ATTACKIQ

Industry Brief

The Healthcare Industry Secures Sensitive Data with AttackIQ's Security Optimization Platform

The Healthcare Challenge

Over the past few years, and especially during the COVID-19 crisis, healthcare continues to be a major target for cyberattacks worldwide. In 2019, major healthcare data breaches in the United States grew at a record rate of 90.18 percent to a total of 310 events attributed to "IT/Hacking." These breaches include the compromise and theft of over 38 million patient records, a substantial increase from the 9.9 million patient records breached in 2018. The estimated population of the United States in 2019 was 329 million, so as much as 11.5 percent of the U.S. population may have been impacted due to these data breaches, assuming no overlap in the compromised medical records.

Cyberattackers target our major healthcare institutions today for all of the same reasons as in years past. Economic gain through extortion and theft of intellectual property is in the center of the bullseye. Medical records are lucrative to steal because cyberthieves can use them to facilitate credit card fraud, identity theft, and much more. Medical records sell in bulk on the dark web, which is highly attractive to organized crime because it dramatically reduces their risk of being identified in the transaction.

The rise of targeted ransomware has hit healthcare institutions hard. Since 2016, a total of 172 ransomware attacks have cost U.S. healthcare organizations a total of $172 million. This attack vector makes it easier and faster for organized crime to gain access to profits, as there is no need to post and sell the records, at least initially. In some cases, cybercriminals have extorted well over $1,000,000 in ransom from a targeted hospital and could then take their time selling of any medical records they stole during their access to the hospital's internal networks. Untraceable cryptocurrency payments make ransom easy and convenient.

Healthcare networks are complex and present more vulnerabilities for attackers to exploit. The Internet of Things (IoT) connected medical devices are part of the problem. Medical devices are virtually everywhere in the healthcare ecosystem. Every hospital, nursing facility, surgical center, MRI center, medical group, diagnostic lab, and physician's practice typically has multiple medical devices within its networks. Hospitals beds may have as many as ten to fifteen connected medical devices each, and intensive care units have many more. According to a survey of 700 security decision makers, 82 percent of healthcare organizations have experienced an IoT-focused cyberattack. The great majority of the commercial cyberdefense currently deployed in the healthcare industry is not able to detect attackers within these medical devices.

Medical devices are, by definition, FDA approved and, thus, closed devices. You cannot modify their internal software or load your endpoint software without the risk and liability of potentially harming patients. The FDA regulations don't allow it. This leaves medical devices wide open to attack. You have neither visibility into their internal operations nor any ability to efficiently remediate malware, even when you find it, other than by having the manufacturer reload all of the device software. Once malware moves through hospital networks, even if eliminated from most endpoints by your standard security software suite, it can still infect medical devices and then establish command and control from within the medical device.

Leading Healthcare Institutions Implement Attack IQ's Security Optimization Platform

A Leading Nonprofit Health System.

This leading faith-based nonprofit health system uses the AttackIQ Security Optimization Platform to secure its hospitals, outpatient facilities, and physicians groups. With more than 20 hospitals, 50 outpatient facilities, 5000 physicians, and 15,000 employees, it is one of the largest health systems within its state. Excellence in patient outcomes is important for it — it has been consistently ranked as one of its state's best hospitals for both quality and safety for several years. It has also been selected as one of the best workplaces in its state by Fortune Magazine and has won awards for its effective use of information technology systems to improve patient safety and outcomes.

A Leading Integrated Healthcare Services Provider.

This leading provider of integrated healthcare services uses the AttackIQ Security Optimization Platform to secure its rehabilitation hospitals and home health agencies. It operates more than 100 hospitals and 200 home health facilities across the United States. It has been selected as one of Fortune's 100 Best Companies to Work For.

A Leading Healthcare Insurance Provider.

This leading non-profit healthcare insurance agency uses the AttackIQ Security Optimization Platform to secure its information technology assets and PII data. This includes more than 20,000 healthcare providers in its state, 10,000 employer groups, and 3 million members. It is committed to member advocacy, access to quality care, and empowering members to lead healthier lives.

The interconnected ecosystem in healthcare is huge; this brings more vulnerabilities. A single network may link physician practices, hospitals, ambulatory physicians, MRI and CT scan centers, eye surgery centers, general surgicenter, physical therapy, dialysis centers, skilled nursing facilities (SNFs), short and long term care facilities, and more.

Finally, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) brings considerable compliance oversight to protecting personally identifiable information (PII). HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH) make it clear that healthcare management must rigorously address the protection of patient data, perform regular risk analysis, and institute strict controls around data privacy and security. Significant and onerous penalties may accompany the investigation following a major data breach.

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 organization's IT security strategy and tactics. This survey included leaders in healthcare from hospitals and other important healthcare 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 actually failed to do so;
- 31 percent have no set schedule for penetration testing; and,
- 68 percent find that continuous security validation is effective or very effective in finding gaps and mitigating the risk of a data breach.

The Solution for Healthcare

Security Optimization

AttackIQ's Security Optimization Platform is a leading offering for the healthcare breach and attack simulation (BAS) market. Our platform supports the automation and operationalization of the MITRE ATT&CK® framework. This gives healthcare 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.

Healthcare 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.

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 important part of threat-informed defense®.

Security Optimization (cont.)

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 healthcare 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 really 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.

Often existing security controls are not configured correctly or integrated properly 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 healthcare 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 healthcare 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 term "threat-informed defense" was coined by the MITRE Corporation 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.

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.