Reach

DATASHEET

Close Security Control Gaps Before AI Attacks Exploit Them

AI Attackers Move Fast. Reach Moves First.

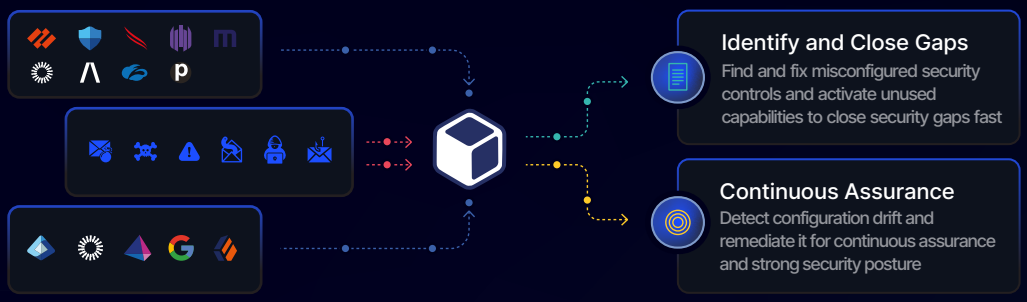
Cyberattacks target any kind of exploitable weakness across your defenses, including misconfigured security controls, unused security capabilities, and configuration drift. A stale firewall rule, a weakened EDR control, or a conditional access policy that drifted from security baselines can become the opening an attacker needs to breach your defenses. In fact, 97% of security professionals experienced a confirmed breach or near miss due to a security control misconfiguration in the past year.

AI has drastically accelerated the speed, scale, and volume of these attacks. An LLM-driven NTLM relay attack can complete in under three minutes. Multi-stage attacks can execute in minutes what would usually take hours or days for a group of humans to execute. And the volume of these attacks will increase by 89% year-over-year.

Human-powered defenses are too slow in comparison. Organizations review configurations 6.5 times per month on average, but once a misconfiguration is identified, remediation takes 8.3 days on average. Only 2% of security teams can fix issues in less than a day. It's simply not fast enough to keep up with AI-fueled attacker-side speed and precision. As a result, AI-powered attacks can find and exploit misconfigured security controls and drift faster than security teams can fix them.

> 97% of security professionals have experienced a confirmed breach or near miss due to a security control misconfiguration in the past year.
>
> Configure → Drift → Breach → Repeat: A 2026 research report from Reach Security

Only AI-powered defenses can outpace and stop AI-powered attacks. Reach is the AI-native operating system for your security controls. It connects with your existing security technology stack to continuously analyze the security control plane across identity, endpoint, email, firewall, SASE, and other critical defenses. Powered by a mixture of precise reasoning models and purpose-built cybersecurity domain-specific language models (DSLMs), Reach proactively identifies and remediates misconfigured controls, activates underutilized capabilities, and continuously monitors for configuration drift to close security gaps faster than AI-powered attacks can exploit them. Reach then continuously validates that security posture remains strong and defenses stay aligned with policy.

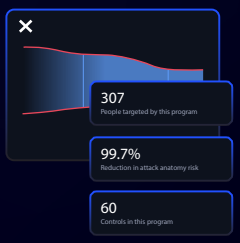


Reach Helps You

- Identify security blind spots from misconfigured security controls before AI-powered attacks can exploit them
- Prioritize action based on real-world risk and control capabilities
- Proactively remediate to rapidly deploy fixes and improve security posture
- Continuously validate that controls remain aligned to security baselines

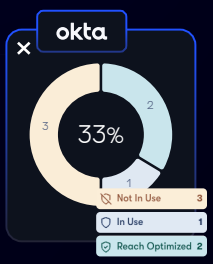
reach.security

Identify Blind Spots from Misconfigured Controls



Misconfigured and underutilized 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, and more – and analyzes millions of data points using cybersecurity domain-specific models. Reach sees your environment and 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.

Proactively Remediate at the Speed of AI

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 Security Controls

At Reach, AI isn't an add-on; it's the core engine that powers how we solve security problems. Reach uses 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, provide a comprehensive understanding of risk across the organization, and harden security controls faster than AI-powered attackers can find and exploit hidden weaknesses.

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 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 and control integration vs. shallow visibility
- Continuous validation vs. point-in-time reports

Get Started!

reach.security/connect

reach.security