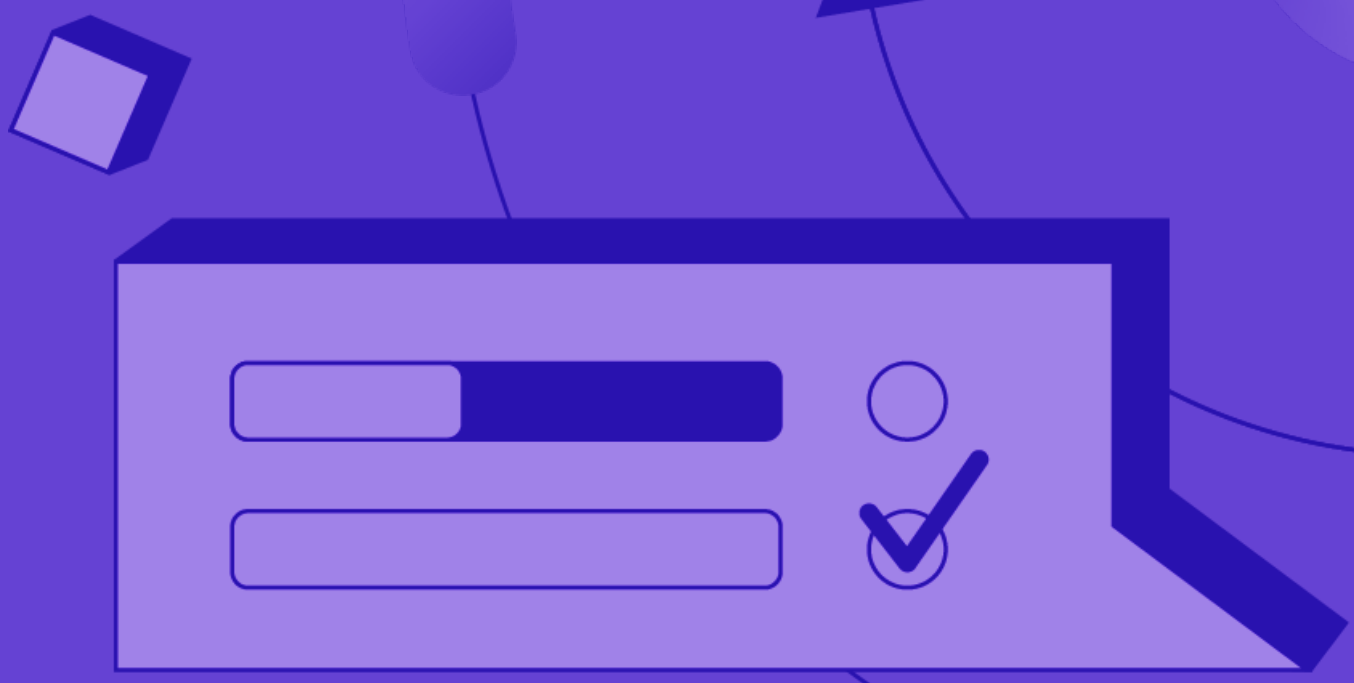
ATTACKIQ®

Case Study

U.S. Defense Contractor Harnesses AttackIQ to Improve Customers' Operational Readiness



As challenging as cybersecurity is for companies, threats are even more intense for the U.S. military. The teams responsible for securing the military's IT infrastructure work in a state of perpetual danger from ransomware and other types of attacks. That is where one defense contractor comes in: The organization helps ensure the operational readiness of the military divisions that are its customers.

"It's crucial for our customers to act as though they are always being targeted," says one of the defense contractor's Security Incident Response Analysts. *"They have to hunt for things that they need to fix, before a breach happens and it becomes a huge issue."*

The defense contractor takes on end-to-end responsibility for customers' digital security infrastructure. *"Our key goal is to keep our company, our assets, and our customers safe from intrusions and malicious cyber activity,"* says the analyst. *"We need to make sure all the products we use are effective in defeating both domestic and international threats. And we need to know whether an attacker may be able to exploit vulnerabilities across our network or our customers' systems."*

Penetration testing has long been a key element of the defense contractor's service offerings. And for the past several years, the company has relied on the AttackIQ Security Optimization Platform to accelerate these assessments—enabling more frequent testing of client systems, faster evaluation of security solutions' performance against specific threats, substantial cost savings, and a big boost to customer satisfaction.

Manual Testing and Infrequent Red Teaming

Before it began working with AttackIQ, the defense contractor assessed customers' security controls through largely manual processes that incorporated an open-source testing tool. *"We were following the methodology that the open-source organization put forth and using their tool to run traditional penetration testing,"* says the company's Senior Information Security Analyst and Security Tester. *"We were looking for specific exploits, but the degree of manual effort involved limited how frequently we could run the tests."*

> *"AttackIQ gives us instantaneous results when a scenario has finished running. That means we find out about problems and get them fixed months sooner than when we were using an external red team."*
>
> - Senior Information Security Analyst and Security Tester, Defense Contractor

The firm also engaged external red team testers once a year. However, the limited resources, combined with the narrow time frame in which the third-party testers were available to the defense contractor's staff, led to challenges. The red team could not perform as many assessments as the defense contractor would have liked, nor could they complete them as frequently or quickly as the defense contractor preferred. The company needed an automated testing solution in order to confidently tell its military and Defense Department customers that their controls could hold off an attack.

CUSTOMER

U.S. Defense Contractor

LOCATION

United States

INDUSTRY

Defense, Transportation

HIGHLIGHTED SOLUTION AREAS

- Security Control Validation
- Cloud Security Optimization
- Internal Automated Quality Testing: Development

BUSINESS IMPACT

- Insights into defenses' effectiveness against threats available in hours, rather than days
- Improvement in customer satisfaction due to faster communication around emerging threats
- Increase in revenue due to customer satisfaction improvement
- Less staff time spent on routine testing as a result of automation
- Cost savings through elimination of red team testing and extraneous security solutions
- Routine security assessment results available months sooner than with third-party red teaming in the legacy environment
- Strengthened security posture because mitigation activities can be retested immediately

The team evaluated the ability of the AttackIQ Security Optimization Platform to replicate real-life threat scenarios on live, production systems, without putting those systems at risk. They were pleased with the results and decided to roll out the breach and attack simulation (BAS) platform.

Automation Makes Assessments Routine

The defense contractor incorporated the AttackIQ Security Optimization Platform into control assessments for customer systems. The team runs one-off simulations of individual attacker techniques, as well as attack graphs, which string together a series of attack scenarios to emulate multistage attacks. *"We have fully integrated the AttackIQ platform into our penetration testing methodology,"* says the security tester. *"Because it is automated, we can test more scenarios in less time. That enables us to do thorough white box and gray box capabilities testing, as well as relevant tests targeted to a customer's specific industry and geographic region."*

"I run AttackIQ on my systems every two weeks," he adds. *"The AttackIQ Security Optimization Platform is central to my routine testing process, checking vulnerabilities I know about and looking for new ones."*

The incident response team also uses AttackIQ to confirm that the company's own security infrastructure is effective. *"For example, we make sure our EDR [endpoint detection and response] product is stopping certain kinds of scripts,"* says an analyst. *"Another example is that recently I was running AttackIQ to see how our Azure environment would handle a 'spring for shell' scenario."*

> ***"AttackIQ shrunk our response time for zero-day threats from days to hours. That has been really helpful to our business."***
>
> - Senior Information Security Analyst and Security Tester, Defense Contractor

In the event that a simulation or attack graph reveals a control gap, the AttackIQ platform provides the relevant teams with that information much more quickly than they would have had it in either the manual or external red teaming environment.

"The third-party testers used to take their sweet time," says the security tester. *"We would have to wait a couple of months for their report. Then we would meet with them to get their recommendations. We would remediate whatever particular vulnerabilities they uncovered, but then we would have to wait until their next engagement to confirm that the fix was fully effective."*

By contrast, adds one of the incident response analysts, *"AttackIQ gives us instantaneous results when a scenario has finished running,"* the tester explains. *"That means we find out about problems and get them fixed months sooner than when we were using an external red team."* It also means the team can retest as soon as they have taken action to mitigate a control gap, to assess whether the change eliminated the vulnerability. *"That entire process takes much less time with AttackIQ."*

Defending Against Emerging Threats

When a new type of incident arises, AttackIQ quickly provides new simulations to test defenses against it. *"AttackIQ is very good about keeping up-to-date as new exploits emerge,"* says one of the incident response analysts. *"That is an important benefit of the platform: The scenarios are always being updated, and new scenarios are created very quickly anytime the external environment changes."*

The firm responds to emerging threats by using the MITRE ATT&CK framework to determine which tactics, techniques, and procedures (TTPs) pose the greatest risk. *"Then we run scenarios that simulate the zero-day incident,"* the analyst explains. *"We run those scenarios against our tools to see whether an attack might affect our environment or our customers. AttackIQ makes it easy to run these different kinds of tests, with a wide variety of scopes, to see how our other security tools handle the threats that we may be facing."*

By enabling the team to respond more proactively to emerging threats, the AttackIQ Security Optimization Platform has significantly improved the service that the defense contractor can offer its customers. In the past, the security tester explains, customers would hear about a threat and contact the firm asking whether their security infrastructure was prepared to effectively defend against it. Getting that information was usually a slow process, and customers often escalated these questions to the firm's management team in an effort to get an answer more quickly.

> ***"One of the deep-dive scenarios that I ran on Azure was successful. We were not expecting that because we had applied the appropriate security updates end-to-end. That knowledge enabled us to close the gap before an attacker could exploit it."***
>
> - Senior Information Security Analyst and Security Tester, Defense Contractor

"But since we deployed AttackIQ, anytime there is a new adversary or a new attack scenario, analyzing whether our controls are effective against it takes a click of a button," the security tester says. *"Within hours of a threat first being reported, I can run a test and confirm with the customer that our defenses are sound. Before they even come to us, I can send a message to our customers telling them, 'This new attack is happening, but don't worry: We are already up to date.'"*

"AttackIQ shrunk our response time for zero-day threats from days to hours," he continues. *"That has been really helpful to our business."*

The security tester has begun utilizing the AttackIQ Security Optimization Platform in the cloud, as well. *"We have customers whose infrastructure is in Azure, so AttackIQ provided me with scenarios for Azure testing,"* he says. *"I have been integrating those into my regular assessments, to make sure we are protected against cloud attacks."*

The Only Way to Be Prepared

AttackIQ attack graphs have occasionally revealed a security control failure that the defense contractor was previously unaware of. *"One of the deep-dive scenarios that I ran on Azure simulated a very complex attack as per the MITRE framework, and the attack was successful,"* the security tester reveals. *"We were not expecting that because we had applied the appropriate security updates end-to-end. My initial reaction was alarm. But that knowledge enabled us to close the gap before an attacker could use it."*

For one of the incident response analysts, getting a 360-degree view of how the security infrastructure would respond to a prospective attack is another key benefit of the AttackIQ Security Optimization platform. *"When we run our regular scenarios, we can follow those simulated attacks not just in AttackIQ, but also in our other security tools as they detect and respond,"* he says. *"That is a great learning experience. We're learning from both sides—from the defense standpoint as well as the attacker standpoint."*

The teams regularly report to management on the effectiveness of their security infrastructure, and AttackIQ makes that process easy. *"The reports are easy for management to understand; we do not get many questions about them,"* says one of the analysts. *"Also, the AttackIQ Security Optimization Platform enables us to run monthly scenarios emulating the latest threats showing up in the news. Because we understand, and can demonstrate, whether our systems and processes will prevent specific current threats, we can quickly communicate to our leadership what the risk level is."*

Ultimately, the security tester says, AttackIQ strengthened the defense contractor's internal security and service offerings because it enabled the firm to establish a perpetual cycle of confirming controls' effectiveness. *"I recommend AttackIQ for all the security teams out there,"* he says. *"To keep up with threats that are constantly emerging, you have to be constantly testing. If you are a little bit sloppy, someone is going to take advantage of you. Test your key controls, act on that information, and test them again. That is the only way to be prepared."*

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 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 Engenuity's Center for Threat Informed Defense

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