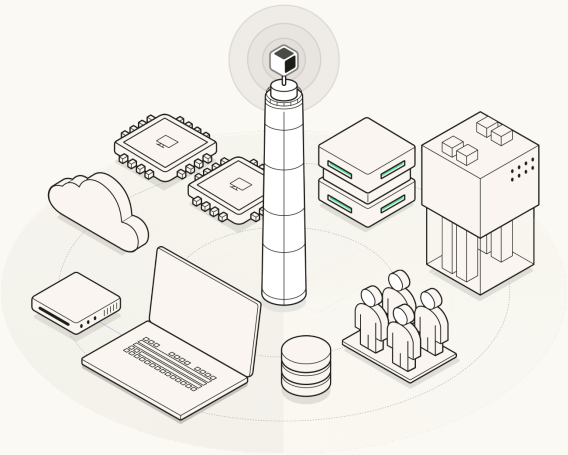
Reach

DATASHEET

Autonomously Close Defensive Gaps Before AI Attackers Exploit Them



THE PROBLEM

AI is transforming the speed and scale of cyberattacks. Attackers can rapidly discover and exploit weaknesses across enterprise defenses, from misconfigured security controls and configuration drift to unpatched software vulnerabilities (CVEs).

Enterprises have invested heavily in security technologies across identity, network, endpoint, and other domains. But these tools are constantly changing. New configurations, policy exceptions, disabled protections, and configuration drift can silently weaken defenses and create open doors for attackers. At the same time, vulnerability volume continues to grow, making it impossible to patch everything immediately.

Defenders are struggling to keep pace. Security teams already own powerful controls that can stop many of these attacks, but knowing how those controls should be configured, whether they are actually enforcing protection, and how to use them to mitigate vulnerabilities requires deep expertise and constant attention across siloed teams and tools.

ATTACKERS RUSH IN

72 minutes

from intrusion to exfiltration.[1]

VS

DEFENDERS CAN'T KEEP PACE

8+ days

to find and remediate a security control misconfiguration.[2]

THE CONSEQUENCES

97%

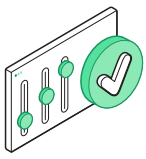
of security practitioners experienced a breach or near miss due to a security control misconfiguration.[2]

THE SOLUTION

AI Attackers Move Fast. Reach Moves First.

Reach gives defenders the intelligence and automation to find and close defensive gaps before AI-powered attackers exploit them. Powered by purpose-built AI, Reach continuously analyzes and strengthens the security controls you already own to deliver two critical capabilities:

Automatically Find and Fix Misconfigured Security Controls



Reach continuously detects and fixes misconfigured controls, dangerous control changes, and configuration drift across your defenses. It assesses their security impact, prioritizes risky exposures, and provides step-by-step remediation guidance or autonomous remediation. Security teams can continuously validate that security controls remain properly configured, actively protecting, and aligned with security policy. Defensive gaps remain closed to would-be attackers.

Mitigate Vulnerabilities with Compensating Controls



AI-powered vulnerability discovery is increasing CVE backlogs. Security teams can't patch fast enough, leaving organizations exposed to attack. Reach finds and deploys compensating controls to mitigate vulnerabilities and keep exploits out until patches go in. Reach analyzes exploitation techniques, identifies security controls capable of blocking attacks, verifies they're correctly configured and enforcing protection, and continuously monitors for changes that could reopen exposure.

[1] Unit 42 Global Incident Response Report 2026. [2] Reach Drift Research Report 2026. Survey of 250 security practitioners.

Your Security Controls Source of Truth. Powered by Mastermind AI.

Reach brings deep, specialized intelligence to your existing security stack. It understands how security controls work, how they should be configured to stop real-world threats, and how controls across identity, network, endpoint, and other domains work together to disrupt attacks throughout the attack chain.

At its heart is Mastermind AI, which combines two complementary technologies:

Cybersecurity Domain-Specific Language Models (DSLMs)

Purpose-built models trained on vendor configurations, threat intelligence, security best practices, and frameworks like MITRE ATT&CK. They understand security control capabilities and how to configure and coordinate them to stop real-world attacks.

Deterministic Reasoning Models

Structured, evidence-based reasoning that continuously analyzes your actual configurations, settings, and policies. These models validate that controls are properly configured and enforcing protection, identify defensive weaknesses, and recommend precise remediation actions.

Together, these technologies give Reach a continuously validated source of truth about your security controls, enabling reliable decisions, automated remediation, and stronger defenses at machine speed.

Put Reach to Work Wherever You Work

Reach's capabilities are available through its user interface, but organizations can also embed its security controls expertise and intelligence directly into existing SOC, SIEM, and frontier AI workflows.

SOC & SIEM WORKFLOWS

Enrich Alerts. Accelerate Triage. Fix Root Causes.

Enrich security alerts with protection status, control configurations, and changes to help analysts investigate faster, identify root causes, and remediate underlying gaps to reduce future alert volume.

YOUR FRONTIER AI MODELS & AGENTS

Bring Your AI. Give It Reach.

Through Reach's MCP server, equip your frontier AI models and agents with Mastermind AI's specialized security expertise and validated controls intelligence to identify gaps, guide remediation, and automate defensive action.

Stronger Defenses. Less Manual Work.

Using Reach, organizations eliminate manual analysis, accelerate investigations, and get more protection from existing security investments.

95hrs

time saved per employee per month

Insurity

90%

reduction in manual security tasks

NUTANIX

“Reach is our source of truth. It gives us continuous proof that our controls are doing their job. Because Reach uses AI to continuously review and tune every control, we keep pace with rising attack volume without adding headcount.”



Sebastian Goodwin
Chief Trust Officer
at Autodesk

AUTODESK