# Utilizing Breach and Attack Simulation Tools to Test and Improve Security

**Published:** 17 May 2018 **ID:** G00349154

**Analyst(s):** Augusto Barros, Anton Chuvakin

Security testing is so challenging for technical professionals focused on security operations that many don't try it. Breach and attack simulation tools help make security postures more consistent and automated. Gartner has evaluated these tools to provide guidance for implementation and operation.

## Key Findings

- The focus of most breach and attack simulation tools is testing preventive controls; however, some also help with detection technologies and processes. Initial use cases include chief security officer testing of the infrastructure, testing versus "threats of the day" and activity testing after exploitation.
- BAS tools deploy from agents to browsers to agentless, peer-to-peer, and with/without SaaS modules. Testing scope differs across tools, from exploitation to postattack actions and phishing.
- Some BAS tools help prioritize the findings, and some assume you know your risks and can map findings to them. BAS findings prioritization is a key challenge for many tool users.
- Basic asset inventory, network topology and environmental awareness are critical, because tools won't test what they don't know is there. Hence, organizations with less-mature security postures might not benefit fully from implementing BAS.

## Recommendations

Technical professionals focused on security operations and monitoring should:

- Use these tools only if they're prepared to act on the findings and prioritize them based on the risks. Test security controls first, because they're the more mature use case for BAS tools.
- Select BAS tools focused on critical security testing requirements, such as preattack and postexploitation, and the components of infrastructure to be tested.
- Use the agent-based tools on select systems, and deploy network controls widely to test network security measures, from firewalls to data loss prevention.

- Expand from preventive technology controls testing (e.g., firewall, endpoint protection platform and secure web gateway) to detection technologies (e.g., DLP and security information and event management), and then to process testing (e.g., security operations center triage).

## Table of Contents

## List of Tables



## List of Figures



# Analysis

An interesting paradox has emerged in information security. Penetration testing has been part of the information security lexicon for nearly a quarter of a century. However, most organizations — even some with nine-figure security budgets — have no idea how operationally effective their security technologies are. Has penetration testing just been done badly, or it is the wrong tool for the job?

Although it may sound overly dramatic, there is a veritable epidemic of misconfigured, disconnected, turned off, and nonoptimized security tools all over the organization. There is also a possibility that an attacker that compromises a system and breaches an organization will disconnect the controls or interfere with their operation. Many recent breaches involved information security controls that have failed to pick up evidence of the attacker's activity, as well as controls that were disabled by an attacker or an IT team.

Similarly, there's no proven way to test managed services SLAs and security effectiveness, except when it's too late, because the organization is already under attack. Even when organizations are aware of gaps in the security posture, they don't know where to start, especially in the case of a recent acquisition, in which the new environment might be completely unknown.

What is the answer to this scary situation? Admittedly, simply insisting on more diligent audits of deployed technologies is not the answer. If that worked, we wouldn't be where we are now. Rigorous penetration testing by consultants of ever-increasing skill may be part of the answer. However, expert-led penetration testing is inherently an infrequent activity. It is inconsistent, possibly disruptive to the organization and its mission, and it's often scoped incorrectly (quality penetration testing is also expensive).

Recently, a new category of solutions has emerged to help with this problem. This new technology, known as breach and attack simulation (BAS) tools, enables organizations to perform many types of security testing, attack and threat simulation, and control effectiveness assessments. BAS vendors promise that their products achieve these tasks with a high degree of automation, a high level of safety (because no attacks hit production assets), and directly on the clients' production networks.

This research looks at this emerging technology and provides guidance on the selection, deployment and operation of these tools. Notably, few best practices have emerged thus far, even though some organizations have successfully used these tools for several years.

This research also addresses the blurred line between these tools and other testing approaches and technologies. For a comprehensive look at the modern security testing landscape, review "Pragmatic Testing Approaches for Security."

## What Are BAS Tools

As with any emerging tool category, the challenge is often about defining the boundaries of this new technology, compared with adjacent tools and product categories.

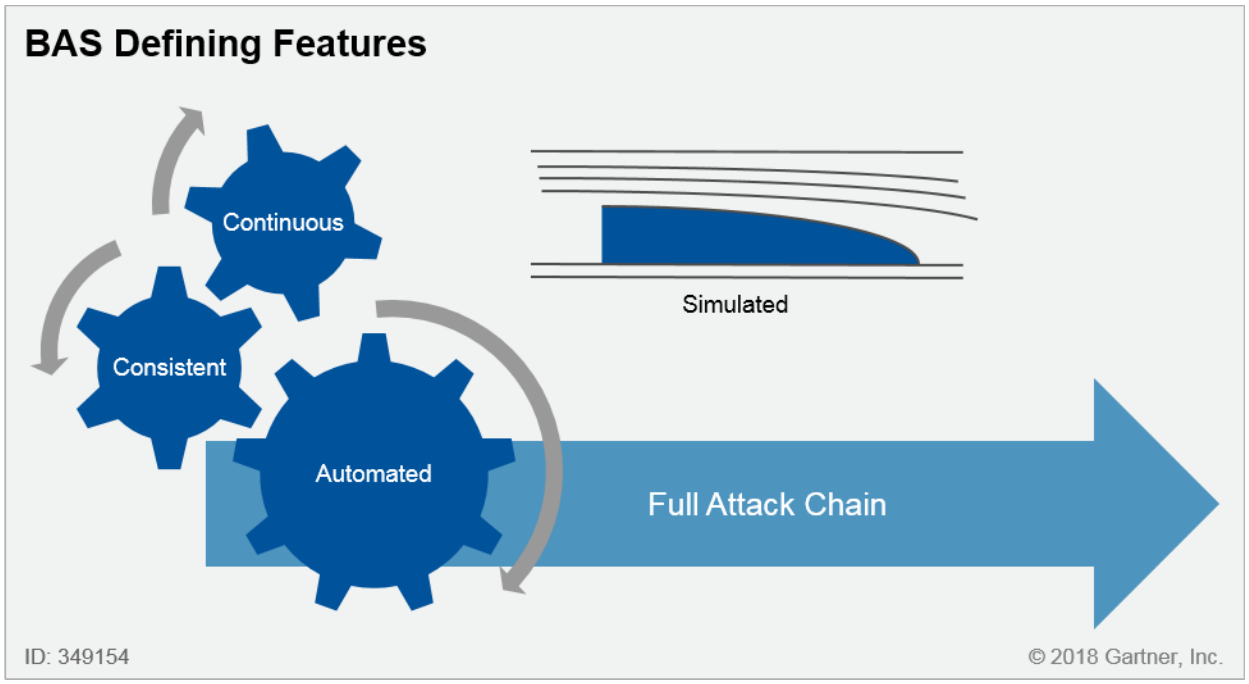
---

BAS tools simulate a broad range of malicious activities (including attacks that would circumvent their current controls), enabling customers to determine the current state of their security posture.

---

Some exclusively focus on postexploitation stages, such as lateral, data exfiltration, etc.; others also cover the exploitation stages. An additional discussion is required to explain what "simulate" really means, and what exactly is being simulated, versus what is being executed (see Figure 1).

Figure 1. BAS Defining Features




Source: Gartner (May 2018)

An interesting observation emerged during this research. Some BAS vendors represent their tools as essentially a way to simplify, optimize and improve penetration testing, such as by making it continuous or by extending it to cover more attack phases and/or more assets. Other vendors vehemently argue that their BAS offerings have nothing to do with the art of penetration testing and, instead, represent a way to instrument security control effectiveness testing.

One BAS tool user pointed out that penetration testing helps answer the question "can they get in?" while BAS is answering the question "do my security systems work and work well?" These questions are clearly connected, but they're not the same.

> Penetration testing helps answer the question "can they get in?"; BAS tools answer the question "does my security work?"[1]

For example, Verodin and Circumventive highlight that they are deployed to check the effectiveness of security controls and to provide evidence for selecting and deploying security technologies.

The most difficult separation between BAS and adjacent tools would be related to so-called penetration testing tools, such as Core Impact, Rapid7 Metasploit and Immunity CANVAS. At this time, Gartner believes that the critical differentiating factor between BAS and these tools is that BAS is meant to operate automatically, often in a continuous way, whereas the other tools need a human

operator to drive them. The other critical distinction is that BAS capabilities do not include hurling real exploits at real targets. This said, some vendors actually combine BAS capabilities with penetration testing and exploitation capabilities, and can be switched from simulation mode to attack mode (Picus Security and XM Cyber are two examples).

Another category that may be confused with BAS is a traditional vulnerability assessment (VA) tool. The notable difference is that VA tools check systems for published and known vulnerabilities, while BAS focuses on multiple stages of the attack. Exploiting vulnerabilities may be one of those stages; however, they also include data exfiltration, lateral movement and other attacker actions unrelated to exploitable vulnerabilities. Some BAS vendors actually cover the entire cyber kill chain.

Finally, BAS testing may be occasionally confused with an audit of controls, frequently mandated by some compliance frameworks, standards, regulations and contracts. These audit procedures often focus on the presence of controls, but without verification of their effectiveness against realistic threats or the control outcome. BAS tools are focused on outcomes only, identifying issues on the real behavior and outcome of the controls.

An organization using a BAS tool, for example, was able to identify that a certain implemented security control was not blocking attack attempts during certain times of the day. After investigation, the issue proved to be a control technology problem during peak capacity situations. This type of situation can't be identified during a simple control presence verification, but can be identified with consistent BAS-based testing.

## Simulation or Execution?

Understanding exactly what BAS tools do and whether you need to deploy one, is heavily influenced by the concept of simulation. Specifically, it's worth questioning whether these tools present a good way to test real-world security controls, if all they do is simulate real threats. So, how real should such simulations be?

---

Are BAS tools a good way to test real-world security controls, if all they do is simulate real threats? How real should such simulations be?

---

Naturally, a security professional operating a BAS tool for your organization is not a threat actor, a case of malicious insider notwithstanding. Hence, the threat is definitely not real, but simulated. However, performing a simulated attack by downloading real malware on a production system may end up becoming a real threat, if executed wrong. The same applies to any tests in which vulnerabilities in production systems are exploited — it is well known that system exploitation may have adverse effects and cause denial of service (DoS) conditions.

There is a clear limitation on the attacks that can be simulated by BAS tools. These tools can only simulate known attack techniques; no BAS tools will be able to simulate an attack based on a technique or even on an exploit that is still unknown. Many BAS vendors run research labs that may invent new attack techniques, which are then included in their test libraries. However, some of the

attacks known to a simulation vendor may well not be known to clients and their security vendors, essentially acting as an unknown attack.

An expanded view of the real and simulated activities performed by BAS tools is presented in Table 1.

Table 1. BAS Tool Functionality (Real and Simulated)

| Action | Simulated or Real? | Explanation |
|---|---|---|
| Threat | Always simulated | The intent of an employee running a BAS tool is not the same as the threat actor performing similar actions. |
| Breach | Always simulated | BAS tool operation is not a data breach, because data access is not obtained by nonauthorized malicious parties. |
| Malware | Simulated, real | BAS may use real malware in a safe setting (e.g., transfer, not execution), defanged malware or custom malware-like, but harmless code. |
| Exploit | Simulated, real | Some BAS tools can use real exploits, versus simulated targets; others will generate data and perform activities similar to those performed by the exploit, but without actually attacking. |
| Postexpolitatation<br>Pre-exploitation | Real | BAS performs the same actions for reconnaissance, lateral movement or data exfiltration that the attacker would perform. |

Source: Gartner (May 2018)

The above framework enables clients to evaluate the reality of their BAS-focused testing. For example, organizations planning to test exploit mitigation controls will need to deploy a BAS tool that executes real exploits, because there are limits on how one can simulate that type of activity. However, if the intent is to check data exfiltration detection, then simulated attacks will be enough to achieve the desired outcome, as long as data is being transferred from inside to outside in a manner similar to existing exfiltration techniques.

## Security Measures Tested by BAS Tools

Understanding the expectations for the tests performed by the tool is important when selecting the right simulation approach, as well as confirming that the tool is trying to answer the right questions.

An overview of how BAS tools can test certain controls and what type of activity is employed for each case is presented in Table 2. Use this information to determine whether the tool being considered will be able to test the right controls against the expected threats and scenarios.

Table 2. Control Type and Security Process Testing

| Controls and Processes | Question Asked |
|---|---|
| Attack Prediction | Where would an attacker more easily start?<br>How many steps may be needed to achieve a particular outcome? |
| Preventative Controls | Was the attack blocked before reaching the target?<br>Was the attackers able to achieve their goals via this action?<br>Was the connection to a malicious site successful? |
| Detective Controls | Was the activity logged?<br>Was the right alert triggered?<br>Did security information and event management (SIEM) correlation work? |
| Monitoring Process | Did a human analyst respond in time?<br>Was an analyst able to notice, prioritize and act on the alert? |
| Response Process | Was an incident response process triggered? |

Source: Gartner (May 2018)

## A Key Question: BAS Versus Penetration Testing

BAS tools' proximity to penetration testing activities necessitates an additional discussion, because some BAS vendors sometimes link BAS with penetration testing capabilities and activities.

Table 3 illustrates some of the differences between using BAS tools, penetration testing and red team operations.

Table 3. BAS Versus Penetration Testing and Red Team Testing

| | BAS (tools) | Penetration Testing (process) | Red Team Assessment (process) |
|---|---|---|---|
| Timing | Continuous | Periodic | Periodic |
| Primary objective | Control testing | Validation/break-in Compliance | Readiness and training |
| Consistency | Complete (can run exactly the same test every time) | Low to medium (may follow a script, but still human-driven) | None (tailored to the conditions found during execution; delivers maximum sophistication) |
| Real attacks and malware artifacts | Yes (malware, real exploits versus simulated targets) | Some | Yes |
| Simulated attacks and malware artifacts | Yes | No | No |
| System compromise | No | Yes | Yes |
| Role of a human operator | Defines the tests; then it runs automatically | Perform the test using some automated tools, and manual actions | Define, perform test using human creativity; may use custom tools |
| Automation | Testing, results analysis and reporting | Some, such as scanning address spaces, looking for vulnerabilities to exploit | Very limited, to avoid detection |
| Reporting | Tool provides a report | Human crafts the report | Human crafts the report |
| Killchain elements | All stages; often a heavy focus on stages (lateral, exfiltration, etc.) postexploitation | Usually a heavy focus on recon, exploitation and breaking in | May include all attack steps, but some variation according to scenarios (e.g., internal threat scenario) |

Source: Gartner (May 2018)

The table shows that some activities or objectives are better-suited to penetration testing and red teams. Organizations may decide to replace some of those activities by running a BAS tool; however, the practitioners are still required for certain objectives. BAS tools may be used to test some human-driven processes; however, those are usually better assessed by human-driven exercises. If you want to check how an incident response team reacts to the presence of a threat actor in the environment by adapting their tactics and tools, BAS tools won't be able to do that.

If you look at how mainstream, especially compliance-driven, penetration tests are performed, you'll see that it's not very different from a vulnerability scan followed by some exploitation. However, it's

different, because it involves exploiting the issues, and that exploitation can move the assessor to another point in the network that can be used for another round of scanning and exploitation. This is a type of penetration test that may eventually be replaced by BAS tools, at least those tools that combine BAS functions with real exploitation capabilities.

Some BAS tools can automate that simple penetration test, performing the basic cycle of scan, exploit and repeat. If this can now be done with the simple click of a button, why would you use a human to do it? The tool can ensure consistency, provide better reporting and do the work faster, not to mention it requires less skill. With the availability of BAS tools, you can rely on humans for the red team type of activities, while leveraging the tool for the simple tests.

## The Role of BAS in Security Testing and Assessment

As described in "Pragmatic Testing Approaches for Security," organizations use different types of tests and assessments, based on their objectives. Some processes, such as the secure development life cycle (SDLC), are most often assessed indirectly. If BAS tools are just one more way to perform security testing, what is their role in your organization's overall toolkit of security testing and assessment practices?

---

BAS tools are the best option when consistent, systematic and frequent tests of production security controls are required.

---

Large enterprises report having 30 to 70 security vendors. These controls are often touched and changed to keep up with threats and business needs. Frequent changes introduce errors and deficiencies, and some temporary changes can become permanent unintentionally. On the other hand, some organizations' rigid change management processes prevent beneficial changes and evolution of their controls.

Without continuous testing, errors and deficiencies may go unnoticed for a long time, or worse, be discovered by real attackers during a real incident. Using BAS is the most effective way to continuously check for issues and fix them before an attacker is able to exploit the deficiencies.

BAS tools can also play a role in less-frequent assessments. Just as security auditors use vulnerability scanners during their assessments, BAS can be used as part of point in time assessments. However, this opportunity is limited by the architecture of most BAS tools. These tools require the deployment of components in the many segregated networks that may be sources or targets of malicious activities. This complex deployment process reduces its usefulness for a single, point-in-time assessment. Still, a new security program, a corporate merger and other major changes may necessitate a one-off BAS use.

BAS can also be used by organizations trying to improve their awareness of current risks. BAS findings may be seen as more meaningful than simple VAs. These findings can be incorporated in a broader security assessment, but the need to properly assess the risk related to the identified

issues may be overwhelming. Assessing the findings from a higher-level point of view is an alternative to avoid that pitfall.

## Build Your Business Case Using BAS Adoption Drivers

What motivates organizations to procure, deploy and operate BAS tools? The following drivers were observed:

- The desire to save money by maximizing the effectiveness of existing security controls
- The desire to obtain an objective and repeatable measure of their security posture
- Past incidents that were supposed to be prevented or detected by existing controls
- The need to determine the right security control mix versus the realistic risks they face
- The need to quickly determine the exposure to certain threat scenarios

One of the BAS vendors has defined their primary mission as "validate the system of systems is working correctly" and it serves as a useful underlying theme for all of the above.

---

The mission of BAS is to validate whether the security "system of systems" is working correctly.

---

Use this information to define and refine your business case for procuring a BAS tool. The above also means that procuring a BAS tool in the absence of some security controls configured to the best of your ability is inadvisable. Most organizations are focusing on ensuring that existing controls are performing according to their expectations. The absence of controls can be identified by simple paper assessments that are faster and less costly to perform than implementing a BAS tool.

## Observed BAS Use Cases

Identifying and understanding the BAS use cases most relevant to your organization is a critical step in understanding if you really need this type of tool. Narrowing down your use cases will help you identify the optimal tool for your environment and your needs. Gartner research reveals the following use cases for BAS tools:

- Control effectiveness measurement
- Enhanced penetration testing and red team operation
- Reporting and prioritizing security controls
- Security purchase improvement
- Reporting on security controls

- Proof of controls and compliance

BAS use cases are discussed in depth in the sections that follow.

### Control Effectiveness Measurement

This principal use case is roughly what these tools are all about today — determining how effective your deployed security technologies are, as an overall system of security systems.

Specific examples include:

- Continuously finding control mistakes, such as configuration errors and disconnected sensors
- Other security product configuration assessments
- Testing deployed, preventive control configurations versus recent threats
- Finding gaps in controls to mitigate them before the attackers show up
- Testing security operations center (SOC) alert triage and response processes
- Testing and assessing managed security service provider (MSSP) SLAs: this creates alerts and evaluates how MSSPs handle them.

### Enhanced Penetration Testing and Red Team Operation

Although this research explains that BAS tools are not equivalent to penetration testing, several of the tools have been used by internal red teams and penetration testing units quite successfully. Augmenting penetration test operations is a use case for many BAS tools. Some organizations choose to enhance testing with continuous, BAS-based testing between official quarterly or annual penetration tests. Others may choose to run a BAS tool after the penetration test lessons have been incorporated, as a validation control. Yet another group uses BAS to expand the scope of their testing, and focus their tests on the assets typically not in scope for a full-blown penetration test.

Furthermore, some will use BAS tools to free up penetration testing time, budget and opportunity to perform more-sophisticated tests. These may include real threat replication or focus testing in areas that are difficult to automate, such as application-oriented testing.

### Security Purchase Improvement

A separate use case from the control assessment, this focuses on improving the utilization of the security budget and identifying which tools to purchase or maintain. Depending on the results, BAS tools can also be used to justify the retirement of existing, but no longer effective, controls. Some other specific opportunities related to this use case are:

- Improve, validate or accelerate proofs of concept (POCs) of new security tools.
- Run the same consistent tests against the shortlisted security vendors
- QA test the vendor product configuration after deployment

- Find gaps in existing controls to help identify new controls for purchase

### Reporting and Prioritizing Security Controls

This use case is related to the creation of security metrics and performance indicators. The tools are used to create a consistent baseline of overall security, using repeatable and automated methods to continuously assess security status. The key capability of BAS tools for this use case is the ability to perform the same testing approach consistently. With consistent testing, it's possible to compare the results between two instances of the same test. These results are turned into metrics that are tracked and included in reports to CxOs and the board.

Some organizations may use it to generate a risk scorecard, eventually leading to partial competition with integrated risk management (IRM) solutions. In those cases, the tool operators must understand the limitations due to reporting only the risks that the tool is able to technically test.

### Proof of Controls and Compliance

Although no compliance mandate prescribes these tools by name, Gartner clients report using the tools to prepare for audits and assessments. Few, if any organizations, have purchased the tools for this, so this is not a driving use case, but an auxiliary one. Some will use the tools to provide evidence to clients and business partners about their security posture, eventually replacing the need for a test or an assessment by them. Some may also try to fulfill compliance requirements, such as penetration testing for Payment Card Industry Data Security Standard (PCI DSS). However, there are still questions about whether BAS-performed tests are acceptable by each compliance mandate, framework or even a contract.

## BAS Technology in Depth

At this time, the BAS technology spectrum covers multiple form factors, testing methods and deployment methodologies, aimed at specific types of controls and environments.

### Basic BAS Tool Functionality

Identifying a set of mandatory functions for this new tool category is difficult, and many vendors vary not only in the functionalities delivered, but also in their philosophies about security testing. However, the list below may be treated as an emerging set of functions that BAS tools will converge to in the near future, while some of them are already mostly there.

Emerging core BAS capabilities and functions include:

- The ability to test all phases of an attack, from the exploit to postexploitation, persistence and maintaining access (some BAS tools place much higher importance on postattack activities)
- The capabilities to test continuously, periodically and on-demand

- The ability to deliver safe tests with no or extremely low chances of interfering with business operations, and no to low user interference when deployed on production assets
- Functions to test both network and endpoint security controls
- An out of band (OOB) attack method library, ideally based on or mapped to MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and pre-ATT&CK frameworks (library should have individual tests and attack campaigns)
- Content updates for the library to continuously deliver simulation content relevant to the threats of the moment
- A customizable attack/campaign logic that is flexible enough to address present and likely future threats
- Some form of severity prioritization for test findings
- Integration with external tools, such as security operations, analytics and reporting (SOAR) or SIEM, to gather logs and alerts, test detection, etc.

This list is not exhaustive, nor is it a defining list of characteristics of BAS tools. The disparity of approaches and capabilities from one vendor to another is substantial, which is a common attribute of nascent markets.

As the market evolves, this broad set of characteristics should converge to indicate what the minimum and defining capabilities of these tools are. Until then, organizations should carefully assess whether the capabilities of the tools being considered for deployment are aligned to their most important use cases.

## BAS Testing Methods

BAS tools can perform multiple types of tests according to the security controls under scrutiny or the threat scenarios being simulated. Table 4 presents the most common tests provided by these tools and the components required to perform them.

Table 4. Testing Methods and Required Components

| Domain | Test | Deployed Components Required | Activity Performed by a BAS Tool |
|---|---|---|---|
| Network | Firewall test | Sensors deployed on multiple segments/ sides of the firewalls, and on the internet | Connection attempt |
| Network | Network intrusion prevention system (NIPS) test | Sensors deployed on both sides of the firewall or NIPS | Remote exploitation attempt or replication of traffic generated during exploitation |
| Network | Data loss prevention (DLP) test | Sensors deployed in the environment protected by network DLP | Data exfiltration attempt, such as file upload |
| Network | Segmentation test | Sensors deployed on both sides; intended connection | Access, connection or data transfer attempt |
| Email | Email data exfiltration test; secure email gateway (SEG) test | Component deployed on one client machine and outside the perimeter | Email with confidential data sent out |
| Email | Phishing email delivery | Component deployed on one client machine and outside the perimeter | Phishing email delivery to a sample client mailbox |
| Web | Secure web gateway (SWG) test | Component deployed on one client machine and outside the perimeter | Access or data transfer to a malicious site |
| Endpoint | Malware download and execution | Test component on template system OR Test component on a sample of production systems OR, Rarely, test component on all production systems | Transfer and/or execution of malware on a test system |
| Endpoint | Privilege escalation test | Test whether regular credentials on a production endpoint can be used to obtain privileged credentials | Extracting credentials from memory; executing local privilege elevation exploits |
| Monitoring | SIEM test | A component integrated with an SIEM via API | Inject events into a SIEM and see whether it correlates them to generate the right alert |
| Response | SOC process test | Any detection control: NIDS, network traffic analysis (NTA), DLP and/or SIEM integration | Trigger events and use the alerts to refine SOC triage and initial response processes |

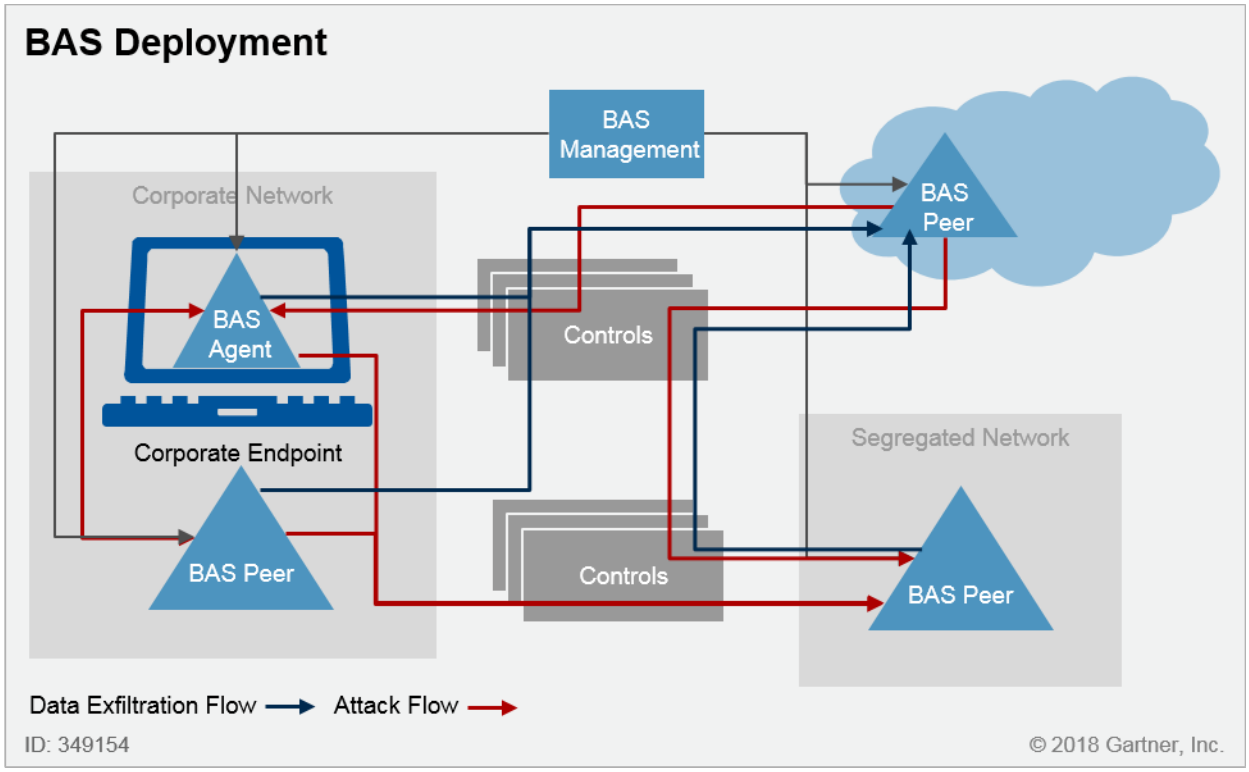
Source: Gartner (May 2018)

Knowing and understanding the available testing methods will enable you to better compare the solutions available in the market. Another useful way to assess available testing methods is to map them to the MITRE ATT&CK framework. This mapping will provide a good understanding of what types of malicious activities are tested by the tools and which ones are not in scope for the tests.

## Example BAS Deployment Architecture

Figure 2 represents a typical BAS deployment architecture. Not every vendor offers agents, network components and cloud components, and not all of the components described may be necessary for your use cases.

Figure 2. BAS Deployment




Source: Gartner (May 2018)

As shown, the deployment is likely to cover one or more endpoints (some vendors aim at fewer agents; others suggest covering all production endpoints) and one or more BAS peers (i.e., separate systems deployed in their own network segments). In addition, it may also include a management server and cloud components (i.e., anything deployed outside the client environment).

BAS vendors with more complex deployment architectures typically provide a broader set of testing methods and technologies. For example, many tools require the deployment of more than one internal component (such as the "BAS Peer" from the figure above) to effectively test attacker lateral movement.

Some BAS tools suggest deploying their agents on every production system and link into the SIEM for detection testing. This will allow you to test endpoint security controls in place, and not rely on sampling. The SIEM integration delivers closed-loop automated detection testing, such as what Verodin does to test SIEM detection content and tuning. The question of whether such complexity is

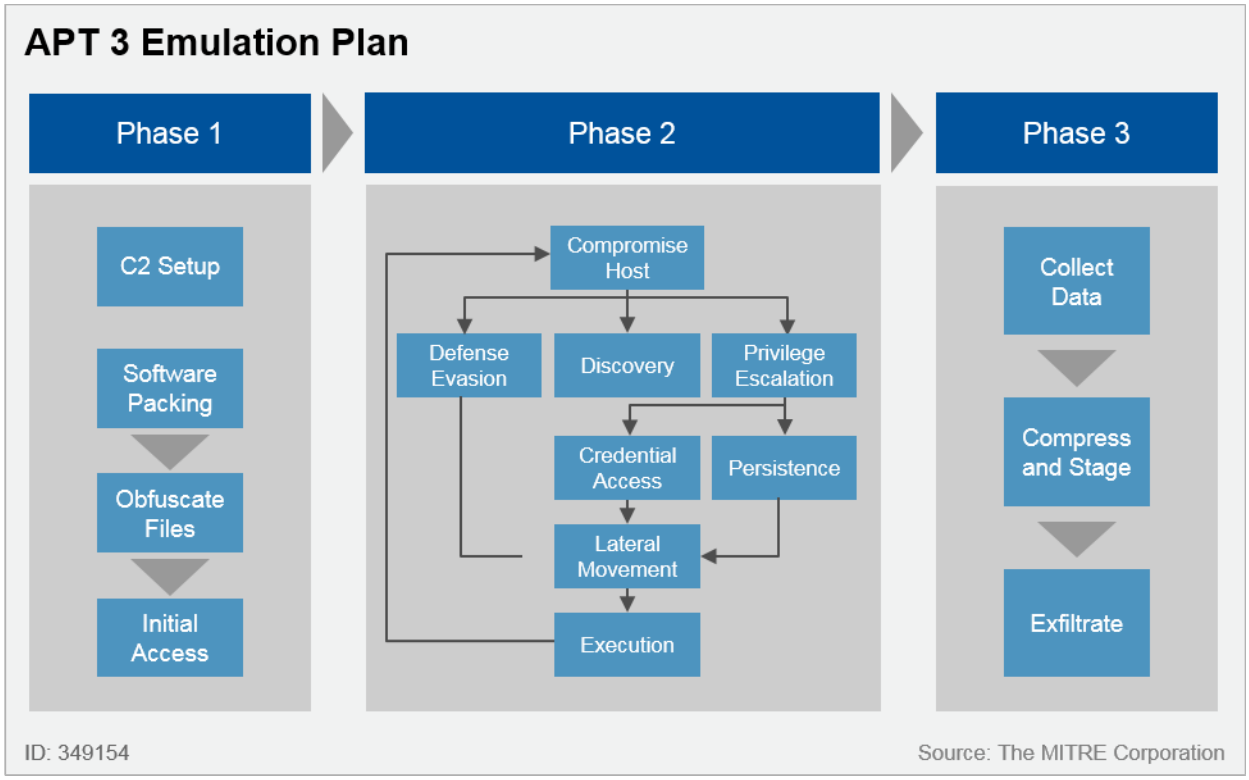
really necessary can be answered by your use case requirements and risk tolerance (not only the risk of not properly testing something, but also of causing business disruption through testing).

There are also tools that deploy only a single component. They are dramatically simpler, but only execute a small library of tests, typically involving inside to outside connectivity. For example, ThreatCare is deployed as a simple, browser-based component that can be used to perform a small lineup of tests, such as for data exfiltration and malicious site access.

## Complete BAS Test Example

Several excellent examples of a complete threat simulation can be found on the MITRE ATT&CK site. The main advantage of these examples is that they are not tied to any particular BAS vendor. For example, a complete APT3 (named so by FireEye, also known as GOTHIC PANDA in CrowdStrike materials) simulation can be found at Adversary Emulation Plans (see Figure 3).

Figure 3. APT 3 Emulation Plan




Source: MITRE

The plans cover the methods, tools and tactics by this particular threat actor, such as their preferred exploitation tools, methods of lateral movement, stolen data staging and exfiltration.

(For additional details, see "APT3 Adversary Emulation Plan.")

## Critical: Dealing With Test Results

The value of any security testing or assessment practice is directly related to how the findings are used. Although it may seem trivial, for some practices that have been around for years, such as VAs, acting on the results remains a major pain point. This is no different with BAS tools.

---

Simply running a BAS tool will not make any organization more or less secure. Only the actions performed based on the results will demonstrate whether the tool was able to provide value.

---

As mentioned in the use cases section, some organizations use BAS to obtain better situational awareness and to understand and communicate their own risks. This doesn't mean the results are not being used operationally. As long as the results produced by the tool are being fed into a process that provides value and are useful for that process, the tool is providing value.

Nevertheless, the most common objective of organizations using BAS is to find issues to fix. First, the security team should develop an appropriate definition of roles and responsibilities. Organizations should not underestimate the resource requirements, including skills requirements, that are necessary to deal with the results of this additional testing layer. The second, but no less important, concern is how the findings will be prioritized.

Prioritization of security findings is also a common problem for other types of tests and assessments. The best practice is to address findings based on risk, but that may not be as easy as it sounds. How should you compare the risk of an intrusion prevention system (IPS) not blocking certain attacks versus the possibility of lateral movement to a segregated network? Some tools will provide a rating for the severity of the finding, but as they often lack the internal context of the involved assets, it will not be enough to allow a proper risk comparison to be made.

Assessing the risk related to findings from BAS tools should consider information about threats and potential impact. Some of the findings may be related to attack vectors that are not popular and may not be a concern for your organization. They may also be related to unimportant assets or networks, which could indicate a low impact for a potential breach.

In some cases, BAS tools may be used in a manner similar to VA tools. They are usually applied for frequent testing (monthly, weekly or even daily) and can uncover a large number of issues to be addressed. Cases like this should be controlled out of the overall risk management program. Findings are managed through an operational policy that reflects the risk appetite of the organization. For example, a vulnerability management policy may establish that vulnerabilities with a certain level of severity must be remediated in less than 30 days. Unless the issue is not treated as defined by the policy, it is not reflected as an individual risk on the higher-level risk management process. Issues that cannot be treated as defined by the policy may be individually assessed for risk and inserted into a risk register.

Finally, BAS test results are sensitive data, because (in a manner similar to VA results) they reveal your organization's security holes, weaknesses and deficiencies. Treat the reports and outputs as

sensitive data and make a decision regarding the use of cloud storage for such data, based on your policies.

## BAS Vendors and Open-Source Alternatives

Gartner has encountered many BAS vendors with different test libraries, deployment form factors and even philosophies regarding security testing. Due to rapidly evolving vendor capabilities, no technical comparison is realistic at this time — a representative list of vendors is noted below:

- **AttackIQ** has functions for testing controls and processes, as well as creating the remediation plans for findings. It also maintains a user community to share content, such as test scenarios.
- **Circumventive** has its DNA in DLP "leak testing," but has recently expanded to a framework for mostly network-based threat simulation.
- **Cymulate** is a relative newcomer to BAS, performing agentless and agent-based tests (with a minimal number of agents needed), robust email tests and the ability to model tests according to the most common threat scenarios.
- **Pcysys** is another option that performs real exploitation as part of its attack simulation. Pcysys is an agentless solution and its tests will automatically identify new targets for exploitation and leverage obtained credentials and privileges as part of the attack.
- **Picus** has a well-balanced feature set that includes both network and endpoint testing; the tool has exploitation functionality in addition to BAS.
- **SafeBreach** is one of the oldest BAS vendors, with a sizable client base and a mature, well-balanced set of functions.
- **ThreatCare** aims at low-maturity clients, and shines with its basic, browser-based deployment (and optional agents); however, it sacrifices some categories of testing approaches as a result.
- **Verodin** is notable for its approach to detection and monitoring testing via a bidirectional SIEM integration, and for popularity among the well-resourced large clients.
- **XM Cyber** sits firmly between BAS and penetration testing, and delivers capabilities focused on their threat research. The tool can also exploit a system, if configured to do so.

### Related Open-Source Efforts and Frameworks

Recently, notable open-source options for threat simulation have emerged. Many take advantage of the MITRE ATT&CK framework to provide consistent testing and help drive the community development efforts to those attacks and techniques that haven't been developed yet. Some of the notable threat simulation projects are:

- Microsoft Powershell (Invoke-Adversary)
- Endgame (Red Team Automation [RTA])
- GuardiCore Labs (Infection Monkey)

- Network Flight Simulator
- Metta
- Microsoft Windows Batch (APT Simulator)
- MITRE ATT&CK (CALDERA)
- Atomic Red Team
- NSA unfetter

## The Future of BAS tools

One of the expectations for the future of these tools is, of course, their increasing adoption. As of today, a tiny minority of organizations is using them, and most have large, enlightened security ops teams. Similarly, BAS vendors are expected to expand their coverage of test methods and covered targets. A recent trend has been to mimic the behavior of existing threat actors, such as APT3 and other groups.

Given that some of the vendors are mixing BAS with penetration tester enablement, more of this is expected to trickle down. However, some of the vendors shy away from penetration testing and plan to develop their tools toward broader security instrumentation.

This may lead to a split in the BAS market between the tools that align with penetration testing automation, and those that align with security instrumentation requirements.

Tighter integration of these tools with enterprise risk dashboards and IRM tools is also expected, just as with SOAR for semiautomated resolution of the findings.

## Strengths

BAS technology strengths include:

- **It is one of the first repeatable and objective ways to test security as deployed in the real world.** Most of the currently used security testing methods rely substantially on the expertise of the human expert running the test. BAS technology allows for more automation and offers a more consistent and repeatable approach to testing that can also be done continuously.
- **It can be used for continuous or, at least, frequent testing.** Unlike other methods, finding configuration mistakes and other issues may call for continuous operation, and some BAS tools deliver that capability.
- **It can test a wide range of controls and assets.** It has a wide variety of testing approaches and technologies. These tools can be used to test a broad range of security controls (and their combinations), as currently deployed across a large spectrum of production environments.
- **It does not require expensive human talent and "one-off" methodologies.** Admittedly, successfully defining and considering the testing may require expertise. However, the ongoing

operation of these tools does not require a great deal of knowledge and expertise from the human expert.

- **It can test not just the exploitation, but postexploit attacker actions and even insiders.** BAS tool developers have spent a lot of energy simulating and modeling what the attackers, especially advanced attackers, do once they break into the network. As a result, BAS tools enable substantial postattack activity testing and not just exploitation and penetration.
- **It can simulate particular actors and specific malware that is of interest.** An interesting advantage of these tools is that you can actually use them to model a specific recent threat actor or threatening activity. Thus, you can learn to proactively test your controls against a particular emerging threat.
- **It helps train the security team/blue team.** Some clients report that the primary value of these tools is related to training and making the defenders ("the blue team," the SOC, etc.) better over time, especially in the absence of real advanced threats hitting the company. The value of using BAS for this is similar to that of a cyber range.

## Weaknesses

BAS technology weaknesses include:

- **The nascent market is characterized by a huge difference in technology coverage and test types.** BAS is an immature space, with a wide variety of available methods, technologies and approaches. Given its lack of maturity, comparative testing of the tools will present a challenge to most organizations.
- **It lacks the depth (and "off the books" creativity and adaptability) of a real red team test.** The tools are not expected to replace a human red team test any time soon, because they lack the creativity of advanced human attackers.
- **It puts one more set of action items to the security team plate.** When deployed without sufficient preparation and thinking, these tools may be yet another source of action items on the security team's plate. The risk is that BAS findings may lack priorities and real-world relevance.
- **Tools lack robust prioritization of the findings.** A difficult problem on its own, these tools often lack robust mechanisms to prioritize the findings. Some vendors directly throw this problem "over the fence" to the client, because, presumably, they know the risks better. (Some do, while many don't.)
- **Detection process testing may have many manual steps.** Although testing threat detection is within the capabilities of many such tools, unlike testing the preventative controls, detection testing would involve several manual steps for most tools. Some solutions, such as AttackIQ and Verodin, provide some automated detection testing, but this comes at the cost of a larger initial integration effort.
- **BAS does not simulate application penetration testing.** An inherent weakness of the tool category of BAS tools is that they do not help with application penetration testing, These tools

focus on infrastructure and deployed security controls only. This may appear in the tools in the future.

- **BAS tools do not test recovery and remediation procedures.** BAS is meant to be safe, so, with the exception of special circumstances and manual approaches, BAS will not automate the testing of recovery and remediation procedures.
- **BAS tools that have exploitation and penetration testing functions are a safety risk.** Exploiting real systems is not a core BAS function, but vendors with hybrid BAS-penetration testing tools run increased risks of system disruption.

## Guidance

The guidance section is organized based on the phase of your organization's BAS or security testing project.

### Planning for BAS

#### Include BAS in Your Security Testing Program

Given that this is a new tool category, embark on your journey to deploying BAS tools in the context of your overall security testing effort. This will help your organization mix BAS with other testing methods (such as the staple of many — penetration testing). Thus, you can achieve meaningful security improvements.

Also, include BAS-based testing in all new security technology acquisition plans, because they simplify the testing of new security technologies. This will help identify what security technology needs to be deployed next. Check "Pragmatic Testing Approaches for Security" to see how BAS can be part of a testing strategy and what role it should play, depending on the other tests that are also performed by the organization.

#### Consider BAS After Security Architecture Build-out

Use the tools only after you have deployed your desired controls and optimized them to the best of your ability. Many organizations make the mistake of performing penetration tests on their environments before hardening them. This results in spending money to prove the obvious. Similarly, using BAS tools delivers value only when there are controls to be tested and improved.

#### Gather Prerequisite Data and Plan Ahead

As a key prerequisite, obtain a basic understanding of network topology first. This is especially critical if network segmentation testing is also in scope.

Deploying BAS tools without sufficient preparation will yield another list of things to be fixed. This can be a big issue for overwhelmed security teams. Before you begin, devise a detailed plan for

dealing with the results using the advice in this research. Remember that BAS delivers security value only if you act on the results.

## BAS Selection

### Review BAS Tools Capabilities With the Need in Mind

BAS usage reveals the immature nature of this technology and big differences in test coverage — and even different philosophies regarding security testing manifested by the vendors. The organization should closely watch its requirements versus the vendor capabilities. For example, if focused on testing your detection and response procedures, select the tool with ready-made SIEM integration.

### Find Testing Use Cases, Then Select BAS Tools to Match Them

Furthermore, select BAS tools focused on your critical security testing requirements, such as preattack, postexploit, phishing, etc., and the components of infrastructure to be tested. If you want to know whether the attacker can exfiltrate the data, review vendors' functions focused on many data theft channels.

### Use the MITRE ATT&CK Framework to Compare BAS Coverage

To further compare across the vendors, use the MITRE ATT&CK framework to check coverage. Most BAS vendors map to ATT&CK categories and are able to illustrate how much they cover. Request MITRE ATT&CK mappings from the BAS vendors for easier comparability, but pay attention to whether they perform the tests out-of-the-box or merely can be made to perform them with future configuration work.

### Test BAS for Safety Before Deployment

BAS vendors promise safe tests, but you need to test them for safe operation before deploying to production. In essence, safety-test your testing and simulation tools, and don't just expect the tools to be safe. However, some tools cross over into the domain of penetration testing; thus, they can be run with real exploitation of the targets, incurring availability and integrity risks. Be aware when BAS crosses over into the domain of penetration testing!

## BAS Deployment

### Based on the Use Case, Deploy Network Components or Agents First

On the technical side, BAS deployment may involve running agents on sound production machines to gain traffic visibility for certain network segments (such as to test for attacker lateral movement). Use the agent-based tools on sample systems (such as golden images or sample production systems), and deploy network controls widely to test network security measures (from firewalls to DLP).

Some organizations may eventually evolve to broad coverage by BAS agents, but for many test scenarios, even one agent deployed on a production system inside the perimeter can be valuable (such as for email security testing).

### Watch for Technology and Process Disruptions

Clients are asking about how disruptive BAS deployments will be to their environments. The answer splits into two components: technical and organizational. In most cases, the tools do not exploit systems. So from a safety point of view, the deployment should not be disruptive. Still, test the BAS tool for safety before deploying.

However, from an organizational process perspective, it may be disruptive. More alerts will be generated. New coordination processes to address the findings must be built, or existing security process will need to be adjusted. BAS will be especially disruptive for organizations where the red team or a penetration testing function is separated with a high wall from the blue team or a monitoring function. Those running in a purple team fashion will experience fewer disruptions or none at all.

### Whitelist BAS as Needed — But Not More

You may have to include BAS activity into required whitelists and exception lists if testing certain controls repeatedly. This creates a paradox, because, if the tool is used to test the detection controls, it should definitely not be whitelisted by the detection controls.

On the other hand, if you're using the tool to repeatedly (e.g., hourly) and automatically test certain preventive controls, it's possible that it should be removed from the detection coverage somewhere in the detection chain. One client reported using BAS to confirm that his IDS devices have traffic visibility at all times; however, he had no need to save all of the resulting NIDS alerts.

## BAS Operations and Dealing With Findings

### Define Prioritization Criteria Early

Based on the planning, define how findings will be prioritized. Some vendors provide their own severity ratings, but others assume that a client will relate them to their own awareness of risks. If data theft is a key risk, use BAS to test the controls on exfiltration and data theft. On the other hand, if initial compromise from a business partner connection, boost the signal related to findings from this area.

For example, what is more critical: "Having a DLP miss a triple-archived data file as email attachment" or "Having a way to transfer data between two network segments without any detection"? There is no Common Vulnerability Scoring System (CVSS) for BAS findings (unlike for vulnerabilities), and clients report challenges deciding what to fix first.

There is no standard and accepted scoring system for BAS findings.

### Update or Refresh Risk and Threat Assessment to Drive BAS Finding Prioritization

Clients are expected to rely on their own threat models and risk assessment, no matter what. Your BAS vendor may have more prioritization features, or fewer, but all BAS tools expect the user to be the ultimate arbiter for the dreaded "What do I fix first?" question.

### Integrate BAS Into Security Operations Processes

On the process side, using BAS tools means integrating them into testing and assessment processes. For example, you can configure BAS to automatically simulate a set of common threats after a major network change to reveal configuration mistakes and gaps.

### Escalate Few BAS Findings as Organizational Risks

Ultimately, BAS will identify gaps in your security posture and, thus, new risks. Define the relationship of the BAS findings and process with the overall security risk management (SRM) process. Gartner clients report using a process similar to the one they use to risk-prioritize penetration test findings and VA findings.

You are advised to keep BAS results at the operational level. Move only consistent exceptions (such as, "We do not have DLP coverage for some email channels and we plan to keep it that way") up to risk management and the organization risk register. However, the consistent use of BAS will deliver a proxy for overall risk and can be used to boost the awareness of how prepared the organization is to face current threats.

### Find Your Test Frequency

Some best practices are emerging regarding the frequency of assessment. Although some tools can perform continuous assessment, few clients seem to be adopting this practice. However, clients that use these tools to identify configuration mistakes rapidly are, in fact, choosing continuous assessment. In this case, if your DLP system is disconnected, you will want to know within minutes, rather than weeks.

### Evolve to Link BAS With Your SIEM and SOAR

Some BAS tools link into your SIEM to do full-cycle detection tests — use this capability to simplify detection process testing. However, most organizations choose to start their testing from preventative controls, such as firewalls, NIPS, web application firewall (WAF) and DLP. Link BAS to SOAR to automate and streamline action on certain types of findings, such as security tool misconfigurations.

## Gartner Recommended Reading

*Some documents may not be available as part of your current Gartner subscription.*

"Pragmatic Testing Approaches for Security"

"Using Penetration Testing and Red Teams to Assess and Improve Security"

"Understand the Types, Scope and Objectives of Penetration Testing"

### Evidence

[1] Naturally, the exact version would be, "Does my security work against the attacks and malicious activities that my BAS vendor knows about and has correctly implemented in its tools?"

**GARTNER HEADQUARTERS**

**Corporate Headquarters**
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

**Regional Headquarters**
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp