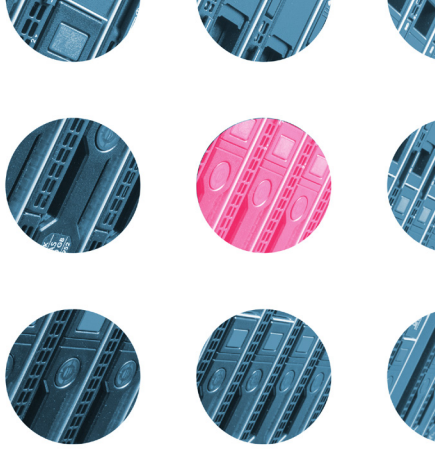
SafeBreach



Validating Cloud-Based Security Controls

Optimize Your Multi-Cloud Security Posture

Analysts forecast that 70% of enterprise workloads will run in the cloud by 2028. As more areas of the business move to the cloud—and leverage multiple cloud providers—organizations are exposed to new security challenges that increase exposure and risk. The SafeBreach platform improves cyber and operational resilience by validating the efficacy of your cloud security controls, identifying vulnerable attack paths, and expediting remediation. Whether you utilize Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). SafeBreach can continuously validate your cloud control and data planes to ensure your cloud estate is protected against risks like:

Misconfiguration

Misconfiguration of cloud-based applications and security controls can include retaining default accounts and passwords, not turning off publicly-accessible links to files and folders, unencrypted data, and not applying appropriate updates and patches.

Account Hijacking

Cloud account hijacking is a common tactic for adversaries to gain access to cloud-based data assets. Attackers often use a compromised email account or other credentials to gain access to the cloud estate and conduct malicious or unauthorized activity.

Unauthorized Access

Cloud security breaches can include unauthorized access to user data, theft of data, and malware attacks. Businesses must implement strong authentication and authorization controls to ensure only authorized users have access to sensitive data.

Lack of Visibility

With cloud computing, visibility is vital. Businesses must regularly audit security operations and procedures to proactively detect vulnerabilities and threats before they become a problem.

Test Cloud-Native Environments Against Advanced Threats

SafeBreach offers continuous security validation powered by breach and attack simulation (BAS) to test the effectiveness of all layers of your security stack independently. With support for the most popular cloud platforms, the SafeBreach platform enables security teams to execute breach scenarios across the entire cyber kill chain, automate and prioritize remediation, and strengthen your cyber resilience to:

Simulate Advanced, Multi-Phase Threats

Automate multi-stage attacks across the entire cloud stack, including end-user devices, networks, cloud services, and applications. Employ known IOCs and threat-actor-behavioral techniques to replicate attempts to access metadata, extract configuration information, exfiltrate data, and execute server-side request forgery.

Ensure Containers Are Secure

Extend attack simulations to container-based infrastructures running Docker to test the data plane, network, and API against a range of tactics, including process injection, rogue applications, system changes, and lateral movement from container to container.

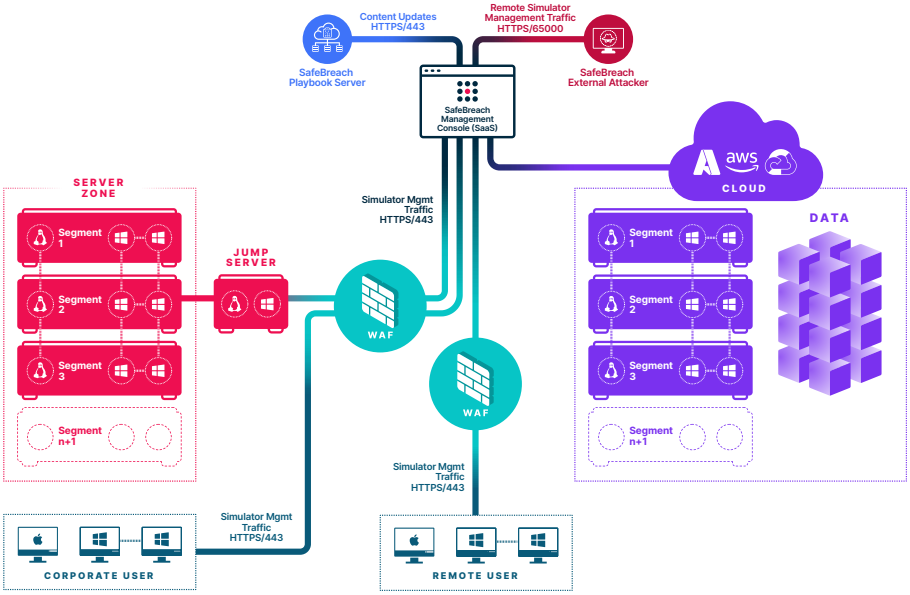
Identify Gaps & Prioritize Remediation

Analyze and visualize test results to quickly identify and prioritize security gaps. Use remediation insights to facilitate and automate resolution. Customize dashboards and reports to communicate status and risk level to key stakeholders.

Test Cloud Apps During Development

DevOps teams can leverage contextual insights from simulated attacks to continuously assess the security and integrity of web applications at each stage of development, allowing them to identify and address vulnerabilities before releasing an application into production.

Cloud & On-Prem Security Validation in a Single Platform



The SafeBreach Advantage

- **Most comprehensive multi-cloud-focused attack coverage of any BAS platform**
- **Largest attack playbook in the industry, with 30,000+ attack methods**
- **Only BAS vendor providing a 24-hour SLA for US-CERT and FBI Flash alerts**
- **Widest MITRE ATT&CK coverage of any BAS platform**
- **Scalable, enterprise-ready platform with simple deployment**
- **Broad technology partner ecosystem to support integration with existing controls and business systems**
- **Award-winning customer success team to help you deploy and manage your BAS program**
- **Supports attack scenarios for AWS, Azure, GCP, multi-cloud, and cloud-hybrid environments**

SafeBreach

US Headquarters

526 W Fremont Ave #2880
Sunnyvale, CA 9408

Israel Offices

HaMasger St 35, Sky Tower, Floor 8
Tel Aviv-Yafo, Israel