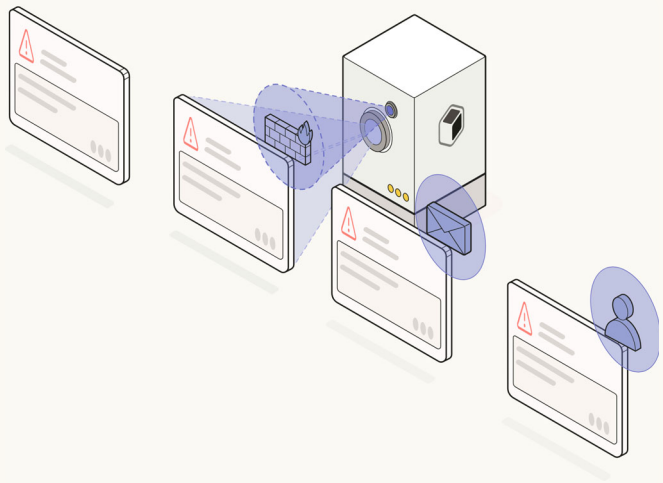
Security Controls Context for a More Resilient SOC

Embed Reach in your SOC to investigate faster, fix the root cause of security events, and reduce future alert volume.



THE CHALLENGE

SOC alerts tell you what happened, not why your defenses failed.

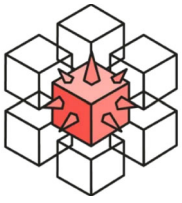
SOC teams are built to move fast, but the alerts they rely on rarely explain whether the security controls that should have stopped an event were actually enforcing. An analyst may know that malware executed, a risky login occurred, or suspicious traffic was allowed, yet still not know whether the right policy was applied, an exception or override weakened it, or a recent configuration change created the gap.

Getting those answers often means leaving the investigation, jumping between consoles, reconstructing policy coverage and change history, or chasing the team that owns the control.

SIEMs capture massive volumes of log data, but correlating an event to the relevant control state and configuration changes is difficult, costly, and slow. Under pressure, the SOC contains the incident and moves on, while the faulty control can remain in place, leaving other assets exposed and creating repeat incidents and alerts.

Alerts show the details of the event, but rarely show whether the security controls that should have stopped it were actually enforcing.

Analysts chase policy coverage, exceptions, configuration changes, and control owners across tools to understand what went wrong.



Once the incident is contained, the faulty security control can remain unfixed in the environment, creating repeat incidents and alerts.

SIEMs capture immense amounts of log data, which makes correlating events to configuration changes costly and time prohibitive.

THE SOLUTION

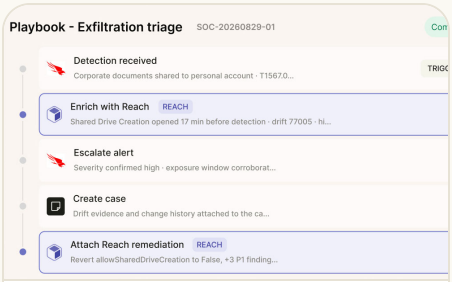
Enrich every SOC alert with security controls context

Reach gives SOC teams the security-control evidence traditional detection and response tools lack. For every alert, Reach connects the event to the controls that were supposed to protect the affected asset, identity, or workload, showing whether protection was actually enforcing, whether the relevant policy applied, and whether exceptions or overrides weakened it.

Reach also surfaces the configuration and drift history behind the incident, including what changed, when it changed, who changed it, and the before-and-after state. Analysts can then understand why it was allowed to happen and exactly how to fix the underlying control weakness.

That evidence improves the entire investigation. Analysts can triage faster, prioritize alerts based on actual exposure, remediate the specific control failure, and quickly identify other assets affected by the same condition.

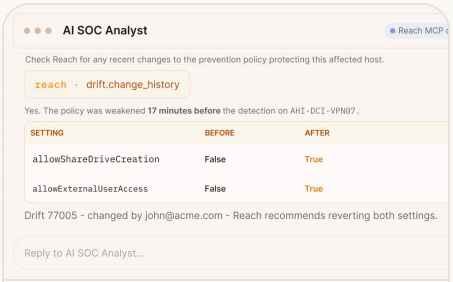
Reach brings this context directly into the SIEM and AI workflows analysts already use through APIs for repeatable workflows and MCP for dynamic investigation. The result is faster answers, more precise remediation, fewer repeat incidents and alerts, and a SOC that gets stronger with every investigation.



01

Triage Security Events Faster. Prioritize Better.

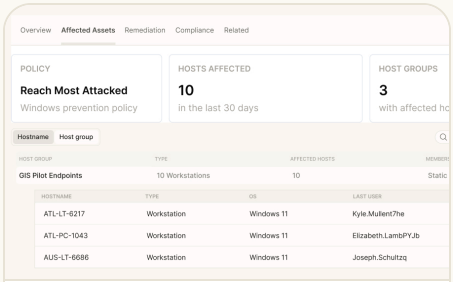
See control state, policy coverage, and configuration change history to make faster and more informed triage decisions. Prioritize alerts based on actual exposure and the effectiveness of the security controls protecting each asset.



02

Fix the Root Cause. Reduce Alert Volume.

Connect the alert to the control failure behind it and fix it fast. Reach adds specific remediation guidance so teams can fix the weakness, reduce handoffs, prevent repeat incidents, and ultimately, lower recurring alert volume.



03

Build a More Resilient SOC

Break the reactive cycle by fixing the control weaknesses behind incidents. Prevent repeat events, reduce alert volume, strengthen defenses, and give analysts more time to focus on the threats that matter.

Faster Answers. Stronger Controls. Fewer Repeat Alerts.

LEARN MORE AT

reach.security/connect