Guide:

Alert Logic vs. Arctic Wolf®

Head-to-Head Comparison

ALERT LOGIC™

INTRODUCTION

No level of investment prevents 100% of threats to your critical IT systems. As hackers become savvier, attacks can increase in sophistication and more effectively evade existing prevention tools. Rising staff shortages add to the risk which has forced a growing number of organizations to partner with cybersecurity providers — with proven technology and experts — to minimize damage and disruption to business operations.

This guide, designed for security professionals investigating the processes, challenges, and best practices of choosing a managed detection and response (MDR) provider, presents a transparent, side-by-side comparison of the services and capabilities of Alert Logic and Arctic Wolf®.

White-Glove Customer Experience

The most effective cybersecurity solution should be tailored to your environment and organization, not as a separate feature or paid upgrade, but ingrained into the product itself. Likewise, an MDR solution provider should be keenly focused on delivering an exceptional customer experience and the security outcomes you seek.

ARCTIC WOLF	White-Glove Service	ALERT LOGIC
8+:1	Ratio of Security Analysts to Customer Accounts (1:N)	6:1
Yes	24/7/365 Security Operations Center (Eyes on Glass)	Yes
No	Named Security Analyst Dedicated to the Customer	Yes
No (Best Effort)	Documented SOC SLA *	Yes (15Min/<1%FP)
Yes	Dedicated Concierge Deployment Team	Yes
	THREAT INTELLIGENCE	
Yes	Threat intelligence and Hunting Capabilities	Yes
Yes	Breadth and Depth of Threat Vector Coverage	Yes
Yes	Use of AI/ML in the Discovery and Research Phases of Threat Intelligence	Yes

Evaluation

Alert Logic

Alert Logic's white-glove approach to cybersecurity is what makes us stand out in a crowded field of solutions. Through the personalized relationships we build with each customer and our use of data and analytics to protect your most critical assets, you will always have visibility into your security posture. Our white-glove service includes a dedicated team of experts, wholly committed to your success and delivering the greatest protection for your organization.

Arctic Wolf

Arctic Wolf provides their customers with a concierge service for deployment and continued maintenance of services. However, they do not provide dedicated security analysts who work hand-in-hand with their customers daily to provide tactical and strategic planning, post incident, monthly, quarterly, or annual security reviews, as Alert Logic does.

Alert Logic provides dedicated deployment teams, customer-and industry-specific tuning, as well as post incident reviews. With Alert Logic you get the service your fast-paced security environment requires without, in most cases, the additional fees charged by many of our competitors.

Scalable MDR Platform

What is scalability?

According to Gartner, "scalability is the measure of a system's ability to increase or decrease in performance and cost in response to changes in application and system processing demands."

Why is scalability in the platform important?

Scalability is of utmost importance because it affects the functional and operational effectiveness of a platform, especially in digital interfaces, where the platform may perform services like ingestion of data from a common funnel. Without scalability, performance issues, disruption of service, and loss of log data could occur frequently — directly impacting the abilities of security analysts to monitor and manage your environment.

What is software scalability?

Software scalability is the ability to grow or shrink a piece of software to meet changing demands from a business. It is critical to support growth, but also to pivot during times of uncertainty and scale back operations, as needed.

How does scalability affect business operations?

Scalability of the platform from a technological and financial perspective seeks to ensure you will not incur extra and unexpected costs. Creating a platform utilizing scalable best practices and techniques enables users and customers to use the platform without fear of overrunning its capabilities. Building in a scalable environment such as AWS allows for expansion or reduction of resources depending on the customer's utilization habits and parameters. By building a scalable platform, the service provider can set thresholds which automatically expand resources to meet the needs of the customer in real-time, then automatically reduce the resource utilization when the threshold is met to scale back resources. By doing this, the service provider and customer can maintain predictable costs.

Alert Logic MDR® Monitors...

>1m

Servers, Containers and Endpoints

140b+

Log Messages per Day

17pb

Customer Log Data Available in a Single Data Lake for Security Operations Analysis and Reporting

3.5m

Security Events per Second

What are the requirements of a scalable MDR solution?

- **Performance:** Platform must provide speed and functionality that can expand and reduce based on utilization.
- **Availability:** Platform must be robust and provide an elevated level of uptime, preferably 99.999% availability.
- **Reliability:** Platform must work well with degraded infrastructure or seamlessly fail over to infrastructure that is not degraded until primary infrastructure is repaired.
- **Cost:** Platform design and implementation must be cost-effective and have stable infrastructure and application costs that will not drastically increase because of fluctuation to meet utilization needs within the prescribed service tier.

ARCTIC WOLF	**Platform**	ALERT LOGIC
Yes	Platform Scalability (AI/ML, Modern Architecture)	Yes
Multiples	Single Pane of Glass/Integrated Service/Tiered Pricng	Yes
No	Cloud/Container Coverage	Yes
Yes (Limited)	Response via Agent for Mitigation or Remediation*	Yes (Multiple Intelligent Response Actions)
Some	User Behavioral Analysis	Yes
Yes, by Request	Detailed Reporting	Yes
No	Playbooks for Intelligent Response Capabilities	Yes
No	Pure Play Integrated SaaS Platform with Owned Intellectual Property (IP)	Yes
	LOG INGESTION & RETENTION	
No	Packet Flow (NetFlow/J-Flow) Monitoring	Yes
Yes	Syslog Monitoring	Yes
90 Days	Syslog, Netflow, IDS Data Retention Timeframe (Hot Storage Indexed and Searchable)	365 Days
	INTRUSION DETECTION	
Yes	Built-in Intrusion Services (Integrated IDS not Third-Party with API integration)	Yes
Yes	IDS has Visibility to North/South Traffic	Yes
Dependent on Monitored Devices	IDS Has Visibility to East/West Traffic	Yes

VULNERABILITY MANAGEMENT		
Yes (Separate SKU)	Automated and Manual Vulnerability Scans	Yes
Yes (Separate SKU)	Vulnerability Tracking and Monitoring	Yes
CONFIGURING SCANNING		
Yes	End Point Configuration Scanning	Yes
No	Cloud Asset Configuration	Yes
No	Network and Cloud Configuration Management	Yes

Evaluation

Alert Logic

Scalable Platform: Scalability is the cornerstone of Alert Logic MDR® and maintains effective performance, even when the workload increases. This ensures the customer has a stable and high performing platform that changes at the speed of their environment. Partnering with AWS also enables Alert Logic to develop a platform that is not only scalable to workloads from the customer but also scalable to the business office. We are then able to provide our customers with a fixed rate for MDR services without fear of major overages or serious performance issues.

Outcome Based Security for the Whole Computing Environment: Alert Logic's proprietary MDR platform and team of security experts deliver outcome-based security by collecting network traffic and more than 140 billion log messages each day. We provide coverage across vulnerabilities and attacks by bringing together asset visibility and security analytics for networks, applications, and endpoints on-premises, hybrid, and cloud environments.

Alert Logic MDR® integrates with common business SaaS applications, providing comprehensive visibility. Our security researchers and experts are continually focused on the development of new and innovative technology to maintain pace with the ever-changing threat landscape. Because our platform is SaaS-delivered, these innovations are generally included at no additional cost.

Alert Logic Intelligent Response™: The platform also includes Alert Logic Intelligent Response™ which is designed to minimize the impact of a breach via embedded SOAR capabilities with workflows to enable response actions across network, endpoints, and cloud environments.

Arctic Wolf

Spanning 2300 installations, the Arctic Wolf platform claims to process over 200 billion security events daily. Built on an open XDR architecture, the platform collects endpoint, network, and cloud telemetry, and then analyzes it with multiple detection engines. Machine learning and custom detection rules then deliver personalized protection for your organization.

Arctic Wolf touts unlimited data retention and recall, however, their platform only stores, indexes, and makes searchable 90 days of ingested log data. Additional fees are required for longer than 90 days. Alert Logic retains and makes searchable 365 days of ingested log data as standard.

Arctic Wolf only allows for physical sensors to be placed on-site, not permitting customers to use their virtualization platforms. The result: customers are forced to add hardware which requires valuable physical space in the datacenter and drives hardware sprawl.

Finally, Arctic Wolf offers vulnerability scans as managed risk, MDR, cloud detection and response (CDR), cloud security posture management (CSPM), and managed security awareness. However, set your expectations for disparate systems with separate dashboards. Their security analysts and yours will need to monitor multiple interfaces to decipher the activities in your environment.

Sensors for Any Environment

Ingesting logs from hundreds of data sources is not an easy task while simultaneously performing multiple types of scans, as well as an inline intrusion detection system. It requires a powerful engine in the same environment where the log sources reside. Sensors must be versatile, flexible, and consistently built across the entire supported host environment.

ARCTIC WOLF	Sensor Features	ALERT LOGIC
Yes	Physical Sensor for On-Prem	Yes
No	Virtual Sensor for On Prem (e.g., VMWare, Hyper-V, etc...)	Yes
Yes	Virtual Sensor for AWS in Marketplace	Yes
Yes	Virtual Sensor for MS Azure in Marketplace	Yes
No	Virtual Sensor for GCP in Google Cloud Store	No
No	Virtual Sensors for Cloud Support Monitoring Containers	Yes
Yes	Virtual Sensor Provide Coverage via VPC	Yes
Yes, via API	Cloud Infrastructure Integration and Monitoring	Yes (Natively)
Yes	Cloud Software as a Service Monitoring and Integration	Yes

Evaluation

Sensors deployed for either of these providers are extremely important. A sensor deployed incorrectly can mean the difference in security success and failure. The security platform sensors perform a plethora of tasks and services such as scanning, discovery, vulnerability, and configuration. They may also do things like integration with third-party utilities and services like Office 365, EDR, Firewalls, and other devices and services.

Alert Logic

Alert Logic MDR® provides the same security outcomes no matter where systems are hosted — across public cloud, hybrid, and on-premises. Our award-winning MDR solution ensures coverage across all environments and adapts to your architecture — traditional network and firewall, pure cloud automation, or any mixture. Within a single service, Alert Logic powers your security maturity to provide asset discovery, internal and external vulnerability scanning, and log and network-based threat detection.

To reduce the likelihood of successful attacks, Alert Logic continuously evolves our solution to integrate and secure the assets upon which our partners and customers rely on most — today and in the future. Our steadfast focus is on those sources that offer the most potential to generate security value:

- Cloud Platforms (AWS, MS Azure, Google Cloud Platform)
- Container Security
- Database
- Email Security
- Endpoint, Anti-Virus, Encryption
- Firewall
- Identity and Access Management
- IT Service Management
- Messaging
- Network
- Operating Systems
- Productivity Platforms
- Virtualization
- Web Server
- Other Security Tools and Utilities

Arctic Wolf

The most important service the sensor performs is log ingestion from various monitored devices across the environment. Log sources identify issues, anomalies, and incidents that might not otherwise be discovered. Arctic Wolf only offers physical hardware sensors for on-premises deployment, not virtualized. The lack of virtualization for the on-premises sensor means the customer cannot use their own hardware/virtualization stack. This is an issue when the datacenter is constrained on physical space, or the customer is performing resource optimization and wants to minimize hardware sprawl. Having a single, static deployment technology with no support for the latest technology can create a reduction in efficiency and productivity.

Another differentiator between the two solutions is that Alert Logic integrates with cloud providers based on native integration, while Arctic Wolf integrates only through API. Other areas of consideration include the support for containers, and the inability of Arctic Wolf to support the ingestion of Netflow/J-Flow logs. Furthermore, Arctic Wolf does not provide onboard IDS services from the sensor, only ingesting IDS/IPS from third-party solutions. While pure-play solutions are recommended where possible, often pure-play IDS within a customer's network — especially for east-west traffic — is not a practical solution when considering overall cost versus the benefit of deploying IPS/IDS in small to mid-size enterprise networks.

> **“Real-time alerts can proactively maintain current and accute awareness. Having Alert Logic handle the detection and response allows our IT team flexibility to help in areas that need constant supervision.”**

Brett T.
IT Infrastucture Engineer, Alert Logic Customer
G2 Review

Alert Logic's Coverage for Major Platforms & Services Includes:

aws

Microsoft Azure

Google Cloud

Office 365

okta

ESCALATE & RESPOND

Alert Logic white-glove customer experience

3-minute response **time** for high or **critical incidents** for all managed service customers

Better Outcomes Across Your Entire Cybersecurity Compliance Program

Regulatory cybersecurity compliance related to data protection and privacy involves a landscape of laws and standards. Using a single system of policies across your entire compliance program enables you to implement best practices at a lower total cost. However, without a guide to assist with policy mapping, you run the risk of compliance gaps and increase your risk of audit failure.

ARCTIC WOLF	Compliance Report	ALERT LOGIC
Yes	ISO 27001	Yes
Yes	HIPPA	Yes
Yes	PCI-DSS	Yes
Yes	SOC 2 *	Yes
Some	NIST 800-171	Yes
No	NIST 800-53	Yes
Yes	Gramm-Leach Bliley Act (GLBA)	Yes
Yes	The Cybersecurity Maturity Model Certification (CMMC)	No
Yes	CIS Controls	Yes
NoI	HITRUST	Yes
Yes	Sarbanes Oxley (SOX)	Yes
Yes	GDPR	Yes

Evaluation

While not every compliance or IT governance is met by either provider, the reasons for not advancing a particular compliance are primarily based on services offered.

Alert Logic

Many of the technology requirements are easily met with Alert Logic's robust monitoring platform. Compliance and IT governance achieved within our solutions are based on the existing customer base, markets served, and anticipated requirements by existing and future customers.

At present, many request at least one of the above listed compliance requirements be met and, in most cases, multiple compliances are requested with the most desired being PCI-DSS. Alert Logic maintains the Payment Card Industry Authorized Scanning Vendor certification (PCI-ASV) to assist our customers with their PCI-DSS scanning requirements.

Organizations accepting credit card data must have quarterly vulnerability scans to help ensure credit card data is safe. Certification ensures the vulnerability scans performed by Alert Logic rigorously validates customers are not vulnerable to the increasingly sophisticated attacks on their systems.

Arctic Wolf

Comparing the various compliances across the board, Alert Logic and Arctic Wolf are fairly equal in capabilities. A few exceptions are HITRUST and NIST 800-52 compliance which Arctic Wolf lacks. Arctic Wolf does attest to meeting some parts NIST 800-171 but does not meet all compliance mandates. While Arctic Wolf does support the Cybersecurity Maturity Model Certification, Alert Logic is in the process of developing reporting to meet the CMMC compliance mandate. This is not an all-inclusive compliance list, as compliance requirements change on an almost daily basis. New compliance and regulatory standards come out on a yearly basis, as well.

Corporate Overview

Corporate leadership and governance are extremely important to the overall service and performance of any service, provider. From strategic vision to planning and execution, leadership within a service organization sets the tone not only for the service provider, but also the customer's business, as well. Many companies come into existence on the heels of a few pioneers who have blazed a trail, made mistakes, and set the standards for how to provide a service, or develop and deliver a technology.

ARCTIC WOLF	Corporate Overview	ALERT LOGIC
Minnesota	Location of U.S.-Based HQ and SOC	Texas
Germany	Location of Global SOC	UK
10	Years in Business	20
2300+	Number of Customers *	4000+
1,326	Number of Employess	700+
	COPORATE COMPLIANCE AICPA SERVICE ORGANIZATION CONTROL REPORTS	
Undocumented	SSAE 18/ISAE 3402: SOC 1 TYPE II	Yes
Yes	SSAE 18/ISAE 3400: SOC 2 TYPE II	Yes
Undocumented	PCI-DSS	Yes
Undocumented	ISO27001 (United States)	Yes
Undocumented	ISO27701 (European GDPR)	Yes
Yes	EU-U.S. Privacy Shield Framework (Legacy Data)	Yes
Undocumented	Cloud Security Alliance (CSA) STAR Self-Assessment	Yes

Exceptional stewardship is one of the most important aspects of business that corporate leadership can undertake:

- Make the most out of their financial investments
- Communicate a vision to stakeholders internally and externally
- Inspire the highest level of productivity, industry defining standards, and a global presence
- Ensure all customers have what they need when they need it

These unique abilities transform a service provider into an industry leader.

Evaluation

Alert Logic

Service organization reports assist providers who operate information systems and offer information system services to other entities. These tools help build trust and confidence in their service delivery processes and controls through a report by an independent certified public accountant.

Alert Logic has made substantial investments into ensuring the security of customer and employee data. Those investments are in monetary and man-hours to build a relationship of trust and goodwill with our customers and partners. Attestation of the above listed certifications are available up on request.

Arctic Wolf

Arctic Wolf had minimal documentation on their corporate compliance. Of the seven compliance audits listed, Arctic Wolf attested to complying with just two in their public facing website. There was no documentation as to the attestation status of the others.

Key Considerations

If you are evaluating Alert Logic vs. Arctic Wolf for managed detection and response, ask Arctic Wolf the following questions:

Does their concierge service provide a dedicated analyst throughout your tenure?

People are a critical component of Alert Logic MDR® and we have invested in security talent since 2002. A broad range of security, technology, and customer experience professionals are assigned to each customer — providing a personalized level of service that considers the context of your organization and role:

- **Customer Success Manager:** As part of a larger MDR Concierge team, this single point of contact is an expert in the delivery of Alert Logic MDR®. They understand each customer's unique business needs to ensure the best possible service and protection.

Alert Logic MDR®

Delivers massive scale and integrated services which discover risks to the security of your organization and detect breaches — reducing noise and false positives to enable rapid response.

Alert Logic assesses your security posture and collects data across **ALL** your systems to analyze, prioritize, and validate threats **BEFORE** escalating only those that may impact your business — providing vital and actionable intelligence.

10k+ **Types of Configuration Problems Assessed**

144k+ **Unique Vulnerabilities Scanned from a Continually Updated Library**

Alert Logic provides a comprehensive view and robust understanding of your unique security posture through **reporting**, **dashboards**, and **expert services**.

- **Dedicated Security Expert:** Veteran security analyst in the Alert Logic SOC, delivering individualized protection and customized response plans.

What intrusion detection functionality do they provide in AWS, Azure, and Google clouds?

Alert Logic is a cloud security pioneer. We collect and analyze ingress, egress, and lateral network traffic from across all cloud and hybrid environments.

What visibility do they have into container traffic?

Alert Logic provides the industry's only network intrusion detection solution and log management for containers. We detect threats to containers running on AWS, Azure, and on-premises deployed Docker, AWS Elastic Container Service (ECS), Kubernetes, AWS Elastic Beanstalk, and CoreOS.

How many new or evolving threats were they first to discover?

Alert Logic tracks new vulnerabilities and emerging threats across over 4,000 customers. For example, our researchers discovered vulnerabilities in WordPress WP Live Chat and developed techniques for exfiltrating credentials via DNS. We leverage our findings to create a community defense and rapidly provide protection for our customers' most critical threats. Plus, our single platform continuously and efficiently consolidates and analyzes threat data, research, and attack behaviors from hundreds of thousands of systems.

Summary

As previously stated, even the best solution cannot prevent 100% of all attacks. The need to continuously identify and address breaches or gaps before they cause real damage is imperative. With limited expertise and a cloud-centric strategy, this level of security can seem out of reach. Therefore, partnering with an MDR provider with a proven track record and a best-in-class solution is essential to achieve your security goals.

Since 2002, Alert Logic as helped organizations around the world better protect their most business-critical environments through the installation and configuration of security agents, management of data feeds, and wading through alerts. We specialize in helping businesses who have endured the frustration of traditional security outsourcing vendors that fail to deliver little more than yet another high-cost alert stream. Security professionals left on their own by vendors who provide security products but not threat intelligence or expertise find our MDR solution delivers the comprehensive coverage they need and expect. Find out how Alert Logic can better meet your security needs, meet your budget and staffing requirements, and give you greater peace of mind.

With Alert Logic, rest easier at night knowing our team is on the job 24/7, escalating only incidents needing your attention.

200K

Incidents per Month

analyzed through machine learning and other methods to eliminate false positives becomes

26K

High and Critical Incidents

> **"The Best Threat Detection & Analysis Tool for Your Business"**

Leonard A.

IT Admin, Alert Logic Customer
G2 Review

> **"Our Program to Maintain Our Security at All Times"**

Katie S.

Manager Assistant,
Alert Logic Customer
G2 Review

About Alert Logic and HelpSystems

Alert Logic is the only MDR provider that delivers comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Our cloud-native technology and white-glove team of security experts protect your organization 24/7 and ensure you have the most effective response to resolve whatever threats may come. Founded in 2002, Alert Logic is headquartered in Houston, Texas and has business operations, team members, and channel partners located worldwide. In March 2022, HelpSystems, focused on helping exceptional organizations secure and automate their operations, acquired Alert Logic as the cornerstone of its comprehensive cybersecurity portfolio.

Businesses of all sizes look to Alert Logic to establish a hybrid IT approach to meeting their cybersecurity goals and applicable compliance mandates. Alert Logic is the industry leader in MDR for cloud environments, with more than 4,000 customers and an extensive partner ecosystem around the globe. Its comprehensive coverage paired with human oversight, enables organizations to meet key regulatory requirements, including PCI DSS, HIPAA, HITECH, GDPR, Sarbanes-Oxley (SOX), SOC 2, NIST 800-171 and 800-53, ISO 27001, COBIT, and more.

Finding the right MDR provider can seem like a daunting task, but when you compare them side-by-side the strength and value of Alert Logic shines through. Our cloud-native technology and white-glove team of security experts deliver peace-of-mind and ensure you have the most comprehensive protection on the market today.

AWARD WINNING
CYBER SECURITY TEAM & SOLUTION

Cybersecurity Excellence
AWARD WINNER

Global infoSec
AWARD WINNER

G2 MDR Leader
AWARD WINNER

CRN Channel Chiefs
AWARD WINNER

Contact us at **www.alertlogic.com** to speak with an Alert Logic MDR expert and learn how Alert Logic can help.

UNRIVALED SECURITY FOR YOUR CLOUD JOURNEY.