IDC PlanScape

IDC PlanScape: Breach Attack Simulation Services

Curtis Price Christina Richmond Craig Robinson

IDC PLANSCAPE FIGURE

FIGURE 1

IDC PlanScape: Executive Summary of Breach Attack Simulation Services

Source: IDC, 2021

May 2021, IDC #US47649921

EXECUTIVE SUMMARY

This IDC study describes breach attack simulation (BAS) services, an increasingly crucial component of professional and managed security services. BAS providers assume many different approaches in testing and simulating attacks of an organization's environment that creates confusion in the market. IDC interviewed nine companies that provide a range of BAS capabilities, some more limited in scope and some that go beyond BAS. This document is not an exposé or evaluation of these firms but is intended to shed light on the importance of BAS and the opportunities it can provide in improving the security posture and to point out the breadth of offerings available.

BAS is one of the newest services — in addition to managed threat detection and response (MDR) — to help shift the security discussion to breach prevention — the optimal way to avoid costly disruptions that may tarnish reputations and disaffect customers. Thwarting entrance to the organization's infrastructure as early as possible by fixing high-priority, exploitable vulnerabilities improves an organization's security posture significantly. BAS services also are an excellent strategy to offset the critical cybersecurity skills shortage and overwhelmed security personnel. The automation built into BAS offerings simplifies and augments other threat detection and response tools while improving cybersecurity team efficiency and effectiveness. Diverse metrics help prove the value of BAS services and their outcomes.

Compared with traditional point-in-time penetration testing (pentesting) that covers only a small percentage of an attack surface, BAS services offer comprehensive visibility and centralized testing, which can be continuous or scheduled as desired. Alignment with the MITRE ATT&CK framework empowers cybersecurity teams to grasp tactics, techniques, and procedures (TTPs) quickly and take the recommended steps to remediate gaps in security controls that lead to vulnerabilities. IDC believes that BAS will likely displace a portion of pentesting over time with the exception of social engineering pentests and in the case where regulations explicitly call for pentests.

With BAS services on the security front line, operating independently or in support of red/blue/purple teams, organizations gain a valuable feedback element needed in security testing and simulation capabilities that can ultimately reduce overwhelm in the security operations team. The feedback validates that security controls are working as intended to protect critical assets and potential attacker routes to critical assets are secured.

This IDC study describes breach attack simulation (BAS) services, an increasingly crucial component of professional and managed security services.

"Organizations that adopt BAS services are enhancing their breach prevention," says Craig Robinson, program director of Security Services at IDC. "BAS capabilities can help cybersecurity teams discover and remediate gaps in the security posture using the same advanced technologies used by attackers. The 'fight fire with fire' strategy delivers key security outcomes: strengthening cyberdefense and helping IT/security teams do their jobs better and faster."

WHY IS BREACH ATTACK SIMULATION SERVICES IMPORTANT?

Organizations need reliable security controls more than ever to combat the dynamic threat landscape, protect their perimeter-less environments, stop malicious activity, and manage risk. Given all the variables in play, security controls and IT/security teams are hard pressed to keep up with relentless, agile attackers.

Digital transformation initiatives, cloud migration, work from home (WFH), 5G, edge computing, and emerging technologies expand the attack surface, multiply the number of potential vulnerabilities, and increase the risk of breach. At the same time, adversaries use the latest technologies to launch zero-day threats and known threats using myriad TTPs.

Complex security environments hinder swift, efficient detection and response. In an effort to increase protection, organizations purchase additional technology that may not be used fully due to time constraints, lack of skills, or lack of resources. Unfortunately, an excess of tools, however well intentioned, creates even more complexity and leads to more alerts, potential exploits, and missing or misconfigured security controls. Given varying integration levels, settings, and configurations, security controls can be complicated and difficult to manage — a situation that intensifies with an increase in security tools, assets, remote workers, and adopted technologies.

Another obstacle to effective detection and response is lack of broad visibility into TTPs or an organization's state of incident readiness. When IT/security teams fly blind in some areas of the business or aren't clear about mitigation processes, they may not be able to fix specific vulnerabilities quickly. The unintended outcome of unidentified and unmanaged issues — misconfigurations, weak passwords, poor credential management, poor IT/user hygiene, and other vulnerabilities? Increased risk.

With the use of BAS services, organizations can strengthen their defenses by using advanced technologies such as AI and ML and the MITRE ATT&CK framework and knowledge base in an easily consumable manner. While BAS approaches vary, the cybersecurity truths behind breach attack simulation are constant:

- Unknown vulnerabilities will likely always exceed known vulnerabilities. In spite of rigorous vulnerability management and penetration testing, many unpatched or unknown vulnerabilities exist.
- Known vulnerabilities exist in critical applications that go unpatched because the applications can't be down. Compensating security controls are in place to help make sure vulnerabilities can't be exploited.
- When security controls and IT hygiene practices are in place and working properly, they provide essential protection for critical assets and increase organizational security confidence.

BAS platforms deliver services to help IT/security teams answer questions such as:

- Are security controls working as intended?
- How can security resources and efforts be prioritized and allocated to improve overall security and reduce risk?
- Remediation of which security gaps will thwart the highest-priority threats?
- What are the likely travel paths that an attacker might take after they gain a foothold in the environment?

BAS offers an automated, scalable way to assess and improve an organization's security posture immediately and over time to thwart always-active assailants searching for exploitable vulnerabilities on their march toward critical assets. In contrast, pentests can be costly and labor intensive and merely reflect a point in time. While they still provide another useful way of providing a test against an organization's current posture, their inability to be rapidly performed in a sustained and regular way to reflect changes in the organization's cyberhygiene, or changes in the TTPs of cybermiscreants,

reduces their effectiveness. As regulatory bodies become educated on the capabilities of BAS, IDC predicts that regulations that specifically call for pentests will be amended allowing BAS services to replace them.

WHAT ARE BREACH ATTACK SIMULATION SERVICES?

Definitions of BAS vary, which is to be expected in a nascent, fragmented category. Providers describe their offerings as automated penetration testing, red team augmentation, ethical hacking, continuous security control validation, security controls testing, attack-centric exposure management, security validation, and cyberdefense validation.

BAS services reflect the different approaches providers are taking. These are highlighted through descriptors such as the following:

- The ability to test vectors (pathways such as email gateways, endpoints, and web application firewalls) as routes to gain access to systems and resources
- Connection and translation of data on demand, which unites security tools, to help ensure tools are properly implemented, configured, and tuned
- Ability to provide a dynamic view of the attack life cycle and what attackers are doing in the moment
- Assessment of the resiliency of private and public cloud environments to post-breach attacks and lateral movement
- Empowerment of red/purple/blue teams to improve cybersecurity resilience with simulated attacks
- Unification of threat intelligence, vulnerability management, and attack simulation
- Modeling attack paths toward critical assets
- Dedicated network segmentation testing

At a high level, BAS functions are attack (mimic real threats), visualize (see exposures), prioritize (assign a severity or criticality rating to exploitable vulnerabilities), and remediate (address gaps). Optimally, BAS completes these activities as a closed-loop service that allows IT/security teams to evaluate an environment for threat indicators and attack behaviors, unprotected assets, misconfigurations, human errors, log gaps, IT hygiene issues, and more. Armed with this information, security personnel can take the recommended actions to close gaps, fix misconfigurations, strengthen credential management, and so on. In contrast, open-loop testing, such as red team exercises, involve people who find vulnerabilities, write them up, and hand them off for investigation, analysis, and remediation. Still red teaming is a valuable exercise to test security analysts (aka the blue team) in hand-to-hand combat against a highly skilled, ethical attacker versus the real adversary.

Attack scenarios, which are mostly but not always based on playbooks, are designed to accomplish a specific objective, whether that is to bypass controls or uncover possible routes to critical assets. BAS functions run in the background, generally in production environments, although at least one provider's offering runs in test environments as well. The ability to function in a test environment can be significant when dealing with highly sensitive operational technology (OT), industrial IoT (IIoT), or medical IoT (MIoT) devices that do not allow for even a hint of an invasive security test.

Testing options include on demand, continuous, or set intervals. On-screen, real-time visualizations present a variety of findings, including vulnerabilities, severity ratings, and remediation steps. Standard

and customizable reports present insights on diverse topics to audiences ranging from technical to executive.

The important point to keep in mind is that the ultimate goal of BAS services is similar across providers: to uncover vulnerabilities and to prioritize and remediate them, thereby protecting critical assets and reducing risk.

Reducing Confusion

As mentioned previously, BAS creates some confusion in the market as it bumps into legacy red/blue/purple team exercises and pentesting engagements. Table 1 highlights key differences and use cases.

TABLE 1

Differences Between BAS and Other Testing and Attack Simulation Exercises

	Core Functionality	Use Cases
Breach attack simulation	Automated testing of the existing security infrastructure; model attack chains to identify the most likely path an attacker would use to compromise an environment	This involves continuous testing of security controls with gap remediation recommendations.
Penetration testing	Manual testing used to help test the effectiveness of an organization's vulnerability management program and associated controls within a defined scope	Test-specific predefined networks, assets, platforms, hardware, or applications are vulnerable to an attacker. Penetration tests are not focused on stealth, evasion, or the ability of the blue team to detect and respond, since the blue team is fully aware of the scope of the testing being conducted.
Red teaming	Designed to achieve specific goals, such as gaining access to a sensitive server or business-critical application	Emulate an advanced threat actor by using stealth, subverting established defensive controls, and identifying gaps in the organization's defensive strategy to better understand how an organization detects and responds to real-world attacks.
Blue teaming	Refers to the internal security team that defends against both real attackers and red teams; should be distinguished from standard security teams because of the mission to provide constant vigilance against attack	An ongoing team of defenders may engage against known or unknown red team attack exercises. Defenders can also benefit from purple team exercises that integrate defensive tactics and controls from both the attacker and defender teams.
Purple teaming	Manual, human-based exercise using real user behavior and exploits, with scenarios aligned to the organization's network to expose blind spots in security analyst response, tool efficacy, and gaps in security controls	Purple teaming aligns red and blue teams to provide an end-to-end and realistic APT experience and prioritized vulnerabilities to the organization.

Source: IDC, 2021

WHO ARE THE KEY STAKEHOLDERS?

The key stakeholders are listed in Table 2.

TABLE 2

Key Stakeholders

Role	Responsibility
Board members and C-suite	Protect the interests of shareholders and overall organizational well-being. Set strategy and long-term objectives, ensure sound financials, safeguard reputation, and provide leadership support for the security program.
Chief information security office (CISO)	Understand and maintain the security posture and resiliency. Communicate security priorities to other decision makers. Increase security effectiveness and efficiency.
Chief compliance officer (CCO)	Minimize noncompliance and related fines, loss of revenue, reputational damage, and potential lawsuits.
Security operations center (SOC) manager	Gather, correlate, and use threat intelligence to speed detection of threats and vulnerabilities and provide swift, effective response.
IT/security managers	Protect gateways, networks, endpoints, and cloud applications and workloads.

Source: IDC, 2021

HOW CAN MY ORGANIZATION TAKE ADVANTAGE OF BREACH ATTACK SIMULATION SERVICES?

Breach attack simulation services are relatively easy to get underway. Nearly all providers offer subscriptions, but there is one free, open source download. An evaluation based on IT/security objectives will help organizations identify outcomes and benefits, which will likely include the elements discussed in the sections that follow.

Improve an Organization's Security Posture

BAS services are a proactive way to reduce the number of vulnerabilities that threat actors can exploit, especially when they are used frequently or continuously. Point-in-time testing can miss vulnerabilities linked to periodic actions such as backups and related configurations. With BAS services, organizations can validate the security pipeline and confirm that security controls are working properly and delivering the expected level of performance. By closing gaps and addressing weaknesses in areas such as configurations, password/credential management, and IT/user hygiene, organizations bolster security, enhance resilience based on current threat conditions, and decrease the risk of breach.

Insert a Feedback Element Often Missing in Security Programs

Shape-shifting threat actors search for vulnerabilities they know are increasing with cloud migration, WFH, digital transformation, and other technology initiatives. Manual penetration tests and red/blue/purple team exercises cover only a small percentage of the attack surface. BAS services can supplement these traditional testing methods. Frequent or continuous testing helps organizations keep up with evolving standards and regulations as well as the constantly changing threat landscape. With BAS feedback, organizations can:

- Increase visibility and eliminate security blind spots.
- Test systematically all security controls in scope along the kill chain and implicate the diagnostics around the controls to identify points of failure.
- Capture quantitative metrics that help prove the value of security investments.
- Empower IT/security teams to combat the latest TTPs through alignment with the MITRE ATT&CK framework.

Increase the Effectiveness and Efficiency of Security Operations

Ideally, organizations can mature their cybersecurity posture and bolster detection and response capabilities through continuous controls testing and without adding complexity — a high priority given the talent shortage.

IT/security teams can zero in quickly on the most important threats and vulnerabilities and take immediate action to improve security controls informed by the MITRE ATT&CK knowledge base. This approach saves time and results in better resource utilization. As security controls are improved, potential exploits and routes to critical assets are reduced.

BAS services also enhance collaboration and communication by unifying cybersecurity teams, threat intelligence, and vulnerability management in the testing environment. Current cybersecurity team members can deploy BAS, minimizing the need to bring in outside resources or hire specialists. BAS providers also offer their capabilities through managed and professional service providers as buyers engage these providers to identify security gaps and perform any necessary remediation on a client's behalf.

In addition, an open BAS platform allows security teams to add their own content to the service provider's content. This results in a remediation "library" that is independent of individuals and boosts efficiency through knowledge sharing.

Make Informed Decisions Based on Visualizations and Reports

The BAS dashboard, visualizations, and reports save time, accelerate vulnerability and misconfiguration remediation, and improve security IQ. Provider offerings vary but include scorecards, heat maps, security postures, kill chain views, a zero trust assessment, MITRE-recommended mitigations, resilience scores, and critical assets at risk. Visualization capabilities include:

- Simulated attacks as they are happening, including attacker pivots and paths toward critical assets
- Aggregate views and drill downs on specific events
- Current test results and timeline trending

Executive-ready reports aid communication with security decision makers or influencers as well as board members.

ADVICE FOR TECHNOLOGY BUYERS

IDC analysts augmented internal research with briefings from AttackIQ, Cymulate, Guardicore, Pcysys, Picus, Reliaquest, SafeBreach, and XM Cyber.

IDC's view is that BAS services are an important capability for CISOs to have in the fight against determined adversaries to help organizations strengthen defenses where they are most needed. Given notable differences in provider capabilities, however, decision makers should be as clear as possible about what they are trying to accomplish before selecting a provider.

Essential guidance to buyers includes the following recommendations:

- **Clarify a provider's approach.** Determine whether the approach, such as attack simulation (or emulation), modeling attack routes to critical assets, or automated penetration testing, aligns with security objectives. No actual exploits should be used.
- **Understand a provider's go-to-market strategy.** Assess the fit with respect to geography, vertical industry focus, customer size, purchase routes, partnerships/strategic alliances, and support options. As providers mature, they are likely to begin or to expand their channel strategy, particularly through global consultancies, managed service providers (SPs), and managed security services providers.
- **Verify the scope of testing.** Be sure a provider can clearly describe each action undertaken by the platform, how it is executed, and how cleanup occurs after a breach attack simulation. Understand the role, if any, of playbooks, and how many a provider offers. Ask about the number and types of attack scenarios offered and understand the "build your own" options.
- **Explore the dashboard.** A comprehensive demonstration allows decision makers to assess the ease of navigation; the choice of testing types, such as what-if scenarios, playbook-based scenarios, and custom scenarios; the ability to set parameters for IP ranges; and other functionality. At least one provider offers the option of noisy or stealth mode. In addition:
  - Focus on scheduling flexibility for continuous, on-demand, and periodic testing, whether that is daily, weekly, monthly, or other options.
  - Evaluate visualizations for their ease of comprehension, drill downs, and links to related information and recommended actions.
  - Assess the metrics and measurement capabilities.
  - Walk through the standard and custom report options. Optimally, a BAS provider offers audience-specific reports and executive reports. The value of reports is higher when they link to security and risk controls.
- **Investigate platform architecture.** Validate the platform's ability to scale both testing and assessments. Be sure the following implementation variables align with organizational preferences and/or objectives:
  - **Range of capabilities (e.g., operating systems, on premises (production and/or test environments), multicloud, WFH/VPN, IoT, and sandboxes).** Be clear about connections with cloud providers. Discuss cloud security and the depth and breadth of compliance with standards and regulations.

    - **Installation.** This may involve agentless, agents/sensors, or deployment of dedicated machine or test points. Be clear about the inferences for the broader environment that can be drawn from dedicated machines or test points. Understand the time and resources required to deploy and start a service.
    - **Openness.** This allows users to build and add their own content in addition to receiving the content that comes with the service and/or ingest vulnerability scans from other sources.
    - **Vendor neutrality and/or integrations with third parties.** Understand, for example, how incidents are recognized and alerts are generated to trigger remediation. Determine the extent of alignment or integration with the MITRE ATT&CK framework.
    - **The endpoint of BAS services as well as the BAS provider responsibilities.** This includes post-testing cleanup. Security product configurations are generally owned by the subscribers.
- **Understand what remediation of security gaps entails.** Variables may include how severity ratings are determined, how risk is mapped and/or measured, and the scope of recommendations for some or all known vulnerabilities. Some BAS providers go beyond TTP information and offer overlays of attack vectors. Confirm the ability to identify root cause and to obtain additional relevant information and recommendations related to how to fix a vulnerability, how to retest, and where configurations need attention. Ultimately, security leaders will want to know to what extent vulnerability remediation can be ROI based.
- **Discuss use cases.** Use cases should demonstrate how organizations can accelerate security program optimization. Examples of use cases include red team augmentation, security control validation, product evaluation, managed security SP SLA validation, compliance mapping, and AI/ML engine training. The documentation for each use case should include guidance on how to execute the scenario.
- **Consider a provider's customer satisfaction/renewal rate.** Speak with an IT/security user in a peer organization to understand how BAS services were deployed, their value, and any limitations or concerns that arose through use.
- **Identify support options.** Support may be available directly from a BAS provider and/or from channel partners such as managed security SPs. Organizations with audit requirements may need 24 x 7 support.
- **Evaluate a BAS provider's consulting capabilities.** Determine if it makes sense to augment internal IT/security team skills gaps or accelerate testing/assessment with external experts. Also consider how external experts may be able to assist in areas such as education, tool rationalization, or customization of attack scenarios.

Before a final decision is made, pause for a reality check. However innovative the technology, its capabilities and metrics need to align with organizational objectives and contribute to desired outcomes. High-value outcomes in the fight against cyberattacks include improving the security posture, increasing IT/security team efficiency and effectiveness, and reducing risk and cost through breach prevention.

RELATED RESEARCH

- *IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment* (IDC #US46235320, September 2020)
- *MDR: The Next Generation of Managed Security Services* (IDC #US46427920, June 2020)

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com