Arctic Wolf® Cloud Security Posture Management (CSPM)

DATASHEET

Identify and Close Security Gaps Within Your Cloud Infrastructure

Cloud threats take advantage of the fact that most organizations don't have the broad visibility necessary to take inventory of their cloud systems or discover cybersecurity risks in their cloud infrastructure environments. What's more, these businesses rarely optimize their configurations to harden their posture and comply with regulations. To address this, organizations should adopt Arctic Wolf Cloud Security Posture Management (CSPM) for their cloud infrastructure.

What Is CSPM?

CSPM is a continuous process of cloud configuration monitoring and adaptation to reduce the likelihood of a successful attack. It includes use cases for compliance monitoring, DevOps integration, incident response, risk assessment, and risk visualization.

Protect Your Cloud Environments With Arctic Wolf®

As part of Arctic Wolf® Managed Risk, the Cloud Security Posture Management feature scans environments (AWS, Azure, and GCP) against thousands of generally accepted cloud configuration benchmarks managed by your Concierge Security® Team (CST). The CST provides you with:

Cloud Inventory Reporting

Returns a complete inventory and categorization of all assets found within the cloud environment for auditing, monitoring, and executive reporting purposes.

Cloud Environment Benchmarking

Assigns a cloud environment risk score to quantify how your environment compares to generally accepted cloud configuration benchmarks.

Posture Hardening Recommendations

Your Arctic Wolf security operations expert provides you with rich context and remediation recommendations to close cloud vulnerability gaps and harden your security posture.

Cloud providers have hundreds of services with thousands of configuration options. Your Arctic Wolf Concierge Security® Team (CST) works closely with you to identify and close security gaps within your cloud infrastructure, such as:

- Servers that are publicly exposed to the internet
- Unencrypted databases and data storage
- Lack of least-privilege policies
- Poor password policies or missing multi-factor authentication (MFA)
- Misconfigured backup and restore settings
- Data exposure and privilege escalation

"Through 2024, organizations implementing a cloud security posture management (CSPM) and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%."

— Gartner

Arctic Wolf Provides the Human Element

Cloud security posture management products require continuous monitoring, reconfiguration, and remediation to be effective. The trouble is most IT departments are not equipped to handle the influx of alerts from yet another source of security telemetry.

This is where Arctic Wolf comes in. Security operations experts from your Concierge Security Team are paired with you to provide greater context into your cloud environment, identify gaps according to generally accepted configuration benchmarks, and provide you with posture hardening recommendations that strengthen your cloud security posture.

Why Customers Choose Arctic Wolf for Cloud Security Posture Management

Working with a customer in the financial services sector, the Concierge Security Team completed a CSPM scan and found a critical misconfiguration in the customer's environments (AWS, Azure, and GCP) not commonly identified by other approaches. This gap would allow all S3 buckets to be easily changed and enable further movement from bucket to bucket.

The CST worked with the customer to provide strategic guidance on how to address the exposure, and further harden their IaaS. Had this misconfiguration gone unnoticed, these S3 buckets could have easily been exploited — resulting in the potential exfiltration of sensitive information and exposure into the public domain.

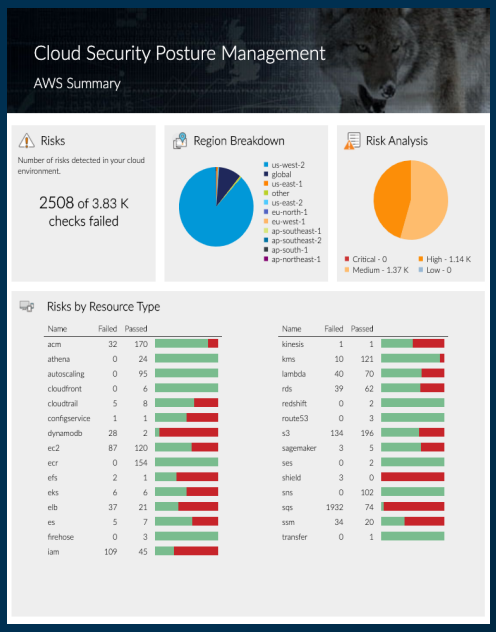

Figure 1: Sample CSPM report provided by the Concierge Security Team

About Arctic Wolf®

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, identity, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

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

SOC2 Type II Certified

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE