Reach

Reach + TAG

EXECUTIVE BRIEF

ROI Analysis for Security Posture Assessment and Remediation from Reach Security

Prepared by TAG Infosphere,
in partnership with Reach Security

Introduction

This executive summary highlights key findings from a third-party ROI analysis conducted by TAG Infosphere on the Reach Security platform. The full report presents both qualitative and quantitative justification for investing in Reach, including two detailed case studies. The conclusion: Reach Security delivers operational value and measurable ROI, helping security leaders proactively address misconfigurations, improve resilience, and reduce exposure across their environments.

> "This is the classic 'ounce of prevention' ROI scenario."
>
> Dr. Edward Amoroso
> Founder & CEO
>
> TAG

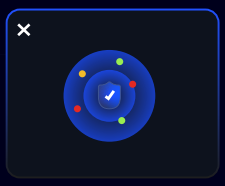
Why It Matters: Security Teams Are Stuck in Reactive Mode

Despite increased effort and investment, most security teams are still grappling with exposures that persist due to misconfigurations, weak controls, or poorly aligned tools. TAG's analysis confirms that Reach Security shifts teams toward proactive remediation improving risk reduction without increasing staff burden.

Platform Overview: Reach Security in Practice

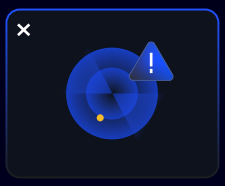
Reach Security integrates with identity, endpoint, email, and network security tools to identify and fix misconfigurations, uncover hidden exposures, and strengthen resilience. The platform connects to ticketing and messaging systems to operationalize fixes and updates, making security improvements actionable, not just observable.

Reach Supports Three Core Functions:



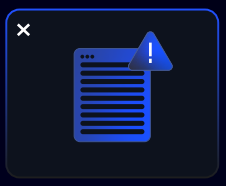
Threat Exposure Management:

Identifies real, reachable exposures (e.g., ransomware risk from end-user devices).



Security Posture Management:

Finds weak controls that open the door to APTs, session hijacking, and lateral movement.



Configuration Management:

Detects misconfigurations across the enterprise stack and drives policy alignment.

Reach Helps Customers

- Identify security blind spots from misconfigured and underused security and IT tools
- Prioritize action based on real-world risk and control capabilities
- Guide remediation to rapidly deploy changes and improve security posture
- Continuously validate to detect configuration drift, keep defenses aligned to policy, and maintain a strong security posture

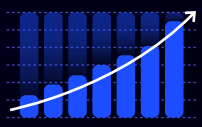
Reach + TAG

Reach empowers teams to take action, not just generate reports

Case Study #1: Budget-Based ROI for a Large Bank

In one analysis, TAG evaluated a representative bank (assets $250B–$500B). Prior to Reach, the bank relied heavily on consultants and maintained significant reserves for incident response. Following deployment:

- Consulting costs were reduced through less reliance on contractors.
- Incident response budgets were decreased due to lowered risk exposure.
- Result: 100% ROI, based on real cost reductions.



Summary

- Reduced contractor spend
- Reduced incident response reserves
- ROI: 100%

Case Study #2: Productivity-Based ROI for a 50-Person Team

Another enterprise assessed Reach's impact on operational efficiency across nine core security tasks. The greatest time savings occurred in:

- Security Controls Review
- Posture Assessment
- Incident Investigation

These reductions freed up over 160 hours per week for high-value work, translating into measurable business value and an ROI of 156% based on hours saved.

Key Time-Saving Areas:

- Security Control Reviews
- Posture Assessment
- Incident Investigation

Additional Qualitative Benefits

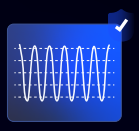
Beyond budget and time savings, Reach delivers security and operational improvements:

Strengthened Security Posture:

Continuous detection of drift and misconfigurations.

Improved Consistency:

Guardrails that standardize and enforce configuration policies.



Reduced Analyst Fatigue:

Visible, validated configurations build analyst confidence.

TAG's independent analysis confirms that Reach Security delivers compelling ROI and improves security resilience by design. For security leaders seeking to operationalize risk reduction and justify budget allocation, this report provides both the evidence and the insight.

Download the Full TAG ROI Report on Reach Security

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

Get Started!

reach.security/try-reach

Join the growing community using Reach to reduce risk, maximize the value of their existing tools, and strengthen security without added complexity.

reach.security