ATTACKIQ®

Case Study

Major General Insurer Boosts Cybersecurity Readiness Across a Broad and Diverse Infrastructure

A fast-growing global insurer has rapidly expanded through acquisition. This emphasis on mergers and acquisitions (M&A) has proved a successful business strategy. It has also increased complexity within the organization. Many of the global insurer's business units operate with a significant level of independence, even in the realm of IT security.

"Our business consists of multiple companies with multiple controls, and in some cases there's a lack of uniformity in those controls," says its director of information security. *"For example, when I took this role, the company was running eight different antivirus solutions, all with different policies. One of my main objectives from the beginning was to build a more defensible architecture in which everyone is in sync."*

Complexity Breeds Opacity of Security Effectiveness

Each of the company's lines of business has its own security organization, run by a CISO who reports up to the global corporate CISO. The divisional CISOs are responsible for compliance, audit, and cybersecurity risk management throughout their business unit. The director's team, which also reports to the global CISO, has responsibility for threat detection and incident response across the entire company.

"We manage all alerts, follow up on security incidents, and triage impacts," he says. *"Our team is like a managed security service provider (MSSP) inside of the company. Our customers are the various security teams within the business units. In addition to incident response, we provide reporting to our customers, and we escalate to them infrastructure changes that are needed to improve company security."*

The global insurer outsources red team testing, with the director's information security team coordinating those assessments. But the insurer also needs frequent feedback on the effectiveness of security controls. For the information security group, up-to-date visibility into the company's diverse infrastructure is key to being prepared for prospective incidents. That's why they began looking for a breach and attack simulation (BAS) software solution.

"We needed to be able to validate controls," he says. *"We needed to better understand which threats will get through and which will be blocked in every part of the organization. A business unit security team might say they're locking down a certain type of traffic, but I'd rather run a test and know for sure. We also saw testing as key to understanding where there were gaps in our team's coverage — where an attack might not result in a notification to us."*

> **"For companies doing M&As, it doesn't make any sense to not use a technology like AttackIQ."**
>
> — Director of Information Security, Global Insurer

CUSTOMER

Global Insurer

LOCATION

United States

INDUSTRY

Insurance

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Control Auditing
- Investment Decision Support
- Mergers and Acquisitions

PROJECT BUSINESS IMPACT

- Supports recommendations around threat mitigation, potentially including investment in new security tools
- Enables internal incident response team to prepare more effectively for prospective attacks
- Ensures that all acquired companies meet corporate security standards

A New Approach to Control Validation

Frequent manual testing throughout the global insurer's 100-plus locations was not feasible for the small team. They needed to automate control testing, so they evaluated several BAS systems that could simulate real-world attacks. Their due diligence revealed that the AttackIQ Security Optimization Platform provides accurate assessments of security control effectiveness. They also liked the AttackIQ software-as-a-service model. *"Being able to roll out agents, then pull back and redeploy if needed, was the big selling point for AttackIQ,"* the director says.

The corporate information security team rolled out the Security Optimization Platform with an aggressive approach to assessments. *"We ran very intensive attacks to see how far they could get in the organization,"* he says. If the team heard about a new tactic that attackers were using, they would try to emulate the full-scale ransomware or malware attack. They soon shifted gears.

"In many cases, it does not make sense to run such large attacks, because they might reveal an overwhelming list of changes we need to make," he says. *"Instead, we decided to focus on smaller wins, on making it more difficult for an attack to run from beginning to end. We pivoted to evaluating how our security infrastructure stacks up with regard to specific pillars in the MITRE ATT&CK framework."*

> **"The fact that I can roll out an agent on a machine in one of our offices, run a test, and see whether that particular area of the network is blocking a specific threat is invaluable. And it's so much more efficient to do it with AttackIQ."**
>
> — Director of Information Security, Global Insurer

The information security team focused on early stages of execution, such as privilege escalation and defensive evasion techniques. They ran the same assessments within every business unit, then compared the results. *"For example, if one group was blocking a UAC [user account control] bypass attempt, while other groups weren't blocking it, we would talk to the teams to figure out what made the one group successful,"* he says. *"The results of these narrower tests are actionable throughout the different business units."*

Better-Informed Defense and Response

The global insurer has used the Security Optimization Platform for the past two years, and automated testing through the AttackIQ solution is central to the company's cybersecurity readiness planning.

The director's team runs weekly assessments, testing scenarios focused on specific control sets across every business group's unique infrastructure. They prioritize controls for testing based on external threat intelligence and guidance from the group CISOs. They have standard expectations for how security solutions should respond companywide — for instance, firewalls that are properly configured should prevent certain types of outbound communications.

"Throughout the year, we're continuously performing control validation tests," he says. *"The results from these tests are automatically sent out to the CISOs and our SecOps team which gives us instant visibility into the gaps in our preventative and detective controls. If our systems don't prevent an attack, or even alert on it, we can take appropriate action."*

Better-Informed Defense and Response (cont.)

In some cases, the assessment results identify configuration issues with security tools. *"If there's a proxy bypass that we're blocking across the board, and we see it open in one part of the organization, we know that group's controls aren't configured properly,"* he says. In other cases, closing a control gap might require investment in new solutions — and the assessment results may be a powerful resource in building the case for funding.

"AttackIQ has done wonders in terms of giving us a clear picture," the director says. *"One CISO responded to the results of a test and said, 'I don't believe this.' We got some engineers to perform an independent validation and, sure enough, the AttackIQ results were correct. Having assessment data at my fingertips is very useful when I need to push a team to take certain actions."*

The director's team also uses the Security Optimization Platform to validate that the business units have taken appropriate corrective action. *"They might think they've successfully closed a control gap,"* he says. *"We can prove whether that's true; we don't have to take their word for it. Without AttackIQ, it would be possible for my team to do that, but it would be extremely time-consuming. They would have to reach out to the end user support team, get a machine on the network in question, then run the attack and see whether it succeeds. With Attack IQ, we just push a button to re-run the test that revealed the problem in the first place."*

Security Standardization and M&A

The automated assessments benefit the incident response capabilities of the director's team. *"If we ever were to fall victim, the information coming out of these tests would help us understand whether the threat was real,"* he says. *"Thanks to the Security Optimization Platform, we know what capabilities and policies we have, what's allowed and not allowed in different parts of the company. So if something were to happen, we would know how to work our way through the incident."*

They use the results of the assessments to update their playbooks for specific types of attacks, as well as to support risk management teams in compliance and cybersecurity insurance processes. *"We try to get out in front of the exploits that are known out in the wild,"* he says. *"A lot of times, when there are news stories around cybersecurity events, our internal customers are quick to check on whether we're prepared for those threats. We're usually already a step ahead of them."*

"AttackIQ has done wonders in terms of giving us a clear picture. Having assessment data at my fingertips is very useful when I need to push a team to take certain actions."

— Director of Information Security, Global Insurer

His team is also using information from the assessments to build companywide security standards. *"We give guidance to all the teams,"* he says. *"Because of the complexity of our infrastructure, we are focused on getting our arms around shadow IT. The fact that I can roll out an agent on a machine in one of our offices, run a test, and see whether that particular area of the network is blocking a specific threat is invaluable. And it's so much more efficient to do it with AttackIQ."*

Security Standardization and M&A (cont.)

These capabilities are especially critical considering the company's ongoing M&A strategy. After an acquisition, he says, *"we immediately work to build visibility into their security systems and processes, we make sure their teams understand our standards for setting up a defensible architecture, and then we validate that they are following through."* He adds, *"For companies doing M&As, it doesn't make any sense to not use a technology like AttackIQ."*

In fact, he concludes, *"security teams that aren't doing any control validation — any breach and attack simulation — have a serious gap in their visibility. Companies like ours, where different business units have different controls in place and maybe different security technologies, need insights into where each organization stacks up. Breach and attack simulation software is a good way to ensure that you're well-positioned to respond to an actual attack."*

ATTACKIQ

U.S. Headquarters
171 Main Street Suite 656
Los Altos, CA 94022
+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 identify 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 MITRE Engenuity's Center for Threat Informed Defense.

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