SafeBreach

Remote Workforce Security Validation

Service by SafeBreach

Our customers now face 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.

To support our customers in this time of crisis we developed a new service offering, Remote Workforce Security Validation as a Service (aaS). The SafeBreach team of security experts 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.

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 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).

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 Lab team will continue to build on the latest attack methods as they evolve.

SafeBreach Labs

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

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 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 detailed actionable data:

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

FAQ

1. Is there a risk of the VPN/Network to be overloaded by the testing?

SafeBreach testing generates a very low footprint on CPU, memory and network. Assuming the endpoints tested are already connecting to the corporate network using the VPN, the additional load associated with SafeBreach testing is expected to be negligible. For further technical details, please ask your customer success representative for SafeBreach footprint measurements technical note.

2. How is the data generated from the service maintained secure?

SafeBreach service is based on the same platform and data security standards as a cloud SafeBreach deployment including strict security standards. If you are interested to learn more about our cloud security standards please visit our knowledgebase or ask your customer success manager for our security standards documentation.

3. Are changes to my existing production or PoV deployment required?

Yes. The SafeBreach team will deploy simulators to each of the remote employees you designate, to run the security validation.

4. Can I exchange simulators between endpoints?

You can absolutely change simulators between tests but not on the same test. Note, that exchanging simulators between tests means that the baseline you are following to measure your posture will be based on a different set of employees and hence will affect the measurement of risk and the ability to validate risk reduction between tests.

5. What is the pricing model for the service?

The first assessment is free of charge.

The pricing model is adjusted to a service model with pricing per simulator. The pricing includes: SafeBreach security experts deploying simulators on your remote workforce laptops and desktops, running, maintaining and updating the Remote Workforce playbook and supplying a prioritized remediation plan to close up security gaps. Our team will deploy 100 to 100,000 endpoints of your remote workforce, based on your needs (critical employees, key departments or across the full remote workforce organization).