


The logo for TAG, consisting of the letters 'TAG' in white, bold, sans-serif font, centered within a dark blue rectangular box.

TAG

RETURN ON INVESTMENT (ROI) ANALYSIS:

ESTIMATING RETURN ON INVESTMENT FOR THE ACSENSE PLATFORM

A decorative graphic consisting of several overlapping, wavy, translucent bands in shades of light blue and light green, flowing horizontally across the lower half of the page.

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

The logo for acsense, featuring a stylized lowercase 'a' in purple and green, followed by the word 'acsense' in a bold, dark purple, sans-serif font.

acsense



RETURN ON INVESTMENT (ROI) ANALYSIS:

ESTIMATING RETURN ON INVESTMENT FOR THE ACSENSE PLATFORM

DR. EDWARD AMOROSO
THE TAG ANALYSTS

EXECUTIVE SUMMARY

This report summarizes a return on investment (ROI) analysis performed by TAG Cyber for the acsense platform. The analysis compares an Okta identity and access management (IAM) customer using acsense with one not using acsense to illustrate both the qualified and quantified benefits. It is shown that under reasonable circumstances, use of acsense with Okta can produce roughly 200% year-over-year ROI. This provides useful operational and budget assistance for both IT professionals and security teams with responsibility for IAM.

INTRODUCTION

It is generally accepted by enterprise IT and security practitioners that identity and access management (IAM) has become the new primary cyber security control in any modern zero trust computing environment, supplanting previous reliance on the corporate firewall-enforced perimeter.¹ This control emphasis applies to employees, third parties, customers, and other stakeholders who require access to resources in an enterprise.

As a result, considerable emphasis has emerged in the IT and cybersecurity communities, including in both business and government, for how to optimize the protection of deployed IAM platforms – and, in particular, the [Okta platform](#) – from cyber threats, including human error and misconfigurations. Okta is generally recognized by most experts as an industry leader in cloud IAM support – and it is central to many cybersecurity architectures in place today.

In this report, we summarize an analysis by the [TAG Cyber](#) research and advisory team² into the return on investment (ROI) that emerges upon deployment of the acsense platform, which is designed to reduce the risk of IAM-related breaches for enterprise users, including those using Okta. The ROI considers both qualitative and quantitative factors and makes a broad assessment of the savings likely to come with investment in acsense.

The analysis outlines the ROI-related factors of acsense and then introduces two representative enterprise companies (created here using reasonable, aggregate data from live engagements) – one that uses acsense with an IAM solutions, Okta in the analysis, and the other that does not. The IT and security enterprise conditions created for this analysis based on discussions with the vendor, review of customer deployments, and the practical experience of the analyst team.³

Furthermore, throughout the analysis, we assume that the IT and security teams follow the common Shared Responsibility Model (SRM) as introduced by the Cloud Security Alliance.⁴ This model designates that cloud providers are responsible for many of the platform operational burdens that would have been normal for IT and security teams to have to deal with data protections in the traditional corporate data center model.

It is shown through this ROI analysis that a typical enterprise company using acsense with Okta can expect to avoid at least one major IAM incident, reduce the intensity of several minor incidents, and generally improve compliance activities, resulting in an 200% ROI for acsense usage. The implication here is that by taking preventive steps up front regarding IAM security, the enterprise avoids high response costs post-breach.

OVERVIEW OF ACSENSE PLATFORM

acsense offers a commercially available IAM resilience platform that is designed to provide a quick and easy recovery solution for and breaches for enterprise teams using IAM platforms such as Okta's Cloud Identity and Access Management (IAM). The specific protection functionality embedded in the acsense solution focuses on the following three areas of IAM-related security – with emphasis on Okta:

- *Recovery* – Improving the business continuity, disaster recovery, and compliance of the IAM solution (e.g., Okta) system for cloud IAM in an enterprise setting. As one would expect, improvements in IAM recovery will have qualitative and quantitative benefits.
- *Reliability* – Reducing the single point of failure (SPOF) risk for IAM deployments and data which can be targeted by an adversary. This is especially important since IAM failures could lead to significant business outages in certain cases.
- *Configuration* – Addressing common IAM administrative and misconfiguration risks which can lead to cyber breaches. Experience suggests that a large percentage of breaches to enterprise stem from misconfigured IAM settings.

These functional cybersecurity benefits provide only a high-level summary of the advantage of the acsense platform in the context of an Okta IAM deployment for enterprise. Interested readers are advised to visit the [acsense website](#) for more detailed technical, marketing, and product information on the platform.

ROI ANALYSIS

The underlying model driving the ROI analysis includes management decisions about cloud IAM security that will influence investment costs and associated qualitative and quantitative benefits of using acsense. The best way to explain the model is to list the relevant high-level areas below, along with a brief rationale for why that aspect of the framework is relevant to enterprise security risk management and business continuity for Okta deployment.

- *Consequence Avoidance of Major IAM Incidents* – The primary ROI-related benefit that comes with use of acsense involves the significantly reduced potential that a major IAM incident will create meaningful consequences in a given calendar year, causing considerable detection, response, and recovery expense, including from IAM malfunctions.

- *Consequence Avoidance of Minor IAM Incidents* – A complementary ROI-related benefit is that use of acsense will significantly reduce the consequences associated with multiple minor IAM incidents to occur in a given calendar year, causing detection, response, and recovery expense for each incident.
- *Operational Support for Preservation and Backup* – An additional ROI-related business continuity benefit from use of acsense is that reduced need for preservation and backup of IAM-related data, thus reducing the expense needed for a separate data security platform or managed data security service.

Our focus on these three quantifiable ROI-related categories of security, recoverability, and business continuity benefit does not reduce the value of more qualitative benefits that come from use of acsense. By qualitative benefits, we mean those improvements in the local environment that do not typically result in a meaningful reduction in the expense or capital portion of an annual operating budget.

As an example, consider that acsense improves the ease with which an enterprise team’s Okta deployment can be managed and tracked (i.e., changes in the system during on-going management). This typically also involves acsense helping with compliance obligations, where many complex requirements often exist in popular frameworks such as NIST 800-53 for backup support for critical systems such as Okta. Backup support, as most practitioners know, is helpful to reduce the risk of threats such as ransomware.

These qualitative advances are clearly real and tangible benefits, but we choose to not include them in the financial ROI quantification. Readers who disagree with this decision are welcome to estimate the benefits in their own local instantiation of the ROI calculation (which will improve the numbers we report here). The ROI approach is simple enough (see below) that making such adjustments should be straightforward.

CASE STUDY: ACME ENTERPRISE VERSUS CONSOLIDATED INDUSTRIES

The methodology to demonstrate financial ROI for the acsense platform involves the comparison of two representative companies with typical operating budgets, both presumed to be large enterprises. We reference the first example as ACME Enterprise and the second as Consolidated Industries. Both are created specifically as generic companies to emphasize that they could be from any industrial sector.⁵

We will assume that both ACME Enterprise and Consolidated Industries are [Okta customers](#), using the platform for identity cloud support for consumer and SaaS apps. This includes support for universal login, single sign on (SSO), passwordless or adaptive multi-factor authentication (MFA), and other capabilities.⁶

Baseline ACME Enterprise Scenario

ACME Enterprise is presumed to be a mid-to-large sized (Fortune 1000) company providing a digital experience to their customers, which we will assume to be a large mix of consumers and businesses. Financial service companies, insurance companies, and banks are typical examples of such firms. Cybersecurity for the on-line digital experience is supported using Okta for various IAM-related features.

The baseline case on which we evaluate the overall ROI for acsense starts with a foundational scenario in which no investment is made in the platform by ACME. This results in an Okta deployment that must rely on manual or ad hoc procedures for identity-related security support. In this situation, we can accept that the near-term financial benefit involves avoidance of acsense licensing fees, but that later compliance and response costs will be considerable.

It should be noted that the analysis presumes the occurrence of one major IAM-related incident that requires substantive response. This is a reasonable assumption, albeit perhaps somewhat conservative for most larger organizations. The associated non-investment and in-year, recurring cost increases correspond to various activities which would have to be performed by employees, consultants, or third-party providers.

We explain these activities below and then show a waterfall visualization of ACME’s non-investment case. This first visualization is done to demonstrate the in-year cost license cost avoidance being balanced by higher subsequent costs for compliance and response. None of these costs should be viewed as controversial by readers, since it is such a well-established fact that identity-related security is an increasingly difficult operational challenge.⁷

- *Compliance Cost (Consultants)* – We assume that ACME will require consultants to assist with identity-related tasks in support of its Okta deployment and operation. This is not a core competency for most security teams and poor identity management tools generally lead to manual tasks – hence our inclusion of consultants in the baseline estimate.⁸
- *Response Cost (Consultants)* – We can also assume here that ACME will need consultants to assist with incident response-related tasks. This is also not a core competency for most security teams, so ACME will need to augment its core staff with consultants to support response processes.⁹
- *Response Cost (Service)* – Most larger organizations subscribe to response services, and the costs are typically variable depending on the circumstances. This can include, for example, legal and public relations (PR) support during and after an incident, so it is reasonable to correlate an incident with increased service spend.¹⁰

To make estimates of the actual financial investments an enterprise security team would make on acsense, we avoided the complexity of determining percentage of annual spend that a team would make for acsense based on a percentage of Okta spend. Instead, we made a broad assumption that a mid-to-large sized organization might spend roughly \$250K in a given year on a typical acsense deployment.¹¹

Readers are warned that this is a rough estimate and that the specifics will vary considerably between different users. For larger Okta deployments, the acsense investment would likely be much greater than \$250K. Similarly, we make broad assumptions about response and compliance costs that are reasonable with respect to a typical mid-to-large sized organization, but that should also be tailored to the specifics of the local environment.

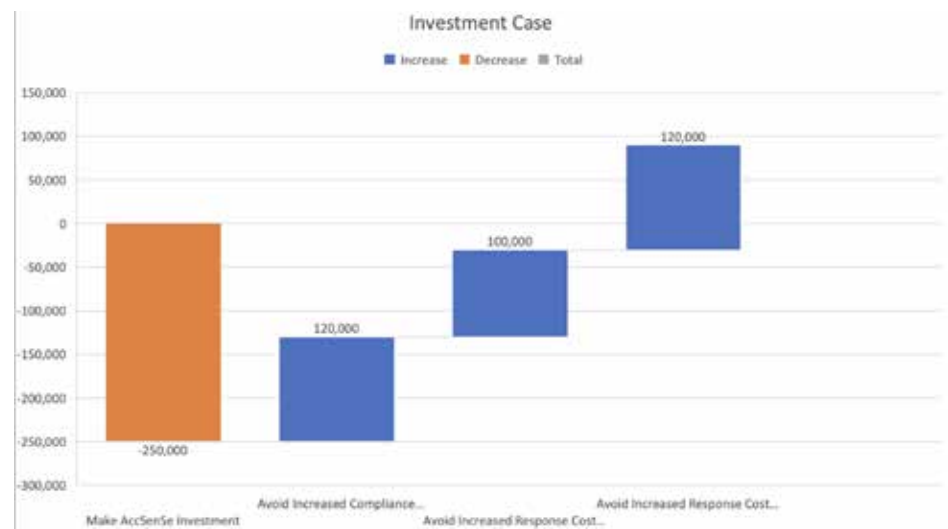


Figure 1. Baseline In-Year Waterfall View of acsense Non-Investment Case

The implication of ACME's non-investment in acsense is that they would spend an estimated \$340K on dealing with identity-related incidents (\$120K on compliance consulting, \$100K on response consulting, and \$120K on response services), but that they would also avoid the license fee of \$250K to acsense that would have been required to avoid these response and compliance fees.

This scenario can be interpreted in two ways: First, it should be clear that the organization will see a \$340K impact to their in-year budget for the on-going IAM work and the presumed major incident that occurs in-year. That said, we can acknowledge that they also avoid the \$250K fee to acsense, which results in a presumed net (\$90K) negative overall budget impact compared with the investment case.

CONSOLIDATED INDUSTRIES SCENARIO USING ACSENSE

Consolidated Industries is also presumed for our ROI analysis to be a mid-to-large sized company providing a digital experience to their customers, which we will also assume to be a large mix of consumers and businesses. Security for the digital experience is also assumed to be supported using Okta for the IAM-related features and acsense for enhanced reliability, configuration, and administrative support.

In this enhanced analysis case, it is assumed that Consolidated Industries does decide to make an investment in the acsense platform. This results in an Okta deployment that benefits qualitatively from advanced identity-related security support. In this situation, we can also accept that the near-term financial investment involves acsense licensing fees, but that later compliance and response costs will be avoided.

This analysis, like the previous one for ACME, presumes the occurrence of one major incident that requires substantive response. This is again a reasonable assumption, albeit perhaps conservative for most larger organizations. Our financial estimates for Consolidated are the same as for ACME, not just to simplify the comparison, but to emphasize that these numbers are broad estimates, so minor adjustments would be misleading.

We explain the positive impact on IAM-related activities below and then show a waterfall visualization of Consolidated's investment case for comparison to ACME's non-investment case. This visualization is done to demonstrate the in-year cost license cost being balanced by lower subsequent costs for compliance and response. Again, as suggested earlier, it is not controversial to suggest that up-front investment lowers later compliance and response costs.

- *Compliance Cost (Consultants)* – We assume that Consolidated will no longer require consultants to assist with identity-related tasks in support of its Okta deployment. The fees associated with such consultancy are assumed comparable to ACME's.
- *Response Cost (Consultants)* – We can also assume here that Consolidated will no longer need consultants to assist with incident response-related tasks. These fees are also held comparable to the previous case.
- *Response Cost (Service)* – Finally, we can assume that Consolidated will no longer need to pay any incident-related one-time fees for response services. The service fees for this case are assumed to not change with respect to ACME's response service.

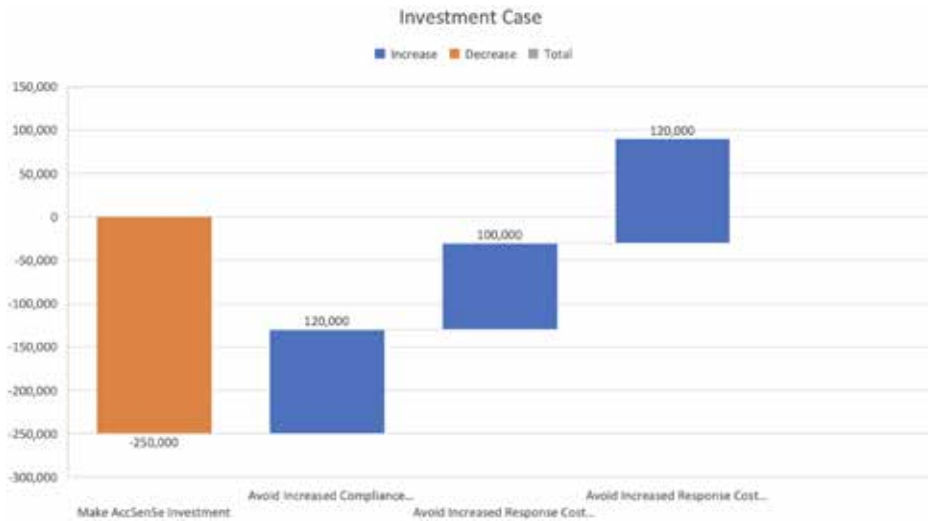


Figure 2. Enhanced In-Year Waterfall View of acsense Investment Case

Note that this case essential inverts the baseline case for ACME. That is, where ACME’s financial decisions result in either costs savings or cost spend, Consolidated’s decisions should here are the opposite. This simplicity of comparison should not detract from the basic message – namely, that when improvements are made to the IAM infrastructure, that positive financial benefits will accrue.

The summary implication of Consolidated’s investment in acsense is that by spending \$250K on the platform, corresponding \$340K in benefits will emerge. The overall budget impact of a typical year in which a major incident has occurred is that instead of the case where ACME’s budget saw a negative of (\$90K), the investment case here is that the impact of cost avoidance is a positive \$140K to the overall budget.

APPENDIX A: TAG CYBER ROI METHODOLOGY

The TAG Cyber ROI methodology quantifies investment returns in financial terms (i.e., measured units are dollars). Qualified returns are not included in the numeric analysis. Instead, they are identified and shown to provide benefits that improve a work environment, but in non-financial ways. Three possibilities emerge for a given investment case. In the investment case, the costs incurred exceed the qualified returns, in the positive return case, the costs incurred are lower than the qualified returns, and in the accretive case, costs equal returns.

Accretive Case:

$$\text{Incurred_Costs} = \text{Quantified_Returns}$$

Investment Case:

$$\text{Incurred_Costs} > \text{Quantified_Returns}$$

$$\text{Incurred_Costs} = \text{Quantified_Returns} + \text{Investment}$$

Positive Return Case:

$$\text{Incurred_Costs} < \text{Quantified_Returns}$$

$$\text{Incurred_Costs} + \text{ROI} = \text{Quantified_Returns}$$

¹ The shift toward identity as the new perimeter has been gradual and on-going now for many years. See this [Wired Article](#), for example, from a decade ago that points to the trend. Most readers will agree that identity has become as important, if not more important, than traditional perimeter networks. This is an important observation for the ROI analysis here since enterprise security teams have long agreed that augmentation of their perimeter network with additional tools is a good investment. The acsense platform does much the same thing for identity systems (Okta, in particular).

² TAG Cyber is a division of TAG Infosphere Inc. which is a research and advisory firm headquartered in New York City that focuses on major societal issues such as cybersecurity, artificial intelligence, and climate science. ROI analyses from TAG Cyber are custom designed to the platform circumstances, and use data from TAG Cyber research, customer provided data, and vendor supplied information. All TAG Cyber researchers are present or former practitioners, which helps to ensure that ROI estimates are reasonable from a practical perspective.

³ The approach of creating representative companies involves using experience and observations from hundreds of enterprise security team interactions at TAG Cyber. The details of the estimated pricing require a collage of observations of response, compliance, consulting, and related costs. Obviously, these costs will vary between live engagements, so readers are welcome to insert and adjust the numbers.

⁴ See <https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/> for a clear explanation of the SRM model and how it presumes shared and coordinated responsibility between providers and users.

⁵ Our day-to-day research and observations at TAG Cyber suggests that budget implications for any IAM improvement will be comparable across different countries (no impact from one to another) and also between government and business organizations. Comparable qualitative and quantitative benefits are expected for any and all of these groups.

⁶ We focus on use of Okta for customer identity-related services, rather than include the system for traditional enterprise IAM support, even though the company offers such capability. This decision is made to simplify the ROI analysis, but readers are welcome to extend the analysis toward their employee base if this is an important use-case for their local environment.

⁷ Note that the license fee shown in the waterfall example in Figure 1 is not representative of what an acsense customer should expect during negotiation of their own license amount. The values selected here are purely notional and selected to demonstrate the relationship between spend and savings. In some cases, the actual amount could be considerably higher, or in other cases lower – but the relationship should remain constant.

⁸ Our assumption here is that a typical professional IAM consultant working compliance-related project support issues such as framework mapping or evidence collection (including review of documents, artifacts, and system output) would involve roughly \$10K per month in costs, resulting in calendar year costs of \$120K for such IAM consulting related costs. Obviously, a typical enterprise team might have more consultants than this, but our observation is that IAM talent is limited, so it is common for enterprise security organizations to include non-employee staff support (including on-site contractors).

⁹ Estimating the costs for response experts is more difficult because their work tends to (1) vary based on the intensity of an incident and (2) serve on a more on-demand basis than as an on-going monthly fee for their support. As such, we choose to include \$100K as a representative estimate for a typical engagement that involves a significant IAM-related breach – one that includes loss of customer credentials. We view this as a conservative estimate, since these costs can easily go up into the many hundreds of thousands of dollars for more intense breaches at larger organizations.

¹⁰ Response services are common across enterprise (originated with the Mandiant offer created in 2004), but the fees associated with such services vary obviously. We arrived at \$10K per month as a reasonable and highly conservative estimate for a professional response firm to charge an enterprise of the size included in our case studies.

¹¹ As one would expect, we mark this estimate with a major caveat, since it will vary significant with the size of the organization and the complexity, scope, and reach of the Okta deployment. By choosing \$250K as our acsense annual fee, we presume that the organization is spending roughly \$2.5M annually on Okta and that 10% of this spend is directed toward the acsense platform. But every engagement will vary, so buyers should use this information to guide their understanding of the broad ROI methodology rather than as a pricing guide.

ABOUT TAG

Founded in 2016 by Dr. Edward Amoroso, former executive at AT&T Bell Labs, TAG Infosphere, Inc. is a trusted research and advisory firm, providing unbiased insights and recommendations to commercial vendors, government agencies, and business groups. The focus at TAG is on three areas of considerable importance to our world: Cybersecurity, Climate Science, and Artificial Intelligence.. TAG bucks the trend of pay-for-play research by offering in-depth analysis, expert consulting, and personalized content based on thousands of engagements with clients, all from a practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso, TAG Analysts

Publisher: 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.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Infosphere, Inc." Non-press and non-analysts require TAG's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG's analysts are subject to change without notice and should not be construed as statements of fact. TAG Infosphere, Inc. disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: acsense commissioned this book. TAG Infosphere, Inc. provides research, analysis, and advisory services to several cybersecurity firms that may be noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.

Copyright © 2023 TAG Infosphere, Inc. This report may not be reproduced, distributed, or shared without TAG Infosphere, Inc.'s written permission.

