

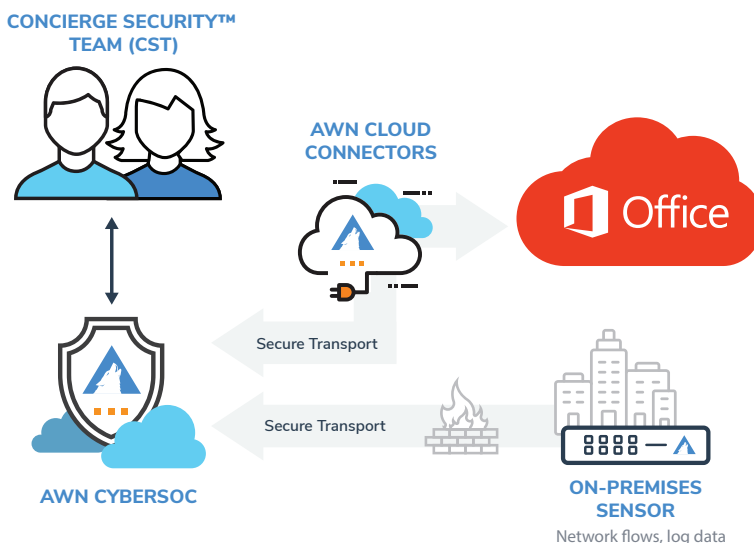
AWN CyberSOC™ Monitoring for Office 365

Arctic Wolf's Awn CyberSOC™ service detects and responds to advanced threats targeting your Office 365 SaaS application and helps you comply with regulatory mandates like PCI, HIPAA, and SOX. Every customer gets a dedicated Concierge Security™ team, which provides the security expertise you need to rapidly detect and respond to threats across your on-premises and cloud deployments.

Accelerate Monitoring of Your Office 365 Service

The cloud-based Awn CyberSOC provides comprehensive visibility into the utilization of your Office 365 service to detect malicious activity. Arctic Wolf's cloud security solution enables you to:

- **Secure your Office 365 SaaS Solution:** get 24x7 monitoring from the Awn CyberSOC service
- **Add Arctic Wolf security expertise:** Leverage the expertise of the Arctic Wolf Concierge Security™ team (CST) to serve as the trusted security advisor to your IT team
- **Optimize threat detection:** Office 365 events utilize the same Awn CyberSOC alerting framework as our on-premises detection, delivering greater flexibility and tuning for your specific environment and policies
- **Leverage detection that uses a unified view of your attack surface:** across both your on-premises network infrastructure and your cloud-based applications



Office 365 Visibility and Alerting

The Awn CyberSOC™ service provides comprehensive monitoring of Office 365.*

- 50+ alerting rules upon setup, plus additional customization with the CST
- Comprehensive monitoring
 - Active Directory
 - SharePoint
 - OneDrive
 - Exchange admin and mailbox
- Alerting rules for:
 - Authentication: users and access
 - Resource sharing
 - Mail and file operations
 - Mobile device administration
- Detailed reporting
 - Executive summary (overall view)
 - Usage reports (login activity, AD service events, exchange online service events, OneDrive service events, SharePoint service events, service administrative activity)

Office365 monitoring requires Awn CyberSOC

AWN CyberSOC™ Monitoring for Office 365

Gain Visibility into Attacks Targeting Your Office 365 Service

- **Detect suspicious Office 365 actions:**
 - Authentication settings modified
 - Anomalous sign-in activity, user account status
 - User password changes and resets
 - Unauthorized, geo-based access
 - Mailbox settings updates, inbox rule creation, etc.
 - DLP rule violations
 - Anonymous links to file resources, ACL updates
 - Resource downloads/uploads, renames, deletions, etc.
- **Detect unauthorized access of the Office 365 application (examples):**
 - Brute-force login attacks
 - Concurrent access from multiple geos
 - Download/upload sensitive data

Industry's Most Fierce 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 medium enterprises. So, many take the easy route and invest in security products, but investment in new point security products 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 Office 365 applications and data.

AWN CyberSOC differs from traditional managed security services. It is a dynamic combination of world-class Concierge Security™ teams (CSTs), advanced human augmented machine learning, and comprehensive, up-to-the-minute threat intelligence. Your CST conducts both routine and non-routine tasks to protect you from known and emerging threats.



©2018 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.



SOC2 Type II Certified

Contact us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

