PICUS

10 Criteria for Choosing the Right BAS Solution

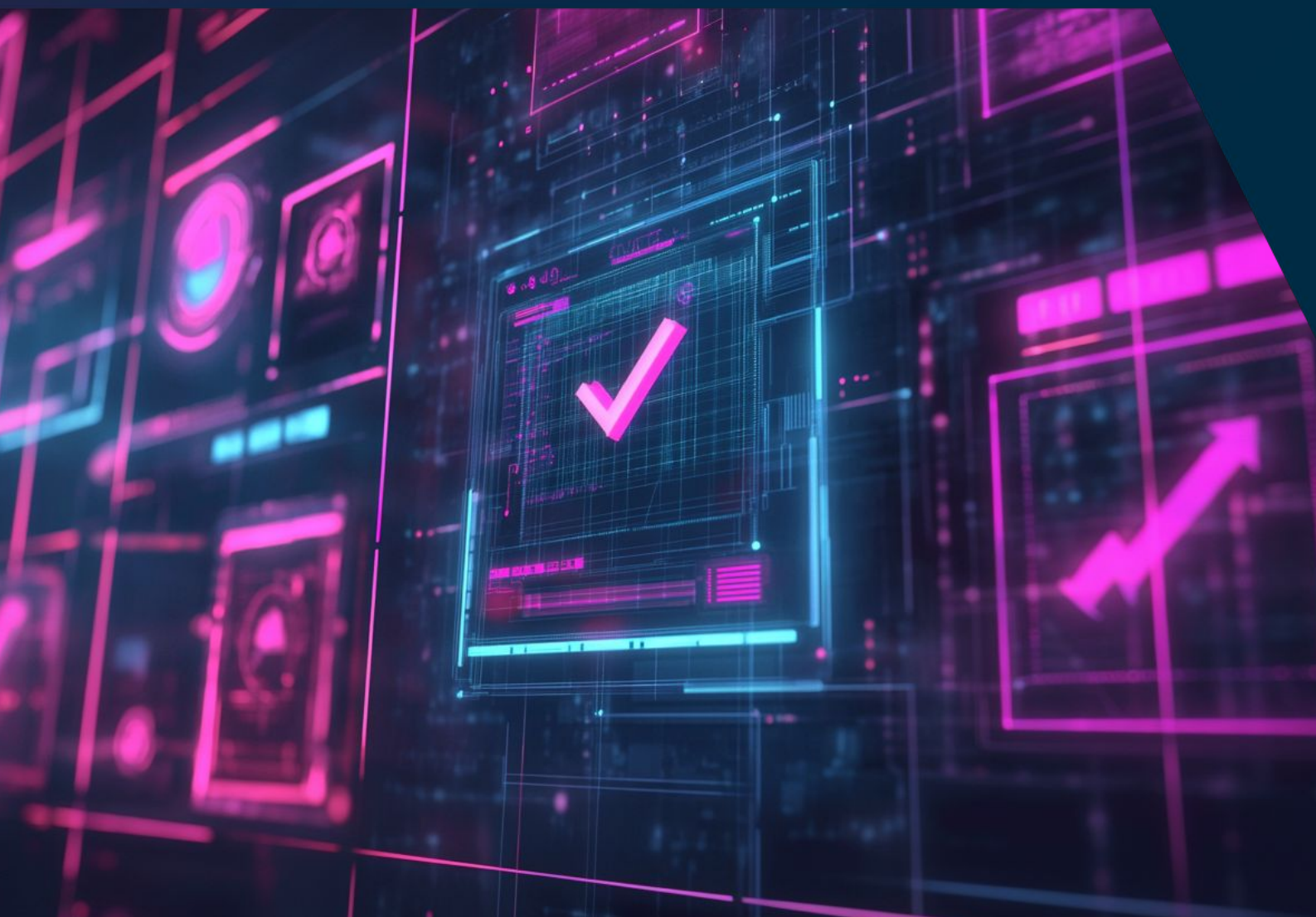


Table of Contents

Executive Summary

The cyber threat landscape expands as threat actors develop new attack techniques, and new technologies introduced by digital transformation extend the attack surface. However, despite increased investment in cybersecurity solutions, allocating more resources does not ensure organizations' ability to prevent or detect cyberattacks. To maintain a robust security posture, organizations must continuously evaluate their security controls to quickly identify and address vulnerabilities.

Breach and Attack Simulation (BAS) has become the most effective solution for security control assessment and has taken its place in the organizations' toolset along with traditional assessment methods such as vulnerability scanning, penetration testing, and red teaming. Unlike other assessment methods, BAS offers real-time visibility, automated gap analysis, and actionable mitigation insights in a cost-effective manner.

By simulating real-world threats, BAS enables organizations to continuously validate their defenses and strengthen cyber resilience. There are numerous BAS solutions, but not all are created equal. This whitepaper lists and describes essential BAS features to narrow your search for the right solution.

Introduction

Increased complexity of security controls and defensive security operations may lead to inefficiencies and valuable and limited resources being wasted. Evidently, we need to develop a scalable and less resource-intensive approach rather than spending more money to solve the problem.

Organizations often ask similar questions themselves at different levels of responsibility. The answers to these questions may serve different purposes. However, they are essentially derived from the same question: **How effective are our security technologies against cyber attacks?**

Traditionally, security teams answer these questions with assessment methods such as vulnerability scanning, penetration testing, and red teaming. However, these methods fall short of measuring the effectiveness of security controls because they:

- have limited test scope
- are highly dependent on human operators' skill sets
- are resource-intensive
- do not provide consistent outputs
- are conducted at a single point in time

Thus, organizations are shifting from isolated assessments to continuous security assessment tools such as Breach and Attack Simulation (BAS). According to MarketsandMarkets, the Breach and Attack Simulation market has grown from USD 134 million in 2019 to USD 557 million in 2023 and is expected to reach USD 729 million in 2024 [1].

In this paper, we explain the criteria that organizations should consider when selecting a BAS tool. The first section focuses on the challenges that organizations face in their cybersecurity operations. The second section describes traditional security assessment methods and BAS. The last section details the requirements of a mature BAS solution for security control validation.

Challenges in Enterprise Cybersecurity

Organizations worldwide continue to improve their cybersecurity capabilities as cyberattacks become more prevalent and pose a great risk to business continuity, reputation, and overall success of companies. Consequently, global cybersecurity spending continues its rising trend and Gartner expects it to exceed $211.5 billion in 2025 [2].

Although the cybersecurity budget of organizations increases, their cyber resilience might not scale proportionally. Allocating enough budget for security technologies and skilled cybersecurity professionals is only a part of building and maintaining a solid security posture. Thus, the best approach is to identify the challenges in enterprise cybersecurity and allocate resources to overcome these challenges.

Challenge 1:
Lack of Cyber Threat Visibility

The cyber threat landscape is different for every organization. Threat actors target specific industries and geographical locations according to their motives. However, organizations do not have the full picture when it comes to their cyber threat landscape. As a result, security teams can only configure their security controls against the threats they know, and the unknown threats still remain a great risk to their organization.

70% **of organizations are not confident that they can prevent serious cyber disruptions or respond quickly enough to threats [3].**

Challenge 2:
Emerging Threats

The cyber threat landscape is not static; it evolves and grows as threat actors develop new malicious techniques and exploitation methods. New critical or high-level vulnerabilities found in widely used products may lead to large-scale cyber attacks. These vulnerabilities or campaigns are called Emerging Threats, and they require an immediate response from security teams. Since the average remediation time is too long, emerging threats have ample time to cause major damage.

The average time taken to remediate is 35 days for critical web application vulnerabilities and 61 days for Internet facing host/cloud critical severity vulnerabilities [4].

Challenge 3:
Underutilization of Security Controls

As mentioned previously, organizations are investing in new cybersecurity technologies and spending more money in recent years. However, their security posture does not improve proportionately with the cybersecurity budget. This is partly because organizations do not utilize their new or existing security controls to their fullest extent.

Configuring and tuning security controls is a continuous process, and there is no silver bullet solution that can fit all organizations. Security controls that are misconfigured or in default configuration cause not only underutilization but also create a false sense of security.

Out of 136 million attack simulations, security controls were able to detect only 12% of them in 2024 [5].

Challenge 4:
Alert Volume and Delayed Response to Cyber Threats

On average, organizations deploy 80 security controls. Developing custom detection rules for all of them is a highly technical and resource-intensive process. Too broad rules lead to false-positive alerts and alert fatigue, and too narrow rules have limited detection capabilities.

The statistics show that security controls fail to detect the majority of security breaches. When it is combined with the shortage of skilled cybersecurity professionals, SOC teams cannot respond to security incidents in a timely manner.

On average, it takes organizations six months or longer to detect and respond to an incident [6].

Gartner

There is a veritable epidemic of misconfigured, disconnected, turned off, and non-optimized security tools within organizations. [7]

Evaluating the Operational Effectiveness of Security Controls

Traditionally, organizations have relied on vulnerability scanning to find the gaps in their network perimeter, plus penetration testing and red teaming to assess their security posture. Although these methods still provide some value, they have major shortcomings and cannot fully assess the security posture of the organization. As a result, the modern security approach is to leverage automated and continuous technologies such as Breach and Attack Simulation as part of the security operations toolset.

Vulnerability Scanning

Vulnerability exploitation is a significant attack vector used for initial access to a target network and escalating privileges. Many cyber attack campaigns rely on critical vulnerabilities found in the target network.

Vulnerability scanning allows security teams to identify vulnerabilities in their networks so that they can run risk assessments and patch management for the found vulnerabilities. Although vulnerability scanning is used to identify the weaknesses in the network, the following steps are resource-intensive:

- The found vulnerabilities should be prioritized according to the organization's risk assessment plan.
- Patching and remediation processes can be lengthy and difficult.

Penetration Testing

In a penetration test, a trusted third party attempts to breach the organization's network using the tools and techniques that an adversary might use. Penetration testing is a widely accepted security assessment method among security professionals, and regulatory institutions such as ISO and PCI require organizations to conduct penetration testing regularly.

Although penetration testing is an established way of testing security controls, it has major shortcomings.

- Security operations are continuous processes, and penetration tests validate only a snapshot of that continuous process.
- Penetration tests are not consistent. The outcome of the penetration test heavily relies on the technical skills of the penetration tester.
- Test scope often does not cover the entire network.

Evaluating the Operational Effectiveness of Security Controls

Red Teaming

In red teaming practices, security teams run full attack campaigns and test security controls against real-world threat scenarios. Red teams provide valuable data for blue teaming, risk management, and mitigation processes so that organizations can learn and take corrective actions to better their security posture. Even though it is better at simulating real-world threats than penetration testing, red teaming is a highly technical and time-consuming process with several drawbacks.

- Red teaming requires skillful red teamers. Red teaming exercises are highly complex and may take many weeks.
- Red teaming is not a continuous and automated process that can provide 24/7/365 security control assessments.

Breach and Attack Simulation

In recent years, Breach and Attack Simulation (BAS) solutions have become an indispensable technology for many organizations regarding security control evaluation.

Gartner definition: Breach and Attack Simulation (BAS) technologies allow enterprises to continually and consistently simulate the full attack cycle - including insider threats, lateral movement, and data exfiltration - against enterprise infrastructure, using software agents, virtual machines, and other means [8].

At first glance, the definition might mislead people to think BAS solutions aim to replace previously mentioned methods. Actually, BAS solutions provide an automated solution for security posture assessment and allow security teams to identify and mitigate weak points in their security without wasting time and valuable resources.

Although Gartner gives a clear definition of BAS, different vendors label various tools and services as Breach and Attack Simulation, and the mislabeling leads to confusion in the BAS market. In this paper, we provide a solid checklist that expands on Gartner's definition of BAS and can be used to help organizations select the best BAS solution for security control validation.

Key Selection Criteria for a Breach and Attack Simulation Solution

Gartner's definition describes some fundamental characteristics of Breach and Attack Simulation. When it is combined with the current regulatory environment and operational requirements for organizations, ten selection criteria for BAS emerge.

Criteria 1:
Threat Simulation across the Attack Lifecycle

The cyber threat landscape consists of thousands of stand-alone attack techniques, and technically savvy adversaries can chain multiple techniques to create high-impact attack campaigns. Understanding how threat actors gain initial access to a network and move laterally in a network is the important first step in configuring security controls. Therefore, a comprehensive library of cyber attack simulations that covers all steps of the cyber kill chain is a must for a BAS solution.

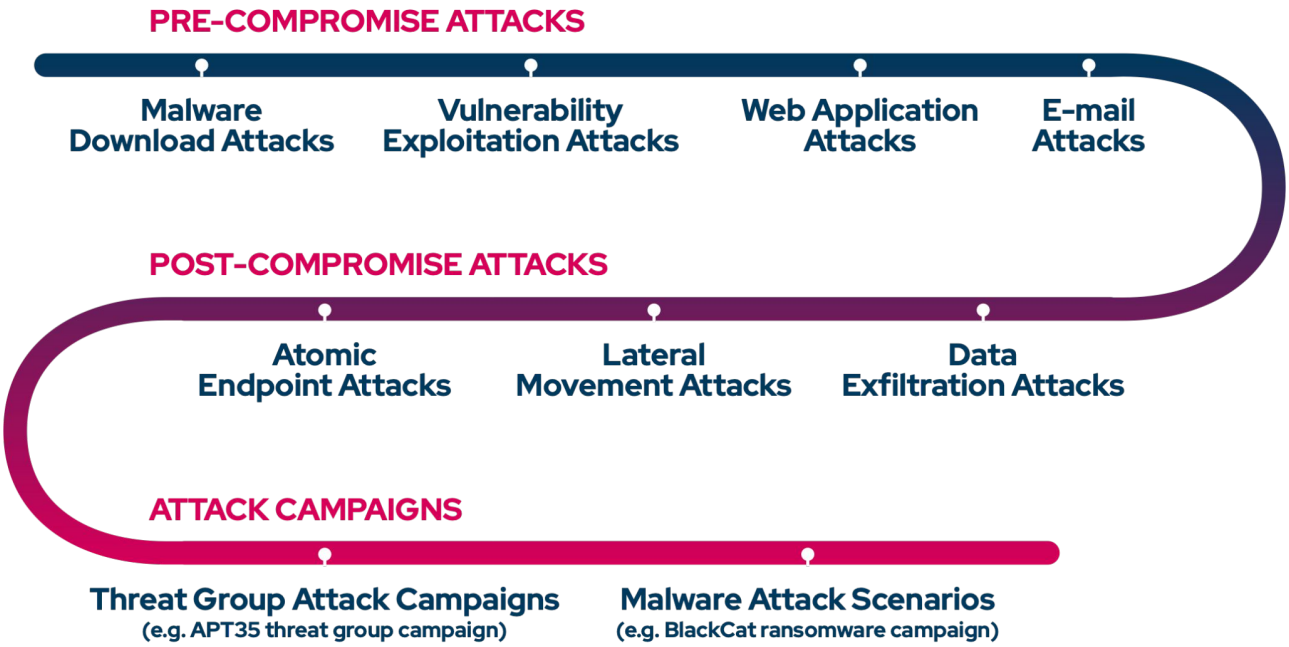
Many BAS vendors curate a threat library to represent and simulate the cyber threat landscape. The threat library must cover both pre-compromise and post-compromise phases of the attack cycle. Also, the threat library should provide predefined and customizable adversary attack scenarios to simulate the entire attack lifecycle.

- **Pre-compromise attacks**
  - Malware download attacks
  - Vulnerability exploitation attacks
  - Web application attacks
  - E-mail attacks
- **Post-compromise attacks**
  - Atomic endpoint attacks
  - Lateral movement attacks
  - Data exfiltration attacks
- **Attack campaigns**
  - Threat Group attack campaigns (e.g. APT35 threat group campaign)
  - Malware attack scenarios (e.g. BlackCat ransomware campaign)

Key Selection Criteria for a Breach and Attack Simulation Solution

Like every controlled test, the consistency of the simulation is important so that security teams can change a single variable and check its effect on the security controls. Similarly, consistency in attack simulations is a must for BAS. Otherwise, security teams cannot objectively evaluate their security controls or configuration changes.

Another important requirement of any simulation is that it should be safe to perform in a live operational setting. Under any circumstances, attack simulations should not hinder the CIA triad of cybersecurity. Since many services, such as banking and utilities, cannot be paused for a security control evaluation, security teams test their security controls without obstructing or delaying daily operations. Therefore, organizations expect a BAS solution to conduct attack simulations consistently and safely without interrupting any of their operations.



Key Selection Criteria for a Breach and Attack Simulation Solution

Criteria 2:
Up-to-date Against Current and Emerging Threats

In the first criterion, we explained the need for a broad threat library that represents various cyber-attacks and adversary campaigns. Since the cyber threat landscape evolves and expands constantly, a BAS tool's threat library should be able to keep up with the threat landscape with swift updates. These updates should incorporate emerging threats as they pose a significant risk to organizations. Thus, a BAS solution needs to be backed up by a vast threat library, and the threat library should be updated constantly and quickly. However, be aware that some vendors might charge a premium for early access to newly added simulation content.

Criteria 3:
Validation of Enterprise Security Controls

Organizations deploy numerous security controls with varying capabilities to defend themselves against cyber attacks. These security controls may also be used in different networks and geographical locations. Since the robustness of security controls is measured by its weakest element, BAS should be able to assess the entire security infrastructure holistically and identify the gaps in the security chain so that security teams can mitigate the security gaps.

A mature BAS solution should provide seamless integration with a wide range of prevention and detection technologies, such as

- **Network Security Controls**
  - Intrusion Prevention System (IPS)
  - Next-Generation Firewall (NGFW)
  - Secure Web Gateway (SWG)
  - Web Application Firewall (WAF)
  - Data Loss Prevention (DLP)
- **Email Security Controls**
  - Secure Email Gateway (SEG)
- **Detection Controls**
  - Endpoint Detection and Response (EDR)
  - Extended Detection and Response (XDR)
  - Intrusion Detection System (IDS)
  - Security Information and Event Management (SIEM)

Key Selection Criteria for a Breach and Attack Simulation Solution

Criteria 4:
Direct and Actionable Mitigation Insights

Attack simulations are a great way to assess security controls and identify the gaps in the security posture. However, the ultimate goal of identifying these gaps is not just awareness; it's remediation. Remediating security gaps can be a complex and resource-intensive process. Since delays in addressing security gaps can increase an organization's exposure to cyberattacks, remediation should be swift and effective.

A mature Breach and Attack Simulation (BAS) solution should go beyond merely identifying weaknesses. It should deliver direct, actionable mitigation insights for simulated attacks, enabling security teams to immediately address vulnerabilities, whether by applying patches, updating prevention signatures, or deploying detection rules.

For preventive security controls such as NGFW, WAF, and IPS, BAS solutions should offer vendor-specific prevention signatures that are directly applicable without requiring extensive customization or manual tuning. Importantly, these prevention signatures should be pre-validated by the BAS vendor to ensure their effectiveness against the simulated threats. This not only enhances the precision of preventive measures but also reduces the risk of unnecessary operational overhead caused by unoptimized signatures.

For SIEM, EDR, and XDR platforms, the BAS solution should provide detection rules specific to the organization's deployed SIEM, EDR, and XDR solutions. Generic rules or reliance on SIGMA converters often fall short, as they may generate ineffective alerts or produce a high volume of false positives. Instead, BAS tools should ensure that the detection rules are fine-tuned to the nuances of each SIEM or EDR solution, enabling accurate and efficient detection of simulated threats.

Criteria 5:
Detection Rule Validation

False-positive alerts in the detection of malicious activity cause inefficiencies in incident response and cost organizations time and resources. Also, too many false positive alerts may lead to alert fatigue, and SecOps teams may have difficulty distinguishing between actual malicious activity and false-positive alerts. Therefore, minimizing false positive alerts is highly beneficial for the effective use of security controls.

BAS should be able to run detection validation and verify the alerts created by the security controls. Detection validation can help security teams evaluate their detection rules and fine-tune them to reduce false-positive alerts.

Key Selection Criteria for a Breach and Attack Simulation Solution

Criteria 6:
Threat Profiling and Customization

The cyber threat landscape of organizations changes depending on various factors such as their industry, geography, infrastructure, and many others. Hence, the threat landscape is unique to each organization. Consequently, organizations prioritize some threats over others and divert their resources to specific threats.

BAS should ease this process and provide threat profiling for organizations. The threat profiling maps threats to organizations' threat landscape and guides security teams on threat prioritization.

After threat profiling, security teams may want to create custom attack campaigns to simulate their specific threat landscape by chaining different attack simulations together and by testing their own payloads and data exfiltration samples. So, a BAS solution should allow security teams to build their custom attack campaigns to assess their custom security infrastructure.

Criteria 7:
Continuous and Automated Simulation

Continuous and automated simulation capability sets BAS solutions apart from other security assessment methods, such as red teaming and penetration testing. Red teaming and penetration testing assess the security posture for a brief time period and only report on that specific timeframe. However, continuous testing allows BAS to expose weak points in security controls against

- ever-changing threat landscape
- configuration changes in security controls
- addition or removal of security controls

BAS is also expected to provide automated simulations so that it does not need an operator to conduct attack simulations. When combined with automated testing, continuous testing allows security teams to quickly detect security controls that are disabled and in bypass mode.

Due to their great benefit, organizations should look for a BAS solution that has 24/7/365 continuous and automated simulation capabilities.

Key Selection Criteria for a Breach and Attack Simulation Solution

Criteria 8:
Real-Time and Customized Reporting

A thorough assessment of security controls generates enormous amounts of data, and the generated data can be used to produce numerous assessment reports that are required by different teams in the organization. As a result, a BAS solution should be able to automatically generate assessment reports for target audiences such as executives, security leaders, and incident responders.

The report of a security assessment should include real-time metrics such as

- overall security score
- detection rate
- mean time to detect (MTTD)
- trend statistics on
    - log collection
    - detection
    - prevention
- compliance-related data

Criteria 9:
Mapping to MITRE ATT&CK and Other Frameworks

Security professionals worldwide use the ATT&CK framework as a reference and guide to explain malicious actions employed in cyberattack campaigns. The MITRE ATT&CK framework has become the common language for describing adversary techniques and sharing threat intelligence. Also, many organizations and regulatory bodies use heatmaps mapped to the MITRE ATT&CK framework; these heatmaps give a simple and easy-to-understand visual representation of the cyber security assessments.

Due to its widespread use, a BAS solution should provide automated mapping to the MITRE ATT&CK framework. A mature BAS solution should provide automated mapping for:

- simulated threats
- each adversary action in a simulated attack scenario
- identified security gaps (heatmap)

Providing mapping to other popular frameworks, such as Cyber Kill Chain, is a great plus.

Key Selection Criteria for a Breach and Attack Simulation

Criteria 10:
Ease of Use and Ease of Deployment

An enterprise-level network infrastructure typically utilizes many different security technologies, and managing these technologies requires a great deal of attention from security teams. Since the infrastructure is already complex enough for many organizations and security teams, a BAS solution is expected to be easy to use and hassle-free. Also, BAS should support easy deployment on the cloud and on-premises and have a small footprint in the organization's infrastructure.

A mature BAS solution should

- have a simple and easy-to-understand interface
- avoid adding complexity and workload
- make optimizing security controls easier
- empower security teams to achieve greater impact with less effort
- be easy to deploy on the organization's existing infrastructure
- support cloud and on-premises deployment

Conclusion

As the cyber threat landscape expands and cyber-attacks become more prevalent and impactful, organizations look for ways to improve their security posture and minimize cyber risks. However, organizations cannot overcome the challenges in enterprise cybersecurity with traditional security assessment practices such as vulnerability scanning, penetration testing, and red teaming. The complicated and rapidly changing threat landscape, underutilized security controls, and overwhelmed security teams should be addressed with an automated solution that can tirelessly assess the organization's security posture while reducing the workload of security teams.

Breach and Attack Simulation allows organizations to test their security controls against real cyber threats and adversary campaigns. The attack simulations provide a clear picture of the security posture and help security teams identify the gaps in their security controls. Although many vendors name their solutions as BAS, not every BAS solution is the same or capable of assessing security controls thoroughly. This paper explains essential criteria for organizations in their quest to find the best BAS solution. These selection criteria describe a mature BAS solution that can help organizations overcome the challenges in enterprise cybersecurity and improve the efficiency and effectiveness of their cybersecurity operations.

References

[1] "Automated Breach and Attack Simulation Market," MarketsandMarkets. Available: https://www.marketsandmarkets.com/Market-Reports/automated-breach-attack-simulation-market-43164821.html

[2] "Website." Available: https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

[3] "pwc 2024 Global Digital Trust Insights" Available: https://www.pwc.com/hu/hu/kiadvanyok/assets/pdf/pwc-2024-global-digital-trust-insights.pdf

[4] "edgescan 2024 Vulnerability Statistics Report" Available: https://info.edgescan.com/hubfs/23DOWNLOADABLE%20CONTENT/Vulnerability%20Statistics%20Reports/Edgescan_VulnerabilityStatsReport2024.pdf

[5] Picus Labs, "The Blue Report 2024," Jul. 30, 2024. Available: https://www.picussecurity.com/resource/report/blue-report-2024

[6] "Is your greatest risk the complexity of your cyber strategy?" Available: https://www.ey.com/en_gl/insights/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy

[7] "CrowdStrike Global Security Attitude Survey 2021" Available: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021CSGlobalSecurityAttitudeSurvey.pdf

[8] "Hype Cycle for Threat-Facing Technologies, 2018," Gartner. Available: https://www.gartner.com/en/documents/3882466

About the Picus Security Validation Platform

Reduce your threat exposure with real-world attack simulations and AI-driven insights.

Security Control Validation

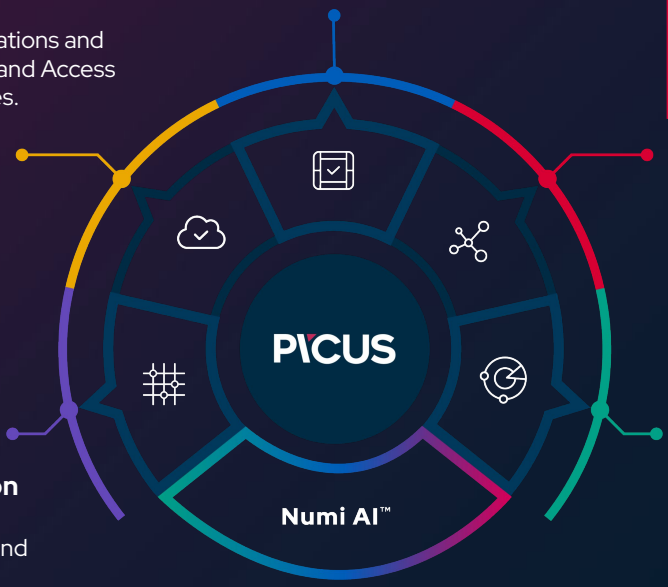
Measure and optimize the effectiveness of security controls with Breach and Attack Simulation.

Cloud Security Validation

Identify cloud misconfigurations and overly permissive Identity and Access Management (IAM) policies.

Attack Path Validation

Eliminate high-risk attack paths that attackers could exploit to compromise users and assets.



Attack Surface Validation

Enhance visibility of internal and external cyber assets and the security risks they pose.

Detection Rule Validation

Optimize detection efficacy by identifying performance issues affecting detection rules.

Elevate your security capabilities with the Picus Security Validation Platform

REQUEST A DEMO

PICUS

picussecurity.com

FROST & SULLIVAN FROST RADAR™ LEADER Global Breach and Attack Simulation 2022

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2024

Gartner Peer Insights Customers' Choice 2024

4.8/5.0

Highest-rated vendor*

Breach and Attack Simulation

*Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024