SOC-as-a-Service for Cloud Infrastructures and SaaS Applications

Comprehensive Cloud Monitoring

- AWN CyberSOC™ provides comprehensive monitoring for leading SaaS and IaaS platforms.
- Hundreds of alerting rules upon setup per platform, plus additional customization with the Arctic Wolf Concierge Security™ team.

SaaS Monitoring

- Office365
- Salesforce
- Box
- G Suite

IaaS Monitoring

- AWS
- Azure

SaaS Monitoring

- Users and access
- Admin activity
- Data sharing
- Platform-specific activities

Modern enterprises often use hybrid computing architectures that consist of both on-premises and cloud-based resources. A hybrid architecture makes it easier to conduct business but it poses new challenges in terms of security, which becomes a shared responsibility between cloud providers and enterprises. Providers are responsible for operational security and service reliability, while cloud customers are responsible for data security and how they use cloud services.

Attackers are well aware of the shared responsibility security model. Today, they increasingly exploit end-user confusion and security oversight, along with innate vulnerabilities in cloud deployments, to attack enterprises that naively believe they're secure.

Cloud systems, by nature, are especially vulnerable to threats such as unauthorized access and data loss:

Attack Category	Description/Examples	Cloud Vulnerability
Unauthorized Access	Malicious login activity for users and admins, admin settings changes, privilege escalations, logins from unusual international locations, phishing and credential theft	Cloud services are designed for access from multiple locations and come with support for multiple devices and operating systems, making them particularly vulnerable to unauthorized access.
Data Exfiltration	Data breaches, where attackers attempt to acquire sensitive data, such as personally identifiable information, intellectual property, etc.	Cloud systems enable remote access, data download, and ubiquitous mobility. 3rd party API access and OAuth token issues may expose sensitive data. Compromised mobile devices may also result in data loss.
Resource Misuse	Cryptocurrency mining, "cryptojacking," hackers exploiting corporate resources to provide services	Cloud instances are easy to create without authorization and control remotely. They often lack comprehensive visibility and native alerting.
Insider Threat	Human error, accidental data exposure, malicious insiders	Cloud platforms facilitate data mobility. Hybrid architectures rely on multiple platforms, and many cloud services enable easy creation of public-facing links.

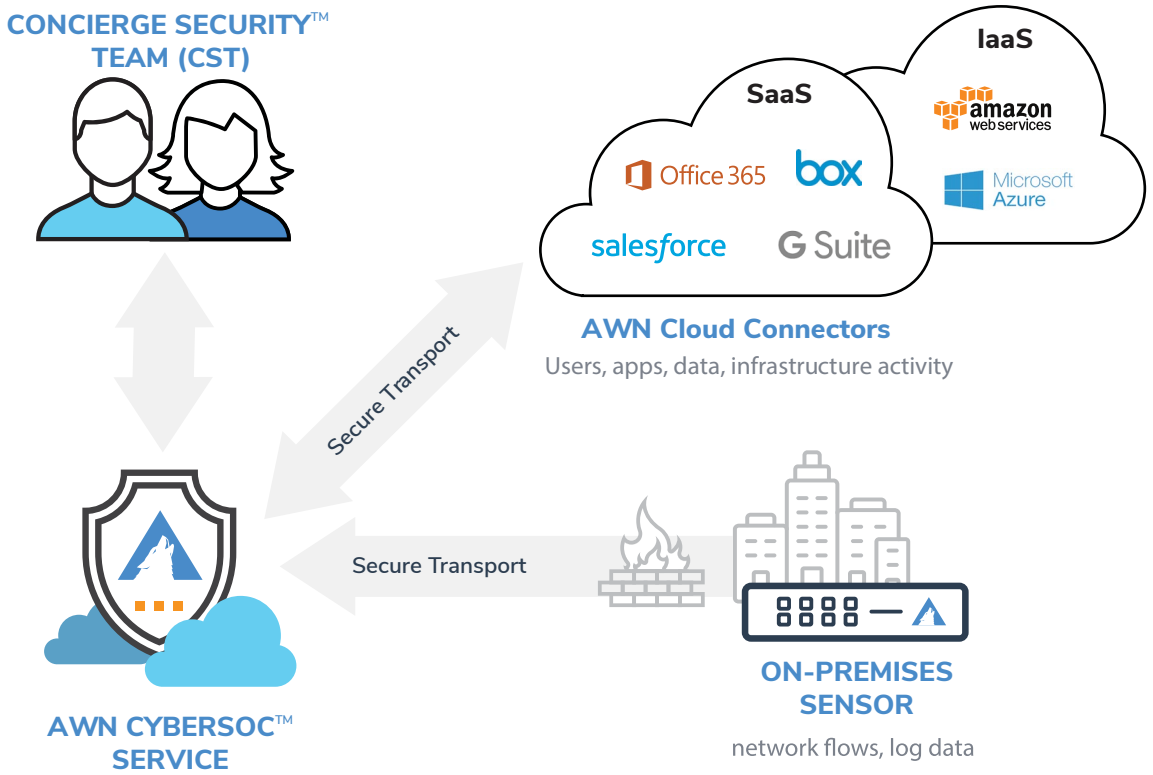
Because of these threats, cloud security is vital to defend hybrid IT ecosystems, and IT professionals need robust cloud security strategies to protect their companies. It is a mistake, however, to focus on cloud-exclusive solutions. That type of fragmented approach to security prevents centralized monitoring and exposes enterprises to even greater risks. Instead, enterprises need a centralized security monitoring solution that protects them across platforms, whether on-premises or in the cloud.

Arctic Wolf detects and responds to advanced threats targeting on-premises systems, infrastructure-as-a-service (IaaS) instances in AWS and Azure, and several leading software-as-a-service (SaaS) applications. Every customer gets a dedicated Concierge Security™ team that correlates activity across systems to deliver comprehensive security visibility and rapid threat detection.

Accelerate Monitoring of Your Cloud Services

In addition to monitoring on-premises environments, the AWN CyberSOC™ provides comprehensive visibility into use of your IaaS and SaaS applications to detect malicious activity. The Arctic Wolf cloud security solution provides:

- **24x7x365 continuous monitoring** to ensure business information uploaded to SaaS applications and infrastructure workloads on IaaS services remain safe
- **Single pane of glass across attack surfaces and common incident response framework** to centralize monitoring and correlate attacks across network infrastructure and data in cloud, hybrid, and on-premises environments, including SaaS applications, Active Directory, FW/IDPS, endpoints, email, switches, wireless APs, cloud workloads and more
- **Effective low-noise threat detection** via the Concierge Security team that sets customized rules to limit false positives from native events and identify threats specific to your environment and business
- **Regulatory compliance** for PCI DSS, HIPAA and SOX with expert support and custom and pre-defined reporting



Gain Visibility into Attacks Targeting Cloud Services

Detect suspicious activity in:

IaaS	SaaS
Supported Platforms	**Supported Platforms**
AWS	Office 365
Azure	Salesforce
	Box
	G Suite
Supported Alerts	**Supported Alerts**
Suspicious resource usage, access, and deletions	Modified administrator settings
Changes to profiles and access	Administrator privilege escalation
Brute-force logins	Resources accessed or altered
Concurrent access	OAuth token and API access changes
Blacklisted IP sign-in	Group privacy or domain changes
Hijacked admin accounts	SSO configuration changes
	Anomalous login activity
	Brute-force logins
	Concurrent access across geos
	Compromised mobile device activity
	DLP violations
	Changes to file and folder permissions

The Industry's Fiercest SOC-as-a-Service

A security operations center (SOC) is the most essential element of modern security. But a SOC is expensive to build, complicated to manage, and far beyond the reach of most small to midsize enterprises. So, many take the easy route and invest in new point security products, which is no guarantee of better protection. The cloud-based AWN CyberSOC™ service provides comprehensive 24x7 monitoring of both your on-premises network infrastructure and your cloud-native SaaS applications, such as G Suite. AWN CyberSOC differs from traditional managed security services, as it dynamically combines a world-class security team with advanced human-assisted machine learning and comprehensive, up-to-the-minute threat intelligence to protect you from known and emerging threats.

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com