SafeBreach

SafeBreach Propagate

Test Network Attack Paths to Understand Post-Breach Blast Radius

Enterprise security teams are responsible for the critical task of regularly testing internal network security to gain visibility into potential vulnerabilities and attacker targets. Popular tools like manual penetration testing only provide limited, point-in-time assessments that are quickly outdated. Other automated solutions are either not scalable or have the potential to introduce additional problems during testing.

SafeBreach Propagate is an attack path validation tool that simulates attacker movement within the network to help security teams understand potential post-breach impact. This capability is specifically designed to augment the perimeter testing offered by SafeBreach Validate, our award-winning breach and attack simulation (BAS) tool, by using an "assumed breach" mindset to further validate network defenses against behavior often seen from ransomware and nation-state advanced persistent threat (APT) groups. SafeBreach Propagate allows you to:

- Uncover high-risk paths to critical organizational assets and crown jewels.
- Identify security gaps and strengths among and between network endpoints.
- Prioritize remediation activities to focus on the most critical exposures.
- Streamline communication with key stakeholders using built-in reports and dashboards.

Propagate Benefits

Accurately Identify High-Risk Attack Paths

Run advanced lateral movement attacks to understand the real blast radius of a successful breach within your network.

Save Time through Focused Remediation

Prioritize remediation activities based on vulnerable endpoints that provide the greatest risk to organizational assets and crown jewels.

Make Informed Security Decisions

Leverage structured reporting with clear findings to make informed security and business decisions to improve organizational resiliency.

Elevate Your BAS Deployment

Leverage Validate to first identify security gaps, then dig deeper with Propagate to understand attacker motives and their potential impact for a more comprehensive nderstanding of risk.

Propagate Use Cases

Attack Path Mapping

Understand and document likely attack targets and the ability of attackers to move laterally within the tested network.

Assess Post-Breach Organizational Exposure

Gain visibility into post-breach risk with reporting on gaps and opportunities to optimize identity and vulnerability protections.

Enterprise Safety & Scalability

SafeBreach Propagate was purpose-built for enterprise organizations and provides the highest level of protection against risks that other forms of security testing can introduce. It includes safety measures to ensure optimal adherence to enterprise-grade security standards and organizational security policies, including:

Scope Limitation

Customers can limit the scope of propagation to specific regions/machines by using “allow” and “block” lists of IP ranges.

Attack Customization

Users can define and customize the port scan allow/block list to decide which ports are included/excluded based on organizational security policies. This flexibility enables targeted and efficient testing, while minimizing any impact on critical services.

Credential Validation

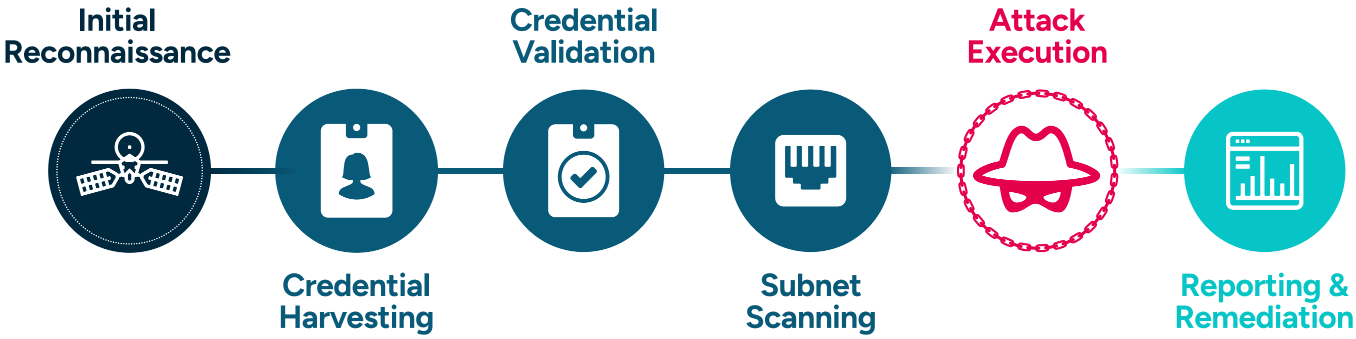
Propagate makes an effort to validate both offline and domain based credentials and won’t use invalid credentials in lateral movement attacks. This provides a second safety layer to minimize unnecessary attacks or lockouts.

Secret Safety

Credential recovery messages are securely transmitted via HTTPS to a cloud backend using a hybrid encryption model to protect any sensitive data. These credentials are encrypted and stored in a secure manner using a protected vault.

System Stability and Resource Consumption

Propagate enumerates only required users, files, and other resources. In addition, SafeBreach tests the attacks to verify that they do not affect the stability of the systems.



Initial Reconnaissance

Credential Harvesting

Credential Validation

Subnet Scanning

Attack Execution

Reporting & Remediation

How Propagate Works

1. Initial Reconnaissance

By leveraging an existing endpoint as "patient zero", Propagate performs reconnaissance and information gathering to identify which attacks can be successfully used to achieve its objectives.

2. Credential Harvesting

Credential harvesting attacks are executed that target OS operations (e.g., targeting registry, memory dump), password managers, and browser storage to discover gaps in areas where sensitive data may be stored.

3. Credential Validation

Collected credentials are verified to ensure they can provide access without triggering any lockout mechanisms. Domain hashes and plain-text passwords (domain and local) are verified to ensure their validity.

4. Subnet Scanning

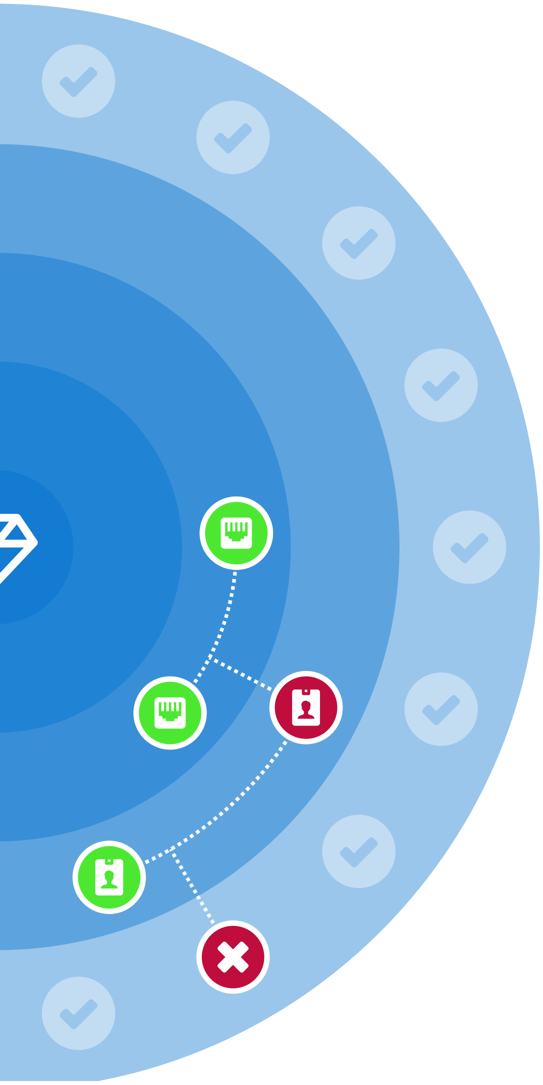
The local Class C subnet is scanned for open ports and services to identify a potential point of entry for lateral movement.

5. Attack Execution

Several attacks are executed to gain access to a target via lateral movement. These attacks include RCE via PAExec, Pass the Hash, WMI lateral movement, WinRM lateral movement, RCE via Invoke Command (WinRM), RCE via RDP, and RCE using PAExec and SSPI.

6. Reporting & Remediation

A structured report that highlights identified gaps along with actionable recommendations is available to make mitigation decisions.



Why Propagate?

SafeBreach Propagate saves enterprise security teams time when looking to identify post-breach exposures and understand the potential impact of an attacker moving laterally inside their organizational network. With Propagate, security teams gain the ability to:

Prioritize exposure remediation by combining the context gained from their BAS findings with identified attack paths to the organizational crown jewels.

Run continuous attack path mapping/validation to ensure a consistent level of protection and visibility inside their network.

Quickly identify the impact of credential harvesting by an attacker to identify potential admin account takeovers and exposures that can lead to data theft and exfiltration.

Get Hands-On with Propagate

Schedule a personalized demo today to learn why enterprise security leaders choose SafeBreach Propagate to enhance the quality, efficacy, and value of their security programs.

ABOUT SAFEBREACH

SafeBreach is the leader in enterprise-grade exposure validation, providing the world's largest brands with safe and scalable capabilities to understand, measure and remediate threat exposure and associated cyber risk. The award-winning SafeBreach Exposure Validation Platform combines pioneering breach and attack simulation and innovative attack path validation capabilities to help enterprise security teams measure and address security gaps at the perimeter and beyond. Backed by a world-renowned original threat research team and world-class support, SafeBreach helps enterprises transform their security strategy from reactive to proactive safely and at scale. To learn more about how SafeBreach helps enterprises with end-to-end exposure visibility, visit **www.safebreach.com.**