ATTACKIQ

Industry Brief

The Financial Industry Protects Client Assets with AttackIQ's Security Optimization Platform

The Financial Industry Challenge

Organized crime and hostile nation-states continue to invest in new malware tools and techniques to compromise financial networks. These attackers will do whatever it takes to steal financial assets, intercept financial transactions, acquire customer identity data, and capture financial data of almost any kind.

The data speaks for itself — the banking and financial services industry has consistently been one of the top targets for cyberattacks. In 2019 the financial services industry was, in fact, the most targeted sector in the majority of countries around the world. Over 21 percent of sensitive files in financial services firms were exposed — this is larger than any other industry other than manufacturing, which was the same. The banking industry had the most substantial financial toll from cybercrime, costing an average of $18.3 million per company surveyed.

It has been estimated that financial organizations worldwide may lose from $100 billion to several hundred billion dollars annually from cyberattacks. The banking and financial industry experienced approximately 7.33 percent of all data breaches in 2019. This included the breach of over 100 million sensitive records. The financial sector also had the highest percentage of confidential personally identifiable information (PII) records exposed at 61 percent in the United States.

The internet has provided cybercriminals with unprecedented access to banks around the world. The digital transformation continues to bring new vulnerabilities to financial organizations. The mix of on-premise, cloud, and SD-WAN-connected remote facilities has required an increasingly complex set of differing security stacks for adequate defense and threat mitigation. New technologies for mobile payment systems have also substantially increased their risk footprint. All of this complexity just gives cyberattackers more potential vulnerabilities to exploit.

Financial payment networks like the Society for Worldwide Interbank Financial Telecommunication (SWIFT) have been targets of cyberattackers since 2015. Many millions of dollars have been defrauded. These cyberattackers understand bank operations and can often remain resident for months within the bank networks after penetration, observing bank operations and the process used internally for applications such as financial payment transfers.

SWIFT is like any other financial application. While the application itself may be secure, if an attacker has penetrated the network and can observe traffic and capture and intercept authentication data, application security is irrelevant. Automated teller machine (ATM) networks have been targeted for years, and attacks against them continue to succeed. Once an attacker is within the network and can observe network traffic undetected, all applications on that network become vulnerable.

Leading Financial Services Institutions Implement Attack IQ's Security Optimization Platform

A Leading Bank in Asia.

This leading bank uses the AttackIQ Security Optimization Platform to secure its banks and facilities in over 15 markets globally, including Hong Kong, Singapore, India, and Taiwan. This bank is large and growing, and it places continued emphasis on securing the information technology assets and customer information used by its over 20,000 employees. This bank manages over $400 billion in assets and delivers a full suite of commercial and consumer banking services within its target markets. It has received multiple awards for excellence, corporate responsibility, and overall bank services within its target markets.

A Leading Bank in the United States with Operations in Asia.

This leading bank secures its domestic and international banking operations by using the AttackIQ Security Optimization Platform. With over 100 locations in the U.S. and many more in Asia, it facilitates essential trade and commerce for both consumers and commercial customers. This bank has received multiple awards from partner banking networks for excellence in processing and quality recognition.

A Leading Global Financial Services Firm.

This leading financial services firm secures its investment management and banking services by using the AttackIQ Security Optimization Platform. It continues to innovate and deploy industry-leading digital platforms to serve its clients and partners. Its headquarters is in the United States, but it has many other offices and operating facilities in Europe and Asia. It works diligently to secure its operations and customer data. It regularly performs red team testing and employee education in addition to validating its security controls to improve defense resiliency and reduce risk.

Security Control Performance Must Improve

Sponsored by AttackIQ, in 2019, the Ponemon Institute surveyed 577 IT and IT security practitioners in the United States who were knowledgeable about their organizations' IT security strategy and tactics. This survey included leaders in financial services from banks, brokerage, and other important financial organizations. These leaders were also involved in evaluating or responsible for their organizations' technology investments. These were the summary results of this important survey:

- 53 percent of these experts admit that they don't know if their security controls are working as they expect to protect the network;
- 45 percent say they do not know all of the gaps in their security posture;
- 63 percent reported that they had observed a security control indicating it blocked an attack when it failed to do so;
- 31 percent have no set schedule for penetration testing; and,
- 68 percent find that continuous security validation is effective in finding gaps and mitigating the risk of a data breach.

The Solution for Financial Services

Security Optimization

AttackIQ's Security Optimization Platform is a leading offering for the financial services breach and attack simulation (BAS) market. Our platform supports the automation and operationalization of the MITRE ATT&CK® framework. This gives financial services a powerful capability to continuously test, measure, and validate the performance of security controls, personnel, and processes against the tactics and techniques in the MITRE ATT&CK framework.

AttackIQ's Security Optimization Platform uses MITRE ATT&CK to simulate the full attack chain against enterprise infrastructure. AttackIQ delivers continuous and objective measured validation of financial services enterprise security programs. You can find the performance gaps, strengthen your security posture, and improve your incident response capabilities. AttackIQ's Security Optimization Platform assesses readiness and validates that your enterprise security systems are performing as originally intended.

According to a 2020 presentation by Jon Oltsik, Senior Principal Analyst and Fellow at ESG, a typical enterprise may utilize 10 to 75 or more security controls across the security organization, often with significant overlap and redundancy. The sheer number of cybersecurity vendors and unique security controls can become overwhelming in a large organization burdened by regulatory and compliance demands. For most of these enterprises, it is unclear how well these security controls work and what areas and gaps require additional investment. AttackIQ's Security Optimization Platform helps you develop a smart strategy, validates that you have a resilient security control architecture, and objectively supports your budgeting decisions.

Leading Financial Services Institutions Implement Attack IQ's Security Optimization Platform

A Leading Hedge Fund.

This leading hedge gains much better visibility into the operations of its cyberdefenses by using the AttackIQ Security Optimization Platform. The hedge fund has billions in assets under management and over 1,000 employees located in offices around the world. Its portfolios are complex, developed with proprietary techniques, and managed carefully with proprietary risk management techniques. Over the past few years of increasing cyberthreat activity, it was deemed critically crucial by this hedge fund that it becomes better equipped to accurately and objectively assess the performance of its security controls, personnel, and related processes. It felt that a breach and attack simulation (BAS) system operationalizing MITRE ATT&CK® would best enable it to reach these goals. After considerable review, this leading hedge fund chose the AttackIQ Security Optimization Platform to support its efforts.

Financial Services Use Cases Improve Defenses, Reduce Risk, and Deliver Return on Investment

Security Control Technology Validation.

Security Control Technology Validation is used to measure security control efficacy based upon the expected technical capabilities of the security control. Security control technology validation starts with the technology — not the threat. It provides a technology-centric approach to validating that specific controls provide the expected protection capabilities as expected as they are currently configured and optimized for your production environment.

Security Optimization (cont.)

Often existing security controls are not configured or integrated correctly with the security ecosystem. AttackIQ's Security Optimization Platform can identify potentially costly misconfigurations that could be found and targeted by malicious actors. In any scenario, your cyberdefense will not work if the security controls do not perform as you expect. AttackIQ's Security Optimization Platform will enable you to rapidly operationalize MITRE ATT&CK and get the most from the security controls, personnel, and procedures you have today.

AttackIQ's Security Optimization Platform brings scale and flexibility for the largest financial services organization. AttackIQ automation enables the platform to work autonomously and to scale. This includes support for live production environments — even the small changes to configurations or administration can open new vulnerabilities in your cyberdefense. This helps identify and close the ever-present gap between financial services test environments and the live production environments that, undetected, will ultimately compromise the entire organization.

The AttackIQ Security Optimization Platform will also help you improve your total security program by ensuring that existing production investments are measured and monitored from a threat-informed perspective. The MITRE Corporation coined the term "threat-informed defense" as it made the MITRE ATT&CK framework operational. As MITRE says, a threat-informed defense strategy "applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks." MITRE ATT&CK is a foundational framework for testing your security against known threats. Only with accurate data about your team's performance against real-world threats can you make informed decisions to optimize your security program.

Financial Services Use Cases Improve Defenses, Reduce Risk, and Deliver Return on Investment

Purple Teaming.

Purple teaming uses a methodology that fosters and supports collaborative communication between the red and blue teams. Purple teaming enables the blue team to participate in the security assessment of its people, process, tools, and technologies while fostering agreement and the sharing of threat intelligence, testing methodology, findings, and remediation recommendations. Successful purple teaming helps the entire cybersecurity operations organization rapidly and efficiently improve cyberdefenses.

Threat Emulation.

Threat emulation enables organizations to safely emulate adversarial behavior, while empirically proving the existence and effectiveness of security controls and exposing gaps within the cybersecurity defense architecture. Cyberdefense teams can then provide evidence of current capabilities and best use existing resources and team members to optimize security control defenses. Threat emulation is driven by adversary and attack intelligence and a threat-centric viewpoint, an essential part of threat-informed defense®.

ATTACKIQ

U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with the MITRE Center of Threat Informed Defense.

For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.