To combat this, many hope for a solution through increased investments in technology. As a result, we are ingesting more data from our customers, **now topping 330 trillion raw observations** during the 12-month period of this report and generating **one alert for every 138 million observations ingested**. This is a 38% increase from last year in the amount of observations required to generate one alert. Compounding this challenge, nearly one-sixth of weekly alert volume occurs on weekends — a time when many understaffed organizations are least prepared to respond.

Ultimately, this report offers more than reflection — it is a roadmap. Whether you are a security leader, practitioner, or executive, our goal is to help you better understand the evolving threat landscape, benchmark your operations, and make informed decisions as we work together to end cyber risk®.

LISA TETRAULT
Senior Vice President, Security Services, Arctic Wolf

Key Takeaways

Here are some of the top takeaways included and explained within this report.

24x7 MONITORING IS NOT OPTIONAL, IT'S CRITICAL

51% of alerts are generated outside of traditional business hours, and nearly one-sixth of each week's total alert volume occurs on the weekends.*

330 TRILLION

THREAT SIGNALS ARE BURIED IN MOUNTAINS OF NOISE

From **330 trillion raw observations**, Arctic Wolf generated one alert for every 138 million. This staggering ratio highlights the difficulty of spotting real threats hidden within vast volumes of benign activity.

860,000+

AI SUPERCHARGES HUMANS — IT DOESN'T REPLACE THEM

Alpha AI eliminated the need **for 860,000 + manual ticket reviews**.

NOT EVERY ALERT IS A THREAT

71% of all ingested alerts are suppressed by applying customer context and threat intelligence to identify expected or benign activity.

ATTACKERS TARGET THE VULNERABLE

Education, healthcare, and manufacturing top the charts for attack volume. Shared traits: outdated infrastructure, high-value data, and low tolerance for downtime.

**Data was normalized by region and local time zone*

Key Takeaways (continued)

PREVENTION TECH WORKS — IF YOU USE IT RIGHT

Aurora™ Endpoint Defense prevented **84,000+ unique threats** from executing within customer environments in just the first three months of its launch.

37% ▼

FAST RESPONSE = LOWER RISK

Our mean time to ticket (MTTT) is 7 minutes and 5 seconds, a **37% decrease** from 11 minutes and 19 seconds two years ago, enabling faster threat validation and response.

EARLY DETECTION IS KEY

Of 9,000+ security investigations, only 2% were confirmed threats. Arctic Wolf's SOC excels at early detection — most investigations relate to initial access attempts, with very few escalating to confirmed incidents.

33 BILLION

VISIBILITY IS EVERYTHING

The average customer generates **33 billion observations annually**. Without full-spectrum telemetry, threats stay hidden.

72% OF ACTIVE RESPONSE ACTIONS WERE IDENTITY BASED

This ratio highlights the critical role of managing compromised credentials to stop threats early and prevent breaches.

Data Sources

> While portions of this report may cite other Arctic Wolf publications and third-party sources for context or clarity, the majority of facts, figures, and statistics presented here are based upon the nearly 330 trillion analyzed observations made between the period covering May 1, 2024, through April 30, 2025, identified in our customer base of 10,000+ organizations in 100+ countries.

To obtain the full visibility necessary to accurately detect and respond to potential threats, these observations are sourced from a broad range of attack surface telemetry including endpoint, network, cloud, log sources, behaviors, and third-party alerts. By ingesting telemetry from a balanced set of attack surfaces into our vendor-neutral platform, we get the full picture of what's happening in each customer's environment.

330 Trillion
ANALYZED OBSERVATIONS

10,000+
ORGANIZATIONS

100+
COUNTRIES

Detecting Threats Across the Entire Attack Surface

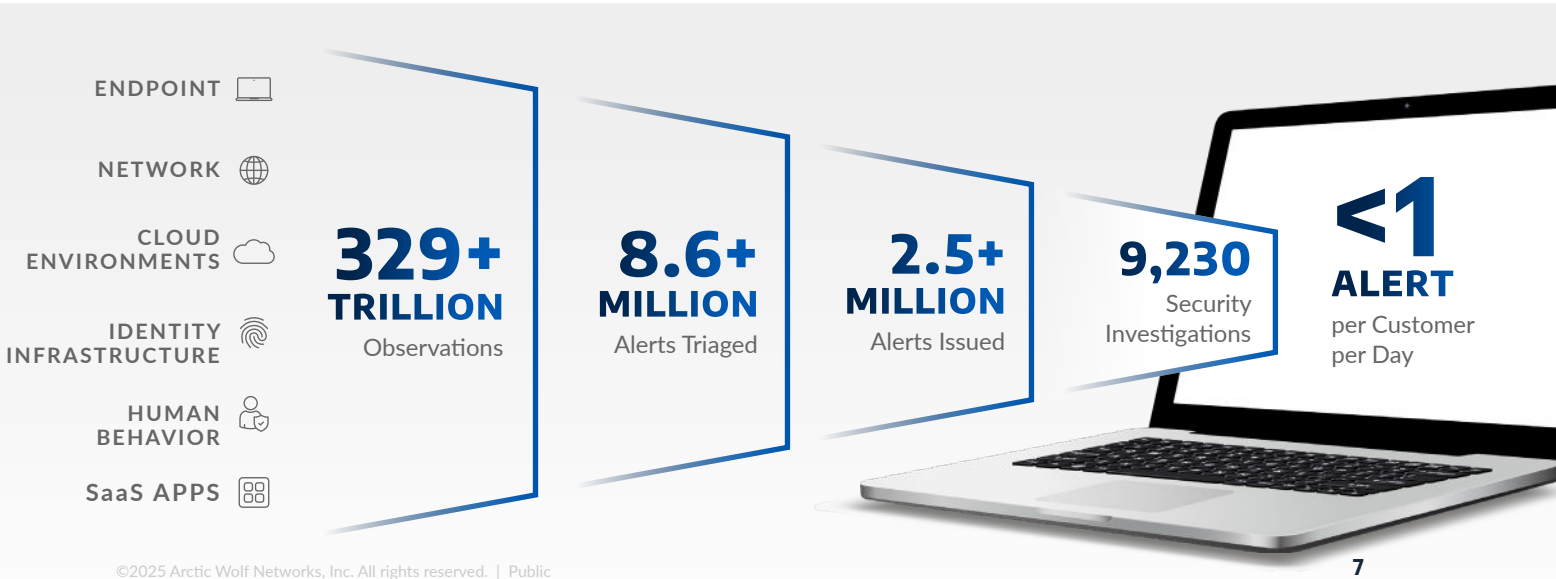
KEY TAKEAWAYS

- For the 12-month period covered by this report, the **Arctic Wolf Security Operations Cloud ingested 329+ Trillion raw data observations** — an increase of **more than 30% over the prior period** — from more than 10,000 unique customers.
- The amount of observable data produced by an organization that is potentially obscuring threat activity can easily become overwhelming as evident by our data showing **the average customer's environment produces almost 33 billion observations annually.**
- Endpoint prevention, when implemented and managed efficiently, can greatly enhance your security posture, considering that **Aurora Endpoint Defense identified and blocked over 84,000 unique threats from executing within customer environments** in just the first three months of its launch.

As cyber threats continue to grow in volume and sophistication, organizations face increasing pressure to detect malicious activity as early as possible. In this landscape, full visibility across the IT environment is not just helpful but essential. Even minor visibility gaps can result in delayed or missed detections. Early detection, however, hinges on correlating telemetry from diverse sources to uncover hidden patterns. Ultimately this results in the need for a platform that can ingest and analyze an ever-increasing amount of security relevant telemetry.

For many organizations however, achieving the level of visibility necessary for accurate threat detection may seem like a daunting task. The amount of observable data produced by an organization can easily feel overwhelming. Our data shows that the average customer environment **generates nearly 33 billion observations each year**. Fortunately, a systematic approach has proven successful in making security operations more accessible to organizations of any size.

Our recommendation is to start with a foundation built on visibility: work to ensure your organization collects telemetry across endpoints, networks, cloud environments, identity technology, human activity, and applications.



Introducing Aurora™ Endpoint Defense

In February 2025, Arctic Wolf was excited to complete the acquisition of BlackBerry Cylance, a top-tier provider of endpoint security technology.

Now updated and reintroduced to the market as Aurora Endpoint Defense, this next-generation solution expands Arctic Wolf's visibility and response capabilities while providing customers with more choice as they look to harden their security postures.

In the three-month period since the release of Aurora Endpoint Defense, this powerful solution has:

- **Prevented 750,928 attacks from executing at the endpoint level**
- **Identified and stopped 84,587 unique malicious threats**

Analyzing Telemetry to Uncover Potential Threats

KEY TAKEAWAYS

- **Threat signals are hidden by a tremendous volume of noise:** on average, Arctic Wolf produces one alert for every 138 million raw data observations.
- **Threats do not have weekends off: nearly one-sixth of a week's total alert volume is generated on weekends.** This highlights a threat being equally as likely on a weekend as during the week.
- **24x7 threat detection is critical: 51% of alerts were generated outside of the traditional business hours,** when internal IT teams may not be available and response capabilities may be limited.

The prerequisite necessary for identifying and responding to threats without exhausting security teams with false alarms is to simultaneously achieve both:

- **A low false-negative rate, to ensure that few threat signals go unnoticed**
- **A high true-positive rate, to avoid contributing to alert fatigue**

To do so, the Arctic Wolf Aurora Platform powered by Alpha AI parses, enriches, and analyzes the telemetry stream to raise the signal-to-noise ratio and to help isolate potential security events, thereby producing accurate, context-driven alerts.

For the 12-month period covered by this report, **the Aurora Platform generated more than 8.6 million alerts** from telemetry across our full customer base. It should be noted at this point that these alerts are not simply being forwarded to the customer to transfer responsibility. Instead, these alerts represent the platform escalating a potentially security relevant event to Arctic Wolf human analysts for review.

When we review this data further, we find that this averages to almost **860 raw alerts per customer annually**. Although this may seem like a relatively manageable rate of alerts, we must remind ourselves of

the steps that we're taking to achieve this reduced number and the amount of ingested data analyzed to detect these events.

Highlighting how threat signals are often hidden within a tremendous volume of observational data, **one alert was generated for every 138 million observations ingested.** While this ratio may initially suggest that most of this data is "noise," our review reveals that alerts often stem from broad and unique signals. This emphasizes the importance of full visibility to capture these rare but critical indicators.

Threat Intelligence Spotlight

Infostealer Campaign Serves Fake CAPTCHAS from Compromised Auto Dealer Websites

Overview: On March 11, 2025, the Arctic Wolf SOC and Threat Intelligence Team identified a suspicious trend of more than 20 cases of malicious PowerShell execution affecting customers across all verticals. Upon investigation, a common root cause stemmed from victims browsing compromised auto dealership websites. These sites redirected to fake CAPTCHA sites with instructions for keyboard shortcuts design to execute malicious code, ultimately leading to malware infection and unauthorized access. This unusually blended "high tech/low tech" approach was found to be highly successful and required immediate response.

Initial Access: **Drive by Compromise:** A plugin/script for a popular full motion video player that is commonly used by automotive dealers was compromised via vulnerable extensible components installed on WordPress websites.

Execution: **User Execution**: Victim presented with a fake CAPTCHA page, instructing them to take steps towards malicious code execution.

- Users directed to execute malicious PowerShell commands through a series of keystroke combinations, which ultimately leads to SectopRAT or BaydenRAT malware (Remote Access Trojan) infection

Command and Control: **Non-Standard Port:** SectopRAT, a .NET RAT (Remote Access Trojan) with numerous capabilities with multiple stealth functions, including profiling victim systems, potentially stealing information such as browser and crypto-wallet data, and launching a hidden secondary desktop to control browser sessions.

Arctic Wolf Response

- Impacted customers were identified, verified, and proactively notified
- Analyst-led investigations documented several indicators of compromise (IOCs) where relevant intelligence was collected
- Arctic Wolf Tactical Threat Intelligence Team shared findings and IOCs with a lead emerging threats detection framework making findings available to security community

> *"The simplicity of the attack, leveraging built in system commands executed by the unsuspecting victims, is what made this deceptively unsophisticated campaign so dangerous."*

JON GRIMM
Tactical Threat Intelligence Analyst
Arctic Wolf

24x7 Vigilance Is Essential

Threat actors do not schedule their activities to coincide with their victims' working hours. In fact, some of the most notorious recent cyber attacks were meticulously planned to coincide with long weekends or holidays. Therefore, taking care to normalize data for each customer's local time, and presuming the traditional business hours of 8 a.m. to 5 p.m. and a Monday through Friday work week, our analysis further underscores the necessity of 24x7 vigilance.

During the 12-month period covered by this report:

- In total, **51% of alerts were generated outside of traditional business hours** (Figure 3).
- Each weekday (M-F) averages 17% of organizations' total weekly generated alerts, while the remaining 15% occur on weekends, resulting in **nearly one-sixth of alerts occur over the weekend** (Figure 2).

Weekly Alert Distribution by Day

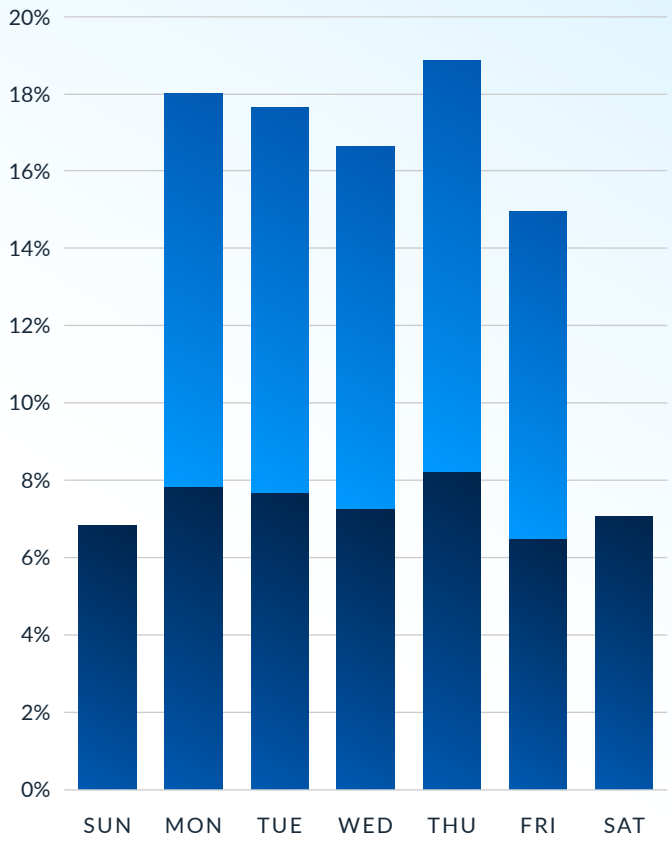


Figure 2 – The average weekday has roughly 2.5 times more alerts than the average weekend day, with the difference almost entirely attributable to benign activity — this added noise presents a major challenge unless sufficient false positive filtering is in place

Overall Alert Issuance

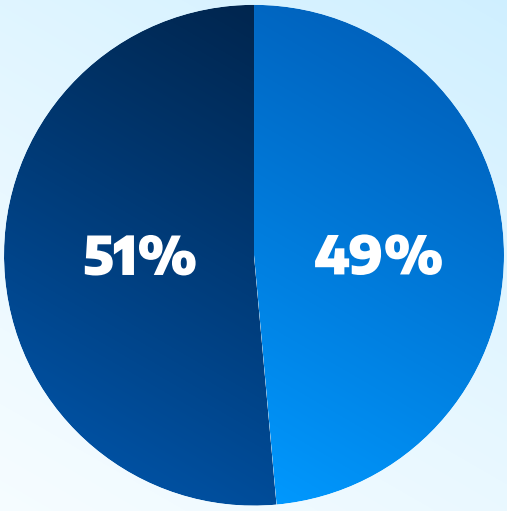
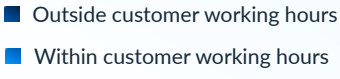


Figure 3 – Even within workdays, only 56% of alerts are generated during working hours, when a company is most likely to have security analysts available



Mega Event Spotlight: Fortinet "Console Chaos"

> Note: A "mega event" is any critical threat event that may affect a significant portion of our customer base. During a mega event, we execute a strategic runbook that combines active investigation and response with a high-touch approach that provides updates and actionable intelligence to our customers.

KEY TAKEAWAYS

- **Managed Detection and Response (MDR) and SecOps can bridge the patch gap:** It can take weeks or even months for vendors to patch vulnerabilities; in the interim, organizations need a way to detect and respond to exploitation.
- **Broad telemetry is growing in importance:** Console Chaos demonstrates the continued shift towards infrastructure exploitation, instead of malware deployment, making visibility across firewalls, VPNs, and DNS essential.
- **Alerts are not enough:** Only a human-led SOC with rapid response capabilities can manage modern breaches and reduce impact.
- **Custom threat intelligence accelerates response:** Arctic Wolf integrated Console Chaos IOCs into our active threat hunt playbooks, preventing similar exploitation even for zero days.

In the waning months of 2024, Arctic Wolf Labs observed an industry- and geography-agnostic campaign dubbed "Console Chaos," exploiting Fortinet FortiGate firewalls (FortiOS versions 7.0.0 through 7.0.16) with internet-exposed management interfaces.

The intrusion sequence followed four distinct phases:

01 **Vulnerability Scanning (Nov. 16–23):** Mass scans were launched to identify devices with exposed management interfaces.

02 **Reconnaissance (Nov. 22–27):** Attackers used spoofed IPs, including loopback and DNS resolver addresses, to initiate anomalous jsconsole logins.

03 **SSL VPN Configuration (Dec. 4–7):** Threat actors escalated privileges by creating super admin accounts, hijacking guest profiles, and enabling remote access via SSL VPN.

04 **Lateral Movement (Dec. 16–27):** Using DCSync techniques, attackers stole domain credentials and expanded their footprint across networks.

Fortinet released patches in mid-January 2025 (7.0.17+ for FortiOS, 7.2.13+ for FortiProxy), which meant that even in the best-case scenario (i.e., immediate patching) Fortinet customers were left exposed to Console Chaos until the patch was released.

Mega Event Spotlight: Fortinet "Console Chaos," (continued)

Arctic Wolf Response

In accordance with our mega event runbook:

- We proactively notified every impacted customer and guided them through immediate mitigation steps.
- Our analysts led investigations to rapidly identify persistence techniques and to escalate observed high-risk changes.
- Our platform performed real-time threat detection by correlating firewall logs, VPN telemetry, and DNS data to uncover behavior-based anomalies — uncovering abuse that traditional EDR solutions missed.
- Human-led threat intelligence and custom detection rules exposed spoofed IP activity that automated tools overlooked.

Customer Outcomes

This rapid and effective response delivered a number of critical customer outcomes:

- **Early detection narrowed threat actor dwell time:** Our SOC identified threats within weeks of exposure, preventing deeper compromise.
- **Firewall abuse was neutralized before escalation:** Admin takeovers were contained, and credential theft was halted.
- **Credential-based lateral movement was stopped:** DCSync-like (i.e., pulling and pushing configuration settings) attempts were traced and blocked before attackers could pivot across domains.
- **Customers remained protected, even when patches lagged:** Arctic Wolf coverage closed the gap between vulnerability disclosure and patch application.

Triaging Alerts to Eliminate False Positives

KEY TAKEAWAYS

- **Alerts and threats are not synonymous. 71% of all ingested alerts are suppressed by applying customer context and threat intelligence to identify expected or benign activity.** The remaining 29% are escalated for deeper investigation, ensuring teams focus only on meaningful threats.
- **Arctic Wolf's Mean Time to Ticket (MTTT) is 7 minutes and 5 seconds, a decrease of 4 minutes and 14 seconds over two years:** MTTT is our internal measurement of the time between an observation being ingested, reviewed, and escalated to ticket to begin investigating.
- **AI should empower security experts, not attempt to replace them:** Alpha AI reduced analyst workload by over 860,000 manual ticket reviews.
- **Malicious activity often masquerades as legitimate behaviors, emphasizing the necessity of human expertise in the triage process.**

As alerts are ingested, we must quickly triage each to determine which can be suppressed as false positives and which should be escalated to ticket for further review. Of the more than 8.6 million alerts triaged during this reporting period, a little over **2.5 million tickets were generated** for further review.

This works out to:

- Overall, **71% of ingested alerts were then suppressed as benign or expected activity**
- The average customer received a total of **250 tickets in 12 months**
- **Less than 50 of these were high or critical** tickets, equating to less than one per week
- The average ticket was resolved with **a single customer reply**

A Ticket is Not a Guaranteed Threat

As tickets are generated, 93% are rated at low or medium criticality, with telemetry and context suggesting minimal likelihood of malicious activity.

Nevertheless, to ensure the safety of the customer environment a ticket may still be generated for lower-priority events (the average alert ticket is resolved with a single reply from the customer).

Top 3 Reasons for Alert Tickets

Our research found that the most common ticketed alert types often stem from routine activity that may also signal serious threat actions.

Without full telemetry and context, distinguishing between benign and malicious behavior can be excessively difficult and time consuming.

01 **Restricted Country Login:** Alerts are triggered when logins occur from unusual or restricted locations, which may indicate the use of compromised credentials or could be the result of legitimate travel.

02 **Firewall Rule Change:** Modifications to firewall settings can be routine administrator actions, or they could be signs of an attacker trying to gain access or establish persistence.

03 **SMTP Forward Rules Created:** Email forwarding rules may be used legitimately by managers or employees on vacation, or in BEC scenarios to monitor or exfiltrate communications.

Not All Alerts Are Equal

As we further reviewed the alert generation and ticketing process, we observed the sophisticated analysis that goes into reviewing each alert for the context and nuances that cross the threshold from suppression to escalation.

We found that the initial alerting process is a fairly binary one. When specific events or actions are observed within the ingested telemetry, an alert is generated for further review. Once an alert is generated, however, it undergoes a series of reviews from advanced detection logic, AI analysis, and human experts attempting to separate routine events from malicious activity. These reviews are seeking small contextual clues that will make the difference between escalated and suppressed.

To the right are some commonly observed events that may also indicate malicious activity and must be reviewed for suppressed or escalated.

To Ticket or Not to Ticket.

The following events frequently trigger alert generation, as they may indicate potentially malicious behavior.

These are also routine network behaviors and may simply be benign events. This highlights the challenge of alert fatigue felt by many security teams who are faced with the decision of reviewing high volumes of false positive alerts or risk missing a legitimate threat.

DCSync

Domain Controller Synchronization is where one domain controller replicates its data to another for domain data accuracy. Threat actors may also attempt a DCSync to obtain valuable domain and credential data.

Last year, 95% of DCSync Alerts were suppressed for being legitimate activity, while the remaining 5% were escalated for review due to existing suspicious indicators.

Administrator Account Lockouts

When an administrator account is locked due to excessive failed authentication attempts, an alert will commonly be generated for review. Unlike the high percentage of suppressed DCSync alerts, 91% of these alerts will be escalated for review. This is often because of the risks associated with a compromised administrator account and the low likelihood that an established administrator account will have enough failed attempts to result in a lockout.

User added to AD Security Group

Similar to the concerns surrounding compromised administrator accounts, these alerts are issued when a standard domain user account is added to an active directory security group. In other words, this indicated a user's account was granted elevated privileges. Since this is considered poor security practice in most environments and instead often indicated a threat actor attempting to obtain higher privileges for a compromised account, 98% of User Added to AD Security Group tickets are escalated for review.

Increasing Efficacy with AI-Powered Human Experts

The further integration of Alpha AI into the Aurora Platform resulted in a marked reduction in workload while accelerating threat response. During this report period, **Alpha AI automatically triaged 10% of alerts generated**, quickly suppressing or escalating before the need for human involvement.

While the current hype around AI may initially make this 10% seem inconsequential, it actually represents a significant impact on triage time and workload. Framing it in a different way, in just the period covered by this report, **that percentage equates to more than 860,000 alerts** that no longer required human validation.

Through the clearing of noise, the enhancement of signals, and the triaging of high-fidelity alerts, this highlights the true value of AI. Not in its unrealized promise of replacing traditional analysts, but in its support of security experts to make informed decisions that require human expertise.

Rapid Detection and Validation are Essential for Reducing Dwell Time

A rapid, accurate, around-the-clock threat detection capability is a necessary condition for an effective defense, but to enable timely response, detection must be paired with a similarly rapid and effective triage process.

To monitor our operations and long-term progress, we use an internal metric called mean time to ticket (MTTT). Unlike the familiar metric of the time to detect a threat within an environment, or mean time to detect (MTTD), MTTT encompasses the time to ingest the data, generate an alert, and validate its potential legitimacy, at which point a ticket is created. We find this to be a more valuable effectiveness metric when compared to MTTD which has the potential to be skewed by false positives.

Our efforts to minimize MTTT have paid off:

In 2023, our MTTT was 11 minutes and 19 seconds.

- In 2024, the introduction of our Alpha AI slashed our MTTT by 33%, dropping it to 7:34.
- As of September 2025, our latest MTTT stands even lower, at 7:05.
- This is a 37% total reduction in a 24-month period. *(1/23-12/24)*

From Weeks to Minutes

In contrast to our latest MTTT of 7:05, according to the 2025 IBM Cost of a Data Breach Report, the average MTTD across all organizations is 194 days.

This means that in many environments it takes over six months, on average, to detect the presence of a threat existing within their network.

Investigating Threats

KEY TAKEAWAYS

- **It takes an astounding amount of data to confirm a limited number of threats:** The Aurora Platform ingested over 330 trillion observations in 12 months, resulting in slightly more than 9,000 investigations. **This is calculated at a 99.99999999% reduction rate** from initial visibility to final determination and action.
- **Actual malicious activity remains uncommon during investigations:** Only **2% of security investigations resulted in confirmed threat activity,** further underscoring how challenging it is to sort through noise.

When malicious activity is confirmed, our analysts then initiate a security investigation to further validate the threat, assess its severity, and determine what response actions are needed. During the period of our report, Arctic Wolf security analysts have conducted more than 9,000 security investigations. This equates to roughly **one investigation for every 35 billion observations.**

Although this ratio is impressive on its own, it really stands out when we put all of this together to view the Aurora Platform's full data pipeline. We can now calculate that from the 330+ trillion raw observations ingested over the 12 months, through alerting, analysis, ticketing, and into an investigation, this results in a **total reduction in noise of 99.99999999%.**

Responding to Threats with Speed and Precision

While swift detection is critical, its true value is only realized when paired with equally rapid and decisive response actions. In July 2024, Arctic Wolf introduced our expanded Active Response capabilities that significantly enhanced our ability to take action in real time when legitimate threats are identified. These capabilities include targeted email management, URL blocking, network response actions such as modifying firewall configurations, and identity-focused measures to contain or manage compromised user credentials. All such actions are performed only after an initial discussion and with prior customer approval, ensuring both precision and trust in the process.

Over the past year we found that 38% of all security investigations required direct intervention to stop an active threat or prevent its recurrence. The majority of these, 72%, were identity-based actions, such as disabling compromised accounts, removing unauthorized group memberships, or enforcing password

How Common Are Threats?

When reviewing the data around ticket and investigation closures or suppression, we found that only 2% of security investigations actually resulted in confirmed malicious threat activity.

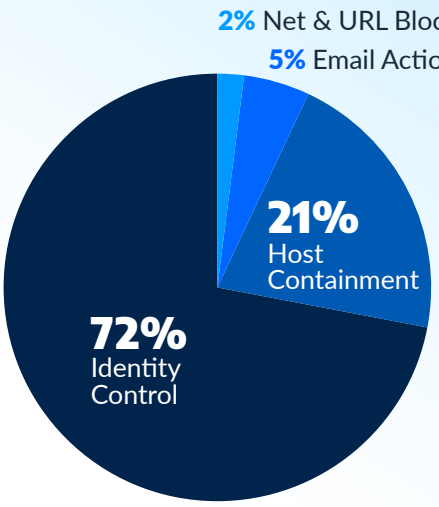
The first instinct may be to see this low confirmation rate and assume that it tells us that threats are rare. In reality, it actually reflects how buried true threats can be beneath the weight of benign activity and false positive alerts.

resets. This high proportion reflects the critical role identity management plays in today's threat landscape where compromised credentials are often the earliest indicators of a threat actor's presence. Direct decisive action at this stage can quickly disrupt their objectives, stopping threats before the attack evolves. By containing account-level compromises, we can prevent lateral movement, block unauthorized access to sensitive resources, and significantly reduce the likelihood of a successful breach.

Host-based containment was initiated in 21% of cases, locking down compromised endpoints before further spread could occur. Additionally, 5% involved removing malicious emails, including phishing campaign attempts, before they could trigger further compromises. Network and URL blocking, though less frequent at 2%, was applied strategically to cut off access to malicious locations in real time.

Together, these results underscore not only the necessity of a rapid and coordinated response plan, but also the effectiveness of our continually expanding Active Response capabilities in applying the right action at the right moment to protect our customers from evolving threats.

Response Actions



A Familiar Trio of Industries Tops the Charts

Threat actors may continue to be opportunistic, but certain industries consistently attract a disproportionate share of attacks due to shared risk factors.

In our normalized analysis, the education, healthcare, and manufacturing verticals generated the highest alert volumes per organization. Though these sectors appear different on the surface, they often share critical vulnerabilities: low tolerance for downtime, vulnerable data (whether personal, intellectual, or operational), and complex, often outdated IT environments.

Manufacturers, for example, face significant concerns over the cost of downtime and risks associated with IP theft. These risks are heightened by the growing attention from nation state actors engaging in industrial espionage, strategic reconnaissance, and theft of trade secrets. This challenge is particularly notable where operational technology (OT) environments lack even basic security controls, leaving critical systems exposed. Educational institutions often prioritize accessibility over strict access controls and operate with limited security staff and resources. This combination makes them attractive targets to financially and politically motivated attackers who exploit these gaps to gain unauthorized access to systems and sensitive data.

Additionally, healthcare organizations contend with many of the same challenges, compounded by the demands of safeguarding highly sensitive personal information. Legacy systems, sprawling infrastructure, and the need to maintain uninterrupted patient care can create persistent vulnerabilities that attackers are quick to exploit.

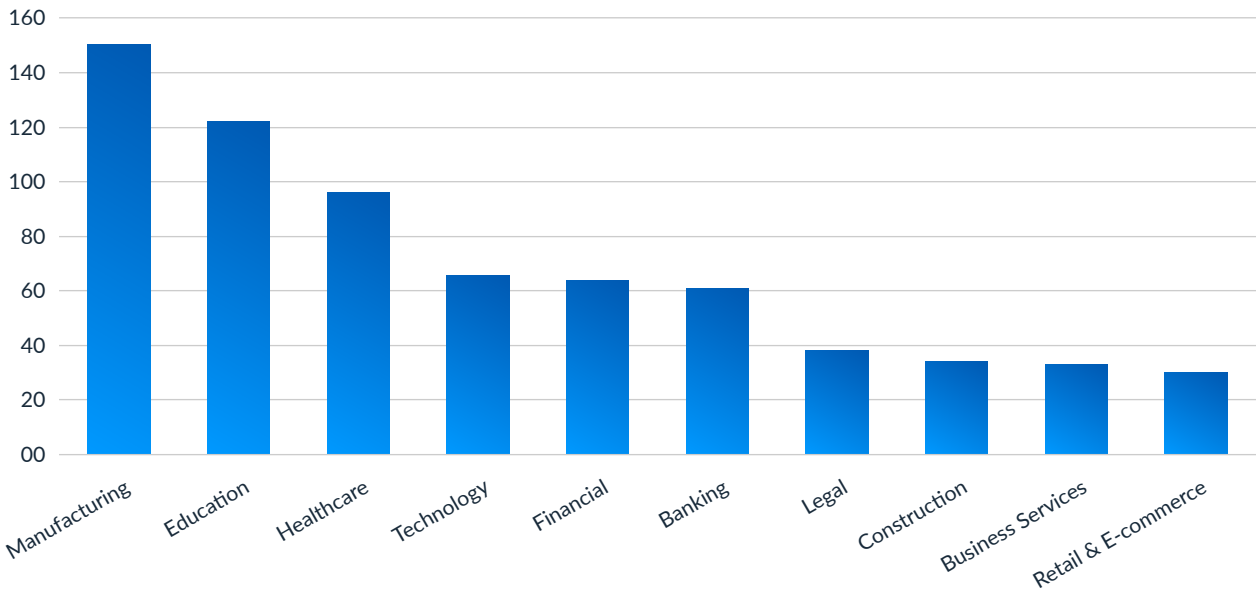
Most Targeted Industries

01 **Manufacturing**
- Mixed OT Environment
- Nation State Attention

02 **Education**
- Limited IT Staff
- Prioritize Access over Security

03 **Healthcare**
- Legacy Systems
- High-Value Data

Average Tickets Per Customer (normalized by customer count)



"From May 2024 to April 2025, the education and healthcare sectors were two industries most frequently targeted by threat actors, driven by distinct but overlapping threat patterns. In education, ransomware groups like Interlock ramped up attacks on K–12 and higher education institutions using ClickFix malware and fake CAPTCHAs, while state-sponsored actors used living-off-the-land (LOTL) techniques, targeting cloud-connected applications to steal research data for the purposes of espionage. Healthcare, meanwhile, experienced a surge in ransomware incidents led by threat groups like Akira, Qilin, and Safepay, often leveraging edge device vulnerabilities for initial access and prioritizing data exfiltration first and encryption later. We observed increased targeting against hospitals, healthcare-related cloud applications, and high traffic healthcare websites. Both sectors faced persistent phishing campaigns, rising malware infections, and significant operational disruptions due to outdated infrastructure and limited cybersecurity budgets. Notably, we have even seen attacks on organizations that bridge both verticals—such as teaching hospitals and educational healthcare systems—making them exceptionally attractive and vulnerable targets."

LAURA STRATTON
Sr. Manager Tactical Threat Intelligence
Arctic Wolf

Mega Event Spotlight: SonicWall (CVE-2024-40766)

KEY TAKEAWAYS

- **The ransomware playbook continues to evolve:** The combination of credential-based access, rapid lateral movement, and infrastructure-wide impact points to a modular, repeatable attack model that traditional tools are ill equipped to stop.
- **Conscious choices and misconfigurations create opportunities for attackers:** Across all observed breaches, an absence of multi-factor authentication (MFA), reliance on local VPN authentication, and legacy firmware were consistent factors — providing low-effort, high-impact entry points for attackers.
- **Backups are worthless if attackers can find them:** Today's attackers employ a seek-and-destroy approach to backups, underscoring the importance of the 3-2-1 backup approach.
- **24x7 coverage and short detection and response times are essential:** Some of these incidents progressed from initial access to system encryption in under 90 minutes, creating a race-against-the-clock scenario.
- **Human-led response is what changes outcomes:** Human expertise is required to identify patterns, prioritize high-risk behavior, and initiate response — and is the deciding factor between stopping ransomware in progress, or reporting on damage after it is done.

In early August 2024, Arctic Wolf began observing a significant spike in ransomware activity attributed to Fog and Akira actors, two ransomware operations exploiting vulnerabilities in SonicWall SSL VPN appliances.

The primary vector is believed to be compromised VPN access on devices running unpatched firmware vulnerable to CVE-2024-40766, a critical access control flaw disclosed and addressed in a patch released by SonicWall in late August 2024.

Victims shared several characteristics that made them vulnerable to this campaign, including a lack of MFA, reliance on local VPN authentication, and legacy firmware.

Although the attacks varied by necessity, they followed a consistent pattern:

01 Attackers compromised SSL VPN accounts on SonicWall devices running unpatched firmware vulnerable to CVE-2024-40766, with malicious logins originating from VPS-hosted IP addresses. Some of these IPs were used by both Fog and Akira, suggesting shared attacker infrastructure.

02 To maximize impact, attackers sought out and encrypted virtual machine storage and backups. Attackers moved swiftly, with time-to-encryption in two to 10 hours — and in some cases under 90 minutes.

Mega Event Spotlight: SonicWall (CVE-2024-40766), (continued)

Arctic Wolf Response

In accordance with our mega event runbook:

- After SonicWall confirmed exploitation of vulnerability, the Arctic Wolf SOC began investigating and tracking cases.
- We proactively notified every impacted customer and guided them through immediate mitigation steps while providing after-hours response and ongoing monitoring.
- Human-led threat intelligence powered by live incident responders and close vendor collaboration supported development of custom detection rules involving cross-telemetry correlation.

Customer Outcomes

Our comprehensive response delivered several important outcomes:

- **Customers remained protected:** Despite automated tools alone being unable to detect these attacks, our human-led SOC was able to keep customers safe.
- **Time-to-detect met the time-to-encrypt challenge:** The attackers moved quickly, but our SOC processes moved even faster.
- **Delays in patching weren't catastrophic:** A patch being available doesn't mean a customer can deploy it immediately, and Arctic Wolf coverage served as a safeguard during this risky period.

Conclusion

This year's Security Operations Report reveals a stark truth that many security leaders have long suspected: cyber threats are accelerating in scale, sophistication, and timing—often striking when defenses are weakest. Despite record investments in security tools, the gap between effort and effectiveness persists, driven not by a lack of technology, but by operational misalignment, visibility gaps, and reactive strategies.

> Yet this year's data also points to a clear path forward. Organizations that prioritize 24x7 vigilance, holistic visibility, and outcome-driven triage are measurably reducing dwell time and improving response efficacy. The integration of AI-powered platforms like Alpha AI, when paired with human expertise, is not replacing analysts—but empowering them to act faster, smarter, and with greater precision.

To move from overwhelmed to secure, we recommend focusing on foundational actions:

- **Refine your triage processes to reduce alert fatigue:** Consider opportunities to leverage AI to support human analysts in suppressing false positives and escalating high-fidelity alerts.
- **Conduct regular visibility audits and configuration reviews across all telemetry sources:** Ensure coverage across endpoints, networks, cloud, and identity sources to reduce detection gaps. Additionally, conducting routine reviews of system configurations helps maintain visibility after regular system updates and changes.
- **Eliminate unnecessary internet-facing management interfaces:** As seen in recent mega events, these are high-risk, often unnecessary entry points.
- **Enforce least-privilege access and monitor cloud configurations:** Misconfigurations—not vulnerabilities—are the leading cause of cloud incidents.
- **Apply threat intelligence to contextualize alerts:** Optimize detection logic and behavioral analysis to distinguish benign from malicious activity.

While these steps may seem daunting for already resource-constrained teams, security operations maturity is achievable. Arctic Wolf's human-centric approach, powered by Alpha AI and our Security Journey framework, helps organizations of all sizes close the effectiveness gap and build resilience into their core operations.

"Ultimately, this research serves to further confirm what we have always believed: Cyber risk is dynamic and your response must be too. Whether you are defending a school district, hospital, manufacturer, a small to medium business, or global enterprise, Arctic Wolf is your partner in turning insight into action. Through a dynamic and evolving security journey powered by the right balance of human expertise and artificial intelligence your organization can protect itself by building a trusted security program that works."

BRETT ROGERS
VP of Concierge Security Services
Arctic Wolf

Arctic Wolf customers rely on us every day to secure their organization against threats – and make security work.

Organizations that embrace security operations are more secure, more resilient, and better able to adapt to the ever-evolving threat landscape — but the reality is that very few organizations have the resources to build such capabilities in house.

We help level the playing field against attackers, ensuring that every organization of every size has the expertise and foundational cybersecurity needed to defend itself.

If you are not getting desired outcomes from the solutions you have today, or if you are looking for ongoing expertise to put your existing investments to work — Arctic Wolf is a trusted security operations partner that builds customers' confidence in their security posture, readiness, and long-term resilience.

END CYBER RISK

ARCTIC WOLF

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, enabling customers to manage their cyber risk via a premier cloud-native security operations platform.

The Arctic Wolf Aurora™ Platform ingests and analyzes more than nine trillion security events a week to help enable cyber defense at an unprecedented capacity and scale, empowering customers of virtually any size across a wide range of industries to feel confident in their security posture, readiness, and long-term resilience. By delivering automated threat protection, response, and remediation capabilities, Arctic Wolf delivers world-class security operations with the push of a button.

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

REQUEST A DEMO