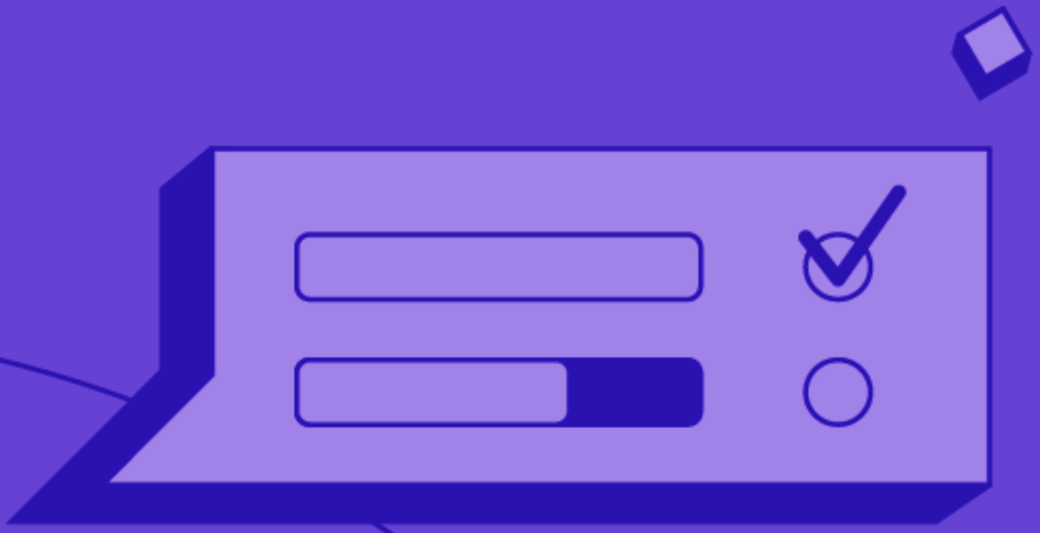
ATTACKIQ



Case Study

Pharmaceutical Services Company AmerisourceBergen Boosts Cybersecurity Health Through Continuous Testing and Improvement

AmerisourceBergen provides pharmaceutical products, value-driving services, and business solutions that improve access to care. Global manufacturers depend on AmerisourceBergen for services that drive commercial success for their products. Tens of thousands of healthcare providers, veterinary practices, and livestock producers trust AmerisourceBergen as their partner in the pharmaceutical supply chain.

"In this business, the core objective is to deliver the right medication on time, in the right package, and at the right temperature," explains Kumar Chandramoulie, senior director of cyber defense and vulnerability management for AmerisourceBergen. *"The health of our customers' patients depends on our efficient management of the supply chain."*

A cyberbreach could potentially result in a logistics problem, such as product being diverted to the wrong location. *"That is why cybersecurity is core to our business,"* Chandramoulie says. *"My challenge is to secure the millions of moving parts involved in ordering and delivering pharmaceuticals across the United States and the globe."*

Threat Hunters Need an Attack Simulation Tool

Three years ago, AmerisourceBergen launched an initiative to build a next-generation cybersecurity program. *"Our goal was to build technology and hire people around it who could protect our systems against whatever attack will be coming five years down the road,"* Chandramoulie says. *"We designed the program to include automation and behavior analytics, and we utilized a SIEM [security information and event management solution]."*

The company undertook a proactive strategy in an effort to foresee and prevent attacks rather than just defending against the inevitable. Chandramoulie hired a team of threat hunters to identify security vulnerabilities in the company's network, data, and applications. It correlates its threat hunting and mapping activities with the MITRE ATT&CK framework. *"There are many compliance frameworks in the security world,"* he says. *"But I think MITRE ATT&CK is the best option for threat-centric security. I believe in using human intelligence to anticipate the advanced threats of the future. The MITRE ATT&CK framework provides an exhaustive list of areas to explore, with a lot of detail, and it helps our threat-hunting team structure their day-to-day operations."*

AmerisourceBergen also deployed an assortment of sophisticated security technologies with the goal of keeping its data and logistics applications safe. *"The technologies were maturing very fast, so we were picking up more and more tools,"* Chandramoulie says. *"We put the solutions in place and got the rules set, but we weren't always sure whether everything was working. We needed to make sure they were doing an effective job for us—to test the efficacy of our cybersecurity."*

He and his team began shopping for a solution that would enable threat simulations and testing. They liked the idea of an attack simulator but wanted a tool that would be easy to use and straightforward to deploy. They wanted to simultaneously evaluate the effectiveness of their security investments and provide the threat-hunting team with information about detected vulnerabilities in the security infrastructure.

CUSTOMER

AmerisourceBergen

LOCATION

Americas

INDUSTRY

Pharmaceutical Distribution

HIGHLIGHTED SOLUTION AREAS

- Automated Testing
- Control Auditing
- Investment Decision Support
- Threat Hunting
- Security Control Rationalization

BUSINESS IMPACT

- Improved configuration of security technologies, design of processes, and hiring/training of staff through targeted adjustments
- Better-informed assessments of prospective security investments
- Faster threat identification and response
- More predictive and preventative cybersecurity program

Threat Hunters Need an Attack Simulation Tool (cont.)

The AttackIQ Security Optimization Platform checked all those boxes, and its software-as-a-service (SaaS) approach made it easy to roll out. Moreover, AttackIQ's commitment to the MITRE ATT&CK framework made the solution a good fit for the threat-hunting team. *"That shows we are very synchronized in our thinking,"* Chandramoulie says.

A Mature Security Offense

AmerisourceBergen deployed the AttackIQ Security Optimization Platform for use by multiple teams. Now, the company's security professionals have access to an automated tool that simulates attacks, enabling them to test their protocols and infrastructure from a variety of angles.

They use AttackIQ for blue team testing, looking for events and alerts within the security controls, as well as for routine simulations of specific attacks on individual pieces of the security infrastructure — for example, the firewall. *"They will go at the firewall to see whether it is scaling up and providing all the value we think it is providing from a security standpoint,"* Chandramoulie says. *"That is our primary use case: determining the security efficacy of specific tools and technologies."*

Chandramoulie has typically seen companies perform breach and attack simulations on an annual or semiannual basis, as part of a compliance audit. He doesn't believe that cadence provides adequate visibility into the performance of the security infrastructure. *"You are adopting new tools and capabilities throughout the year,"* he points out. *"You may be changing settings and configurations in your existing solutions. By automating simulations, AttackIQ enables us to run tests on a weekly basis, so we can frequently check to make sure our security solutions are still working as intended."*

> *"AttackIQ enables us to make sure our security approach is working. If we see news stories about emerging threat actors, we can test right away to be sure our systems will hold up in the face of such an attack."*
>
> – Kumar Chandramoulie, Senior Director,Cyber Defense and Vulnerability Management, AmerisourceBergen

AmerisourceBergen's second use case for the AttackIQ platform is threat actor–based simulation, in which the red team threat hunters plan a simulation based on a type of attack they anticipate. The team receives threat intelligence from more than 100 sources. *"We identify the threats that are most relevant to our industry and our business,"* Chandramoulie says. *"We vet those, then we go into AttackIQ to see whether we can simulate attacks from those threat actors."* For instance, *"if a nation-state is engaging in retaliatory attacks against U.S. businesses, we will look at the threat actors associated with that nation-state and run simulations that we think represent the types of attacks they might use against us."*

Both use cases highlight any vulnerabilities that may exist in AmerisourceBergen security technologies, giving the company's engineers an opportunity to fill those gaps. They also identify any issues with human responsiveness. *"If an alert goes out and nobody responds to it in a timely manner, we can question the people involved,"* Chandramoulie says. *"We can look at the root cause for slow responses and see how to fix them. That has helped us improve security personnel performance as well."*

A Mature Security Offense (cont.)

In a third use case, AmerisourceBergen uses "purple teaming," in which blue and red teams conduct coordinated attack simulations. *"The AttackIQ platform makes it possible to stitch together all the pieces of purple-team testing,"* Chandramoulie says. *"If we discover an issue with the response to a particular simulated attack, we can use the platform to figure out when the alert came in and when the actions took place, and we can compare that with the response in our ticketing systems and our SIEM system. AttackIQ provides an additional layer to the reporting and analysis. We have already seen value from putting that to work."*

Conclusion: The Best Preparation for Advanced and Emerging Threats

The AttackIQ platform has benefited AmerisourceBergen in a number of ways. Primary among those is improving the efficacy of the security infrastructure. *"AttackIQ has definitely helped us make every tool more effective than it was,"* Chandramoulie reports. His teams determine how well their existing tools are working and tweak configurations and settings to ensure they're getting optimal value from their security investments. They also use AttackIQ for "bake-offs" among competitive products, to determine which would do the best job.

"If we were picking an EDR [endpoint detection and response] tool or an AV [antivirus] tool, there would be hundreds to choose from, and their capability charts might all say the same thing," Chandramoulie says. *"How would we know which product would do a better job? In the case of EDR, for example, we would use AttackIQ to run ransomware tests to determine how effective all our options were."*

Automation in the AttackIQ Security Optimization Platform streamlines attack simulation processes, improving the operational efficiency of security teams across Chandramoulie's organization. It also helps them understand where they can further streamline activities. *"It provides insights into response times and the technology landscape,"* he says. *"We can see how efficiently all our tools and processes are operating."*

Perhaps most important, the AttackIQ platform provides visibility into the areas in which AmerisourceBergen can improve security effectiveness. *"Our technology teams can look at the reports and say, 'Here are the things we are missing. Let's go fix them.' We have operationalized ongoing security improvements using the AttackIQ platform,"* Chandramoulie says.

> *"Our technology teams can look at the reports and say, 'Here are the things we are missing. Let's go fix them.' We have operationalized ongoing security improvements using the AttackIQ platform."*
>
> – Kumar Chandramoulie, Senior Director,Cyber Defense and Vulnerability Management, AmerisourceBergen

The end result is more peaceful sleep for Chandramoulie. *"Just deploying security solutions doesn't mean they're working,"* he says. *"AttackIQ enables us to make sure our security approach is working. If we see news stories about emerging threat actors, we can test right away to be sure our systems will hold up in the face of such an attack. We know that attackers don't take breaks."*

Conclusion: The Best Preparation for Advanced and Emerging Threats (cont.)

Even during the coronavirus crisis, threat actors used contract tracing and other public health measures as a phishing tool, he says. *"They will take every opportunity you give them, so you have to be prepared,"* Chandramoulie concludes. *"AttackIQ has helped us drive our cybersecurity program to be more predictive and preventative. Quantifying your cybersecurity in this way is a must for any organization. Whatever your level of maturity in cybersecurity, you have to assess yourself. You need to understand your capabilities at the level AttackIQ makes possible, in order to have your people, processes, and technologies prepared for advanced and emerging threats."*

> *"AttackIQ has helped us drive our cybersecurity program to be more predictive and preventative. Quantifying your cybersecurity in this way is a must for any organization."*
>
> – Kumar Chandramoulie, Senior Director,Cyber Defense and Vulnerability Management, AmerisourceBergen

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 MITRE Engenuity's Center for Threat-Informed Defense.

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