Insight

Hani Bani Amer

Breach & Attack Simulation: A Critical Component of Your Security Strategy

Breach & Attack Simulation: A Critical Component of Your Security Strategy

Author: Hani Bani Amer, Technical Director for iMETA at AttackIQ

At a glance

- 5 minute read
- Background
- What to look for in a BAS platform
- Benefits of Automated Control Validation
- Summary

Background

Cybersecurity is a demanding and complex industry. There are workforce talent shortages; security controls that fail; new adversarial attacks; lack of collaboration between security entities and practitioners; immature laws and governance. The list goes on.

The consequences of a breach can be catastrophic and costly to organizations of any size and kind – from medium-sized enterprises and hospitals to large government agencies. According to the Identity Theft Resource Center, breach volumes for 2021 passed that of 2020 by October. Research from the Ponemon Institute and IBM also found the cost of a breach has increased 10% to $4.24 million.

Cybersecurity teams have invested in a plethora of security solutions; creating integrations between security controls to achieve resiliency against cyberattacks. Yet, despite having a full stack of controls in place, cybersecurity teams still struggle to know if their systems are functioning correctly.

Breach and Attack Simulation (BAS) is a transformative way for cybersecurity teams to continuously measure the efficiency and readiness levels of their cybersecurity controls.

"The consequences of a breach can be catastrophic and costly to organizations of any size and kind – from medium-sized enterprises and hospitals to large government agencies."

It verifies whether the people, processes and technologies in place are properly responding to and stopping cyberthreats by emulating attacks just like bad actors would in real world scenarios.

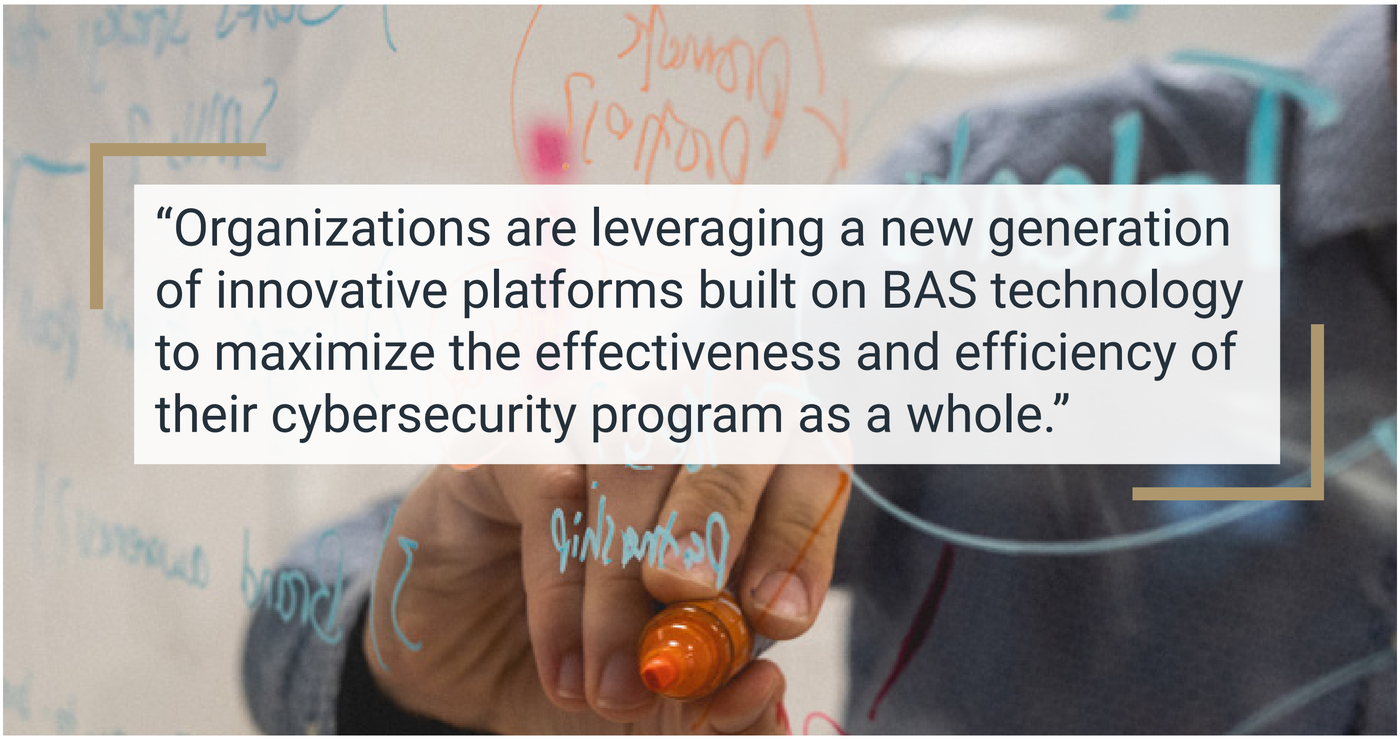
Gartner defines breach & attack simulation (BAS) technologies as solutions "that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement, and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means."

As cybersecurity risks have continued to increase, budgets remain uncertain, and the socio-economic impacts of the COVID-19 pandemic linger, BAS is no longer considered a tool for breach and attack simulation or security control validation exclusively — but as a way to provide business value by maximizing resources and decreasing management burdens on teams. Organizations are leveraging a new generation of innovative platforms built on BAS technology to maximize the effectiveness and efficiency of their cybersecurity program as a whole through security optimization, from technical effectiveness to regulatory compliance.

What should you look for in a BAS platform?

BAS platforms are designed to address cyber security industry problems like lack of security visibility, lack of production security controls testing capabilities, lack of skilled cybersecurity professionals, lack of closed loops feedback to measure the effectiveness of cybersecurity controls, lack of cybersecurity visibility from operational and procedural point of views.

At this year's Gartner Security & Risk Management Summit, Gartner Research Vice President Peter Firstbrook discussed eight critical trends for security and risk-management leaders in his keynote address and one of them was BAS, explaining how BAS solutions provide continuous defensive posture assessments, and challenge limited visibility from annual point assessments like penetration testing.



"Organizations are leveraging a new generation of innovative platforms built on BAS technology to maximize the effectiveness and efficiency of their cybersecurity program as a whole."

When CISOs include BAS as a part of their regular security assessments, teams can identify security posture gaps more effectively and better prioritize security initiatives.

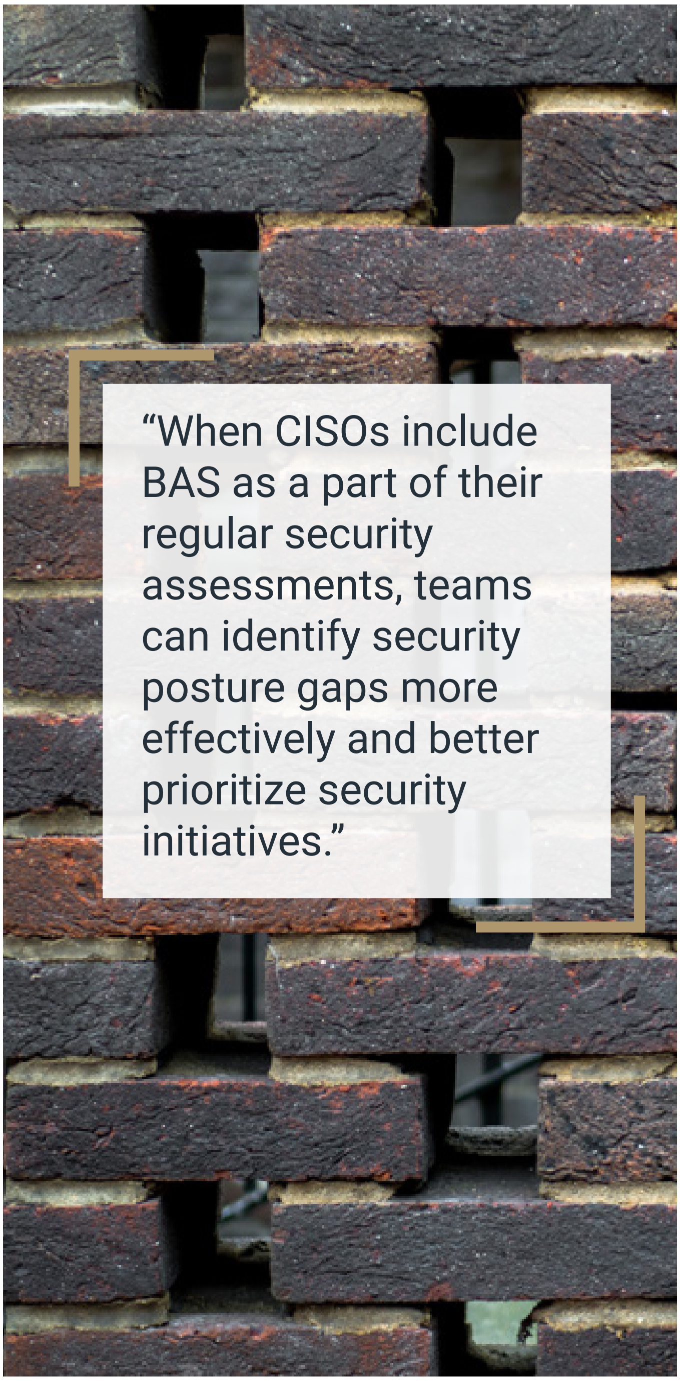
Here are five key capabilities to look for when evaluating BAS platforms for your organization:

1. **Continuous Testing:** An effective BAS platform will have an "assume breach" mindset because it provides the best mechanism to determine the readiness of security infrastructure at every stage of the kill chain. By continuously testing security controls, practitioners can decouple performance measurements of their security program from a point-in-time snapshot that only shows exposure to a specific vulnerability or efficacy against a specific exploit.

2. **Customization:** Users should be able to both perform extensive customization of provided scenarios and create their own from scratch. Look for a platform that provides a robust library of scenarios and assessment templates.

3. **Testing in Production:** Many BAS offerings test in sandboxes. Look for one that tests in production across the entire kill chain, the same way real-world adversaries do. With this capability, security teams can then build a strategic program that delivers both improved effectiveness and efficiency.

4. **Reporting Capabilities:** As the board and c-suite are being called to better understand their organization's cyber security strategy, security teams want the ability to confidently report to their CEOs and board members that controls are working as expected to defend the organization against ransomware attacks and adversaries. Look for a platform that provides easy-to-understand reporting dashboards, so CISOs and risk leaders have actionable information to make sound decisions about their security operations, compliance, and risk management investments.



"When CISOs include BAS as a part of their regular security assessments, teams can identify security posture gaps more effectively and better prioritize security initiatives."

"As the security landscape has become increasingly volatile, BAS gives cybersecurity teams a new way to respond."

5. **Ability to Leverage the MITRE ATT&CK Framework:** The MITRE ATT&CK framework is a globally available, free, open framework of known adversary tactics, techniques, and procedures (TTPs). Built and released in 2015 by the MITRE Corporation, a federally funded nonprofit research and development organization, the ATT&CK framework has gained significant momentum in the public and private sectors as a globally vetted, all-source repository of adversary behavior. ATT&CK has given organizations a stable framework against which they can design their defenses. Used together with a BAS platform you can automate adversary emulations to test your cyber defenses.

Benefits of automated control validation

As the security landscape has become increasingly volatile, BAS gives cybersecurity teams a new way to respond. While there are many use cases and benefits for BAS, the following are the ones most organizations achieve immediately after deploying this solution:

Find and close security control gaps proactively. Get deep and continuous breach and attack simulation analysis to find and close gaps before adversaries exploit them. Share information across security, risk, and compliance teams, and improve the organization's overall security posture.

Improve continuously with evidence. Adversary emulations help you improve the defense capabilities that matter most to you – from endpoint detection and response to next generation firewalls, to security segmentation capabilities, to native internal security controls in cloud providers.

Elevate team effectiveness. Augment your skilled analysts with breach and attack simulation technology. Your scarce resources can use automation and reporting to proactively find and close gaps instead of fighting fires after a breach has occurred.

Reduce costs or reallocate budget. Leverage MITRE ATT&CK tactics and techniques to measure the effectiveness of existing security controls.

By understanding which investments are working and which are not, you can reduce costs or reallocate budget through control rationalization and consolidation.

In summary

Security controls are composed of people, processes, and technologies, and without regular testing against real-world threats, there is no way to ensure they will perform as intended when the time comes.

Legacy manual testing practices are sporadic and provide insufficient coverage to ensure effectiveness. A strong breach and attack simulation platform emulates the adversary and generates real-time data to help identify control failures, resolve structural weaknesses, and make smart investment decisions.

Untested cybersecurity programs are a risk to your business if they fail to stop ransomware or other cyberattacks. Even with the most advanced cyber-defense technologies, controls can fail due to technology misconfiguration, team performance, or capability gaps.

Historically, BAS was largely focused on running attacks and red team augmentation and, as it evolved, to security control validation. Today, the objective is to maximize the effectiveness of the cybersecurity program as a whole.

Ultimately, a security team armed with a BAS platform that helps optimize its entire security program will improve its overall effectiveness and efficiency. You can emulate the adversary with realism to test your security program, generating real-time performance data that allows you to improve your security posture and have confidence that your investments are working as expected to protect your organization.

> “Ultimately, a security team armed with a BAS platform that helps optimize its entire security program will improve its overall effectiveness and efficiency.”