ATTACKIQ®

Industry Brief

Federal Government Defends Critical Infrastructure with AttackIQ's Breach and Attack Simulation

The United States Federal Government remains a prime target for cyberattacks originating from adversaries worldwide and continues to grapple with an escalating wave of sophisticated and malicious cyberattacks. This surge in cyber threats and data breaches directly threatens U.S. government organizations and military operations around the world.

The Federal Government has proactively addressed the escalating cybersecurity threat by implementing new strategies. These include proactive cyberthreat hunting, increased utilization of threat intelligence data, continuous security monitoring, and automated security operations orchestration. These measures are designed to defend against and mitigate cyberattacks.

Despite these efforts, many agencies struggle to respond swiftly to the growing threat. According to a June 2024 Federal Information Security Modernization Act (FISMA) report from the Office of Management and Budget (OMB) to Congress, federal agencies reported more than 32,000 cybersecurity incidents in 2023, which is nearly a 10% increase from 2022. Of those incidents, 38% were due to improper usage, such as violating an agency's acceptable use policy. The second biggest attack vector was email phishing which recorded a 50% increase in 2023 as compared to 2022. The barrage of attacks in 2023 brought opportunity cost, the potential loss of data, and impairment of operations.

Nation-state attacks are among the most sophisticated and dangerous and are not easily detected. The governments of Russia, Iran, North Korea, and China are aggressively using advanced cyber capabilities to pursue objectives counter to U.S. interests and the interests of our allies.

In February 2024, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert regarding the Volt Typhoon. Volt Typhoon, backed by the People's Republic of China, has centered activities on espionage, the collection of intelligence, and the specific targeting of critical infrastructure entities with the U.S. and Guam. CISA has established that it is a fact that highly skilled nation-state threat actors want to invade commercial and government organizations' enterprise networks to preposition malicious software silently. Volt Typhoon provides this malicious software with the capability to deliver a destructive blow to your organization's operational capabilities in the future while silently exfiltrating information today. The Volt Typhoon threat actors may be seeking to breach your networks even now.

FEDERAL GOVERNMENT BAS USE CASES

IMPROVE DEFENSES, REDUCE RISK, AND DELIVER ROI

Automated Security Control Validation

Security Control Validation is used to measure efficacy and validate that specific security controls are working the way they should. Validate that specific controls offer the expected protection capabilities as they are currently configured in your production environment.

NIST Compliance Effectiveness Validation

Close gaps in your security ecosystem by measuring and testing control effectiveness while also ensuring compliance with NIST requirements.

DOD CMMC Compliance Effectiveness Validation

Utilize AttackIQ assessments to validate CMMC security controls and compliance and ensure DoD contractors handling unclassified DoD materials receive specific security certification.

The Costs Remain High

To stem this massive tide of malicious cyberactivity, in 2023, the Federal Government spent approximately $10.9 billion[1] for hardware, software, and services. This expenditure represented an 11% increase from the 2022 budget, which was $9.8 billion. The classified expenditures are informally estimated to be far larger. Yet all of this is insufficient to mitigate the damage due to the theft of critical data or impairment of often essential federal operations.

Security assessments of the Federal Government's high-value assets show many hundreds of security gaps and architecture weaknesses that remain exposed and uncorrected, even as the Federal Government continues to acquire and deploy new security controls at a rate higher than ever before.

Security Control Performance Must Improve

Many organizations implement dozens of security controls to manage risk and protect their data. However, validating these controls can be a daunting task. Ensuring they align with current security and compliance requirements and that they're configured effectively to stop modern threats is extremely time-consuming and complex.

Infosecurity's 2024 study[2] found that the shift to cloud and remote working has driven a 19% increase over the past two years in the number of security tools organizations must manage – from 64 to 76. A similar study by Helpnet Security[3] found that, on average, enterprises already have 53 security solutions in use across their organization; however, despite large security stacks, 51% of enterprises reported a breach over the past 24 months.

Despite the large number of security controls, there is often 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 organizations, it is unclear how well these security controls work and what areas and gaps require additional investment. AttackIQ's BAS Platform helps you develop a smart strategy, validates that you have a resilient security control architecture, and objectively supports your budgeting decisions.

[1] https://www.govinfo.gov/content/pkg/BUDGET-2023-PER/pdf/BUDGET-2023-PER-6-3.pdf
[2] https://www.infosecurity-magazine.com/news/organizations-76-security-tools/
[3] https://www.helpnetsecurity.com/2024/04/19/enterprises-pentesting-frequency/

FEDERAL GOVERNMENT BAS USE CASES (cont.)

IMPROVE DEFENSES, REDUCE RISK, AND DELIVER ROI

Purple Teaming

Purple teaming uses a methodology that fosters and supports collaborative communication between the red team and blue teams. Purple teaming enables a holistic and collaborative approach to threat intelligence, testing, and remediation.

Threat Emulation

Mimic adversarial behavior to expose gaps and best use resources and team members to optimize security control defenses. Threat emulation is driven by adversary and attack intelligence and a threat-centric viewpoint, an essential part of threat-informed defense®.

Cloud Security

Maximize cloud security effectiveness in your AWS cloud with security stack mapping aligned to the MITRE ATT&CK framework.

Often, existing security controls are not configured correctly or integrated correctly with the security ecosystem. AttackIQ's Breach and Attack Simulation Platform can identify potentially costly misconfigurations that could be found and targeted by malicious actors. In any scenario, your cyber defense will not work if the security controls do not perform as you expect. AttackIQ's BAS Platform will enable you to rapidly operationalize MITRE ATT&CK and get the most from the security controls, personnel, and procedures you have today.

The Solution for Federal Government

Breach and Attack Simulation

AttackIQ's Breach and Attack Simulation (BAS) Platform is a leading offering for the U.S. Federal Government. Our platform supports the automation and operationalization of the MITRE ATT&CK® framework.

AttackIQ's BAS Platform gives the Federal Government powerful capabilities to test continuously, measure, and validate the performance of security controls, personnel, and processes against the tactics and techniques in the MITRE ATT&CK framework. AttackIQ's BAS Platform uses MITRE ATT&CK to simulate the full attack chain against enterprise infrastructure.

AttackIQ delivers continuous and objective measured validation of government security programs. You can find performance gaps, strengthen your security posture, and improve your incident response capabilities. AttackIQ's BAS Platform assesses readiness and validates that your enterprise security systems are performing as originally intended.

AttackIQ's BAS Platform brings scale and flexibility to the most significant federal organization. AttackIQ automation enables the platform to work autonomously and to scale. AttackIQ includes support for live production environments — even the small changes to configurations or administration can open new vulnerabilities in your cyber defense. This helps identify and close the ever-present gap between Federal Government test environments and the live production environments that, undetected, will ultimately compromise the entire organization.

The AttackIQ BAS 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 MITRE Corporation coined the term "threat-informed defense" 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 improve and optimize your security program.

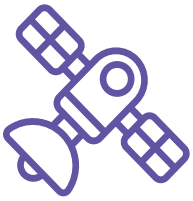
Government Customers Implement AttackIQ's BAS Platform

National Government-Funded Laboratory

This leading national laboratory uses the AttackIQ BAS Platform to ensure the safety, reliability, and security of its information technology assets. With thousands of engineers and research staff members, this laboratory supports a wide variety of funded research initiatives. It works to enhance our defense, reducing the threat of terrorism.

A Defense Agency with Global Operations Reach

This defense agency uses the AttackIQ BAS Platform to assess security control performance and support threat modeling using the MITRE ATT&CK framework. This defense agency includes more than 30,000 officers, 200,000 enlisted personnel, and 200,000 civilian employees. AttackIQ supports this agency's mission in any corner of the world in which it may deploy.



A Leading Aerospace and Defense Contractor

This leading aerospace and defense contractor uses the AttackIQ BAS Platform to secure its delivery of comprehensive services in support of end-to-end IT engineering lifecycle services encompassing design, development, security, integration, operation, training, and maintenance. The contractor's wide variety of services includes but is not limited to, secure programs, enterprise capabilities, compliant enterprise services, support for tiered customer support, and integration of real-time enterprise communication services. These services are delivered to its Department of Defense customers to help ensure and maintain mission readiness. This defense contractor works with both the NIST and MITRE ATT&CK® frameworks. It chose the AttackIQ BAS Platform to operationalize MITRE ATT&CK.

AttackIQ Customers on Breach and Attack Simulation

Effective Controls

"AttackIQ shows that the controls actually work. There is a big push in security now for having certain maturity levels assigned where we have to actually show the process working. It's not enough to say they have a control, but my organization has to show controls are repeatable and that they are working."

Greater Productivity

"Our Security Assessment Team (SAT) is more productive because they don't have to spend time writing attack records and simulating them. Outside of SAT, all the teams benefit from knowing if something's wrong with the internal controls."

Operational Risk

"AttackIQ enables us to have a plan. We have very weak metrics for how we measure operational risk. Having a strategy that measures performance with a validation component is now the plan ... to deal with operational risk management."

Time Reduction

"AttackIQ frees up time in running simulations; it automates a lot of tasks that save time. Also, it brings attacks that are out there for simulation versus writing own script, which can be a time-consuming and costly process."

Test & Analyze

"AttackIQ has given my organization the ability to test and analyze the results and then come up with mitigations to iterate and improve our cybersecurity."

Risk Reduction

"Risk has been reduced because, with AttackIQ, we can measure where things work well. If something isn't working, we can take steps to address that."

Cybersecurity Posture

"AttackIQ was viewed [as] part of the continuous development of our cybersecurity posture."

Automated Testing

"The biggest benefits for my organization are real-time testing, automated testing, and confidence in the controls."

Ability to Measure

"The largest benefit of AttackIQ is the ability it gives us to measure and manage our cybersecurity."

Purple Teaming

"My organization used purple teaming to reduce the number of actual alerts we were getting. We are now much more confident that we're able to detect what we need to. We also have, at the same time, reduced the number of trigger alerts and have reduced by 100-fold the situations that actually require alerts."

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 (BAS) solutions, built the industry's first BAS 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. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and partnership with MITRE Engenuity's Center for Threat-Informed Defense.

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