SafeBreach

Maximizing the Security of Cloud-Based Assets with SafeBreach

The advantages of the cloud are plentiful. So are the risks. The problem is that while leaders are clear on the cloud's benefits, security teams lack visibility into where the gaps are and what to do about them. With SafeBreach, security teams can establish continuous breach attack simulation, so they can spot potential risks before they get exploited.

The Problem: Unrecognized Security Gaps Leaving Organizations Exposed

Within enterprises, the question isn't whether to make the move to the cloud. The questions are when, which cloud provider and how many workloads.

The reality is that cloud services offer a wide range of significant advantages and enterprise leaders will continue to move to the cloud to capitalize on those advantages.

Something else is also abundantly clear: where sensitive data goes, attacks are sure to follow—and cloud environments are no exception. Unfortunately, while the move to cloud environments has been happening fast, security capabilities haven't kept pace.

While cloud providers offer a range of security capabilities and layers of defenses have been established, the reality is that risks remain and many security teams lack the visibility they need to identify threats and address them. Misconfiguration errors are common. Many services are exposed to attacks like server-side request forgery (SSRF). Teams lack visibility into how data could be exfiltrated or held hostage. As a result, they only find out about vulnerabilities too late—after they've been exploited.

For security teams, these stark realities are compounded by a number of factors:

- Increasing complexity. Now, a complex, hybrid mix of on-premises infrastructure, public clouds and private clouds are being relied upon, along with a diverse range of vendors, platforms, and technologies—and each has its own distinct security requirements.
- Increasing pace of change. With intensified reliance upon DevOps approaches and container-based architectures, environments continue to grow more dynamic. With services, resources and environments in constant flux, new vulnerabilities can arise at any time.
- Increasing sophistication and incidence of threats. Whether waged by opportunists or highly organized criminal syndicates or nation-states, attacks continue to grow more prevalent and devastating.

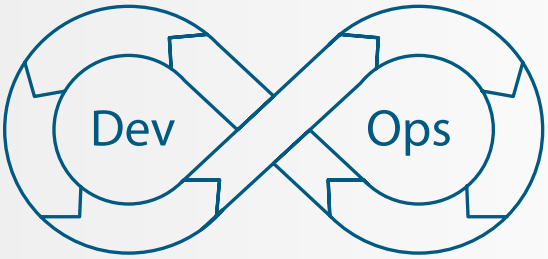
To keep pace with these new realities and mounting demands, security teams need solutions that offer continuous visibility into cloud environments. Teams need to be able to spot vulnerabilities and address them before they are exploited.

The Promise of the Cloud:

Improved agility, reduced capital expenses, enhanced flexibility and more.

The Reality of the Cloud:

For Capital One, it only took a former AWS employee one misconfigured web application firewall to wage an attack. The result: more than 106 million customers exposed, a 5% drop in market capitalization overnight, and $80 million in fines.



The Solution: SafeBreach Cloud-Native Breach Attack Simulation

The SafeBreach platform offers the advanced security capabilities teams need to fully leverage cloud services, while realizing maximum security of cloud-based resources. The SafeBreach platform enables teams to execute attacks safely and continuously, visualize weaknesses and remediate holistically.

Advanced, Cloud-Native Breach Attack Simulation

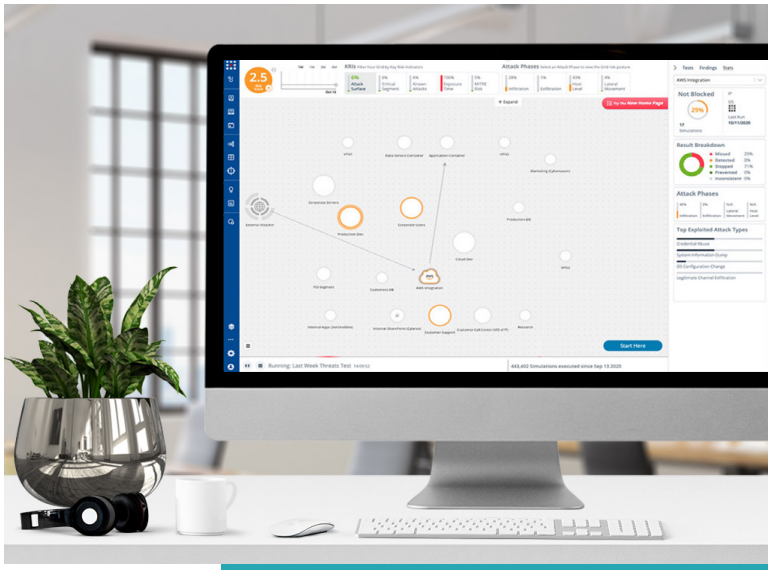
With the SafeBreach platform, teams can execute attacks continuously to test cloud-native environments. With SafeBreach, your teams can:

- Simulate advanced, multi-phase threats. The platform automates the execution of multi-stage attacks, including attempts to access metadata, extract configuration information and exfiltrate data. The platform can determine whether cloud systems and services are exposed to server-side request forgery and other attacks.
- Harness complete cloud environment coverage. The SafeBreach platform can simulate attack methods to uncover the organization's security posture across the entire cloud stack. The platform employs known indicators of compromise and threat actor behavioral techniques across end user devices, networks, cloud services and applications. The platform offers support for the control plane in cloud environments, including AWS, Azure and Google Cloud (GCP).
- Track vulnerabilities in container-based environments. The SafeBreach platform also features cloud-native container security capabilities, extending attack simulation coverage to container-based infrastructures running Docker. It simulates attacks against the Docker data plane, network, and API, employing a range of tactics, including process injection, rogue applications, system changes and lateral movement from container to container.

Visualize Weaknesses

The SafeBreach platform provides an intuitive hacker's view of the company's security posture, revealing key insights via heat mapping and exposure paths. The solution can provide:

- A heat map that portrays problem areas, which is aligned with MITRE ATT&CK framework.
- Views of exposed network paths to reveal the areas with the highest exposure.



Remediate Holistically

The SafeBreach platform offers advanced remediation capabilities that enable teams to quickly and effectively address security gaps. The platform brings together vulnerability management, threat intelligence and breach attack simulation to help teams prioritize remediation based on business risk.

Rather than leaving teams to struggle with piecemeal, ad hoc reports, SafeBreach aggregates simulation data to deliver complete remediation plans. The platform's intuitive, comprehensive visibility enables security, network, endpoint, and IT teams to collaborate effectively, so they can all be better equipped to defend the enterprise against breaches.

DevOps Support

The SafeBreach platform offers indispensable support to security and DevOps teams. The platform's attack simulation can provide continuous insights. With the platform, teams can introduce testing across every stage in the DevOps software development lifecycle, so your teams can address vulnerabilities before they make it to production. Ultimately, the platform offers the capabilities that are integral to establishing true DevSecOps capabilities.

Benefits

SafeBreach, your organization can:

- Establish safeguards that protect cloud-based assets against a broad array of threats.
- Prevent large-scale breaches, and their devastating penalties.
- Improve your risk posture, while more fully leveraging the cloud services that propel your business.

SafeBreach

111 W. Evelyn Avenue Suite 117
Sunnyvale, CA 94086 408-743-5279
safebreach.com

Learn More

Cloud-based assets and services may be exposed now. Now's the time to leverage a solution that enables you to identify those threats and address them.

Request to speak with a SafeBreach expert for an in depth discussion of the SafeBreach cloud native capabilities.

Request a Demo

Here