CASE STUDY

Arvest Bank Automates Threat Response with Cyber Fusion

ABOUT ARVEST BANK

Headquartered in Bentonville, Arvest Bank is the oldest bank in Arkansas and one of the largest in the U.S. Arvest remains committed to its customers above all else—which includes protecting them from fraud and cyberattacks.

Facing a torrent of cyberattacks daily, many targeting mortgage transactions, Arvest Bank sought to better align the aggregate efforts of security, fraud prevention, and IT, while automating key processes to alleviate analyst burdens.

Financial services organizations are targeted by cyberattacks more than any other industry. Attackers typically target attractive financial data, including mortgage transactions.

> *With so much at stake, cybersecurity and fraud prevention are a top priority for Arvest Bank. Cyware helps bridge inter-team silos by consolidating the entire SecOps infrastructure into a single pane of glass for delivering unified, automated threat response with centralized threat visibility, analysis, and control.*
>
> Sajan Gautam, CISO at Arvest Bank

Arvest's Journey to Cyber Fusion

CHALLENGES

- Disconnected tools, processes, and workflows
- Lack of centralized visibility, threat management, and analysis
- Slow incident resolution

CYWARE SOLUTIONS

- Respond (CFTR)
- Intel Exchange (CTIX)
- Orchestrate

TOP OUTCOMES

- Enhanced collaboration
- Greater visibility
- Reduced MTTR
- Reduced risk

Arvest's Journey to Cyber Fusion (continued)

To ensure proactive threat defense and eliminate duplication of efforts and tools, Arvest sought to leverage collaboration, automation and enhanced visibility to help manage threats, responses, and actions and opted to implement Cyware's Fusion Center with three of its modules including:

Orchestrate

Respond (CFTR)

Intel Exchange (CTIX)

Together, these products allow Arvest's threat intelligence, security operations, and incident response teams to freely collaborate and access the tools, functionality, and information to analyze data, track actions, and proactively defend against cyberattacks and fraud.

The team also developed automated playbooks for key use cases, including phishing and ransomware response, brand protection, third-party risk monitoring, and account compromise. Arvest now has hundreds of workflows fully automated, with many more in progress.

Beyond full automation, orchestration, and case management across incidents, vulnerabilities, malware, and threat actor investigation/remediation, Arvest has realized significant time savings by automating incident enrichment and responding to all kinds of cyber threats through a single platform.

Cyware's CISO dashboard allows any CISO to view how each tool, threat intelligence feed source, and vendor performs over time and how effectively each security team is operating to protect the bank and its customers.

In conclusion, Cyber Fusion helped Arvest to realize significant savings by automating incident enrichment and delivering outcome-driven and highly scalable security operations.

Cyware made a difference by:

- **Unifying security processes and teams by providing collaboration tools and centralized analysis, case management, and threat response.**
- **Enabling scalable security automation, informed with complete data visibility to force-multiply capabilities and accelerate threat investigation.**
- **Operationalizing the enrichment and automation of high-fidelity contextual and predictive threat intelligence to assist with proactive threat mitigation and smarter decision-making.**
- **Amplifying security efficacy by ensuring complete data visibility into all assets, users, vulnerabilities, and malware investigation analytics to yield intelligent orchestrated responses.**

Cyware

111 Town Square Place Suite 1203,#4
Jersey City, NJ 07310
855-MY-CYWARE
sales@cyware.com | cyware.com

ARVEST