

Arctic Wolf Managed Cloud Monitoring for Salesforce

Arctic Wolf® detects and responds to advanced threats that impact your Salesforce instance and its data, and helps you comply with regulatory mandates like PCI, HIPAA, and SOX. With Arctic Wolf security operations, 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 Salesforce Applications and Data

The cloud-based Arctic Wolf® Platform provides comprehensive visibility into the use of your Salesforce application, and monitors its environment and operations to detect advanced threats. The Arctic Wolf cloud security solution enables you to:



Secure SaaS solutions: Arctic Wolf monitors your cloud environment 24x7 to detect unauthorized access or misuse of resources



Secure data across hybrid cloud architectures: Concierge Security Teams (CSTs) use a single pane of glass to track, evaluate, and improve security posture for both on-premises and SaaS applications



Add Arctic Wolf security expertise: Leverage the expertise of the CST, which becomes the trusted security advisor to your IT team

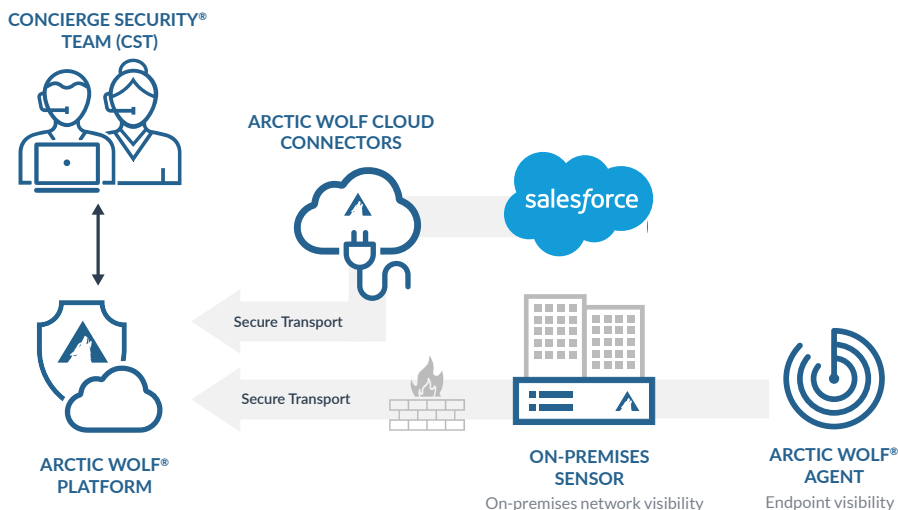


Gain a unified view of your attack surface: Protect both your on-premises network infrastructure and all of your cloud-based applications with the same service

Salesforce Visibility and Alerting

Arctic Wolf security operations provide comprehensive monitoring for SFDC

- ▶ 50+ alerting rules upon setup, plus additional customization with the CST
- ▶ Alerting rules for:
 - Password events
 - Login/logout attempts
 - Integration with third-party resources
 - Mobile device administration
 - SSO provider operations
 - Authentication factor activities
 - User and permissions updates
 - Authorization group changes
 - Resource access or alterations
- ▶ Detailed reporting
 - Executive summary (overall view)
 - Usage reports (login activity, mobile device administrative activity, API activity, authorization and authentication activity)



Arctic Wolf Managed Cloud Monitoring for Salesforce

Gain Visibility Into Attacks Targeting Your Salesforce Instance

Arctic Wolf Managed Cloud Monitoring enables you to detect and respond to the following types of SFDC events and alerts.

- ▶ Detect suspicious SFDC actions:
 - Authentication settings modified
 - Anomalous sign-in activity, user account status
 - User password changes and resets
 - Unauthorized, geo-based access
 - SSO provider changed or deactivated
 - Resources accessed or altered
 - Mobile devices added, deleted, or wiped
- ▶ Detect cyberattack vectors:
 - Brute-force login attacks
 - Concurrent access from multiple geos
 - Sign-in from blacklisted IPs

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_Salesforce_0620

AUTHORIZED
PARTNER

Contact Name
Email Address
Phone Number
Web Address