SafeBreach Platform

SafeBreach

Datasheet

Key Benefits

Simulate

Validate security controls with over 15,000 attack methods contained in the SafeBreach Hacker's Playbook™ to test defenses across your network, endpoint, and cloud solutions.

Visualize

Visualize your security posture mapped to the MITRE ATT&CK™ framework. A detailed network topology view shows all exposures along the cyber attack kill chain.

Prioritize

Data-driven results to prioritize remediation of security controls and vulnerability management patching of systems that are actually exploitable.

Remediate

Collaborate across Security and Infrastructure teams with actionable remediation data - prioritized by business impact - and feed mitigation data to your network, endpoint, SIEM and SOAR solutions.

The Security Team's Challenge

Despite massive and ongoing investments in people and security products, enterprise security teams still struggle to answer fundamental management questions and effectively address 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

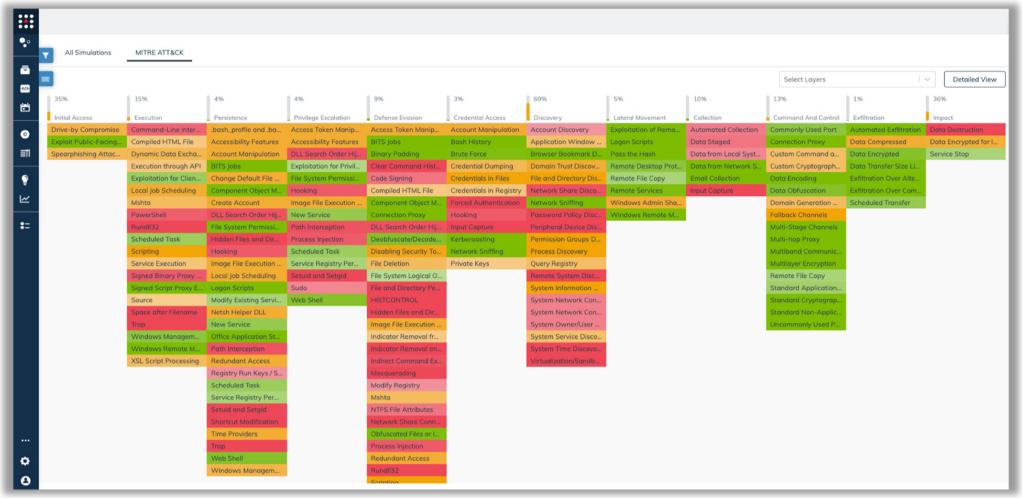
SafeBreach enables security teams to provide data-driven proof of security, eliminate security blind spots and weaknesses, and validate that controls are working as expected.

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

SafeBreach safely executes breach scenarios across the entire cyber kill chain to determine where security is working as expected and uncover areas where specific attacks will break through current defense configurations.

SafeBreach delivers the following key capabilities:

- Automated, continuous and network-wide attacks
- Paint the picture of how an attack would play out in your environment with SafeBreach Explorer view and mapping TTPs to the MITRE ATT&CK framework
- Real-time prioritization of business risks and actionable intelligence on the effectiveness of operational security posture
- Delivers visibility into which vulnerabilities are actually exploitable and sets their prioritization based on your environment



35% Initial Access	15% Execution	4% Persistence	4% Privilege Escalation	9% Defense Evasion	3% Credential Access	69% Discovery	5% Lateral Movement	10% Collection	13% Command And Control	1% Exfiltration	36% Impact
Drive-by Compromise	Command-Line Inter...	.bash_profile and .ba...	Access Token Manip...	Access Token Manip...	Account Manipulation	Account Discovery	Exploitation of Remo...	Automated Collection	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing...	Compiled HTML File	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window ...	Logon Scripts	Data Staged	Connection Proxy	Data Compressed	Data Encrypted for I...
Spearphishing Attac...	Dynamic Data Excha...	Account Manipulation	DLL Search Order Hij...	Binary Padding	Brute Force	Browser Bookmark D...	Pass the Hash	Data from Local Syst...	Custom Command a...	Data Encrypted	Service Stop
	Execution through API	BITS Jobs	Exploitation for Privil...	Clear Command Hist...	Credential Dumping	Domain Trust Discov...	Remote Desktop Prot...	Data from Network S...	Custom Cryptograph...	Data Transfer Size Li...	
	Exploitation for Clien...	Change Default File ...	File System Permissi...	Code Signing	Credentials in Files	File and Directory Dis...	Remote File Copy	Email Collection	Data Encoding	Exfiltration Over Alte...	
	Local Job Scheduling	Component Object M...	Hooking	Compiled HTML File	Credentials in Registry	Network Share Disco...	Remote Services	Input Capture	Data Obfuscation	Exfiltration Over Com...	
	Mshta	Create Account	Image File Execution ...	Component Object M...	Forced Authentication	Network Sniffing	Windows Admin Sha...		Domain Generation ...	Scheduled Transfer	
	PowerShell	DLL Search Order Hij...	New Service	Connection Proxy	Hooking	Password Policy Disc...	Windows Remote M...		Fallback Channels		
	Rundll32	File System Permissi...	Path Interception	DLL Search Order Hij...	Input Capture	Peripheral Device Dis...			Multi-Stage Channels		
	Scheduled Task	Hidden Files and Dir...	Process Injection	Deobfuscate/Decode...	Kerberoasting	Permission Groups D...			Multi-hop Proxy		
	Scripting	Hooking	Scheduled Task	Disabling Security To...	Network Sniffing	Process Discovery			Multiband Communic...		
	Service Execution	Image File Execution ...	Service Registry Per...	File Deletion	Private Keys	Query Registry			Multilayer Encryption		
	Signed Binary Proxy ...	Local Job Scheduling	Setuid and Setgid	File System Logical O...		Remote System Disc...			Remote File Copy		
	Signed Script Proxy E...	Logon Scripts	Sudo	File and Directory Pe...		System Information ...			Standard Application...		
	Source	Modify Existing Servi...	Web Shell	HISTCONTROL		System Network Con...			Standard Cryptograp...		
	Space after Filename	Netsh Helper DLL		Hidden Files and Dir...		System Network Con...			Standard Non-Applic...		
	Trap	New Service		Image File Execution ...		System Owner/User ...			Uncommonly Used P...		
	Windows Managem...	Office Application St...		Indicator Removal fr...		System Service Disco...					
	Windows Remote M...	Path Interception		Indicator Removal on...		System Time Discove...					
	XSL Script Processing	Redundant Access		Indirect Command Ex...		Virtualization/Sandb...					
		Registry Run Keys / S...		Masquerading							
		Scheduled Task		Modify Registry							
		Service Registry Per...		Mshta							
		Setuid and Setgid		NTFS File Attributes							
		Shortcut Modification		Network Share Conn...							
		Time Providers		Obfuscated Files or I...							
		Trap		Process Injection							
		Web Shell		Redundant Access							
		Windows Managem...		Rundll32							
				Scripting							

Actionable Insights

SafeBreach Insights automatically analyzes thousands of results, and continually provides detailed guidance for the security team to quickly remediate gaps or suboptimal configurations in your security controls.

These insights and the detailed action recommendations allow the team to prioritize remediation work by business impact. The team gains the ability to resolve all high-risk and high-impact items quickly and accurately.

The remediation data is shared with a wide number of external security solutions ranging from network, endpoint, cloud, SIEM and SOAR solutions, to enable automated remediation of many incidents.

Integrated Ecosystem

Comprehensive integration with key security technologies and business platforms installed at millions of organizations.

About SafeBreach

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

For more information, visit www.safebreach.com or follow on LinkedIn: linkedin.com/company/safebreach

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

Comprehensive SafeBreach Platform

Integration with Threat Intelligence

Operationalize the latest threat intelligence by safely and quickly testing how your defenses will prevent, detect and respond, with SafeBreach. SafeBreach converts threat feeds to run safely across your network, testing your endpoint, network, email, cloud and container controls to paint the picture of a hacker's view of how your defenses will stand up against an attack.

Testing your defenses against the latest threats is the only way to understand the potential risk to the business.

Risk-Based Vulnerability Management

The biggest challenge in vulnerability management (VM) is prioritization. Because thousands of vulnerabilities may exist in an enterprise environment, it has been virtually impossible for organizations to pinpoint which security gaps could lead to the most damaging consequences to the business.

SafeBreach integration with VM tools clarifies the actual posture of your environment, in terms of what hackers can reach and exploit. By continuously executing attacks in your environment, SafeBreach calculates the risk of both network and host attacks. Combining SafeBreach insights with its results from vulnerability scans, VM teams can focus their remediation efforts on the locations that have the greatest risk of exploitation by adversaries.

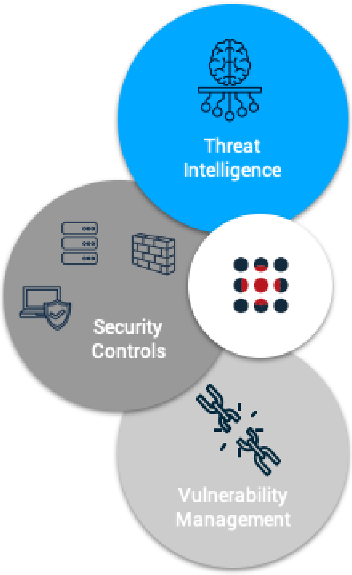
Assess Cyber Risk with Integrated Solutions

To most effectively evaluate how your defenses will respond against both well-known threats and the latest threats seen in the wild requires tight integrations with SafeBreach of the following:

- a threat intelligence system
- endpoint, network and SIEM security solutions
- a vulnerability management solution

SafeBreach will safely execute attacks across your enterprise to validate what your security controls will detect and prevent, correlate the data to your vulnerability scans to prioritized patch management based on what is exploitable, and bring your teams together with a detailed remediation plan to defend your enterprise.

SafeBreach is the only solution in the market that brings together threat intelligence, vulnerability management and security control validation to fully assess an organization's cybersecurity risk.



Key Use Cases

- Measure effectiveness of current security controls
- Improve Security Tool ROI
- Prioritize vulnerability patch management with what is exploitable in your environment
- Understand your security posture against the latest threats
- Effectively measure your cybersecurity risk