AI Agents for Proactive Security

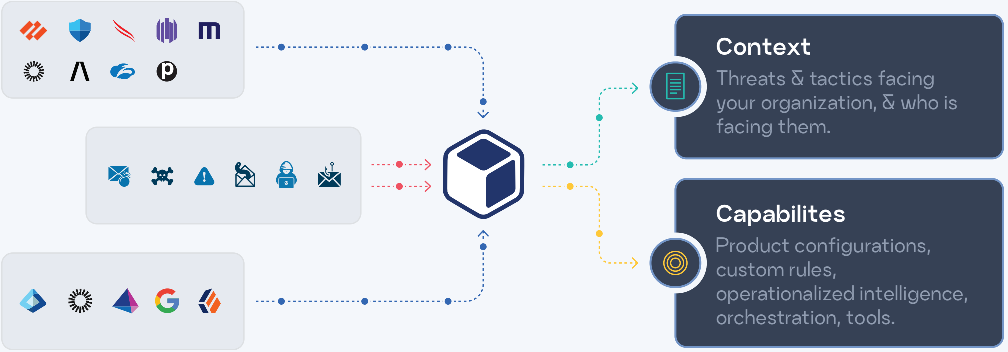
Find and Fix Hidden Risk

The cost of operating your security infrastructure keeps rising, but how much it reduces real exposure is still unknown.

Misconfigurations, underused controls, and incomplete deployments create gaps that attackers can exploit. Even when risks are identified, fixing them is often slow, manual, and resource-intensive. Worse still, configuration drift quietly undermines even the best security plans, introducing new risks as systems evolve and settings shift.

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

Reach uses always-on AI agents to proactively identify exposures, prioritize action, guide remediation, and continuously validate security controls to reduce risk and improve security posture without adding complexity. Security teams can move from reactive firefighting to proactive defense.



Context

Threats & tactics facing your organization, & who is facing them.

Capabilites

Product configurations, custom rules, operationalized intelligence, orchestration, tools.

Reach analyzes the configurations, coverage, and capabilities of the tools you already own, mapping them to how attackers actually target your organization.

Powered by MastermindAI™ and deep product integrations, Reach drives prioritized remediation and reduces the operational cost of managing your security infrastructure.

Identify Exposures from Misconfigured and Underused Tools

×
307
People targeted by this program
99.7%
Reduction in attack anatomy risk
60
Controls in this program

Misconfigured, underused, and incomplete controls leave gaps attackers exploit.

Powered by multi-model AI, Reach reveals hidden exposures at machine speed. MastermindAI™ connects directly into your existing stack—identity, endpoint, email, firewalls, SASE, directories—and analyzes millions of data points with domain-specific LLMs. 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.

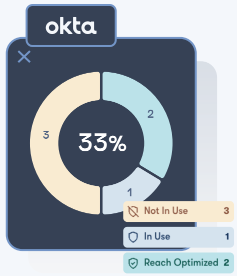
Reach

DATASHEET

Reach Helps Customers

- **Identify Exposure from misconfigured and underused tools**
- **Prioritize Action based on real-world risk and control capabilities**
- **Guide Remediation to improve security posture and maximize ROI**
- **Continuously Validate to detect drift and keep protections aligned to threats and policy**

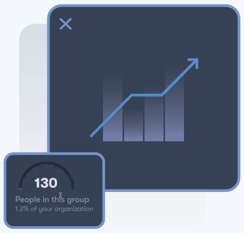
www.reach.security



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. AI agents 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 assess risk – it fixes it for you. Reach AI agents generate detailed configuration guides with context-aware recommendations and step-by-step fixes. Reach then executes tailored remediation workflows—aligned to industry standard frameworks like MITRE and NIST—across your security ecosystem through direct integration with your ticketing systems, including ServiceNow and Jira.

No more static reports or generic advice. Just clear, contextual instructions and automated remediation to fix what's broken.

Continuously Validate That Controls Stay Aligned to Threats and Policy

Security posture isn't static. Configuration drift erodes defenses quietly, leaving gaps over time. Powered by ConfigIQ Drift, Reach AI agents continuously monitor your environment to detect configuration drift, validate that protections are working as intended, and ensure controls stay aligned to policy and evolving threats.

Need clarification about an exposure? Want to understand your risk profile in plain language? Need to create a custom drift rule to close gaps and maintain security posture? Just ask Reacher™ – your always-on AI agent – for help to summarize results, answer questions, and deploy fixes across your ecosystem.

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 language models (DS-LLMs) 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.

AI That Fixes, Not Just Flags

Detection isn't enough. Reach AI agents go further—creating context-aware configuration guides, mapping fixes to MITRE and NIST, and generating remediation workflows in ServiceNow and Jira.

Get Answers and Execute Actions with Reacher™

Reacher™, our interactive AI agent, makes security posture accessible in plain language. Whether it's clarifying exposure details, explaining risk in business terms, or creating custom drift rules for you, Reacher™ helps you get answers and execute fixes on demand.

Reach

Only With Reach

Real-world threat context vs. generic best practices

Domain-specific language models trained on real-world security data vs. bolted on models

Actionable changes across your stack vs. static assessments

Deep, multi-tool integration vs. shallow visibility

Continuous validation vs. point-in-time reports

Get Started!

reach.security/try-reach

Reach is the first platform that delivers agentic left-of-boom risk reduction for security architects.

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

www.reach.security