

WHITE PAPER

# Six Methods to Test Your Organization's Resilience to Cyberattacks

A breakdown of the available tools and approaches to support a continuous security validation program.

# Contents

---

- The Evolution of Cybersecurity Portfolio Testing . . . . . 3**

---

- The Primary Methods of Cybersecurity Portfolio Testing . . . . . 4**

  - Vulnerability Scanning & Assessment. . . . . 4
  - Penetration Testing . . . . . 4
  - Automated Penetration Testing . . . . . 6
  - Red Teaming . . . . . 7
  - Attack Surface Management . . . . . 8
  - Breach & Attack Simulation . . . . . 9

---

- The Right Tools for the Right Environment . . . . . 10**

  - On-Premise Environments . . . . . 11**
    - Pen Testing . . . . . 11
    - Automated Pen Testing. . . . . 11
    - ASM . . . . . 12
    - BAS . . . . . 12
  - Cloud Environments. . . . . 13**
    - Pen testing . . . . . 13
    - Automated Pen Testing. . . . . 13
    - ASM . . . . . 14
    - BAS . . . . . 15
  - Hybrid Environments . . . . . 15**

---

- Conclusion . . . . . 16**

# The Evolution of Cybersecurity Portfolio Testing

A decade ago, IT infrastructure at most major enterprises was on-premise or in a privately hosted facility. A small percentage of enterprise IT was in public clouds or multi-tenant environments on shared hardware, but by today's standards, the topography of the typical IT environment was much less complicated. There was less need to open ports in firewalls to support APIs or partner connections, so security teams testing for vulnerabilities or security holes were defending a hardened perimeter protecting a softer, less protected interior. "White hat" hackers and penetration testers focused primarily on testing the strength and resilience of that outer perimeter, and options for automated testing tools were fewer and far less sophisticated than those available today.

As the IT landscape evolved from on-premise to more flexible and scalable computing models like virtual machines (VMs) and containers running in the cloud or atop Kubernetes, the perimeter was no longer as defined, attack vectors became more sophisticated, and cybersecurity portfolio testing also evolved to include many more testing options. Red teams and blue teams today wage mock battles against one another, probing and testing every layer of the security stack. Automated scanners and simulators can run sophisticated attack scenarios 24/7 and are automatically updated with new malicious tactics based on the latest real-world attacks. With so many options now available, there are major differences between the different solution categories and what they can offer. It is critically important to recognize that not all of the solutions are appropriate in all IT environments and to understand the best solutions for each environment.

In this paper, we will identify the different categories of tools available for cybersecurity portfolio testing and cover the strengths and weaknesses of each. We will also assess which tools are most appropriate for different environments, including on-prem, hybrid, private cloud on shared infrastructure, or public cloud with full multi-tenancy.

# The Primary Methods of Cybersecurity Portfolio Testing

## Vulnerability Scanning & Assessment

Vulnerability assessment is designed to identify individual assets connected to your network, inventory operating details about them, and assess if they are at risk against known vulnerabilities and exploits.

There are dozens of commercial and open-source scanners available in this category offering varying levels of detail and analysis across the network, hosts, databases, and web applications. These scanners may collect data on operating system/application versions, patch levels and settings, storage of sensitive information, network configurations, etc. Different types of scans can include external or internal (i.e., originating from inside versus outside the network) and authenticated or unauthenticated (i.e., identifying vulnerabilities accessible as a known user versus an outside intruder).

Many vulnerability scanners also compare the collected data against databases of known common vulnerabilities and exposures (CVEs) to flag weaknesses that could potentially be exploited. It is important to understand vulnerability scanners typically do not do remediation. Some advanced scanners integrate with helpdesk workflow and patch management solutions to facilitate remediation, but many do not.

### STRENGTHS

Easy to configure and run

Can be fully automated

Freely available if the organization has no budget

Can easily scan the whole breadth of an organization's IT environment

### WEAKNESSES

Very shallow testing

Prone to false-positives

Cannot perform full lifecycle attacks at scale

Generally not integrated with existing security management infrastructure—requires significant manual inputs for remediation steps

The scanner needs to have the ability to reach and scan the network, meaning security controls cannot be evaluated properly

## Penetration Testing

Whereas vulnerability scanning uses automated scanning tools to expose vulnerabilities, in penetration testing (pen testing), security analysts actually mimic the tactics used by hackers to mount a simulated cyberattack against working, in-production computer systems to discover potential vulnerabilities and points of exploitation. Before an exercise, pen testing teams work with admins to designate ground rules and included/excluded devices.

The goals of pen testing are to identify and quantify:

- Potential attack vectors for threat actors
- Exploitation and impact of vulnerabilities
- Overall risk to the client environment(s)

Modern pen testing uses both automated tools, such as scanners and password crackers, and manual penetration tactics, such as buffer overflow, SQL injection, and Javascript manipulation, to compromise the network in a non-damaging way.

Because pen testing is driven by human activity, it does not tend to result in the number of false positives generated by more automated tools. For example, a scanner will indicate a theoretical weakness, but it does not test if an internal security control or a path sanitization technique (e.g., limiting inputs or restricting access to specific IP addresses) blocks the potential attack vector. Pen testing, on the other hand, shows a more complete picture of whether the vulnerability can actually be exploited.

Pen testing is widely practiced and respected, but is often performed for compliance reasons rather than for security reasons. From a security perspective, pen testing is no longer sufficient for conveying proper protection and continuous security for a variety of reasons. Pen testing focuses primarily on finding a way to breach systems and to access critical assets, but does not simulate entire attacks to exfiltrate data or adversely impact systems. Pen tests also do not generally operate at scale—attacks are one-off exercises based on identified weaknesses that require considerable time and effort from human actors. This means pen testing exercises usually require days or weeks of work and cannot effectively cover the constantly morphing IT environment of a medium or large-sized organization.

### STRENGTHS

Easy to customize and focus

Has a robust set of manual tools

Provides evidence to support compliance requirements

Deep testing of a selected environment

### WEAKNESSES

Cannot be fully automated

Requires considerable planning and coordination

Required rules of engagement may limit testing abilities in production

Cannot run continuously

Cannot perform full lifecycle attacks at scale

Generally very manual—tools must be stitched together and there is no automated export of findings to security management infrastructure

Generally not integrated with existing security management infrastructure—requires significant manual inputs for remediation steps

Has a narrow focus and is typically expensive

## Automated Pen Testing

Automated pen testing involves a higher degree of automation and speed than traditional pen testing. Automated pen testing products include a suite of automated tools to scan for various known vulnerabilities across a wide array of software, devices, and endpoints. Newer automated pen testing solutions include some ability to test for API vulnerabilities, although this is still an emerging capability.

Automated pen testing can be a useful tool to augment human cybersecurity capabilities. Compared to manual pen testing, it is better able to scale monitoring and control validation, enable a more frequent cadence of testing, and provide more rigorous quality control and standardization.

However, humans must generally guide the process, targeting, and calibration of automated pen testing, despite the claims of some products that offer “fully automated penetration testing.” Human analysts also usually must validate each finding and research recommended remediation, aside from the most basic fixes. This can create more work for security teams—rather than less—if the signal-to-noise ratio is poor and indicated vulnerabilities do not pose a risk to the organization.

Great care must also be taken with automated pen testing tools so as not to disrupt operations if those tools are run against live environments. To avoid the potential for disruption, most automated pen tests are run against non-production environments or “digital twins.” As a result, those tests tend to lack fidelity because automated pen testing is focused on scanning rather than ensuring target environments are as similar as possible to production environments.

Finally, automated pen testing tools generally exploit first-level security weaknesses but cannot execute complex attacks with conditional capabilities where subsequent steps in the kill chain are dependent on the previous one. This is a significant weakness, as it limits the ability of pen tests to test all security layers. This is especially important as malware and other malicious tools continue to increase in sophistication.

### STRENGTHS

- Can cover more of the IT environment
- Can run more frequently and even continuously
- Enables better longitudinal findings and security control performance metrics
- Internal teams can be trained to perform the exercises

### WEAKNESSES

- Limited to attacks predefined within the tool
- Harder to customize and modify for newer techniques
- Cannot continuously simulate complex breaches and attacks
- Generally not able to analyze the different parts of the security operations chain
- While deeper than traditional vulnerability scanning tools, it is still rather shallow
- Narrow focus that doesn't cover several key aspects of the cyber kill chain

## Red Teaming

Red teaming is similar to pen testing, but with a malicious twist. Red teams may employ the same tactics as a pen test, but often do so under the guise of a real attack and with the intent to avoid detection. Unlike pen testing, red teams seek to access “crown jewels”—the critical systems and data of an organization—and execute full lifecycle attacks, rather than simply identifying vulnerabilities and weaknesses. Red teams are also part of the organization and are able to leverage internal knowledge of the IT environment.

Red team assessments seek to:

- Identify weaknesses across people, processes, and technologies
- Provide a real-world perspective of advanced persistent threats (APTs) and other attackers
- Deliver an “outside” overview of an organization’s environment and real weaknesses

The most important goal of red teaming is to assess how an organization responds to various threats and to identify areas of improvement. Red team exercises may include only IT and technical teams but often incorporate other teams required to respond to cyberattacks. Typically, a red team assessment will have specific objectives and involve more people than a standard pen test. For this reason alone, red teaming is more resource intensive and challenging to run on a continuous basis.

Ground rules are established before the exercise to ensure the red team activities do not disrupt production business functions. However, within the established rules, red teams work as true adversaries, deploying any allowable tools or subterfuge to gain access and compromise systems, including social engineering, physical access, and extensive probes of the attack surface. In general, red teaming is similar to manual pen testing exercises with the key difference being that red teams do not provide warnings, do not cooperate with security teams (blue teams), and tend to be far more improvisational in nature. While red team exercises can incorporate automated results as part of findings, they tend to be more focused on an organization’s response and ability to adapt rather than the initial state of their security posture.

### STRENGTHS

Same as pen testing, with the potential to engage in even deeper testing

Closest simulation to real interactions with adversaries in the wild

More specific to the organization being tested and may include proprietary applications, assets, or threats that are organization-specific

Provides broader organizational context and insights into security posture and response

### WEAKNESSES

Typically requires specialized ethical hacker resources

Requires significant customization

Extremely resource and time intensive

Not easy to scale or repeat

Provides a point-in-time assessment

Can be disruptive if not bounded carefully

## Attack Surface Management

Adoption of cloud computing, digital transformation of many analog processes, the expansion of remote work, and the rise of the API economy has unblocked tremendous operational innovation, but it has also greatly expanded the attack surface of the average organization. As a result businesses are changing the way they approach risk management and the security of their digital assets, which has given rise to attack surface management (ASM).

ASM encompasses the processes and tools to continuously identify, monitor, prioritize, and remediate potential attack vectors across internal and external Internet-connected assets within an organization's IT infrastructure.

ASM processes and tools are generally divided into three categories:

**EASM** **External Attack Surface Management (EASM):** EASM discovers public-facing IT assets and monitors them for vulnerabilities like server, credential, or public cloud service misconfigurations and third-party software code vulnerabilities that could be exploited by adversaries. Think of this as assessing the environment from the outside, the way a hacker would. Many of these technologies also prioritize the weaknesses based on severity of risk to aid in remediation.

**CAASM** **Cyber Asset Attack Surface Management (CAASM):** CAASM technologies also discover assets, monitor for security weaknesses, and can enable organizations to see both internal and external IT assets. However, they rely on API integrations with existing tools, so visibility can be limited by existing inventory data. The value of CAASM is primarily in keeping track of internal assets.

**DRPS** **Digital Risk Protection Services (DRPS):** DRPS tools and services provide visibility into environments like the open web, dark web, and social media to identify potential threats to the organization's digital assets and data. DRPS can be useful as part of comprehensive risk assessments and brand protection, but it does not provide an inventory of the IT assets managed by the organization or assess their risk.

Most ASM tools today include mapping to some elements of the MITRE ATT&CK framework, and some ASM solutions enable users to automatically populate findings in dashboards and integrate—at varying levels—with security management tools like security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions. However, ASM solutions more commonly require manual input of findings and synchronization with other systems.

Finally, it is important to note that ASM technologies are effective at discovering assets across a diverse IT estate, which can make them a better choice than simple vulnerability scanners (which often only scan based on a user-defined IP range). However, like vulnerability scanners, ASM tools usually just look for asset vulnerabilities and configuration weaknesses; they do not actively test the weaknesses to validate if they could be reached and exploited by an attacker.

### STRENGTHS

Better addresses dynamic attack surfaces and lack of hardened perimeters

Designed for more continuous operations

Includes mapping to MITRE ATT&CK

Wider coverage than penetration testing

### WEAKNESSES

Does not attempt to attack weaknesses to validate their exploitability

Cannot illuminate all elements of the kill chain in more sophisticated attacks

Better for historical rather than emergent attacks

Lacks critical integration capabilities

## Breach & Attack Simulation

The most modern and recent solution in the cybersecurity portfolio testing arena, breach and attack simulation (BAS) software is a highly automated solution that safely runs real-world attack scenarios against production applications and infrastructure in an organization's own chosen compute and IT environment. BAS leverages the most current threat intelligence and enables granular customization based on industry, risk profile, and attack surface. Unlike other testing approaches, BAS can continuously, and in near real-time, validate that security controls are in place, properly configured, and working as intended.

Best-of-breed BAS solutions continuously add (or simplify the addition of) new attacks to their playbooks to protect against zero-day attacks and also non-published, iterative attacks. BAS can run these simulations at scale across an entire enterprise with minimal resource consumption and no risk to production environments or processes. BAS can also help reduce the complexity of red-team exercises by enabling red teams to develop and replicate their own custom techniques without requiring coding experience. The most sophisticated and effective BAS solutions also integrate with common security management tools, including vulnerability management, SIEM, and SOAR.

Although BAS validations are called "simulations," true BAS solutions are much closer to real exploits, utilizing multi-stage playbooks and the tactics, techniques, and procedures (TTPs) of real-world attacks mapped to real threat actors. Unlike automated pen testing and ASM, BAS solutions are programmatically tuneable using any combination of frameworks and threat intelligence feeds.

According to Gartner, "Breach and attack simulation tools help make security postures more consistent and automated." This is particularly important given the challenges of running continuous security control validation within an increasingly dynamic IT estate and against a rapidly expanding threat landscape.

Broadly speaking, BAS helps teams become proactive actors against threats and risks emanating not only from superficial vulnerabilities, but also from security drift, configuration errors, insider attacks, and emergent or iterative attacks. Continuous simulations accelerate learning curves, improve security metabolism, and enable accountable metrics based not just on patching, but on the entire security ecosystem's resilience to attacks.

### STRENGTHS

Automatically and continuously validates controls

Runs real attacks safely in the production environment without risk of service disruption

Tests all layers of the security architecture across all stages of the kill chain independently

Highly configurable and adaptable to zero-day, emergent, and iterative attacks

Delivers insights and indicators of compromise across the entire attack lifecycle

Integrates easily with existing tools and reduces security team toil

### WEAKNESSES

Can require tuning for accuracy

Requires a victim simulator in every environment to be tested

Can be challenging to get other groups within an organization to take action on the tool's findings and utilize its highly integrated capabilities

## The Right Tools for the Right Environment

While each of the solutions discussed in this paper have individual strengths and weaknesses, security leaders must consider which environment they seek to protect before selecting the appropriate solution. Today's reality is that most modern IT estates and infrastructure are hybrid affairs. Older and more critical resources may be in on-premise or hosted environments, but the growing majority of new systems and users will be in the cloud, and they likely will not be contained in a single cloud platform. Multi-cloud infrastructure is becoming more common as companies seek to avoid cloud lock-in, achieve higher compound service level agreements (SLAs), and enable greater resilience, while also optioning for price arbitrage across cloud service providers (CSPs).

Industry-specific requirements also dictate the environment. For example, financial services companies may need segregated cloud environments to fulfill government mandates. In this case, vulnerability testing against segregated cloud environments—like virtual private clouds (VPCs) and hosted private clouds—may more closely resemble that of on-premise vulnerability testing. But, generally speaking, requirements and regulations tend to lag technology. For many certifications, annual pen testing is the listed requirement, even if that format may not be the best for a particular organization's IT footprint.

For CISOs, this varied landscape requires different thinking about how to test attack surfaces and system vulnerability. Different tools and solutions are more or less useful for different environments. Knowing what's possible and beneficial is key. In the sections below, we will look at various environments and assess which categories of tools can be used and how. (An important note: these are tools, not teams. Red and blue teams are still necessary in any environment.)

## On-Premise Environments

### Pen Testing

Pen testing evolved for the on-premise world and remains a useful collaborative exercise. On-premise environments will generally entail a smaller IT estate to cover, so the lack of automation and focus on manual inventory work is less of an impediment (although scarcity of experienced analysts may still be a concern). Also, pen testing is highly customizable, which works in favor of on-premise environments, where granular variance based on machine firmware is likely high. In addition, internally coded software is more likely to be a factor in on-premise environments, an artifact of the era before open source.

#### PROS

Designed for on-premise originally

Can be highly customized

Many useful—and often open-source—tools

#### CONS

Time consuming

Requires manual toil and planning

Not effective in highly dynamic internal environments running more modern container orchestration platforms and deploying modern API management systems

Expensive

### Automated Pen Testing

Automated pen testing against on-premise installations is useful because it enables a rapid cadence of testing against common external attack vectors programmatically. This is useful to help ensure security drift is not impacting the external-facing security posture of on-premise infrastructure. As the name implies, automated pen testing tools can run automatically, reducing manual toil. However, test results must be manually incorporated into other tools, such as vulnerability management and threat intelligence, which is time consuming and error prone. Automated pen testing is also useful for organizations that wish to test controls on exposed endpoints that have access back into on-premise assets via VPNs.

#### PROS

Works well with existing pen-testing efforts

Helps teams automate key portions of pen-testing exercises for more repeatable results

Can reduce manual toil

Enables greater scale of testing and a broader array of potential vulnerabilities to scan for

#### CONS

Requires multiple tools that either must be integrated or are incorporated into a third-party product, reducing flexibility

Usually not natively integrated with SOAR, SIEM and VM solutions

## ASM

ASM solutions are not as appropriate for on-premise vulnerability detection because they are designed for more sprawling and dynamic attack surfaces with numerous end-points in the cloud, on the edge, and on user devices. On-premise IT is often behind a massive global firewall, which presents a less convoluted attack surface.

### PROS

---

Good for more porous environments where on-premise is accessible to the outside world via API and other holes in the firewall

---

### CONS

---

Not as relevant for internal IT that is disconnected from the Internet and has a smaller attack surface

---

## BAS

BAS solutions can be extremely useful in on-premise environments, as they are typically highly configurable and adaptable. BAS solutions can run attack simulations from a large playbook to validate efficacy of security controls at multiple levels and can integrate customized “institutional knowledge” to address specifics of legacy, “home-grown” applications designed prior to the cloud era. BAS also enables enterprises to effectively test and validate controls in depth. This enables them to determine and remediate the “blast radius” of secondary and tertiary actions of an adversary that happen to punch through the primary network controls and firewalls. Because it can run continuously with minimal supervision, BAS solutions do not typically tax security teams.

### PROS

---

Flexible and customizable

---

Autonomous and continuous

---

Helps build “defense-in-depth” muscle for on-prem teams

---

### CONS

---

Can require tuning

---

## Cloud Environments

### Pen Testing

Pen testing in the cloud is challenging as CSPs typically do not want to risk impacting other clients in their multi-tenant environments. In a true multi-tenant environment on shared infrastructure, thousands of companies share data-center hardware. In these instances, true full-stack pen testing has the potential to cause outages that can cost CSPs significant chargebacks if SLAs are violated.

Equally problematic, cloud services are tightly linked via API to compute instances, but stress testing or scanning external-facing services, while possible, can inadvertently impact other users unless the IP address range is perfectly controlled. A handful of pen-testing tools and services for the cloud have emerged, but they are lightly adopted and not nearly as useful as pen-testing activities in on-prem environments.

Larger clients with their own dedicated infrastructure inside of a public cloud or managed private cloud can more easily perform pen testing, but even this must be tightly coordinated with the CSPs, who exercise veto power. Lastly, many cloud service providers offer scanning tools and vulnerability and configuration management tools that they are comfortable using.

#### PROS

None

#### CONS

CSPs often prohibit cloud pen-testing on shared environments

Most CSPs only allow limited capabilities for cloud pen-testing tools

Propensity to inadvertently impact other users

### Automated Pen Testing

The risk with automated pen testing in cloud environments is similar to that of traditional pen testing, if not higher. Many of the automated pen testing tools deploy wide-scale scanning of ports, IPs, PIs, and network endpoints. This is particularly disliked by cloud companies that fear poorly operated scanning tools will effectively DDoS unsuspecting customers that are on the same shared services or shared infrastructure—or even in the same data center.

#### PROS

None

#### CONS

CSPs often prohibit cloud pen-testing on shared environments

Most CSPs only allow limited capabilities for cloud pen-testing tools

### ASM

Infrastructure in the cloud changes quickly. Code often ships multiple times a day and applications and infrastructure is much more dynamic. For example, Kubernetes may build and destroy instances many thousands of times a day in multi-cluster architectures. ASM can only scan against public cloud APIs and services as long as it has known or defined IP address ranges for specific infrastructure. That said, this may still be prohibited by CSPs.

ASM also generates mountains of data, and most ASM systems require manual translation of findings into configuration and control adjustments. This challenge is multiplied in the cloud, where businesses tend to have many more services and systems in place than on-prem. ASM was never designed to probe APIs and doing so at required volumes can cause problems to the API service users (e.g., Amazon S3).

In the cloud, the majority of traffic is de facto API traffic, which is a significant limiting factor. Because cloud architecture is primarily service-to-service, horizontal traversal is an increasingly popular tactic. ASM does not cover horizontal traversal or multi-stage attacks. Lastly, the resource and manual data integration requirements of ASM means it does not do a good job of “continuous testing,” which is important in the cloud because of the dynamism of the applications and infrastructures.

#### PROS

---

Designed for distributed and dynamic environments, which is consistent with cloud

---

#### CONS

---

Can be heavy-handed

---

Hard to contain potential impact to other users in shared environments and services—disliked by CSP

---

### BAS

Best-in-class BAS solutions can simulate attacks against either public or private cloud infrastructure without putting the environment at risk of disruption. These solutions address both the control plane (which includes identity and access management [IAM], network, storage, and administrator access) and the data plane (covering lateral movement, system abuse, privilege escalation, and running unapproved processes).

BAS solutions specifically address the concern of running attack scenarios in a shared environment by transparently “cloning” the production environment and running attack simulations against that clone. For this reason, BAS is highly suited to multi-tenant cloud environments because it never puts other tenants at risk and does not have the potential to impact shared services, infrastructure, APIs, or other elements.

Equally important, BAS is designed for continuous testing, which is all the more critical in highly-dynamic cloud environments where containers are created and destroyed constantly and often continuously. One area of caution is that BAS has not yet matured in testing security controls of APIs, which is often a point of weakness in cloud environments.

#### PROS

Designed for isolation, so presents little risk to shared environments and services

Designed for continuous testing that is required for best coverage of virtual and highly dynamic environments

#### CONS

Not mature at API coverage, which is important in cloud environments

## Hybrid Environments

Hybrid environments include both cloud and on-prem or private cloud. As such, all of the above considerations for the two types of environments still hold true for hybrid environments. For this reason, security teams protecting hybrid clouds are best served with a blended approach to vulnerability testing and security control validation. In these situations, security teams may need to determine and prioritize the business value and risks for what is running on-prem versus what is running on cloud and allocate resources to address those risks. Hybrid environments will tend, over time, to move towards more cloud and away from on-premise. This means the longer-term environmental trends favor cloud-effective solutions over on-prem effective solutions.

## Conclusion

All of the tools used to manage attack risk/exposure and test security controls addressed in this white paper have valid use cases. Some are mandated under regulatory structures and are better known, such as pen testing. Others, such as BAS, may be lesser known and newer but more flexible and applicable to multiple resource environments. For ease of comparison, the table below provides a high-level snapshot of the coverage provided by each tool for the various features and use cases discussed throughout this white paper:

FEATURE / USE CASE	Automated			
	VM	PT	ASM	BAS
Scalable testing	●	◐	◐	●
Vulnerability / configuration scanning	●	◐	●	○
Real-world attack simulation	○	◑	○	●
Continuous, automated testing	●	◑	◑	●
Non-destructive tests	◑	◐	●	●
Real-world attack simulations from attacker's viewpoint	○	◑	○	●
Deep, highly customized attack testing	○	◐	◐	●
Attack surface-based discovery and risk identification	◐	○	●	○
MITRE ATT&CK TTP-based testing	◐	◐	◑	●
Single platform support for cloud & on-premises testing	○	○	○	●
Multiple control integrations (SIEM, SOAR, DLP, etc)	○	○	○	●
Discovers risk from attack surface perspective	●	○	●	○
"Purple team" collaboration support	○	○	○	●
Test thoroughness and depth	◐	◐	◑	●
Attack correlation with SIEM data to improve control testing efficacy	○	○	○	●

Over time, as more and more IT infrastructure shifts to the cloud, CISOs will need to consider which tools work better for which environment. This may entail shifting emphasis towards tools that are more "cloud-native" and "cloud-friendly" and away from tools that are unworkable in shared infrastructure in multi-tenant environments. The ephemeral nature of cloud infrastructure and the quickening pace of cyberattacks means any validation technologies must quickly adopt continuous testing if they wish to effectively prevent attacks on cloud infrastructure.

This is not to say the older technologies, like pen testing, are no longer useful. Because these solutions are familiar and mature, they will likely remain a key element in helping CISOs assess security posture and manage risk. That said, CISOs that choose to rely primarily on older tools that are not cloud-native may not have the capability to assess the efficacy of controls continuously and institute prioritization and remediation at the tempo required to secure highly dynamic cloud-native and widely distributed environments.

This is a trend also recognized by Gartner, which noted that organizations that prioritize their security investments based on a continuous threat exposure management (CTEM) program will be three times less likely to suffer from a breach. Gartner's CTEM is a set of processes and capabilities that allow enterprises to continually and consistently evaluate the accessibility, exposure, and exploitability of an enterprise's digital and physical assets. CTEM's overall goal is to help organizations survive breaches, minimize organizational risk, and improve overall security posture. Tools like BAS platforms can help organizations understand their exposure by discovering gaps in security control coverage, prioritize risk based on business impact, and continuously validate their security posture against the evolving threat landscape.

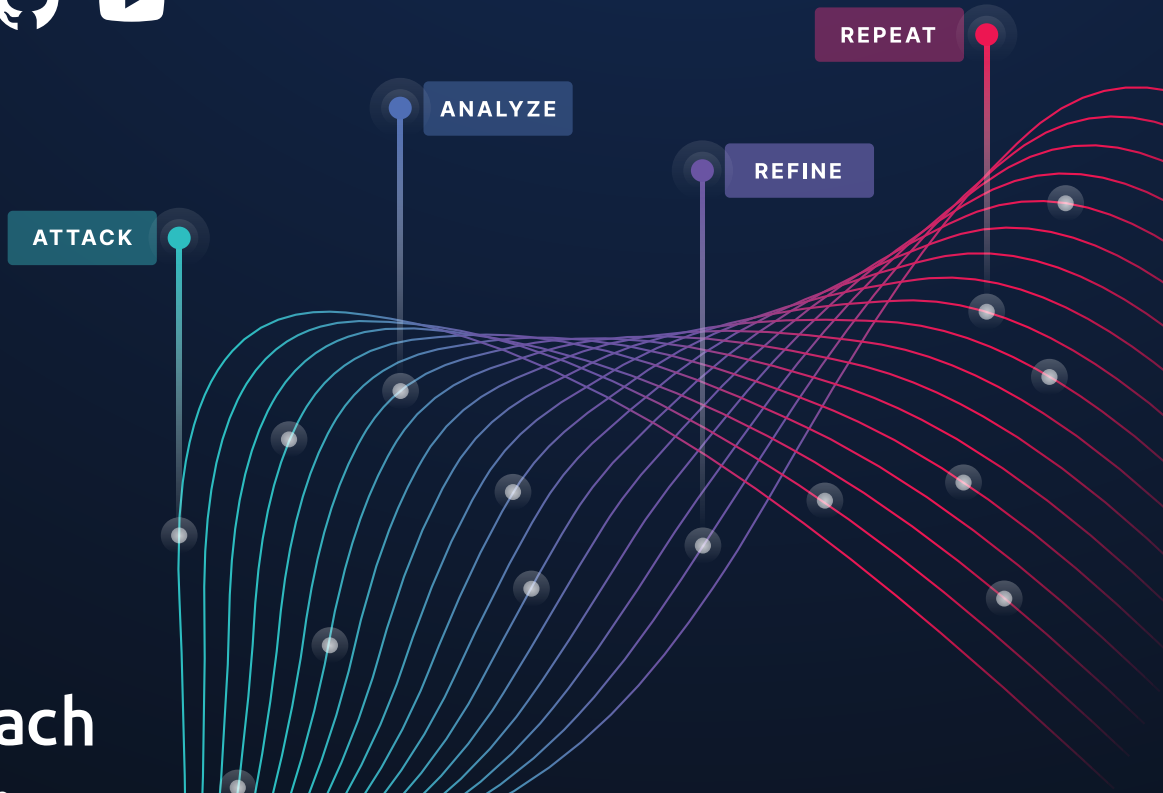
Want to learn more about why leading organizations—like PayPal, Netflix, Experian, and Johnson & Johnson—use the SafeBreach BAS platform to support their continuous security validation programs? **Connect** with a SafeBreach cybersecurity expert or **request a demo** of the platform today.

## About SafeBreach

Combining the mindset of a CISO and the toolset of a Hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security control validation platform.

SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

Learn more at [SafeBreach.com](https://SafeBreach.com).



All content ©SafeBreach 2023.  
All rights reserved.