Stop Configuration Drift

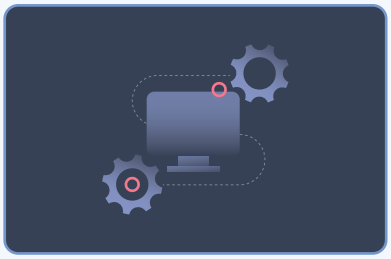
See Drift. Understand Impact. Automatically Remediate.

The challenge

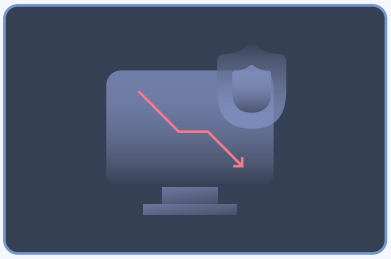
One Configuration Change Can Introduce Risk

Modern security programs rely on a suite of tools – firewall, endpoint security, identity and access, email security – owned and operated by cross-functional teams. While this shared responsibility model brings flexibility, it also introduces operational risk. Configurations change constantly. Perhaps an overly permissive rule was activated on your firewall. Maybe a group exclusion was enabled – or multi-factor authentication was disabled for your CEO – on your identity and access management (IAM) solution. Possibly a file extension, folder, or process exclusion was implemented on your endpoint detection and response (EDR) tool. These changes represent exposures in your environment, and are hard to track and easy to misalign. Unmonitored changes, including break-glass fixes, can quietly degrade security posture over time, increase risk, and force security teams into a reactive, rather thantproactive, stance.

Security teams struggle to keep up with:



Complex, rapidly evolving product configurations



Untracked changes that degrade posture

One-time, break-glass changes that are left behind

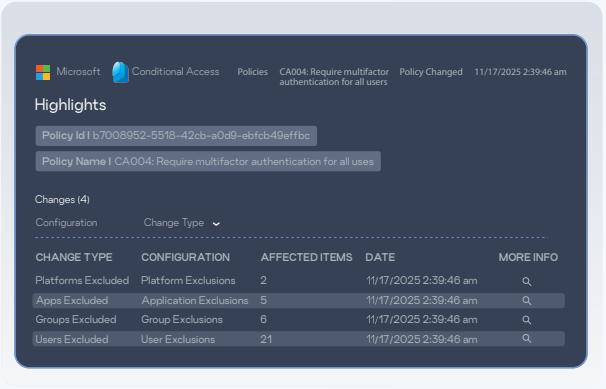
Manual review processes that are slow and incomplete

Customer conversations that reveal out-of-sync platform data

Reach Prevents Drift from Becoming Risk

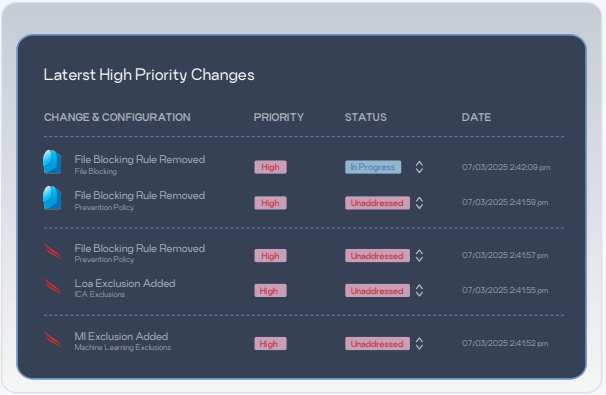
See Drift

Reach AI agents continuously monitor for configuration drift across your integrated security tools – IAM, EDR, firewalls, SASE, email security, and more. Reach detects configuration drift the moment it happens, helping you track changes in real time, stay aligned to policy, prevent regressions, and fix issues before they become exposure. Reach AI agents focus on meaningful drift by highlighting only the configuration changes that impact security posture. This allows you to catch what matters without flooding your team with alert noise and false positives.



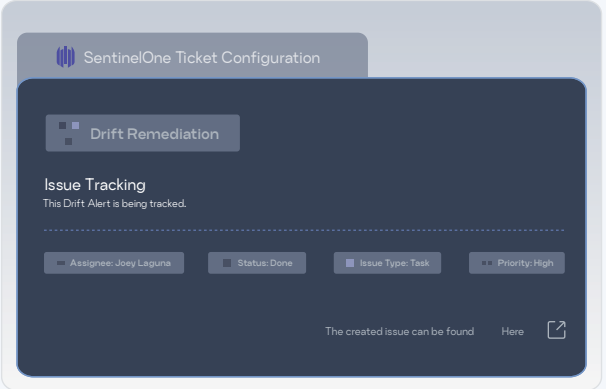
Understand Impact

Reach gives you real-time visibility into impactful changes, with drift alerts tied to clear risk indicators. Visualize drift in a dedicated dashboard that highlights changes affecting posture, flags issues by status, and maintains a full audit trail for compliance. It's a single source of truth to keep teams and data aligned. Disparate teams can review, assign, and resolve issues directly from the platform before exposure spreads.



Automatically Remediate

Reach doesn't just flag drift – it fixes it for you. Reach AI agents generate context-aware fixes and step-by-step guides. Baseline or custom rules can be created and deployed in seconds. Reach can push changes directly–via ServiceNow, Jira, or automation into staging for review before production. 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 our AI agent Reacher™ for help to summarize results, answer questions, deploy fixes, and execute remediation tasks across your ecosystem. Stay ahead of change and ensure posture isn't just assessed – it's maintained.



How it works:

Demo Video

Product Tour

reach.security/connect