TAG

RETURN ON INVESTMENT (ROI) ANALYSIS:

ENTERPRISE RETURN ON INVESTMENT (ROI) ESTIMATE FOR THE TAMNOON ASSISTED REMEDIATION PLATFORM

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

tamnoon

ENTERPRISE RETURN ON INVESTMENT (ROI) ESTIMATE FOR THE TAMNOON ASSISTED REMEDIATION PLATFORM

DR. EDWARD AMOROSO
THE TAG ANALYSTS

EXECUTIVE SUMMARY

An independent return on investment (ROI) analysis was performed by the TAG Infosphere[1] analysts on the Tamnoon service and platform[2] from both a quantitative and qualitative perspective. A positive quantitative ROI of 300% was determined to emerge through case study analysis for a representative enterprise using the Tamnoon solution under typical conditions.

INTRODUCTION

This return on investment (ROI) analysis covers the Tamnoon cloud remediation service designed to assist enterprise security teams with proactive cloud security management. The goal is to summarize the qualitative and quantitative benefits of cloud security alert monitoring, automated triage, proactive remediation, and prevention of misconfigurations offered by Tamnoon.

The analysis results, as shown in the narrative below, suggest a positive quantitative ROI for Tamnoon users of 300% under a reasonable set of enterprise assumptions. The analysis also highlights multiple areas of clear qualitative benefit from the use of the service. Both types of returns are described below and shown to be valuable justifications for any enterprise team considering the deployment and use of Tamnoon to address cloud risk.

BRIEF OVERVIEW OF THE TAMNOON SOLUTION

Tamnoon is a new commercial cybersecurity tech-enabled managed service that provides proactive remediation of cloud misconfigurations intending to fortify cloud security posture. The company was founded in 2022 and is supported by investments from Merlin Ventures, Secret Chord, and Today Ventures. Important functional capabilities in the Tamnoon solution include the following:

- **Detection, Monitoring, Optimization, and Ongoing Assessment** – Cloud security monitoring via expert-curated alert monitoring and cloud network application protection platform (CNAPP) fine-tuning
- **Triage & Prioritization**– Automated triage support tailored to the needs of an enterprise based on business context and the capacity of the security team
- **Configuration Remediation** – Prevention of risks and systematic misconfigurations in cloud security while ensuring safe remediation with no disruption to operations
- **Prevention** – Proactive prevention with high accuracy driven by a combination of artificial intelligence and human expertise while leveraging cloud-native controls

The Tamnoon platform supports the cloud security remediation needs of a business customer's security team through human expertise and AI-driven automation targeting security tasks such as those listed above. These supported tasks are conducted through tool optimization, monitoring, assisted remediation and impact analysis curated and supported by the Tamnoon expert team. The remediation process is tailored to customer environments' security policies and business context. It is also based on each remediation impact analysis to optimize success and eliminate potential disruptions.

Tamnoon integrates with major cybersecurity and cloud service providers such as Check Point, Wiz, Orca, Sysdig, Palo Alto Networks, Crowdstrike, Amazon Web Services, Microsoft Azure, and Google Cloud Platform. These partnerships enable a more secure ecosystem for customer cloud environments. They also help maximize the leverage of automated support and human expertise from each partner organization for customer engagement.

QUALITATIVE ROI

Many qualitative benefits became evident during our detailed review and analysis of Tamnoon, including advantages for both the security and DevOps teams. The assumption is that both teams share responsibility for designing, deploying, operating, and securing cloud applications and workloads to public cloud services from companies such as Amazon, Google, and Microsoft. The most prominent qualitative benefits of Tamnoon are as follows:

Staff Redeployment

The use of the Tamnoon service allows for the redeployment of expert in-house staff working day-to-day cloud security tasks to be redeployed to higher value functions. Such off-loading of support activity to Tamnoon will drive higher work satisfaction and team productivity.

Additional Expertise

The introduction of Tamnoon to the security ecosystem will augment, complement, and often expand the security knowledge and expertise of the local team. Tamnoon becomes a new partner in the security and DevOps ecosystems, increasing the enterprise's ability to deal with risk.

Impact Analysis

The Tamnoon platform supports the goal of performing cloud security impact analysis before changes are deployed to help avoid production impacts and reduce the need for rollbacks and recovery after incidents (see quantitative analysis below for more on this benefit).

Remediation Process

Tamnoon introduces a more structured process to cloud security remediation with support for essential functions such as root cause analysis, alert triages, prioritization of alert handling, and overall security support planning.

KPI Measurement

The use of Tamnoon supports measuring service level agreements (SLAs) and key performance indicators (KPIs) for cloud security remediation. This is supported by dashboard views and metrics that can help to drive improvement initiatives.

Alert Volume Reduction

The Tamnoon platform offers valuable assistance to security teams to reduce the volume of CSPM/CNAPP alerts to support more focused team activity. Reduction of alert handling can dramatically improve the quality of work in a security operational setting.

Audit Efficiency

Using Tamnoon will streamline and improve the compliance and audit process by offering more accurate reporting and tracking of cloud-related security issues. This should save time for security staff by reducing the audit support burden.

Platform Investments

The Tamnoon service also helps to ensure fuller utilization of existing security platform investments in the cloud. Many teams might not be using their existing security platforms to full capability, and Tamnoon creates improved means for correlation and use.

PRODUCTIVITY ROI

The Tamnoon platform helps to address gaps in an existing budget and headcount allocation by driving improved productivity. The goal is to help teams get hours back, thus creating local productivity enhancements for the security team.

This is a sufficiently important return that is worth highlighting below with recognition that the return on investment (ROI) is measurable and could result in a net reduction in a security team's financial outlay through staff or service reductions if deemed appropriate. In most cases, however, the hours saved justify reallocating or deploying team members to complementary or newer security tasks.

The productivity ROI presumes the following estimates: Cloud security tasks are supported by internal security operational staff members with hourly rates on the order of USD$100. (This follows the familiar task of dividing a roughly USD$200K salary by approximately 2000 working hours in a year.) Such an estimate implies that every hundred hours of security work avoided by such staff allows for cost reallocation of USD$10K.

Suppose, for example, that Tamnoon is deployed to a medium-sized business with five security operational staff members. We can assume that the typical daily tasks of cloud security monitoring, triage support and planning based on prioritization, and planning any necessary mitigation or remediation account for 25% of one team member's work. Let's assume that the decision is to redirect that team member away from these tasks in lieu of Tamnoon.

In this case, the team would free up $50K of work (25% of one team member's salary) that could be allocated toward cost avoidance on another project. For example, a consultant or external service might have normally charged that fee – but by freeing up the staff, the team could allocate an internal team member to this work. Readers can do similar calculations, but cost avoidance is a useful ROI component.

QUANTITATIVE ROI

To demonstrate the more quantitative ROI, we will create a representative mid-sized organization called ACME Manufacturing, which we assume includes an internally managed security operations capability.[3] Like most modern teams, we will assume that the ACME security team struggles with many of the issues referenced above in the qualitative assessment. That is, they have trouble with massive volumes of alerts with poor context and little means for prioritizing handling. Teams also struggle with impact analysis and remediation that might not impact production.

BASELINE ESTIMATES FOR ACME

We assume that the ACME team does not use the Tamnoon service and that they experience the usual assortment of misconfigurations, vulnerabilities, and other breach-related issues. Furthermore, we assume they experience several small incidents during the year handled through normal day-to-day processes. Still, at least one major incident will occur that leverages an attack vector using a cloud misconfiguration that was reported but not remediated.

This major incident requires budget expenditure for reporting, response, legal, and related costs. Furthermore, we assume that the probability of one major incident per year is 100%. This decision is balanced by the decision to only include one incident in the calculation (it could certainly be several), along with the observation that without any automated cloud security monitoring, prioritization of alert handling, or support for remediation, the chances of an incident for any non-trivial deployment seem certain.

Readers can insert a probabilistic reduction in the calculations below if they tune down the numbers. Still, as suggested above, this should also be balanced by tuning in a probabilistic estimate of the number of incidents involved, which could be anything from zero to several. We've found that setting the probability of an incident to 100% and the number of potential incidents to one offers a balanced and highly typical view.

The broad annual financials associated with ACME are thus relatively easy to estimate in a typical enterprise security context based on the many years (decades) of experience the TAG Infosphere analyst team has with hundreds of enterprise customers operating their security function in this mode, as well as the personal experiences of the TAG Infosphere analysts managing security teams in the CISO role in this manner. Estimates are as follows:

- **No Tamnoon License** – We can assume that by not using Tamnoon, ACME is saving on the service license fee, assumed here to be $100K. This assumes a greenfield in the ROI – namely, that ACME is not using a comparable solution.
- **One Major Cloud Incident** – We reasonably assume that ACME experiences one consequential and reportable incident during the calendar year that requires expenses in response, legal, reporting, and other areas.
- **Estimated Expenses** – The expenses ACME should expect for its incident include legal fees ($200K estimated), response service fees ($200K estimated), reporting service fees ($100K estimated), and consultants ($200K estimated). This results in $700K in fees.[4]

The waterfall budget representation for ACME based on the financial assumptions listed above is shown in Figure 1 below.

BASELINE ESTIMATES FOR CONSOLIDATED

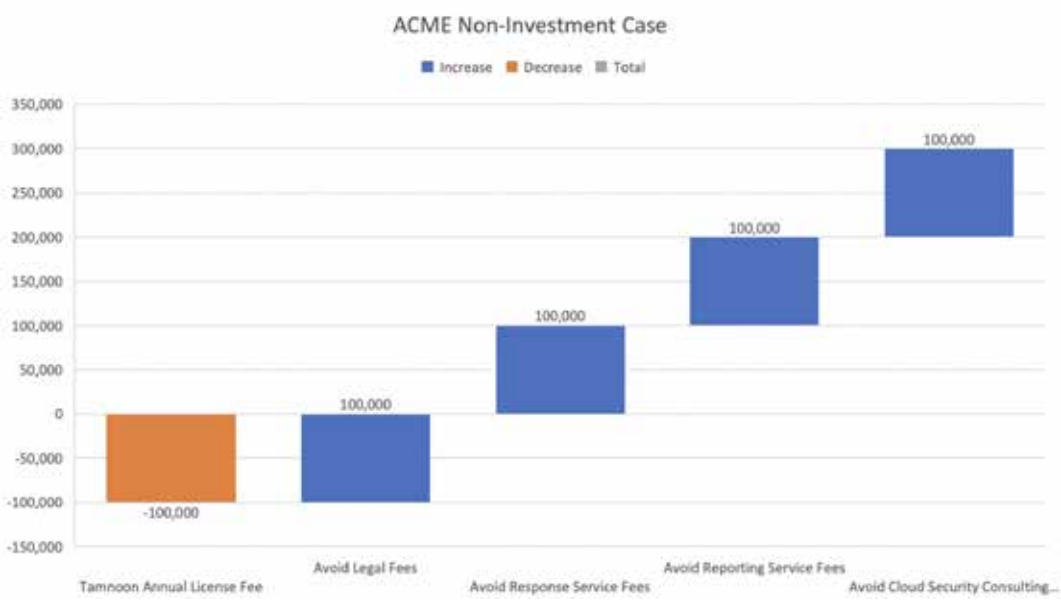

Figure 1. Waterfall Budget Representation for ACME (Not Using Tamnoon)

To highlight the implications of using Tamnoon, we now create a representative organization called Consolidated Industries that does use the Tamnoon service as a means for augmenting their existing in-house security operations functions. Note that we do not assume that Tamnoon replaces or removes staff from the existing security team but that it instead provides positive ROI in the presence of the current employee staffing profile.

The broad annual financials associated with Consolidated are also relatively easy to estimate in a typical enterprise security context based on the experience of the TAG Infosphere analyst team. In contrast to ACME, we assume that Consolidated is using the Tamnoon solution, which has the great implication of improving its ability to avoid consequential cyber threats. The quantitative budget estimates for Consolidated are as follows:

- **Tamnoon License** – We can assume that Consolidated, by using Tamnoon, must pay a service license, assumed here to be $100K. As with ACME, this also assumes a greenfield in the ROI – namely, that ACME is not using a comparable solution.
- **Issue Burndown** – We remind the reader that using Tamnoon, Consolidated can reduce their overall issues and cloud misconfigurations more efficiently. These efficiencies can be represented as human hours saved, which an organization can dedicate to other security activities. This can, in some cases, reduce the need to pay service fees or employ consultants in adjacent areas.[5]
- **Avoidance of Major Cloud Incident** – We make the reasonable assumption that through the use of Tamnoon, the Consolidated team avoids one consequential and reportable incident during the calendar year that requires expenses in response, legal, reporting, and other areas.
- **Estimated Expenses** – The expenses Consolidated should expect to avoid for its incident include legal fees ($100K estimated), response service fees ($100K estimated), reporting service fees ($100K estimated), and consultants ($100K estimated). This results in $700K in savings.

Figure 2. Waterfall Budget Representation for Consolidated (Using Tamnoon)

BASELINE ESTIMATES FOR ACME

The result of the analysis is straightforward: Organizations will generally have the option to avoid an investment in the assisted cloud remediation service from Tamnoon, which saves the solution license fee, but will also result in $300K of incident-related expense (measured to include the $100K in savings from not spending on the Tamnoon license). Certainly, the budget will see the full $400K in expenses from the incident.

Alternatively, an organization can invest in engaging Tamnoon. This requires paying the license fee and avoiding the $400K in legal and response fees to handle the incident. The result is a positive $300K budget impact from the baseline. This implies that organizations can either pay $400K in response (the non-investment case) or they can pay $100K for a Tamnoon license (the investment case).

This further implies that if a CISO invests $100K in Tamnoon, that they can expect to reduce any annual budget set-asides for response by $300K. Readers can interpret this percentage ROI any way they desire, but we usually reference such savings as a 300% ROI, which is a good result for any security solution.

CONCLUSION AND ACTION PLAN

The conclusion readers should draw with respect to the analysis here is that by leveraging. This should come as no surprise since the purpose of any security investment is to reduce the risk of cyber threats. Too many security solutions help teams improve their going-through-the-motions operational tasks without actually avoiding incidents. Assisted cloud remediation will in fact reduce the chance of attack.

To that end, we recommend that an action plan be put in place immediately to review solutions such as Tamnoon, to plan a proof of concept (POC) test, and to begin using and benefitting from such security support. As we've shown above, the qualitative and quantitative benefits are straightforward, and security teams would be wise to take advantage of these desirable properties before the next major cyber incident occurs.

[1] For more detailed information on TAG Infosphere, Inc. and its unique approach to cybersecurity research and advisory support for enterprise customers, see https://tag-cyber.com/.

[2] For more detailed information on Tamnoon and its proactively managed cloud security solution for enterprise customers, see https://www.tamnoon.io/.

[3] Both ACME Manufacturing and Consolidated Industries are created here as representative composite organizations with highly typical financials. Actual Tamnoon customers have confidential deployments and while their input has been helpful, it is not appropriate to reproduce the financials of any actual enterprise, even if the name of the organization is changed.

[4] Note that these estimates are based on sizing for a mid-sized company, one with more than one thousand employees, but perhaps less than ten thousand. For larger companies, such as Fortune 100 organizations with hundreds of thousands of employees and other stakeholders, these estimated fees for legal expense, response services, and consultants will almost certainly be well into the millions of dollars for a typical event. While such numbers are certainly high, our experience is that the impact is proportional to mid-sized companies which have smaller outlays but experience the financial impact in a comparable manner.

[5] We choose to be highly conservative in our quantitative estimates by not including the avoidance of cost to other projects through redeployment or removal of security staff who can off-load designated activities to Tamnoon. Readers are welcome to insert such estimates into their own calculation of ROI, which would obviously improve the numbers considerably.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in climate science , cybersecurity, and artificial intelligence to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: DR. EDWARD AMOROSO, The TAG Analysts

Publisher: TAG, a division of TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.