SafeBreach

Remote Workforce Security Validation

Service by SafeBreach

Organizations are now faced with an unprecedented challenge to extend security beyond boundaries of the enterprise network, to support a remote workforce to ensure business continuity. Now that the massive shift to remote work is established, security needs to be a primary focus because hackers are targeting employees working from home - as highlighted by the latest US-Cert Alert, [AA20-099A COVID-19 Exploited by Malicious Cyber Actors].

Ensure business continuity and safety of your business assets

SafeBreach, with its extensive Hacker's Playbook of breach and attack simulations, enables you to validate how effectively your security controls are blocking cyber attacks. To support organizations that now need to validate the safety of their business assets to support an extensive remote workforce, SafeBreach is offering a new service, Remote Workforce Security Validation as a Service (aaS). The turn-key service is managed by a SafeBreach team of security experts that will perform all the steps needed to validate the security risk and effectiveness of controls for the infrastructure changes to support and help safeguard your remote workforce.

This new service includes:

1. Coverage of the major attack vectors — email, endpoints, VPNs, networks and data leakage — for a remote workforce.
2. A new deployment-at-scale mechanism to enable wide coverage leveraging our cloud environment.
3. Our in-house offensive expertise to execute the validation process, analyze the risk and define the mitigation strategy for you.

Remote Workforce playbook coverage:

Email

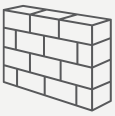
Simulate a range of malicious attachments (e.g. zip, tar, doc and pdf files) and phishing emails (from an extensive and growing list of malicious domains) which were specifically linked to the coronavirus outbreak.

Endpoint

Simulate multiple infection attacks (e.g., phishing, drive by downloads, ransomware, and trojan attacks) to validate that host controls are in place and up to date. Simulate a representative set of attacks that adversaries may attempt for persistence, execution and data gathering on target hosts. (e.g., brute force attacks that threat actors like ATP3 and Lazarus Group have perfected).

VPN

Simulate a representative set of attacks for lateral movement attempts (e.g., brute force, exploit VPN vulnerabilities, and phishing VPN credentials) and other remote exploitation techniques.



Network

Simulate both indicator- and behavior-based attacks (e.g., outbound C2 communication) and a representative set of attacks for multiple infiltration attack vectors (e.g., brute force attacks, malware propagation, and remote exploitation).

Data leakage

Simulate multiple techniques to validate the detection and prevention capabilities of your DLP controls (e.g., data exfiltration, improper permissions, and unencrypted communications).

Benefits

- Enable the business to work remotely and guarantee business continuity, while protecting your data assets.
- Extend visibility of your security posture to encompass the remote workforce, so the business can function both productively and safely.
- Quickly identify and remediate security gaps and drifts to stop cyber attacks and prevent data breaches that would pose major risks to the business.
- Offload security testing for the remote workforce to a team of specialized experts at SafeBreach; leverage our offensive capabilities and enable your employees to focus on business continuity.

Remote Workforce Security Validation Service Offering

The new Remote Workforce-specific playbook is designed with key breach and attack methods to quickly identify and remediate security gaps to safeguard the work activities and data of a remote workforce. The SafeBreach Labs team will continue to add the latest attack methods to the playbook as they evolve, and the SafeBreach security experts will ensure that these new attacks are simulated to validate the security controls in your environment.

SafeBreach Labs

SafeBreach Labs is a dedicated team of offensive security experts that works continually to grow our extensive playbook of attack methods. The team supports our customers with a 48-hour SLA on all US-Cert alerts to ensure our customers' security controls are validated against the latest IOCs. SafeBreach Lab is actively researching and monitoring the methods that attackers are using specifically to exploit the coronavirus crisis.

How it Works

Our team of security experts will deploy SafeBreach simulators across your remote workforce based on your needs to validate the entire remote workforce, or specific core departments (finance, HR, or highly targeted geographical locations) or critical employees (executives or administrators). Our team will then run the Remote Workforce playbook on the simulators and provide the following actionable data in detail:

- Assessment of remote workforce risk
- Detailed findings on attacks performed
- Prioritized remediation plan

About SafeBreach

SafeBreach simulates thousands of attack methods to provide a hacker's view of an organization's security posture, paint a picture of the security exposures to an enterprise and prioritize remediation, securing against TTPs. SafeBreach Labs is dedicated to threat research from real-world investigation with the most extensive breach and attack methods in the industry with over 12,000 attack methods and growing. SafeBreach is privately held and is headquartered in Sunnyvale, California with an office in Tel Aviv, Israel.