First United Bank & Trust

CASE STUDY

First United Bank & Trust "Banks" on Arctic Wolf for Security and Compliance

BUSINESS

First United Bank & Trust (www.mybank.com) is a full-service community bank with 25 branches serving customers in Maryland and West Virginia. First United provides personal and business banking services, as well as investment products and services.

CHALLENGES

- Lack of visibility into a diverse and distributed network
- Complex regulatory compliance requirements
- Constrained IT resources

RESULTS

- Comprehensive visibility across all resources supported by the IT team
- Improved compliance and cybersecurity maturity as measured by the FFIEC Cybersecurity Assessment Tool
- Tailored reporting to communicate security posture to all stakeholders

"Cybersecurity threats continually transform and mature. Arctic Wolf, however, delivers the tools and expertise to continually monitor our environment and alert on these threats. I rest easier knowing our operations are monitored 24x7 with the AWN CyberSOC™ service."

AJ Tasker, Vice President and Director of IT, First United Bank & Trust

Safeguarding Bank Information

First United Bank & Trust is a full-service community bank operating in Maryland and West Virginia that strives to deliver exceptional service to its customers and community. It has 375 employees and nearly $1.4B in assets and provides financial products and services to consumers and businesses through its 25 branches. The bank's information technology (IT) team manages and monitors a diverse infrastructure that includes workstations and servers, as well as ATMs and network infrastructure with a variety of switches and routers.

The bank takes a progressive, "defense-in-depth" approach to cybersecurity to secure bank assets. In addition, the bank works diligently to satisfy legislative compliance requirements that include the Graham-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX), which are part of the Federal Financial Institution Examination Council (FFIEC) guidelines. These FFIEC guidelines for the bank are overseen by the Federal Deposit Insurance Corporation (FDIC).

A Dual Mission: Improve Cybersecurity and Fulfill Compliance Obligations

In 2015, First United had no solution to holistically monitor its infrastructure and detect threats. It knew it needed round-the-clock security monitoring, but that it lacked the 24x7 IT staff required to achieve an optimal security posture. Research and industry trends led First United to seek solutions to improve monitoring and retain log information. According to AJ Tasker, Vice President and Director of Information Technology at First United Bank & Trust, "We needed some way to centralize our logging and also spot anomalous activity that might pose a threat. We recognized that it was crucial to monitor 24x7, around the clock."

First United created a team of executives, IT personnel, and risk management staff to evaluate a variety of security monitoring options. As Tasker explained, "We wanted visibility across our infrastructure. We wanted to identify behavior like privilege escalation or anomalous scanning that might be reconnaissance by bad actors."

First United looked at a number of security information and event management (SIEM) technologies that could be deployed on-premise, but on further investigation found the SIEM approach to be prohibitively costly in software and hardware investments. In addition, there would be significant costs to bring in the necessary staff to manage and monitor it properly. As Tasker described, "SIEMs have a downside in false positive alerts, and we would not have been able to easily hire the two or three additional members to deploy and run a SIEM, and deal with all the fine-tuning involved."

The bank soon discovered that a security operations center (SOC)—with all the required technology, staff, and processes—was needed to continuously monitor its environment, but doing so in-house presented significant challenges. After considering its options, First United decided to outsource some of these responsibilities and go with Arctic Wolf's SOC-as-a-service.

Improving Its Cybersecurity Posture

First United deployed Arctic Wolf's AWN CyberSOC™ service in late 2015 and has leveraged the service to progressively improve its security posture and cybersecurity maturity. As Tasker highlighted, "Having Arctic Wolf in place has allowed us to check numerous compliance boxes. According to the FFIEC Cybersecurity Assessment Tool (CAT) used by financial institutions, we rose another maturity level following the Arctic Wolf deployment."

The AWN CyberSOC provides a high-fidelity threat signal to scale back threat "noise" that comes in the form of false positive alerts. Yet, it also provides flexibility to adapt to different customer needs. While the strong threat signal has helped First United improve its security over time, the bank found that it needed to increase the volume of alerting following periodic penetration testing, so it received all alerts needed to deliver its security posture. Tasker said, "We tweaked the notification priorities so the AWN CyberSOC delivers alerts based on what is uniquely important to First United. Things that others might consider low priority are high priority for us. We were able to iteratively tune the alerting to get exactly what we need."

As far as the reporting provided by the AWN CyberSOC, Tasker said, "We tailored it to meet our needs. Arctic Wolf provides data and statistics that the security committee uses to make decisions, and which also helps us explain our security posture to the board."

Tasker describes his team's rapport with the Arctic Wolf Concierge Security™ team this way: "Arctic Wolf consistently communicates with us around future plans, roadmaps, and—most importantly—cyber events. If administrator accounts get locked out, we are notified and can check with the owner of the credentials to ensure it wasn't a malicious actor. We now see anomalies immediately, so we can quickly take action and if something critical happens outside of typical business hours, Arctic Wolf is on it."

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com