Reach

DATASHEET

Configured Right. Secured Tight.

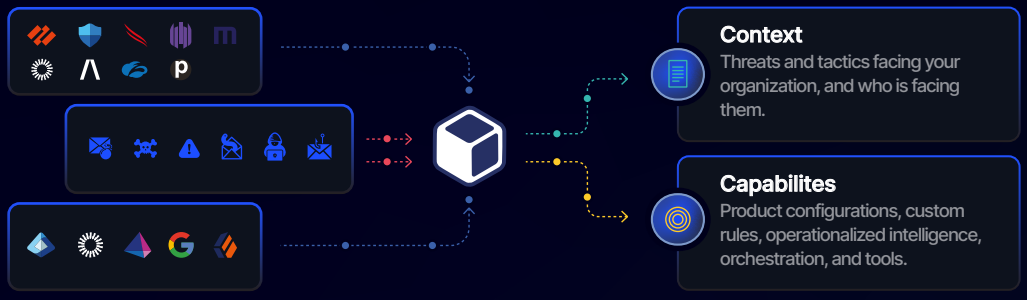
Proactively Find and Fix Misconfigurations to Supercharge Your Security Posture

Most breaches don't occur because attackers are impossibly sophisticated. They succeed because defenses are continually weakened by misconfigured security tools, configuration drift, and unused security capabilities that could block attacks if they were properly enabled.

Correcting these issues manually is a near impossible task. Security toolsets are sprawling, amounting to thousands of configurations that need constant managing. Vendors ship hundreds of feature updates per year, making it unfeasible for teams to learn and deploy these capabilities fast and effectively. Configurations drift as environments change, quietly weakening defenses over time. Security teams are not afforded the visibility, time, and resources necessary to tackle these challenges, and hiring more personnel to manually address these problems will not scale.

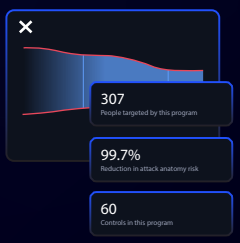
> "Misconfigurations have fueled more than 9.5 million cyberattacks in the first half of the year (2025)"
>
> SonicWall September 2025 Threat Brief

Reach integrates with your existing security and IT tools to analyze the configurations, coverage, and capabilities of the tools you already own, and then maps them to how attackers actually target your organization. Reach can then automatically identify blind spots across your defenses, prioritize fixes, remediate misconfigurations, and activate unused defensive capabilities. Reach then continuously validates over time that security posture remains strong and defenses stay aligned with your evolving environment and threat landscape.



Reach Helps Customers

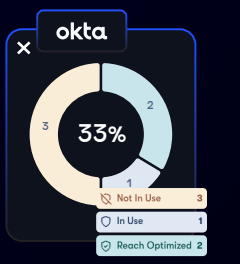
- Identify security blind spots from misconfigured and underused security and IT tools
- Prioritize action based on real-world risk and control capabilities
- Guide remediation to rapidly deploy changes and improve security posture
- Continuously validate to detect configuration drift, keep defenses aligned to policy, and maintain a strong security posture



Identify Blind Spots from Misconfigured and Underused Tools

Misconfigured, underused, and incomplete security controls leave gaps that attackers can exploit.

Powered by multi-model AI, Reach reveals hidden exposures at machine speed. MastermindAI™ connects directly into your existing stack – identity, endpoint security, email, firewalls, SASE, and more – and analyzes millions of data points using cybersecurity domain-specific models. Reach doesn't just see your environment. It understands how your defenses are used (and misused) against real attacker techniques. The result: precise exposure mapping and a clear picture of organizational risk.



Prioritize Action Based on Real-World Risk

Data without context is just noise. Most exposure management tools generate reports and assessments, but don't show you what to do next.

Reach cuts through the noise. Reach's AI models rank exposures by real risk, factoring in reachability, attack behaviors, and configuration context. Reach models how attackers could exploit your environment and matches that to the specific capabilities of your existing security tools. Recommendations are aligned to your business priorities, so you act on what actually reduces risk.

Guide Remediation to Improve Security Posture

Reach doesn't just surface issues - it fixes them for you. Reach generates detailed step-by-step remediation guides, automatically pushes recommended configuration changes into a staged environment for verification, then executes tailored remediation workflows across your security ecosystem via integrations with your ticketing systems – aligned to MITRE, ZTNA, or your chosen framework. Your team can quickly deploy changes and fix what's broken without adding friction to existing processes.

Continuously Validate That Security Posture Remains Strong

Security posture isn't static. Configuration drift erodes defenses quietly, leaving gaps over time.

Reach monitors your configurations over time to detect configuration drift the moment it happens, correct it, and continuously validate that controls are working as intended, security posture remains strong, and defenses stay aligned with your evolving environment and threat landscape. Your team can achieve continuous visibility and control to stay ahead of change and ensure posture isn't just assessed – it's maintained.

Multi-Model AI with Genius-Level Intellect in Cybersecurity

At Reach, AI isn't an add-on; it's the engine that powers how we solve security problems. Reach doesn't rely on a single LLM bolted onto a product. Instead, we use multiple domain-specific models trained on real-world security data, threat context, and a deep understanding of your security tools' capabilities. This unique understanding of both attacker techniques and your defensive controls allows Reach to proactively pinpoint exposures and provide a comprehensive understanding of risk across the organization.

Get Answers and Execute Actions with Reacher™

Reacher™, our interactive AI assistant, makes security posture accessible in plain language. Whether it's clarifying exposure details, explaining risk in business terms, or creating custom drift rules, Reacher™ helps you summarize results, answer questions, and deploy fixes across your ecosystem.

Only With Reach

- Real-world threat context vs. generic best practices
- Purpose-built MastermindAI vs. off-the-shelf models
- Actionable changes across your stack vs. shallow visibility
- Deep, multi-tool integration vs. shallow visibility
- Continuous validation vs. point-in-time reports

Get Started!

reach.security/try-reach

Join the growing community using Reach to reduce risk, maximize the value of their existing tools, and strengthen security without added complexity.

reach.security