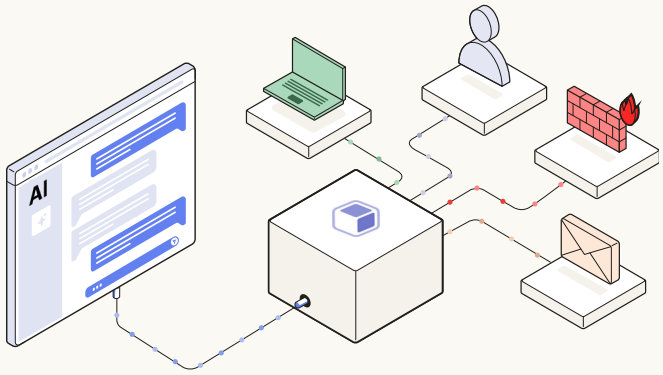
Bring Your AI. Give It Reach.

AI is transforming your security operations.
Ground it in the source of truth for security controls.



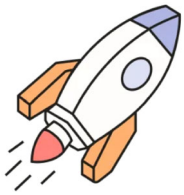
THE CHALLENGE

Frontier AI was not built to understand your security controls

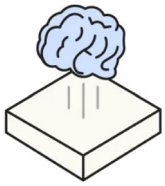
Security teams are rapidly adopting frontier AI to connect tools, analyze information, automate workflows, and accelerate security operations. But a general-purpose AI model does not inherently understand how firewall, identity, endpoint security, email security. SASE, and other security controls work together. It cannot reliably determine whether a configuration change increased exposure, which assets or identities are affected, whether another control compensates for the risk, what action should come next, or how to remediate it.

Those answers require deep context and intelligence across security tool vendors, controls, configurations, policies, identities, and evidence. Simply giving AI models access to security tools and saying "make them better" is not enough. Point an AI model at a security stack it doesn't fully understand and you'll get confident, wrong answers faster.

To safely put AI to work in security operations, ground it in a source of truth for how your security controls actually protect the business. That gives it the context to reason, recommend, act, and make decisions with confidence.

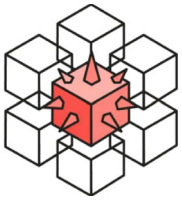


Security teams use frontier AI models to automate workflows, reduce operational burden, and keep pace with attackers.



But these models lack the data, intelligence, and discipline to reliably assess or strengthen security controls.

Without security controls expertise and context, AI models can produce confident, wrong answers and make poor decisions.



Sometimes, AI can hallucinate. Security operations can't afford to. One wrong decision can make you susceptible to attack.

THE SOLUTION

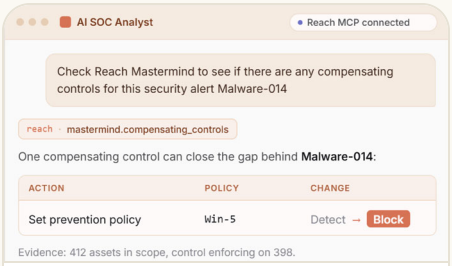
Ground AI security operations in a source of truth for security controls

Reach continuously understands how security controls are configured, how they work together, where they have drifted or become misconfigured, what those weaknesses expose, and how to fix them. At the center is Mastermind AI, Reach's security control reasoning engine. Powered by cybersecurity domain-specific reasoning and AI models, it connects control context, findings, drift alerts, assets, identities, reachability, evidence, and remediation across different security tools to create a source of truth for how controls protect the business. Security teams can quickly understand where defenses are weak, what is exposed, and what should happen next.

The Public API and MCP Server make that context available wherever teams want to use it. The Public API brings Reach findings, evidence, and outcomes into SIEM, ticketing, GRC, reporting, automation, and custom workflows. The MCP Server connects MCP-compatible AI tools directly to Reach. Frontier AI provides the orchestration, while Reach supplies the cybersecurity domain expertise, cross-vendor controls context, evidence, and remediation guidance the frontier model lacks. Reach-published MCP skills add structured security reasoning by defining what evidence to gather, how to evaluate it, and when human judgment is required. The MCP Server is intentionally read-only, so teams can retain control of when recommendations become actions.

And Reach always shows its work. Conclusions include the supporting evidence and level of confidence, so teams can make trusted decisions without forcing certainty where it does not exist.

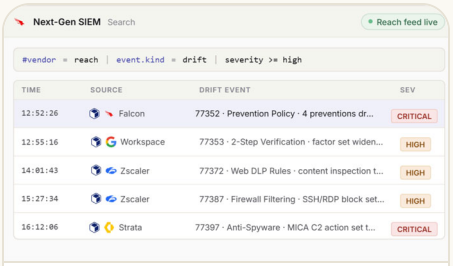
The result: AI security operations grounded in Reach security controls expertise, with the context to reason accurately, move faster, and make the right decisions.



01

Make your AI security-fluent.

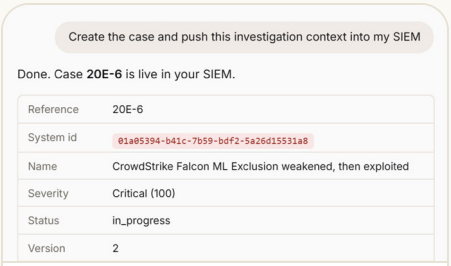
Embed Reach into your AI tools to give them the security-control expertise, context, evidence, reasoning, and remediation guidance they lack. Create a source of truth for how controls protect the business.



02

Control assurance across every workflow.

Bring Reach controls intelligence into the systems where security work happens. The Public API infuses Reach data into SIEM and SOC workflows. The MCP embeds Reach controls expertise into any AI tool used for security operations.



03

Turn days of manual work into minutes.

Eliminate manual evidence gathering, cross-tool findings correlation, and security controls change analysis. Achieve security operations at the speed of AI to close defensive gaps faster than attackers can exploit them.

AI can be confidently wrong. Make it right.

LEARN MORE AT

reach.security/connect