TAG

RETURN ON INVESTMENT (ROI) ANALYSIS:

SECURITY POSTURE ASSESSMENT AND REMEDIATION FROM REACH SECURITY



DR. EDWARD AMOROSO, FOUNDER & CEO, TAG
THE TAG ANALYSTS

Reach

RETURN ON INVESTMENT (ROI) ANALYSIS:

SECURITY POSTURE ASSESSMENT AND REMEDIATION FROM REACH SECURITY

DR. EDWARD AMOROSO
THE TAG ANALYSTS

This TAG[1] report provides a Return on Investment (ROI) analysis of the Reach Security platform. The assessment shows that organizations should expect qualitative benefits from the use of Reach Security[2], as well as quantitative ROI in the range of 100% to 156% under reasonable assumptions. The scenarios covered include the practical use of Reach Security to support security posture assessment and remediation to fix misconfigurations. Two ROI case studies are included that approach the analysis from different perspectives – one from a CISO budget savings perspective and the second from an hours/productivity savings perspective.

INTRODUCTION

This TAG report presents a Return on Investment (ROI) analysis of the Reach Security platform to support the need for Chief Information Security Officers (CISOs) to financially justify their desired investment. As will be shown, Reach Security supports the need to uncover vulnerabilities and exposures to prevent them from becoming much more troublesome and expensive issues later on. This is the classic "ounce of prevention" ROI scenario.

[1] TAG Infosphere is a New York City-based research and advisory firm founded by former AT&T senior executives, including Dr. Edward Amoroso, former AT&T Senior Vice President and Chief Information Security Officer (CISO). Since 2016, TAG has focused on the provision of expert insight and tailored guidance for practitioners in hundreds of enterprise teams, government agencies, and commercial vendors located around the world. TAG offers customer 24/7 access to a modern AI-powered SaaS platform that supports the need for on-demand detailed research and insights in the areas of cybersecurity and artificial intelligence. TAG has been developing ROIs since 2018.

[2] The information in this ROI report comes from technical, business, and product marketing materials shared by the Reach Security team with the TAG analysts, as well as many discussions, briefings, and working sessions including demonstrations of the platform, overviews of live customer case-studies, and reviews of applicable financial and operational metrics.

The analysis here covers both qualitative and quantitative ROI, and shows that in addition to substantive operational advantages, teams using Reach Security under typical circumstances should expect quantitative ROI in the range of 100% to 156%. These figures were calculated using budget estimates based on interactions with hundreds of representative enterprise teams supporting network management and network security objectives.[3]

We present two case study scenarios that approach the ROI analysis from two different perspectives. The first analyzes a typical CISO budget before and after use of the Reach Security platform to demonstrate real financial savings in actual dollar terms. The second, however, reviews how productivity gains are achieved through use of the platform, resulting in the CISO having options in terms of redeployment of staff or reallocation of resources.

OVERVIEW OF THE REACH SECURITY PLATFORM

The Reach Security platform is designed to integrate with identities, endpoint security, email security, and network security tools to help identify and remediate cyber risks in an enterprise. The motivation is that despite CISO-led security teams spending more time and effort trying to reduce risk, the reality is that progress has been slow across the board. Reach Security was created to uncover exposures and help make fixes more practical and easier to deploy.

The way this works is that the platform plugs into existing security infrastructure, as referenced above, and then via integration with ticketing and messaging systems, Reach Security becomes a partner in developing and deploying fixes to configurations, updates to tools, and closure of security gaps. As one might expect, this results in identification and elimination of hidden risks that might be exploited by an adversary or malware. Specific areas of support include:

- **Threat Exposure Management** – This involves finding exposures on assets such as end-user devices, which can then be fixed to avoid subsequent problems such as ransomware attacks. Obviously, this reduces response costs.
- **Security Posture Management** – This involves identification of weak security controls that might allow for attacks such as session hijacking or advanced persistent threats (APTs) leveraging methods such as lateral traversal.
- **Configuration Management** – This involves determining if misconfigurations have been made, which can create exploitable vulnerabilities across the entire enterprise technology stack.

These security posture and remediation benefits to the enterprise are especially valuable because they are designed to be actionable. That is, rather than reporting just for reporting purposes (e.g., dashboards, compliance summaries), the goal of Reach Security platform operation is to create an environment in which managers and practitioners can take steps that will actually result in modifications, updates, and fixes.

Ultimately, the Reach Security solution supports resilience by helping teams to not just fix misconfigurations, but to strengthen their overall resilience against attacks. The platform also drives exposure awareness by making it easier to see and prioritize real exposure across people and tools. Reach shifts teams from point-in-time checks to continuous validation, allowing staff to focus on what matters most. The company goes beyond technical configurations to map exposure to specific users and groups, helping teams understand not just what is misconfigured, but who is most at risk. This user-centric visibility enables more targeted protection and smarter allocation of security resources.

[3] Because TAG has direct access to a large community of Chief Information Security Officers (CISOs) and their enterprise and government teams, we can create highly representative budgets that include fees that we see repeatedly in practice.

QUALITATIVE ROI

To provide a more structured analysis of the benefits of deploying Reach Security to support the various functions mentioned above, we list below a set of qualitative benefits that accrue for enterprise teams in practice. These qualitative advantages provide a foundational basis for the subsequent ROI analysis case studies below that explain the impact of Reach Security on typical CISO-managed budgets as well as productivity.[4] Some qualitative benefits are as follows:

Qualitative Benefit: Strengthened Security Posture Through Proactive Misconfiguration Resolution. Reach Security enables teams to detect and resolve misconfigurations across security tooling and processes before they manifest as incidents. By continuously identifying drift, policy gaps, or unintended changes across detection rules and response workflows, the platform allows security teams to proactively harden their environment. Reach also prioritizes remediation efforts based on the relative exposure risk of each issue, helping teams focus on the changes that will deliver the greatest reduction in risk.

Qualitative Benefit: Improved Consistency and Accuracy in Security Operations. Most misconfigurations result from inconsistent practices, manual errors, or lack of coordination across tools. Reach Security provides remediation workflows and guardrails that ensure security controls behave as intended. By standardizing how configurations are validated, the platform helps eliminate ambiguity in response and enforces best practices.

Qualitative Benefit: Empowered Analysts and Reduced Cognitive Overhead. Analysts can waste time second-guessing whether a detection rule is tuned correctly or whether an automated response will behave as expected. Reach Security addresses this by making misconfigurations visible, enabling analysts to take confident actions. This reduces mental fatigue, shortens the decision loop, and builds team confidence in their tools.

QUANTITATIVE ROI ASSESSMENT

Now that we have presented some of the qualitative advantages that enterprise teams should expect from deployment and use of Reach Security for security posture assessment and remediation, we can begin to analyze and discuss the more quantitative advantages that will come from use of the platform. Based on our collective experience at TAG managing security budgets, we can identify the following areas where budgets are directly affected by platforms:

1. **Staff Costs** – This involves the reduction of human-related costs, which in this case would be associated with the types of manual tasks that are being replaced or augmented with posture assessment and remediation. Usually, these cost reductions involve reducing the number of consultants rather than employees. Employees are mostly redeployed to other activities, whereas consultant reduction is often used to lower budgets.

2. **Platform Costs** – This involves license, renewal, and purchase costs for platforms, systems, and tools which can be removed or reduced after deployment of posture assessment and remediation support from Reach Security. Obviously, this would include rudimentary tools trying to do configuration-related tasks, but it can also include reductions in comparable enterprise security tools.

3. **Service Costs** – This involves reduction or elimination of service costs that address tasks which are less needed once posture assessment and remediation have been implemented from Reach Security. Incident response services, for example, would be less needed if network-related breaches are substantially reduced, which implies that budget line items in this area can be reduced.

[4] Our general assumption throughout this report is that the Chief Information Security Officer (CISO) is most likely to support the budget for Reach Security, but we acknowledge that in many organizations, this responsibility could reside within an outsourced service (e.g., MSSP).

The analysis in the next section provides a highly representative case study of the budget impact one might expect in using Reach Security. The budget is derived from the many dozens of CISO-led teams we advise, coach, and assist with their financial planning for cybersecurity. It is also informed by our decades of experience as CISOs and work with current vendors, where we absorb accurate information about typical annual license costs.

The strategy, as we will show below, involves first showing the typical annual budget numbers associated with the CISO team before they implement controls from Reach Security. Then we explain the positive impact of deploying Reach Security into their enterprise and we show where the most likely reductions should be expected to come. Again, this assessment is based on our decades of practical experience managing these functions and budget line items.

CASE STUDY 1: DEPLOYING REACH SECURITY TO A LARGE BANK

Our first case study involves a representative large bank (assets in the USD $250-500B range) that is dealing with the usual types of misconfigurations in their IT, network, services, and security infrastructure – including in the cloud, that result in higher operating costs, increased need for consulting staff, and heightened budget requirements to deal with backend incident response costs being set aside by the CISO in expectation of significant and costly incidents.

The budget assumptions listed below are representative of this bank, given the circumstances just mentioned. These costs are presented as a basis for analyzing how the various line items will either remain or change, based on the deployment and use of Reach Security. Presumably, the budget implications will be positive, but let's discuss the various costs in place before Reach Security is deployed. Readers can easily adjust numbers as they see fit.

The specifics of the ROI that buyers should expect from use of Reach are driven by the following observations: First, the presumption is that considerable manual effort is being expended toward the identification of exposures and vulnerabilities. In the majority of cases that we've examined in our research and enterprise support at TAG, this is done using consultants, contractors, and augmented labor – which everyone knows can be quite expensive.

In addition, we assume that the CISO, like most enterprise CISOs, is forced to set aside a budget line item to deal with the presumed inevitable serious incident that requires identification, response, reporting, mitigation, and so on. This is done usually by engaging with a platform service vendor such as Mandiant, where an annual fee is paid with add-on consulting if a particularly troubling incident emerges (as one usually does) requiring special attention.

The basis for our quantified ROI analysis for Reach is thus quite simple: We make the case that by deploying and using their platform, the preventive benefit will reduce the need for external contracted labor as well as the amount spent on incident response – simply because Reach reduces the likelihood of such events occurring in the first place. This is a simple equation, but we believe it to be valid.

To explain and illustrate this ROI concept, we list below a portion of a typical enterprise security budget, listing those aspects of the annual budget that we deem to be relevant to the quantitative benefit. As part of the analysis, we need not make broad assumptions about the total security budget, because it does not fundamentally change the ROI. Figure 1 following thus shows a simple portion of budget before the enterprise team has deployed Reach Security.

Vulnerability Management	**0.8M**	Amount is lowered by 100K with deployment of Reach
Contractors	0.4M	Augmented contractors helping with VM and exposure mgmt.
Consultants	0.4M	Augmented consultants helping with VM and exposure mgmt..
Incident Response	**1.5M**	This amount is usually based n empirical numbers from previous years.
Response Annual Service	0.5M	This is a baseline fee paid each year to a vendor for response platform support.
Major Incident Support	1.0M	This is an additional fee paid each year to deal with the challenges of a major incident.
Total for Applicable VM and IR	**2.0M**	This is the applicable portion of the larger security budget influenced by Reach.

Figure 1. Portion of Budget Before Deployment of Reach Security

Readers will note that we have assumed that for this large bank, four consultants and contractors have been hired to augment the employees and staff of the bank in the process of identifying exposures and vulnerabilities. We also assumed that $1.5M was set aside for incident response each year, and this is split between $500K in annual service fees and $1M to address the specifics of the expected major incident.

We now presume that deploying Reach Security involves a license fee of $300K for one full year of support. As will be shown in our estimates below, we believe that it is fully reasonable to assume that two contractors (at a typical average total annual cost of $200K per consultant per year) can be reduced and that the likelihood of an incident is reduced by a conservative 20% - resulting in a reduction in the presumed expected incident fee (see Figure 2).

Vulnerability Management	**7.0M**	**Amount is lowered by 100K with deployment of Reach**
Reach Platform License	0.3M	This is a representative fee (but by no means an actual). License fees will vary.
Contractors	0.2M	This reflects redeployment or reduction of one contractor.
Consultants	0.2M	This reflects redeployment or reduction of one consultant.
Incident Response	**1.3M**	**Amount is lowered by 200K due to deployment of Reach**
Response Annual Service	0.5M	This fee will likely remain the same.
Major Incident Support	0.8M	The likelihood of major event reduces by 20% which can be used to handle budget reductions.
Total for Applicable VM and IR	**2.0M**	**This represents a 300% ROI for deployment of Reach**

Figure 2. Portion of Budget After Deployment of Reach Security

If you do the math, as we have shown in the spreadsheet above, the measure of ROI for this scenario can be viewed as follows: The budget increase by $300K for the Reach license, but decreases by $400K for two reduced contractors, and $200K for the reduced likelihood of a major incident required expensive response. This implies spending $300K to save $600K which implies an impressive expected **100% ROI.**

CISOs will recognize that a reasonable interpretation here might also be non-quantitative. For example, the reduction in contractors and consultants might manifest in these augmented staff being redeployed to other high value activities. In fact, if employees and staff are doing the exposure detection work, then we are confident that this scenario emerges – namely, that these experts are shifted to other high value work.

Similarly, every CISO knows that budget targets change every year, either based on business results, measured actuals, or some other factor including increased (or decreased) threat concerns. We usually expect that CISOs would leverage the ROI from platforms such as Reach to absorb these reductions when they inevitably occur. This is a perfectly valid approach to dealing with ROI from a vendor deployment: Budget improvements occur, but usually dynamically.

CASE STUDY 2: MEASURING HOURS SAVED BY USING REACH

Our second case study involves approaching the ROI from an entirely different perspective, one that is more focused on hours saved due to productivity gains. We fully understand that readers might protest that productivity gains actually save budget dollars – and we agree that time saved rarely results in staff salaries being reduced. Any subject matter experts with the ability to deal with misconfigurations will generally be too valuable to even consider removing.

But there are real savings here, nevertheless. Additional staff hires for high-value activities can be avoided by redeploying resources whose time is saved through use of the Reach Security platform. Similarly, it has been our experience that consultants hired temporarily to assist in tasks such as manually reviewing infrastructure for configuration (e.g., penetration testing) can be reduced, thus resulting in real budget reduction.

The case study presented below considers the usual factors in determining productivity and shows how, by doing the math, real time and productivity gains are achieved. The numbers used here are derived from real numbers obtained from a Reach Security customer who shared their calculations to help illustrate their own decision to procure and deploy the platform. As with most such case studies, we maintain confidentiality of that customer's identity.

Let's start by looking at the categories of work activity that we will consider in-scope to the analysis. Below are the tasks that we would agree to be relevant to productivity enhancement based on the deployment and use of the Reach Security platform. Note that we have grouped the tasks into three "Prevent" activities, three "Detect" activities, and three "Respond" activities, which roughly tracks most defensive framework models:

1. **Security Controls Review (Prevent)** – This is the time spent by security team members to determine if operations, rules, settings, and configurations are correct.
2. **Security Tools Rationalization (Prevent)** – This is the time spent to determine if an optimal mix of commercial tools has been deployed.
3. **Compliance Readiness (Prevent)** – This is the time spent gathering information in support of compliance or regulatory requirements.
4. **Security Platform Tuning (Detect)** – This involves time by security team members adjusting and tuning configurations.
5. **Security Posture Assessment (Detect)** – This is the broad set of activities required to determine the overall cyber risk and protection profile.
6. **Security Alert Processing (Detect)** – This involves time spent dealing with the alerts generated on a real-time basis from security systems.
7. **Incident Investigation (Respond)** – This involves time spent chasing down and investigating incidents or indicators.
8. **Incident Response (Respond)** – This is the actual response work required to deal with an on-going or completed event.
9. **Incident Reporting (Respond)** – This is all the work required to report on the specifics of an incident to any required authorities.

If we assume that an organization properly balances its time spent between Prevent, Detect, and Respond focus, and that for a security team of fifty staff, roughly 50% of their time is spent on these activities – with the balance for training, meetings, and other day-to-day work functions, then the total weekly hours spent on the above nine tasks would be 1000 hours (which is 50 staff times 40 hours divided by 2).

Our contention, and this appears to be supported by evidence shared by Reach Security customers[3], is that each of these tasks will be reduced by some meaningful percentage. The Security Controls Review (Prevent), Security Posture Assessment (Detect), and Incident Investigation (Respond) activities, in particular, can be reduced by as much as two-thirds. If we assume that other tasks are unchanged, then this would result in the following savings:

- **Total Hours** – 1000 hours is spent on the nine tasks
- **Applicable Tasks Affected by Reach** – Three tasks at 333 hours
- **Reduction Percentage** – 50%
- **Savings** – 166.5 Hours per week
- **Loaded Salary** - $175K per year or $3.36K per week or $84 per hour
- **Total Savings** – $13,986 per week or $769,230 per year

If we assume that the Reach Platform license is $300K, then this suggests a 156% ROI just for the hours saved that would have been spent manually on the various tasks.

Additional Information

Readers who are TAG Research as a Service (RaaS) customers can reach out to a TAG analyst for assistance through their RaaS portal account. They, and any other readers, can and should also reach out to Reach Security to obtain additional details on the platform and to engage in a demonstration of how the platform supports modern network exposure management for a wide range of different organizations across all sectors.

---

[3] A detailed breakdown of the hours saved by a Reach Security customer was provided to the TAG analysts for review. We went through each line item and generalized the savings into broader categories and actually made more conservative estimates of reduction than were included in the customer estimates.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.

Copyright © 2025 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere's written permission. The material in this report is comprised of the opinions of the TAG Infosphere analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy, or completeness of this report are disclaimed herein.