




PERSONAL | PREDICTABLE | PROTECTION

Arctic Wolf Managed Cloud Monitoring for Microsoft 365

Arctic Wolf® detects and responds to advanced threats targeting your Microsoft 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 Microsoft 365 Service

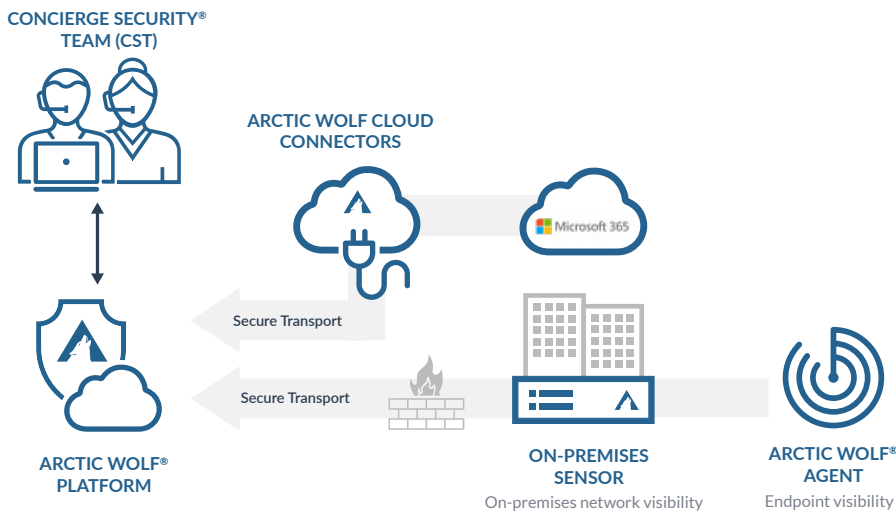
The cloud-based Arctic Wolf® Platform provides comprehensive visibility into the utilization of your Microsoft 365 service to detect malicious activity. The Arctic Wolf cloud security solution enables you to:

- 
Secure your Microsoft 365 SaaS solution
 Get 24x7 threat detection and response from Arctic Wolf Managed Cloud Monitoring
- 
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
 Microsoft 365 alerting uses standard and customized rules, tuned by your Concierge Security Team, delivering flexibility and specificity for your organization's environment, policies, and requirements
- 
Leverage detection that uses a unified view of your attack surface
 You have visibility across both your on-premises network infrastructure and your cloud-based applications

Microsoft 365 Visibility and Alerting

Arctic Wolf security operations provide comprehensive monitoring for Microsoft 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)



Arctic Wolf Managed Cloud Monitoring for Microsoft 365

Gain Visibility into Attacks Targeting Your Microsoft 365 Service

- ▶ Detect suspicious Microsoft 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

Continuous Cloud Monitoring Delivered by Our Concierge Security Team

As businesses everywhere move further into the cloud, they face new security challenges. Legacy security tools, such as firewalls, advanced endpoint protection, or SIEM appliances, cannot defend cloud workloads, and cloud vendors do not take responsibility for many key security areas. Businesses struggle to staff their teams with cybersecurity cloud experts. And the threat to cloud platforms is rising.

Built on the industry's only cloud-native platform to deliver security operations as a concierge service, Arctic Wolf® Managed Cloud Monitoring lets you detect cloud vulnerabilities and attacks as they occur, across multiple major cloud platforms. Your security operations expert from the Concierge Security® Team (CST) works directly with you, using their cloud security expertise to guide implementation, risk-surface identification, and ongoing cloud monitoring to enhance your cloud security posture. For more information about Arctic Wolf Managed Cloud Monitoring and our other security solutions, visit articwolf.com.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public



©2020 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.

AW_DS_CB_Microsoft 365_0620

AUTHORIZED
PARTNER



TECH HEADS