ARCTIC WOLF

Advance FINANCIAL 24/7

PERSONAL | PREDICTABLE | PROTECTION

CASE STUDY

## Company at a Glance

**Advance Financial** (af247.com) offers a variety of financial services through branch offices and online channels. It operates in more than 10 states across the country and handles sensitive customer data for loan processing and bill payment services. Because of this, it must satisfy compliance and regulatory requirements across multiple jurisdictions.

## Challenges

- Lack of visibility into security issues across all branch offices and online applications
- IT team lacked the in-depth security expertise to triage and analyze cyberthreats
- Time-consuming to report on financial regulations (PCI-DSS, GLBA)

## Results

- 360-degree visibility into anomalous activities across on-premises and online operations
- More than 3X savings compared to cost of doing it internally using other SIEM products
- Customized weekly and monthly updates using executive dashboards and reports

# Arctic Wolf Protects a Rapidly Expanding Financial Services Company

> "Arctic Wolf's security experts monitor our networks 24x7 and flag security incidents only when they matter, allowing our IT team to focus more energy around deployments and refining tools. On top of the tremendous cost benefits of the Arctic Wolf SOC-as-a-service, Arctic Wolf has provided better visibility and compliance across all our locations."
>
> — **Patrick Swint,** IT Director, Advance Financial

Advance Financial, founded in 1996, is a family-owned and operated financial services company based in Nashville. The company currently operates more than 80 branch locations throughout Tennessee and offers 24x7 online loan services in nine other states across the U.S. It was recently named to the Inc. 5000 list of the fastest-growing private American companies for the fifth year in a row.

Advance Financial provides a wide range of financial services both in their branch offices and online, which includes cash advances, check cashing, electronic wire transfer, bill payment, prepaid cards, free bill payment and money orders. In fulfilling these services the company processes sensitive customer data, such as personal identifiable information (e.g. social security numbers, drivers licenses), employment data and bank account information for loan processing, and bill payment services. For this reason, Advance Financial is required to continuously monitor its networks across all its locations to protect customer data from data breaches as well as satisfy several financial regulations.

## Protecting Customer Sensitive Data is Paramount

Advance Financial has a small IT team that is primarily responsible for deploying and maintaining financial applications used by its customers, in addition to managing the IT infrastructure used by its employees. Advance Financial's customers can walk into any one of its 80 physical branch locations to perform financial and eCommerce transactions using multiple online applications.

The company's security infrastructure includes a portfolio of point security products including antivirus on desktops, perimeter firewalls, cloud access service brokers (CASB), and web content filters.

However, this became a problem for Advance Financial's limited IT staff, as each of these security products generated millions of alerts. The team was overwhelmed, and they knew that security threats were being missed because they couldn't obtain actionable information as to who, what, when, and where the specific attacks were happening.

The team's primary problems were threefold:

- Lacked centralized visibility into alerts from multiple point security products, 120 servers, 700 endpoints, and more than 70 mobile devices deployed across on-premises and cloud infrastructure
- Limited expertise to triage and prioritize over 400 million security alerts/month and escalate the few security incidents that expose customer sensitive data
- Significant time spent generating customized reports to meet financial regulations (PCI-DSS and GLBA) and demonstrate compliance

Advance Financial considered building its own security operations center (SOC) with security information and event management (SIEM) products from other leading vendors. It soon realized it would be more than three times the cost of buying a SOC-as-a-service from Arctic Wolf, which could deploy quickly in addition to being far more affordable than building a SOC internally.

## Adopting SANS CIS Controls Improves Security Posture

The IT leadership team at Advance Financial was in the process of adopting SANS CIS controls as part of its roadmap when it first considered the Arctic Wolf SOC-as-a-service solution. During their review, it became apparent that the Arctic Wolf SOC-as-a-service helped provide visibility and customized reports for the following SANS basic CIS controls:

- **Continuous vulnerability management:** External vulnerability scans are run by the AWN Concierge Security™ Team (CST) on a regular basis to identify assets at risk and prioritize patching strategy in order to improve Advance Financial's security posture
- **Use of administrative privileges:** Arctic Wolf tracks use of administrative privileges by monitoring the Active Directory and system logs, and flags privilege escalations/misuse
- **Secure configuration of hardware and software:** The Arctic Wolf SOC-as-a-service also monitors configuration changes to all devices and systems in Advance Financial's IT infrastructure
- **Monitoring and analysis of audit logs:** Finally, the Arctic Wolf SOC-as-a-service, with its highly scalable cloud-based SIEM platform, can handle more than 400 million log records from over 80 company branch locations and Advance Financial's online services, and escalates only the handful of security incidents per week that really matter

Deployment was simple. The devices were placed inline as a redundant pair at company headquarters, where they run in a span configuration between Advance Financial's two datacenters. To do so required very little reconfiguration of the company's edge network appliances. Advance Financial now has critical security oversight of admin login attempts, cleartext password usage, and remote command auditing on perimeter firewalls. With Arctic Wolf's cloud monitoring capabilities, it is able to monitor usage of unauthorized SaaS applications (aka shadow IT).

## The Best Customizable SOC-as-a-Service

Arctic Wolf includes everything that Advance Financial sought in a SOC-as-a-service. With the help of a dedicated Concierge Security™ Team, Arctic Wolf provides the customized reports Advance Financial needs to easily meet its compliance requirements, and enables the financial firm to adopt SANS Basic CIS controls that improve its overall security posture and reduce business risks.



ARCTIC WOLF



SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com