ARCTIC WOLF

Planters Bank

PERSONAL | PREDICTABLE | PROTECTION

CASE STUDY

Company at a Glance

Planters Bank (plantersbankonline.com) is a full-service community bank with 13 locations in Kentucky and Tennessee. FDIC-insured with assets totaling more than $1 billion, Planters Bank offers a wide range of consumer and business banking services.

Challenges

- Lack of visibility into a diverse and distributed network
- Need to fulfill audit and regulatory compliance requirements
- Achieving 24x7 monitoring with constrained resources

Results

- IT team now has visibility across the entire environment
- Improved cybersecurity maturity demonstrated through the FFIEC Cybersecurity Assessment Tool
- Tailored reports communicate security posture for executive management

Planters Bank Grows Securely with Arctic Wolf's SOC-as-a-Service

> "We needed proactive insight into what happens on our network. Arctic Wolf raises our level of security awareness and provides valuable support that helps us quickly investigate suspicious behavior. And the service has made it easier to comply with FFIEC and FDIC requirements."
>
> **— Bruce McClure,** Vice President and Manager of Information Systems, Planters Bank

Secure Bank and Customer Information

Founded in 1996 and operating in western Kentucky and western Tennessee, Planters Bank has grown to over 175 employees and more than $1B in assets. The full-service community bank provides financial products and services to consumers and businesses through its 13 branches.

The bank's information technology (IT) team manages, secures, and monitors a diverse infrastructure that includes workstations, servers, firewalls, ATMs, and network infrastructure comprised of switches, routers, and WiFi access points. Planters Bank uses a layered defense strategy to protect bank and customer information, an approach that protects various bank systems and monitors for threats and anomalous activity. In addition, the bank works diligently to satisfy legislative compliance requirements found in the Federal Financial Institution Examination Council (FFIEC) guidelines. The Federal Deposit Insurance Corporation (FDIC) insures the bank and oversees compliance for these guidelines.

Improve Cybersecurity and Fulfill Compliance Obligations

Prior to considering a managed detection and response solution, Planters Bank had no comprehensive approach to holistically monitor infrastructure or glean security insights from log data generated by its various IT systems. While, the IT team had piecemeal systems in place to monitor specific systems and reviewed logs the next day, it knew it lacked visibility and risked missing dangerous threats. What's more, an FDIC examination also recommended that the bank seek ways to improve security monitoring. According to Bruce McClure, vice president and manager of information systems for Planters Bank, "We didn't have 24x7 coverage—we only monitored during bank business hours."

Initially, Planters Bank considered creating its own security operations center (SOC) in-house, complete with a security information and event management (SIEM) platform and associated software. "Planters Bank is a regional innovator for financial services and the IT team has to be forward-leaning to help enable that innovation. In evaluating security monitoring, we looked for a proactive approach to that would allow us to improve our security," explained McClure.

McClure and his team decided that an in-house SOC would be cost prohibitive in terms of both required staffing and necessary technology. Planters Bank then evaluated using a managed security service provider (MSSP) model, but found MSSP offerings lacked the depth of monitoring and threat detection expertise it needed. Next up, Planters Bank learned of the Artic Wolf SOC-as-a-service and its managed detection and response (MDR) approach to cybersecurity. The Planters Bank IT steering committee that included bank executives determined the Artic Wolf SOC-as-a-service was the best option to meet its ongoing challenges and ramp up its cybersecurity posture.

McClure explained the decision this way: "Instead of dedicating staff to tune a SIEM and review event logs all day, we chose to focus on IT projects that would help improve the bank's overall operations and security. We felt Arctic Wolf's approach would give us improved security monitoring and also free our team to focus on projects that are of higher priority and greater interest."

Elevate Bank Cybersecurity

The Artic Wolf SOC-as-a-service was deployed in early 2018 across the Planters Bank environment. "The deployment was quite smooth and straightforward," said McClure. "There were some small configuration tweaks, but nothing significant."

Arctic Wolf has provided Planters Bank with visibility across its environment and helped the bank improve its cybersecurity maturity as measured by the FFIEC Cybersecurity Assessment Tool that identifies risks and determines a financial institution's cybersecurity preparedness. The Artic Wolf SOC-as-a-service quickly identified malware activity and helped the bank's IT team confirm information wasn't transmitted from the compromised system. "We verified the malware had not replicated and that nothing was transmitted out of our organization," McClure said.

Arctic Wolf has enabled Planters Bank to achieve its security and compliance goals. "Arctic Wolf provides an independent set of eyes that is watching our environment," McClure said. "The Arctic Wolf Concierge Security™ Team and the Artic Wolf SOC-as-a-service reporting allow us to understand what goes well and what needs improvement going forward. While 'out-of-the-box' reports work in most cases, we also receive customized reports when we have specific reporting needs. This lets us effectively communicate our security posture to the board and stakeholders."

Implementing Arctic Wolf™ Managed Detection and Response for security monitoring meant Planters Bank could prune its technology. The IT team turned off Solarwinds Log and Event Manager, a syslog server, and open source tools that generated data and alerts but didn't add significant value for the team. According to McClure, "Arctic Wolf has reduced our time to get historical data. We no longer have to dig through logs for what we need. Instead, we go to the Concierge Security Team and they deliver the data."

In McClure's eyes Arctic Wolf has firmly delivered. "Arctic Wolf has helped us improve our security posture and is one of the best companies I've ever worked with. At Planters Bank we've evolved to become a $1 billion-dollar financial institution, and Arctic Wolf helps us continue on our growth path without having to over-invest in security headcount."