# SafeBreach Platform

SafeBreach

Datasheet

## Key Benefits

### Simulate and Test

**Security Control Validation**
Continuously test and report on cyber-risks to critical resources with the industry's most comprehensive playbook of attack simulations

**Security Posture Visibility**
Visibility into your dynamic risk posture, what is working, and what is not

### Prioritize

**Resource Prioritization**
Prioritize remediation efforts on high value assets and threats

**Dynamic Business Impacts**
Ensure that business driven changes do not compromise security

### Mitigate

**Misconfigured assets**
Receive actionable guidance to mitigate gaps discovered

**Integrated Ecosystem**
Comprehensive integration with key security technologies deployed

## Key Features

**Global Risk Director**
Enables linking of asset business value to security control effectiveness delivering data driven risk and mitigation analysis

**Comprehensive Play Book**
Industry leading range of attacks delivers the highest level of coverage

**Advanced Attack Visualization**
Breach Explorer provides visual attack path analysis for root cause analysis

**Attack Insights**
SafeBreach offers comprehensive guidance on remediating security gaps

**Open Attack Development Platform**
Breach Studio enables development of custom attack simulators by the team

## The Security Team's Challenge

Despite huge investments in people and products, security teams still struggle to answer some of the most fundamental questions and empower their teams to efficiently and effectively address the challenges they face every day.

- What are the most urgent risks to the business assets I must protect?
- Are my defenses working as expected?
- Can my current defenses keep up with the growing number of threats?
- How can we most efficiently prioritize our efforts to get the best results?

## The SafeBreach Platform

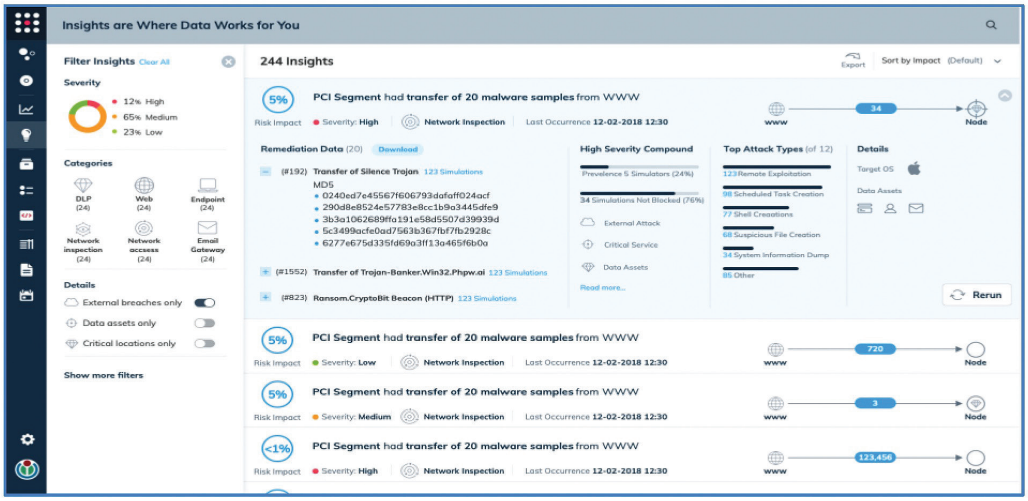
SafeBreach allows security teams to provide data-driven proof-of-security, to eliminate security blind spots and weaknesses, and to validate that controls are working as expected.

To stay ahead of attacks, security teams must harness the same tools and techniques attackers use. The SafeBreach platform safely executes thousands of proven attacks and breach simulations — automatically, continuously, and at scale.

Based on ongoing security research and drawing from actual investigations, SafeBreach safely executes breach scenarios across the entire cyber kill chain to prove where security is working as expected and uncovering areas where attacks will break through defenses.

SafeBreach delivers the following key capabilities:

- Automated, continuous and network-wide attack simulation
- Real time prioritization of business risks and actionable intelligence on the effectiveness of operational security posture
- Most comprehensive coverage of attacks and attack vectors in the industry



Insights are Where Data Works for You

Filter Insights Clear All

Severity
- 12% High
- 65% Medium
- 23% Low

Categories: DLP (24), Web (24), Endpoint (24), Network inspection (24), Network accsess (24), Email Gateway (24)

Details
- External breaches only ●
- Data assets only ○
- Critical locations only ○

Show more filters

244 Insights

Export | Sort by Impact (Default)

5% Risk Impact — PCI Segment had transfer of 20 malware samples from WWW — Severity: High | Network Inspection | Last Occurrence 12-02-2018 12:30 — WWW → 34 → Node

Remediation Data (20) Download

− (#192) Transfer of Silence Trojan 123 Simulations
MD5
- 0240ed7e45567f606793dafaff024acf
- 290d8e8524e57783e8cc1b9a3445dfe9
- 3b3a1062689ffa191e58d5507d39939d
- 5c3499acfe0ad7563b367fbf7fb2928c
- 6277e675d335fd69a3ff13a465f6b0a

+ (#1552) Transfer of Trojan-Banker.Win32.Phpw.ai 123 Simulations

+ (#823) Ransom.CryptoBit Beacon (HTTP) 123 Simulations

High Severity Compound
- Prevelence 5 Simulators (24%)
- 34 Simulations Not Blocked (76%)
- External Attack
- Critical Service
- Data Assets

Read more...

Top Attack Types (of 12)
- 123 Remote Exploitation
- 98 Scheduled Task Creation
- 77 Shell Creaations
- 68 Suspicious File Creation
- 34 System Information Dump
- 85 Other

Details
- Target OS
- Data Assets

Rerun

5% Risk Impact — PCI Segment had transfer of 20 malware samples from WWW — Severity: Low | Network Inspection | Last Occurrence 12-02-2018 12:30 — WWW → 720 → Node

5% Risk Impact — PCI Segment had transfer of 20 malware samples from WWW — Severity: Medium | Network Inspection | Last Occurrence 12-02-2018 12:30 — WWW → 3 → Node

<1% Risk Impact — PCI Segment had transfer of 20 malware samples from WWW — Severity: High | Network Inspection | Last Occurrence 12-02-2018 12:30 — WWW → 123,456 → Node

## Actionable "Insights"

SafeBreach Insights delivers hard data and detailed guidance to security operations to enable quick remediation actions based on an automated analysis of multiple simulation results. These insights allow the team to prioritize their efforts by business impact - in terms of risk and posture allowing the team to resolve items quickly and accurately saving time and money.

The remediation data can be aggregated and exported to a wide number of external security solutions ranging from network security appliances to SOAR solutions for enabling fully automated remediation of many incidents.

## What Customers Say

**"We use SafeBreach inside PayPal to gain a continuous, measurable and complete view of our security posture."**

*Brian Johnson*
*Senior Director of Security*
*PayPal*

**"SafeBreach helps my team prioritize which actions to take to maximize protection, and how to minimize the potential damage we might face if our systems were breached."**

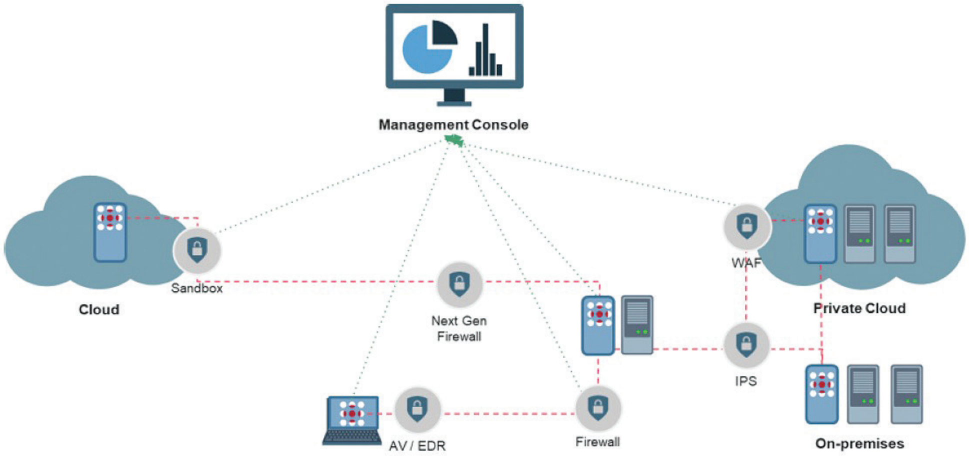
*Yaron Levi*
*CISO*
*Blue Cross and Blue Shield*
*Kansas City*

## About SafeBreach

Headquartered in Sunnyvale, California, the company is funded by Sequoia Capital, Deutsche Telekom Capital Partners, Draper Nexus, Hewlett Packard Pathfinder, PayPal, and investor Shlomo Kramer.

For more information, visit www.safebreach.com or follow on Twitter @SafeBreach.

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



## The SafeBreach Architecture

The SafeBreach Platform is comprised of the following components:

Management server: The centralized management server incorporates the complete Hacker's PlaybookTM of breach methods, and manages a distributed network of simulators. Capabilities include the ability to manage all aspects of simulator configuration, review simulations that have been successful or blocked, and provide the ability to filter, prioritize, and analyze all findings. The management server can be deployed on-premises or in an enterprise cloud infrastructure.

Simulators: The SafeBreach simulators perform the role of the attacker, or the receiver simulating attacks across the cyber kill chain nad covering all attack vectors.

## Unmatched Coverage

The SafeBreach Hacker's PlaybookTM is made up of thousands of real breach methods like phishing, endpoint infection, brute force, covert exfiltration, ransomware and more. Developed by SafeBreach LabsTM, our elite team of ethical hackers and security researchers—the Hacker's PlaybookTM is constantly updated and expanded.

## Comprehensive Integrations

The SafeBreach Platform Integrates with a wide range of security partners and products. Integrations enable automatic mitigation of security gaps identified and enhance the context and information available to the user.

## Key Use Cases

- Measure effectiveness of current controls
- Improve Security Tool ROI
- Proof of Controls and Compliance
- Prioritize Security Team actions
- Enhance Pen Testing and Red Team Operation
- Mergers and acquisitions