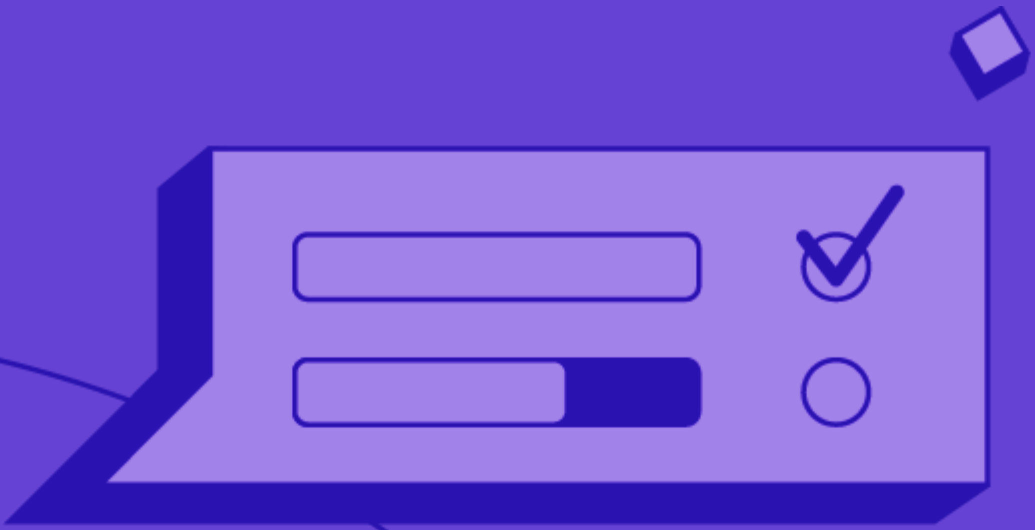
ATTACKIQ®



Case Study

Building Confidence in Security Effectiveness Across a Fortune 500 Retailer's Complex Global Infrastructure

Fortune 500 retailers have, by nature, an extremely broad attack surface. From the network that supports corporate functions around the world to the e-commerce infrastructure to thousands of stores, both domestic and international, a wide range of entry points exist for an individual with malicious intent. As the frequency of ransomware and other cyberattacks escalates, these companies' security teams are increasingly under the gun.

One large digital-first retailer uses a range of best-of-breed security solutions, managed and tested by both internal and external experts, to mitigate the risk. *"Ransomware is a huge priority for us,"* says the company's Director of Security Operations. *"Just watching the news makes it clear that getting our hands around our potential exposure is crucial. Our organization has several security teams, including an in-house penetration testing team, and we also bring in third-party red teams to take a different perspective and make sure we're validating everything we can."*

When the director joined the retailer about a year ago, he was confident in the security infrastructure that it had in place. However, he also wanted a more efficient control validation process.

"I saw an opportunity for an automated attack simulation tool to help us scale up control testing," he says. *"I wanted to establish baselines and then verify through repetitive testing that all our environments around the world meet the same standards. Even with our substantial security staff, it wasn't possible to do that comprehensively with individuals wading through boatloads of logs."*

Why AttackIQ?

The director and his team began evaluating breach and attack simulation (BAS) tools. They considered eight solutions, viewing vendors' slide decks and user interfaces, and doing external research. In addition to offering control validation at scale, the solution the security team sought needed to integrate with the company's SIEM and IDS solutions. Once they narrowed the choices down to a shortlist, the team conducted a hands-on, apples-to-apples proof of concept (POC).

In this testing, the director particularly liked the interface of the AttackIQ Security Optimization Platform, which provides visibility to testing companywide and categorical buckets for organizing results. He also found the AttackIQ approach to testing more suitable to his organization's needs than the other solutions on the shortlist. *"Some of the tools we considered would be helpful for an external pen-testing shop that spends all day trying to breach other companies,"* he says. *"What I was looking for was the ability to validate our different controls at scale, not just test whether we can get into the network. That was the real differentiator in our POC."*

> **"The Security Optimization Platform doesn't just enable us to execute at scale; it also enables us to execute consistently at scale, which is something we couldn't do without underlying technology."**
>
> - Director of Security Operations, Fortune 500 Retailer

CUSTOMER

Fortune 500 Retailer

LOCATION

United States

INDUSTRY

Retail

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Investment Decision Support
- Post-Incident Response Remediation
- Change Management Risk Assessment

PROJECT BUSINESS IMPACT

- Confidence among CISO, other executives, and the board — supported by evidence — that security measures are effective
- Demonstration of compliance with corporate security standards through consistent testing across thousands of locations around the world
- Streamlined answers to internal questions regarding downstream effects of prospective infrastructure changes
- Support for prioritization of strategic security investments
- Planned support for procurement decisions through testing of vendor claims

Testing "as Many Things in as Many Ways as Possible"

The retailer began rolling out the Security Optimization Platform about six months ago and built a wide array of routine tests that run, as the director puts it, *"as close to continuous as you can get without literally running 24×7×365."* The tests measure the company's response to specific use cases that the internal team has identified as important for the business.

Security groups throughout the company collaborated to define those use cases and strategic goals for the testing program. They used the MITRE ATT&CK framework to help define and classify threats, as well as pulling in data from *"every infosec blog under the sun,"* the director says. *"We brought together security teams with a fairly diverse set of interests and built in a lot of activities to ensure cross-pollination among the teams."*

The result is a cadence of tests that evaluate the company's response to atypical behaviors or activities that might indicate malicious intent. For example, the director explains, *"if there is a behavior that we would not expect to see from a certain classification of users, we may try to replicate that behavior through AttackIQ to see if our heuristic detection capabilities pick up on it."*

> **"What the Security Optimization Platform enables me to do is demonstrate to our CISO, other senior leadership, and the board that we are doing the right thing. That is invaluable with an attack surface as broad and complex as ours."**
>
> - Director of Security Operations, Fortune 500 Retailer

"Other than focusing on the types of big attacks that keep people awake at night," he adds, *"our program is designed to test as many things in as many ways as we possibly can. It's critical to cover every base, because whatever we don't test, that is the area of our security infrastructure that is sure to be hit."*

When security teams believe they have remediated an issue that AttackIQ testing revealed, the security operations group will re-test to make sure the remediation is effective. *"We're using that heavily,"* the director reports. *"If we run a test and the results are not what we expected or wanted, we make the appropriate changes. Then that goes into our testing library so that we can periodically re-run that test and make sure we continue to be protected."*

Assessments: Routine, Ad Hoc, and Honeypot

Frequently running the tests in the corporate library will alert the retailer if a change to the security or network infrastructure inadvertently renders a particular control ineffective. Examples of such changes include a server update, which might cause controls to behave differently than they did before, and rule tuning designed to reduce the number of false-positive alerts, which might accidentally result in allowing a dangerous behavior.

The regular cadence of attack simulations enables the security operations team to ensure that no such changes to the corporate infrastructure have downstream implications for security. This is particularly important because the retailer's security infrastructure is so complex.

"We have a variety of controls with so many overlapping components that we have to question whether we are effectively protecting ourselves or we have a false sense of security," the director says. *"We might have controls X, Y, and Z, and a successful attack should be impossible because each of those controls should catch it. But with AttackIQ, we might find that none of the controls actually catches an attack we would expect them all to detect. In a lot of ways, the comprehensiveness and complexity of the security architecture we've built is driving our need for the AttackIQ tool — we need an external capability to see that what we expect to be protected is actually being protected."*

Assessments: Routine, Ad Hoc, and Honeypot (cont.)

In addition, the security operations group uses the Security Optimization Platform to perform ad hoc tests in response to questions about the security infrastructure's detection and response capabilities. Sometimes, the Director says, these are questions from the CISO and others in the C-suite. But not always.

"We also often use ad hoc testing to answer questions that I have for my team or that other internal teams have for us," he says. *"A great example was when another team was looking to change some endpoints' security configuration. They wanted to make certain rules more restrictive, and they wanted to know whether doing so would ultimately improve security on those systems."*

The team wanting to perform the update provided the Security Operations group with two systems, which were identical except one had the prior security configuration and one had the proposed update. The Security Operations team ran the same tests against both systems. *"It was basically a fourth-grade science experiment,"* the Director says. *"Of the 10 attacks we threw at the systems, the old configuration detected six and the new configuration detected nine — and the one it missed was also missed by the old configuration. So we determined that not only would the update increase the endpoints' security overall, but we wouldn't lose any detection capabilities.*

"I was able to assure the other team that the infrastructure changes they wanted to make were a good idea from a security standpoint," he continues. *"And when my boss asked whether we'd signed off on the infrastructure changes, I didn't just say, 'Yes, they explained it all to me.' I said, 'Yes, and we have data, we have testing, we have validation that their changes make sense.'"*

One more AttackIQ use case for the retailer is the ability to test the security operations center (SOC) response to honeypots and canary accounts. *"Those tests are very similar to the other detection assessments we have, but they're higher fidelity in terms of having fewer false positives,"* the director says. *"If we have a server or account whose only purpose is to be a trigger for somebody who's doing something they shouldn't, then no one should ever interact with it, so we can easily see whether each alert that we expect is actually triggered."*

Testing Consistently at Scale

Although the retailer dedicates substantial resources to security, the director says that the cadence of testing they've achieved through the Security Optimization Platform would simply not be possible if tests weren't automated.

"We have a highly competent internal penetration testing team," he says. *"But having them run any test manually — even something simple like double-clicking malware and monitoring the response across the infrastructure — is going to take weeks and weeks to complete across our thousands of locations globally. Instead, with AttackIQ's agent script, my team can spend a day building, testing, and validating the assessment, then we can push it out whenever and wherever we need it. This drastically improves the scalability of our testing regime."*

> **"Running any test manually is going to take weeks and weeks to complete across our thousands of locations globally. With AttackIQ, my team can spend a day building, testing, and validating the assessment, then push it out whenever and wherever we need it. This drastically improves the scalability of our testing regime."**
>
> - Director of Security Operations, Fortune 500 Retailer

Testing Consistently at Scale (cont.)

AttackIQ's library of tactics and techniques further enhances this scalability by accelerating the development of simulations, the director says. *"It might take a team member a day to put together an assessment using the runbooks and templates built into the Security Optimization Platform. The same test might take a week or more to build from scratch. By saving time on architecting the simulations, my team gains more time to spend on validation and testing activities."*

Automation of testing also helps ensure global consistency. *"Even if I had a team of 1,000 people,"* the Director says, *"having them manually perform the same test across all our locations would result in variations. But one of our goals is to run standard tests across all the environments and regions we operate in. We want to know that all our stores have the same security, regardless of where they're located.*

"Because testing in the Security Optimization Platform is programmatic, the tests are done in the same way on every system in every country, on every continent," the director adds. *"If I run the test today, next week, and then again four years from now, the results will be comparable, apples to apples, unless we have purposely changed something. The Security Optimization Platform doesn't just enable us to execute at scale; it also enables us to execute consistently at scale, which is something we couldn't do without underlying technology."*

Additional Use Cases for Automated Testing

Global consistency in testing also helps the retailer weather staff turnover and skill shortages. *"Knowledge transfer is a huge problem for many companies,"* the director says. *"On the red team side, I hope we don't lose any staff. But even if we do, we will retain that knowledge because it's been scripted into the Security Optimization Platform." On the blue team side, the tool enables the director to make sure new hires are responding to threats in the ways he expects them to. "Having a platform to frequently and repetitively execute tests means that we can make sure our controls continue to function properly, even after we have hired new staff,"* he says.

"In a lot of ways, the comprehensiveness and complexity of the security architecture we've built is driving our need for the AttackIQ tool — we need an external capability to see that what we expect to be protected is actually being protected."

- Director of Security Operations, Fortune 500 Retailer

In fact, the director sees AttackIQ automation as an impetus for merging red and blue teams. *"We can produce a realistic attack, validate where controls are successful at detecting or preventing it, identify places where controls aren't working, make sure the SOC and other teams are responding appropriately, and then make improvements where the tests indicate they're needed,"* he says. *"Bringing all those activities together into the same process is, in my opinion, the definition of Tier 1 purple teaming. I think we should focus more on being a purple team than either red or blue, and AttackIQ has been solving that problem for us from the outset."*

The retailer also refers to AttackIQ test results in making strategic decisions about where to focus corporate security investments, and the director expects to eventually use the Security Optimization Platform to validate vendors' claims during the procurement process. *"We are still building that out,"* he says, *"but our intention is to use the tool in POCs. We will run the same tests on multiple competing solutions and see which identifies or prevents the most severe threats, as well as which provides the best insights into the threats."*

Executive Confidence Is Everything

In deploying the solution and developing new use cases for the Security Optimization Platform, the director has been extremely pleased with AttackIQ service and support. *"With other vendors I've dealt with in the past, I might submit a support case, and three weeks later I'm wondering whether anyone has read it,"* he says. *"By contrast, my team will drop a message in the AttackIQ Slack channel, and more times than not, they'll get a message within the hour saying, 'Can you hop on a videoconference right now so I can help you fix it?' That has been great."*

With the help of AttackIQ, the retailer has built a solution that the director says gives him confidence that his organization will not make the news for falling victim to a ransomware attack. *"A company like ours that is hit by ransomware would not be fully operational for weeks,"* he says. *"It's hard to quantify the risk reduction we've achieved, but the lost revenue of a long-term problem with operations would be substantial."*

"What the Security Optimization Platform enables me to do is to demonstrate to our CISO, other senior leadership, and the board that we are doing the right thing," the director concludes. *"I'm not just saying it; I have evidence that proves it. I can run a test and show them exactly how our systems and teams respond. That capability is invaluable with an attack surface as broad and complex as ours."*

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.