PICUS

THE DEFINITIVE GUIDE
FOR CHOOSING THE RIGHT BREACH AND ATTACK SIMULATION TOOL

Evolving threats and attack vectors make maintaining a strong security posture more challenging year on year. Acceleration in digital transformation during the pandemic is also compounding issues with the introduction of new technologies that increased vulnerabilities and introduced new security gaps. Amid these mounting challenges, the most effective strategy is to proactively ensure the efficacy of security defenses against threats—both long-standing and emerging.

To help identify ways to optimize security controls, an organization may look to traditional assessment methods like pen testing, vulnerability scanning, and red teaming. However, these point-in-time assessments can be resource intensive, entails risks, and don't provide real-time visibility.

For greater assurance, organizations need **Breach and Attack Simulation (BAS).**

The Right BAS Tool for Security Control Validation

Breach and Attack Simulation measures and strengthens cyber resilience by automatically and continuously testing the effectiveness of your defenses. An assessment tool with advanced components, there is a myriad of vendors and solutions on offer but not all are created equal.

Use the checklist below to get acquainted with the critical BAS features needed for COMPLETE security control validation and narrow down your search for the perfect solution.

Key Considerations:

Simulation capability

To better understand how threat actors could gain initial access to an environment and move laterally, prioritize a solution capable of simulating a comprehensive library of attacks across the cyber kill chain and via network, endpoint, email, and cloud vectors.

Control validation

A BAS solution should provide a holistic view of your prevention and detection controls, alerting you of attacks your tools might have missed and gaps that can potentially be exploited if mitigating actions are not taken.

Threat coverage

Breach and Attack Simulation should be able to simulate a wide variety of attacks and be reliably updated to incorporate emerging threats.
Be aware that some vendors may charge a premium for early access to new simulation content.

Ease of use

To avoid adding to the workload, prioritize a solution that makes simulating threats simple and hassle-free, and can empower red and blue teams to achieve greater impact with less effort.

Technology integrations

A BAS solution should support a wide range of prevention technologies such as firewalls, email gateways, WAFs, and more as well as provide deep integration with SIEM and EDR detection tools.

Support for ATT&CK

A BAS tool's ability to map the results of simulations to MITRE ATT&CK is a highly desirable feature, helping to visualize threat coverage and improve decision-making.

Cloud and on-premises deployment options

Flexibility in terms of how a BAS solution can be deployed is another important factor. Requirements vary and change over time so choose a solution that is easily scalable and can adapt to support evolving business and security needs.

Real-time reporting

A BAS solution should supply data in real-time and have trend statistics to show the progress of your security posture over time. Automatically generated reports (suitable for security and business leaders) also negate the need for manual processes—saving teams valuable time and resources.

Picus Pro-tip

Whichever solution you choose, the ultimate indicator of a great Breach and Attack Simulation tool is its ability to help you maximize cyber security ROI and empower your organization with direct and actionable mitigation insights—allowing for quick remediation of security gaps and boosting cyber resilience.

About PICUS

At Picus Security, we help organizations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber resilience.

As the pioneer of Breach and Attack Simulation (BAS), our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address them.

FROST & SULLIVAN LEADING VENDOR IN BAS MARKET 2020

2021 Computing Security Awards WINNER Breach and Attack Simulation Solution of the Year

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

CYBERTECH100 2022 The World's Most Innovative CyberTech Companies for Financial Services

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022

Learn how our platform can help you elevate your cyber resilience

SPEAK TO AN EXPERT

picussecurity