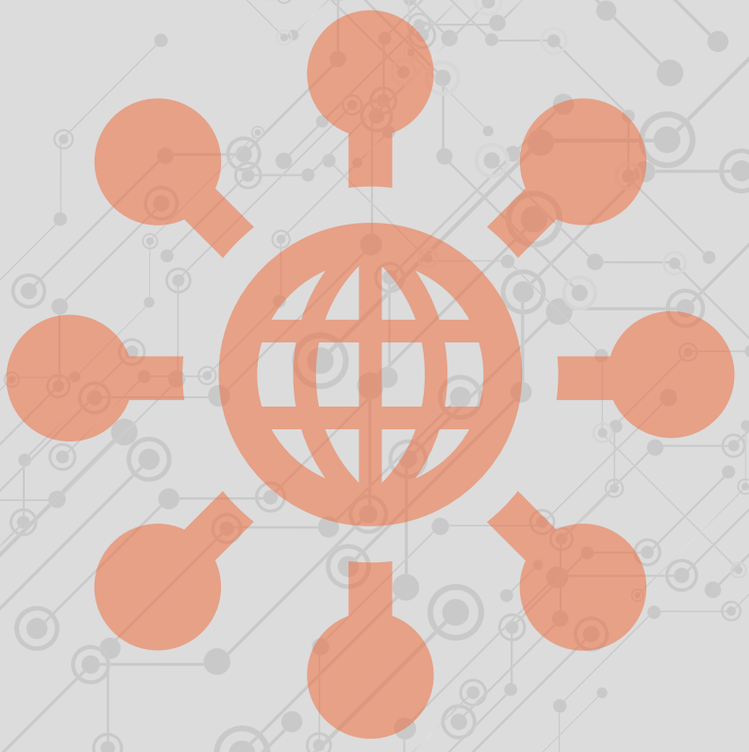
GET A VIRTUAL HACKER ON YOUR SQUAD

Beat cybercriminals at their own game with breach simulations

SafeBreach

ARE WE SAFE FROM CYBERATTACKS?



Hackers > breaches > exfiltration/interruption > damages.

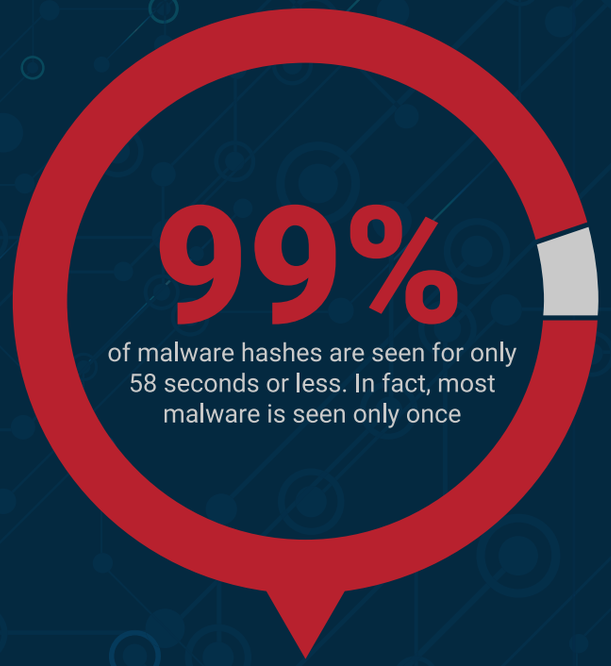
It's is an all-too-frequent storyline that plays out every day in every industry, in nearly all corners of the world. From the Ukraine power grid going dark because of a cyberattack, to the U.S. Internal Revenue Service breach that compromised personal information from more than 700,000 American taxpayers, organizations and governments don't appear to be getting any safer from cyberattack.

That's right, despite organizations collectively spending more than $81 billion annually[1] on cybersecurity solutions, hackers continue to gain the upper hand. Why is that? Here's a hint: It's usually not because we don't have the right security technology in place.

Read on to discover the secret about our current cybersecurity landscape that keeps CISOs from understanding whether their security systems are truly working as expected and knowing what their cybersecurity risks are at all times. When you've finished, you'll know what it takes to confidently answer the board-level question of "Are we secure?"

[1] Gartner, "Garter Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016," August 9, 2016.

WHAT KEEPS CISOS UP AT NIGHT



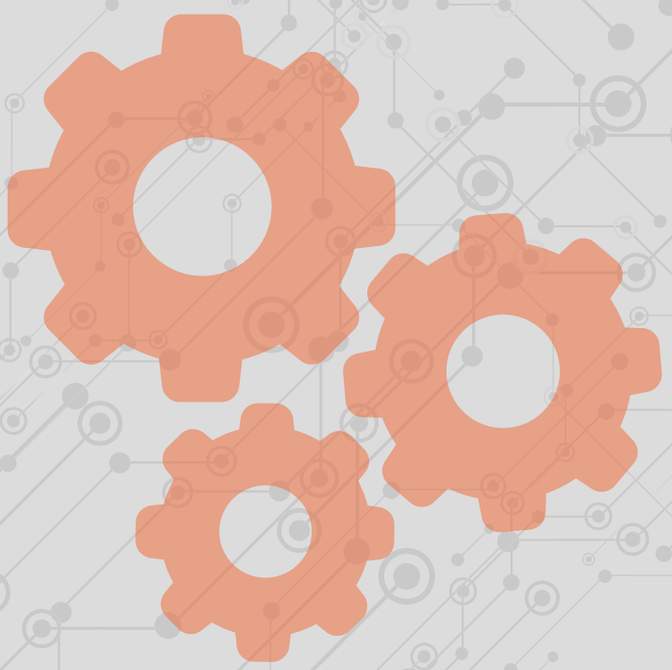
$6 TRILLION

in annual costs due to cybercrime expected by 2021

Sources: “2016 Data Breach Investigations Report,” Verizon;

“Hackerpocalypse: A Cybercrime Revelation,” Cybersecurity Ventures.

ARE YOUR SECURITY MEASURES WORKING?



We all know that hackers are getting faster and more sophisticated. But the cybersecurity good guys are getting smarter, too, right? After all, CISOs and their security teams have spent considerable amounts of time and money implementing best-of-breed technologies and creating the right processes for prevention and detection of cyber threats, including:

Deploying security products such as anti-virus, firewalls, intrusion detection systems, security information and event management (SIEM) systems, user behavioral analytics, and more

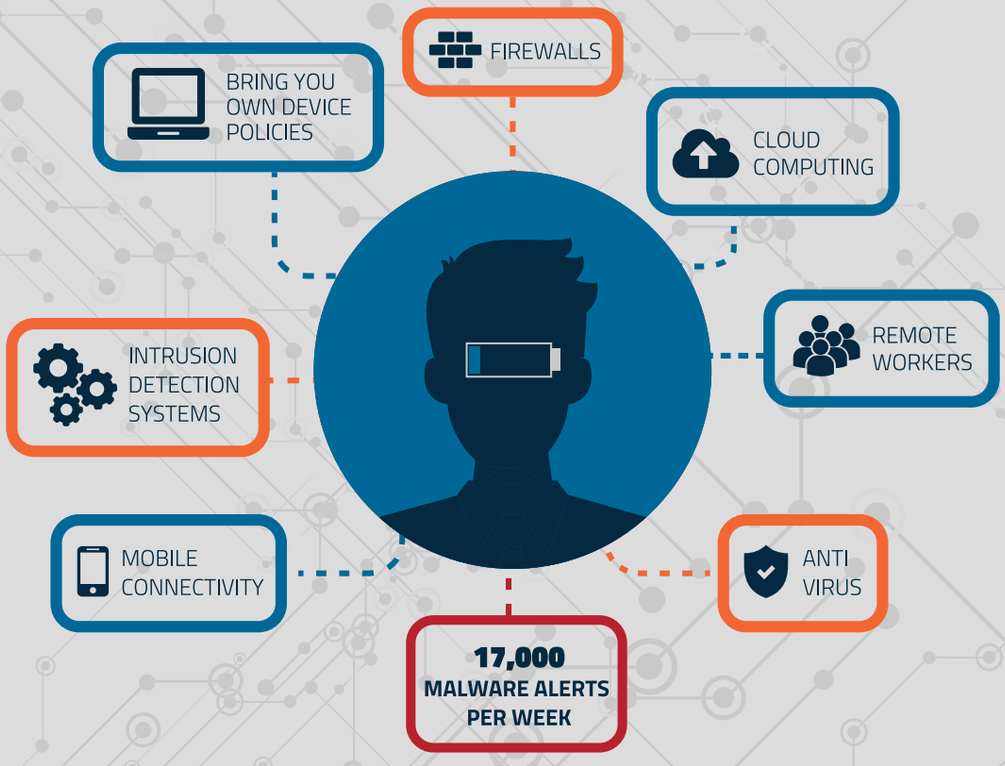
Taking advantage of security best practices

Hiring security professionals for penetration testing and red team services

Running vulnerability scans

Patching new zero-day vulnerabilities

YET, THE BREACHES KEEP HAPPENING.



Why? It's not because these prevention and detection technologies and best practices don't work.

The real reason—and one that is certainly difficult to admit —is that our defenses have become so extraordinarily complex that we don't actually know whether they were implemented correctly or whether they are still working as planned.

The truth is that security teams often can't answer the following questions with certainty:

Are all security products deployed correctly for your environment?

Has the security software been properly maintained and have relevant software updates been applied?

Are configurations still appropriate given the ever-changing business and IT enviorment?

Is the functionality of your security tools keeping pace with the changing threat landscape?

Are your security products optimized to detect and prevent threats to all of your most valuble digital assets?

Do all your security products work correctly with each other?

GETTING AHEAD OF THE BREACH

Given that the problem is complexity and not knowing whether you've implemented and maintained the right defenses in the right way for all the right parts of the infrastructure, then the answer is validating — over and over —that your security measures are accurate and working as expected.

This means discovering for yourself—before a cybercriminal does it for you -whether there are security holes that could allow attackers to penetrate your defenses and successfully exfiltrate data or disrupt the business.
How? By adopting a three-pronged, proactive, and predictive security strategy:

THINK LIKE A HACKER

Put yourself in the footsteps of the adversary and approach your security not from the perspective of managing products and alerts, but thinking about the cyber kill chain and the corporate assets that could be targets.

CHALLENGE YOUR DEFENSES

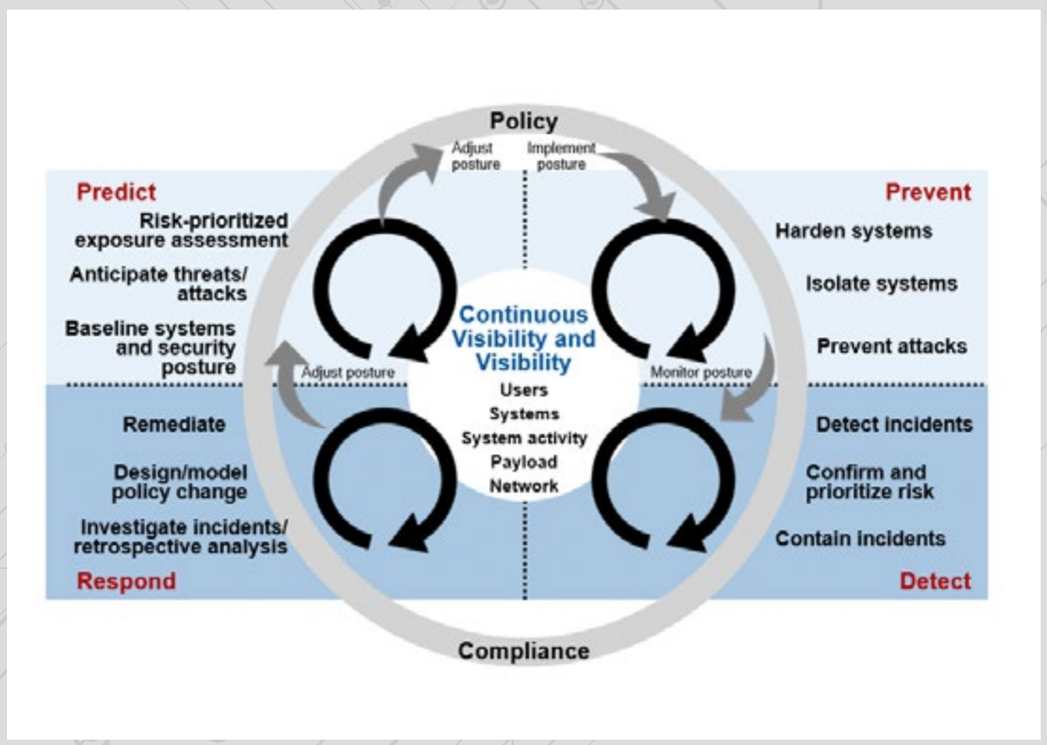
Validate that the security framework you designed (including people, process, and technology) is what is actually being implemented. Train your security operations center (SOC) teams to anticipate what a breach might look like, and ensure the right alerts are triggered and the right people are notified.

CONTINUOUSLY TEST

Hackers are challenging your security controls every day. You need to do the same because your environment changes constantly with new users, applications, devices, and more being added all the time.Continuously challenging your defenses is the best way to proactively improve your security.

Chances are, your security team is already tackling some aspects of a proactive and predictive strategy. But with hackers breaking through defenses every day, it's time to take your strategy to the next level.

PREDICTIVE CAPABILITIES ARE PART OF THE GARTNER ADAPTIVE SECURITY ARCHITECTURE



Source: Adaptive Security Architecture – Gartner, 2016.

Analyst firm Gartner also recommends that organizations develop predictive security capabilities. According to Gartner analysts Neil MacDonald and Peter Firstbrook, “Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective, and response capabilities.”

In the Gartner Adaptive Security Architecture, “Predict” is an important category to proactively anticipate new attacks against the current state of systems and information. The idea is that while organizations should deploy firewalls, intrusion prevention systems, and other traditional prevention and detection security technologies, these solutions alone are not enough without the missing layer of predictive security. By predicting how attacks may occur, enterprises can then adjust their security protection strategies to prioritize and address exposure.

In fact, in most organizations the ability to baseline your security posture and predict breach scenarios is a prerequisite to determining which prevention and detection capabilities are needed.

EXISTING APPROACHES TO VALIDATING SECURITY FALL SHORT

While adopting a predictive strategy is critical for CISOs to understand whether their security investments are working as expected and exactly what their cybersecurity risks are at all times, current efforts based on traditional approaches typically fall considerably short. Here's why:

APPROACH	DRAWBACKS	EXPLANATION
PENETRATION TESTING	Point-in-time only Limited to skillsets of testers	Security consultants hired to conduct penetration testing to validate risks annually or biannually can't keep up with an organization's dynamic environment. These expensive engagements are also entirely dependent on the skillsets of the team members (and their favorite hacking tricks).
SECURITY RED TEAMS	Limited to skillsets and availability of team members	Some larger organizations have developed internal red teams that "play the hacker" and are proactive about finding security risks in their environment. However, there is a general shortage of these elite security engineers with specific offensive-security skillsets. Additionally, security red teams are limited to mature security organizations with significant security budgets.
VULNERABILITY SCANS	Too many false positives Only address vulnerabilities and not other breach methods	Vulnerability management systems are too noisy to provide an accurate view of risks. During an automated vulnerability scan across 100 companies, 900,000 security-related red flags were found, with an 89 percent false positive rate in some industries[2] . A completely-patched system also isn't an indication of a secure environment as there are many other breach methods that a real attacker might use besides taking advantage of a vulnerability.

[2] Pauli, Darren, "Auto vulnerability scanners turn up mostly false positives," The Register, March 14, 2016

CONTINUOUS, AUTOMATED VALIDATION IS THE ANSWER

To effectively adopt a proactive security strategy and overcome the weaknesses of traditional validation approaches, you need to automate the process. With a continuous breach simulation platform, you can automatically simulate hacker breach methods to see how your infrastructure and systems are viewed as a target.

With a continuous breach simulation platform, your organization validates risks in your real production environment, across the entire kill chain, using real hacker breach methods, on an ongoing basis. No more point-in-time limitations or depending solely on the skillsets of your staff or hired security consultants to identify security risks.

Here's what to look for in a continuous breach simulation platform:

USES A REAL HACKER PLAYBOOK

Your automated breach simulation solution should use a black-box approach (no prior knowledge of the environment is required) and incorporate a comprehensive "hacker's playbook" of threat types including brute force, exploits, malware, and remote access tools.

PROVIDES CONTINUOUS SIMULATIONS

Your breach simulation platform must run continuously so that you know at all times - not just annually or biannually - whether your security measures are working properly.

RUNS SIMULATION IN A REAL PRODUCTION

Simulations in an actual production environment are the only way to know if someone can exfiltrate data or infiltrate the network. Breach simulation should simulate breach methods as closely as possible without impacting your environment or creating false positives.

SIMULATES AROSS THE ENTIRE KILL CHAIN

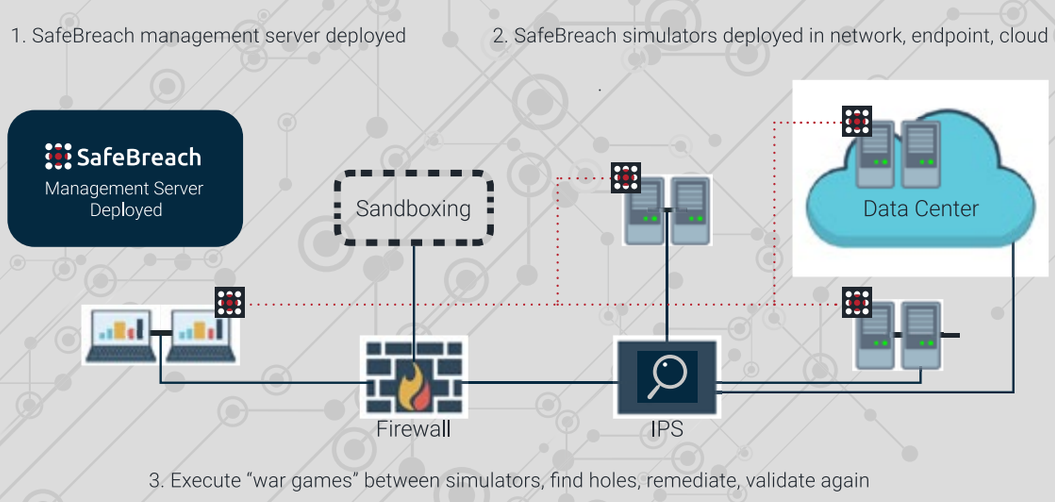
By validating your defenses across the entire kill chain, you can determine your organization's strengths and weaknesses and decide on the most effective way to stop a breach. For comprehensive visibility into risks across the entire organization, the simulation platform must support endpoints, network, and cloud.

WORKS WITH OTHER TOOLS

Your platform must work with the other required capabilities for preventing, detecting, and responding to threats (as described in the Gartner Adaptive Security Architecture). For example, when a breach is simulated, your platform must integrate with ticketing systems to create a task for the blue team, or trigger automated remediation policies in automation and orchestration systems.

UNLEASH A VIRTUAL HACKER

The SafeBreach platform simulates hacker breach methods to find possible breach scenarios in your environment, and then recommends fixes based on what is found. With SafeBreach, you can quantify actual risks of breach, validate whether your security controls are effective, and empower your security operations teams with actionable insight.



How it works:

Deploy simulators that act as “virtual hackers”: SafeBreach lightweight simulators play the role of the hacker. Deploy them in critical segments of your network, in the cloud, or on an endpoint, to simulate the entire kill chain—infiltration, lateral movement, and exfiltration. Simulations run automatically and continuously.

Orchestrate and execute breach scenarios: The SafeBreach management platform manages and executes the Hacker's Playbook of breach methods on our simulators. Our patent-pending technology simulates breach scenarios without impacting users or infrastructure. Breach methods are constantly updated by SafeBreach Labs, our team of offensive security researchers.

Quickly take corrective action: Our platform correlates and analyzes all breach methods, and presents information useful for both security analysts and security executives. You can take a deep dive into breach scenario building blocks and quickly remediate based on SafeBreach recommendations. Use our business insights to engage and educate the board on your true security risks.

IMPROVE SECURITY WITH SAFEBREACH

SafeBreach is a fundamentally different platform that automates adversary breach methods to help you and your security team:

Validate the efficacy of your security defenses: SafeBreach provides continuous insights into how well security controls such as firewalls, intrusion prevention systems, and secure web gateways are working at all times. Often breaches happen because security products are misconfigured or deployed incorrectly. SafeBreach provides definitive validation of whether your security products are deployed correctly and able to withstand an attack.

Shorten exposure time: By continuously challenging your security defenses and identifying gaps in your security posture, SafeBreach shortens exposure time and enables organizations to mitigate issues before an attacker takes advantage of them.

Proactively understand the impact of a breach: By simulating breach methods in the headlines or breaches that are currently happening to your peers, you can accurately show what the impact would be and quantify your specific risks. This information can help you get more budget for needed security measures, reduce your attack surface, and break the kill chain. You can provide precise input to guide board-level and executive investment decisions.

Ensure compliance with regulatory mandates: With continuous validation of your security posture, you can also demonstrate compliance with relevant regulatory mandates. For instance, you can confirm that access to Payment Card Industry Data Security Standard (PCI DSS) zones is properly restricted. Instead of checking a compliance box and finding security gaps later, with SafeBreach, you can verify both security and compliance within your environment.

Empower red team members: SafeBreach empowers red team operations by allowing members to test different breach and what-if scenarios that are specific to their business and industry. It also frees red teams to focus on more strategic tasks by automating validation activities.

QUESTIONS TO ASK YOUR SECURITY TEAM ABOUT THEIR CURRENT CAPABILITIES FOR USING PREDICTIVE SECURITY:

Can you validate that all security technologies and controls are configured and deployed correctly?

Do you understand exactly what a specific breach scenario might look like?

Can you simulate breaches in the production environment and not just in a test environment?

Are the right alerts being triggered and are the right people being called when a simulated breach scenario occurs?

Can you simulate breach methods across the entire kill chain and across all enterprise environments - including network, endpoint, and cloud?

A REAL-WORLD EXAMPLE OF PREDICTIVE SECURITY SUCCESS – LEADING SECURITY SOLUTIONS DEVELOPER

"SafeBreach constantly challenges my security controls to ensure they are working as expected and improves the quality of thefindings of my security teams. It enhances security by identifying potential outbound channels for data, and makes our security team more efficient and effective by focusing them on the right issues."

– Chief Information Security Officer for a leading security solutions developer

CHALLENGE: Protect sensitive data for millions of customers

With network security a primary focus, a well-known financial technology firm consistently strives to proactively gain awareness of all network security risks. The company particularly wanted to find and close any gaps in its infrastructure that would allow a hacker to exfiltrate confidential customer data. According to a senior security architect for the firm, "We wanted to address the last step in the kill chain; getting an actionable list of 'outbound channels' we could close to prevent data from being exfiltrated."

SOLUTION: Validate security controls with SafeBreach

After quickly deploying SafeBreach, the firm began receiving updates on breach scenarios in real time—all without affecting the stability or uptime of its environment. SafeBreach provided a definitive list of roughly 50 ways data could get out of the firm's environment, which helped the company significantly reduce its attack surface. "If you step through everything SafeBreach identifies as risks, you close all the 'unknowns,' which is huge," says the senior security architect.

A REAL-WORLD EXAMPLE OF PREDICTIVE SECURITY SUCCESS – LEADING MOBILE AND ONLINE MESSAGING PLATFORM

"Hackers don't rest, and that means neither can we. Buying and implementing the latest defensive technologies and patching the latest bugs are necessary, but not sufficient. We need to be able to anticipate what an attacker will do next, and get there first. SafeBreach helps us with do this."

– Chief Security Officer, leading mobile and online messaging platform

CHALLENGE: Understand and manage security risks

A messaging platform company couldn't determine the actual risk or potentially successful breach scenarios once someone was inside the company's network. This was despite deploying a variety of vulnerability assessment and change management tools to help it identify, assess, and efficiently manage security risks.

SOLUTION: Deploy the Hacker's Playbook

After evaluating alternatives including hiring ethical hackers or penetration testers, the company decided to implement an automated, continuous validation platform that would not impact stability or uptime in the production environment. With SafeBreach, the company can now simulate breach scenarios across the entire kill chain and validate both internal and external threats. According to the company's chief security officer, "For the first time, we were able to see multiple breach scenarios displayed in one consolidated view or screen. In addition, some of our security controls that we thought were fully deployed were missing in certain segments of the network."

LEARN MORE

To learn more about how automated,continuous breach simulation can help your organization answer the question, “Are we secure?” check out these additional resources:

- SafeBreach Hacker’s Playbook
- Learning from Hackers: Understanding your Adversaries for Better Security
- Playing CyberWar Games for Better Security

ABOUT SAFEBREACH

SafeBreach is a pioneer in the emerging category of continuous security validation. The company’s groundbreaking platform provides a “hacker's view” of an enterprise’s security posture to proactively predict attacks, validate security controls and improve SOC analyst response.

SafeBreach automatically executes breach methods with an extensive and growing Hacker’s Playbook of research and real-world investigative data. The company is funded by Sequoia Capital, Deutsche Telekom Capital, Hewlett Packard Pathfinder and investor Shlomo Kramer.

SafeBreach was awarded a 2016 SINET16 Innovator and featured in the RSA 2016 Innovation Sandbox.

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

SafeBreach

HQ
111 W. Evelyn Avenue
Suite 119
Sunnyvale, CA 94086
sales@safebreach.com

R&D
108 Igal Alon Street
4th Floor
Tel Aviv, 6789146
Israel