TAG

RETURN ON INVESTMENT (ROI) ANALYSIS:

RETURN ON INVESTMENT (ROI) ASSESSMENT FOR FORTRA CLOUD EMAIL PROTECTION

DR. EDWARD AMOROSO,
CEO, TAG INFOSPHERE, INC.

FORTRA™

RETURN ON INVESTMENT (ROI) ASSESSMENT FOR FORTRA CLOUD EMAIL PROTECTION

DR. EDWARD AMOROSO, CEO, TAG INFOSPHERE, INC.

EXECUTIVE SUMMARY

This TAG[1] report provides a high-level summary of the qualitative and quantitative return on investment (ROI) associated with use of the commercial Fortra[2] Cloud Email Protection platform. The assessment shows that organizations should expect excellent qualitative benefits from the use of the Fortra solution, as well as quantitative ROI in the range of 114% to 200% for large and mid-sized organizations under reasonable assumptions.

INTRODUCTION

The need to establish return on investment (ROI) for enterprise security teams has become more intense in the past few years as Chief Information Security Officer (CISO) have been asked to rationalize their budgets.[3] ROI analysis such as presented here helps to determine whether a given platform replacement or investment provides sufficient qualitative and quantitative benefit to justify the effort for deployment, support, and use.

This need for ROI is particularly true for mature security controls that have had uneven results, and many email security solutions fall directly into this category. Most organizations would agree that despite considerable effort, business email compromise (BEC), Spam, and malicious workloads continue to slide through existing controls such as secure email gateways (SEGs) and email security content filters. This is clearly a nagging issue in our industry.

Our objective and focus here is on *Cloud Email Protection* from Fortra. A major benefit of the solution which we will highlight in our qualitative analysis is the combination of a well-exercised email security platform used for many years with a fresh new platform offering developed through acquisition by Fortra and integration with other cybersecurity solutions[4] The resulting platform represents an optimal combination of *mature* with new.

We start with an overview of Fortra Cloud Email Protection and then transition to an analysis of the ROI for the platform. We are sensitive in the presentation below to the various usage scenarios including for customers who might be new to the Fortra cloud security platform as well as existing customers of the Fortra email security platform who are interested in using this ROI for on-going budget planning.

OVERVIEW OF THE FORTRA CLOUD EMAIL PROTECTION PLATFORM

As suggested above, Fortra Cloud Email Protection focuses on modern email security and benefits from the strategic acquisition by Fortra of several component platforms from industry leaders including Agari, Clearswift, and PhishLabs. These acquisitions have been combined to form a strong foundation for cloud email security, covering a wide range of protections, which is a requirement for modern email infrastructure.

To illustrate, recognize that the integration of Agari's DMARC (Domain-based Messaging Authentication, Reporting, and Conformance) technology into Fortra's platform supports the need for authentication against email spoofing threats. By incorporating this authentication technology, the Fortra platform helps domain owners avoid unauthorized access and usage as part of phishing, spoofing and business email compromise (BEC) attacks.

Integration of Digital Guardian's content filtering and data loss prevention (DLP) capabilities adds world class secure information sharing and data protection to the platform, thus enabling organizations to enforce policies that safeguard information sent over email. With this advanced technology, users benefit from enhanced control over email content, thus minimizing the risk of data breaches and compliance issues.

The integration of PhishLabs provides the Fortra platform with advanced threat intelligence, which offers real-time insights into emerging threats and malicious activities targeting email. By leveraging PhishLabs' expertise, the Fortra platform provides users with proactive defenses against phishing attacks, thus enabling much more swift detection and mitigation of potential security breaches.

As will be shown below, these acquisitions provide an excellent foundation for Fortra Cloud Email Protection, one that allows organizations to address the challenges of email security. The combination of email authentication, content filtering and DLP, threat intelligence, and security training simulation (based on the Terranova acquisition)[5] creates an ecosystem that matches up with the types of requirements we see in our work with enterprise teams every day at TAG.

TAG ROI METHODOLOGY

The approach being taken for this Fortra ROI assessment involves identification of two categories of benefit that come from deployment and use of the email security platform. The first involves so-called *qualitative ROI* which includes benefits that are clearly valuable to a given security team, but that do not result in any direct reductions in budget expenditure. Qualitative ROI is certainly tangible, but it is considered non-financial.

In contrast, *quantitative ROI* includes those benefits that have a direct impact on the security, information technology (IT), or related budgets. Such direct impacts include costs for staff, consultants, contractors, services, platforms, or tools. They are usually classified as operating expenses, but in some cases, the costs can be part of a capital budget. In either case, quantitative ROI can be viewed as line-item changes in budgets.

We emphasize the difference here because ROI calculations from many advisory firms will pack the quantitative assessment with savings that any practitioner will immediately recognize as pure padding. For example, enterprise teams report that cyber insurance negotiations are improved when continuous validation is being done – but any claim that insurance premiums will be reduced through deployment of an email security platform are in our view exaggerated.

We should also mention that our approach to ROI calculation is done in the context of sample use-case environments that are derived from our myriad of experience at TAG working with enterprise CISOs, as well as running our own programs for decades.[6] We do generally speak with users of a given platform to validate our assumptions, but we have sufficient access to live CISO budgets and expenditures to understand the qualitative and quantitative ROIs accurately.

SUMMARY OF QUALITATIVE ROI

Measuring the qualitative ROI for any platform requires establishment of a reasonable comparison base. For example, if a company is currently doing little or no security for their email, which might be found in a smaller or mid-sized company, then the benefits of deploying Fortra for Cloud Email Protection will be significant – albeit perhaps requiring the attention of the security team to train on how best to use the new capability.

For larger enterprise teams, however, our experience at TAG is that all are doing some form of email security today. This makes qualitative assessment of ROI more nuanced and dependent on the local environment. Qualitative ROI – which, as explained above, implies benefits that are not directly realized in a security budge – is also often associated subjective views such as local preference or personal experience with a particular tool.

That said, we can make some general comments here about qualitative benefits that come from deployment and use of the Fortra email security solution – and we make these in the context of reasonable assumptions that a given organization is engaged in some types of on-going email security today, perhaps using native email security capabilities from Microsoft or Google.[7] We list these qualitative benefits below.

Qualitative Benefit: Pre-Integration of Features
A major qualitative benefit of the Fortra platform is the high level of pre-integration done by the product team which reduces (or removes) the need for enterprise teams to have to support the engineering effort for such integration upon deployment. While we view this as a qualitative benefit, it is easy to conceive scenarios where this results in considerable savings in terms of staff and consulting costs.

Qualitative Benefit: Use of Mature and Familiar Components
The Fortra platform is composed of a collection of mature, familiar, tested, and dependable tools, systems, and capabilities from well-known vendors with loyal customer bases. This is a massive qualitative benefit because it ensures that Fortra customers will be working with experienced experts who have been supporting customer deployments for many years. This results in reduced risk associated with use of the Fortra platform.

Qualitative Benefit: Simplified Deployment and Support Process
Because Fortra covers so many aspects of the enterprise security ecosystem, deployment and support for these various functions can be amortized across one support team – namely, Fortra. This reduces the need for contracting, procurement, on-boarding, and support from multiple vendors, which in turn reduces the lifecycle time and operating costs associated with any multi-vendor situation.

QUANTITATIVE ROI ASSESSMENT

The approach taken to develop a quantitative ROI for the Fortra Cloud Email Protection solution involves reviewing, under familiar and reasonable assumptions, a typical secure email-related CISO budget before and after deployment of the platform. Such an approach serves to highlight how an investment in Fortra provides tangible reductions in line-item components of a budget.[8] The spend categories considered in-scope for the quantitative ROI include the following:

- **Consulting Costs** – This includes the operating expense costs associated with the provision of contractors and consultants to augment the employee team focused on email security features, capabilities, and services.[9]
- **Security Services** – This includes any external services (professional or SaaS) used to provide for email security or to augment the existing email security solution to assist in either functional or user education tasks.
- **Security Platforms** – This includes any deployed tools, systems, or platforms that are being used for email security – and this includes support for any subsidiaries, merged entities, or other corporate partners.

Including the reduction of costs associated with internal employee staff is not considered a reasonable option at a time when security talent is so difficult to find, hire, and retain. This is especially true for employees with the talent to support email security tasks. That said, if it were the case that mandatory budget cuts demanded reduction in such talent, then introduction of a platform such as Fortra could be used to address this difficult situation.

The approach taken in our quantitative estimation is to create baseline scenarios in which we identify a typical enterprise under reasonable circumstances and view their budget finances before and after use of Fortra. This serves to highlight the impact of non-investment and investment on budget with the situation in each case that spending some money on a good platform such as Fortra obviously produces benefit (see below).

CASE STUDY: MIDSIZED RETAIL FIRM

The first use-case involves a typical midsized retail firm, one that includes support for employees, contractors, and other staff and that maintains a modest-sized IT security team. We can assume that this support team engages an external consultant to help with email security and that it employs a modest security architecture to deal with compliance and avoidance of threats such as phishing which we assume occurs often.

We will assume that the security team includes ten full-time employees and two full-time contractors, and that the budget for email security includes Microsoft E3[10] and several additional security tools supporting user awareness to avoid phishing, and engagement in annual incident response costs with the reasonable expectation that at least one meaningful security event occurs annually that requires focused incident response.[11]

The email security-related financials associated with such a midsized retail firm scenario would include costs for employee staff, which we assume to have an annual loaded cost per headcount (employees and contractors) of USD $200K, as well as costs in each of the categories listed above – namely, contractor fees, platform expenses, and service expenses. These costs are sketched below.

Annual Email Security Budget Line Items	Annual Costs (Operating Expense)	Rationale
Staff Salaries (2 FTE @ $200K per annum)	$400,000	Team supporting day-to-day email security tasks
Contractor Fees (2 FTE @ $200K per annum)	$400,000	Additional two staff supporting day-to-day email security tasks (contracted)
Platform Expenses	$500,000	Deployed security platforms for cloud security
Integrated SEG Augmentation Tool	$250,000	Common for mid-sized team to augment with a tool for cloud email
Microsoft E3 Support (Estimated Email Proration)	$250,000	Estimated E3 license portion for email security
Service Expenses	$300,000	Security services externally contracter
On-Demand Incident Response Services	$300,000	Based on estimated response support for two incidents per year
Total Annual Secure Email-Related Operating Budget	$1,600,000	Total annual email security expenditure - pre-Fortra

Figure 1. Security Costs for Midsized Retail Firm Before Use of Fortra Cloud Email Platform

As should be evident from the email security budget shown above, there is nothing unreasonable that sticks out in the annual fee structure or the decisions made about security. This should look typical and familiar to anyone reviewing the numbers. That said, there are places where this can be improved from a qualitative perspective, especially in the context of the relatively light attention to email security.

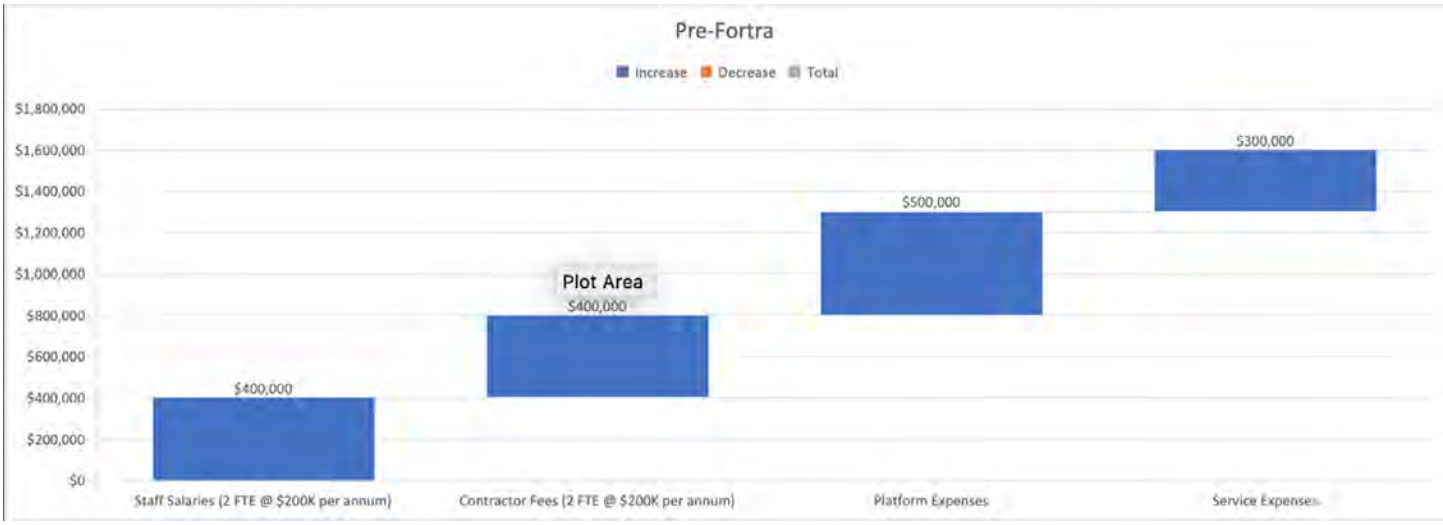

Figure 2. Waterfall View for Midsized Retail Firm Pre-Fortra

If this midsized retail firm were to select Fortra for improved email security coverage, then not only will the qualitative impacts be positive (as listed in an earlier section above), but the quantitative benefits will also be positive. This is true mostly because the preventive nature of improving security controls for email will have direct impact on the likelihood of incident. This in turn reduces the need for consultants, external services, and incident response fees.

We can therefore adjust the firm's annual security financials and roughly calculate the quantitative benefit which mostly comes from (1) the reduction in need to engage augmented platform services, (2) the reduction of one contractor, and (3) the reduced likelihood of an in-year incident, thus resulting in the ability to reduce the security incident service budget and associated incident-related external consulting costs. These new costs are sketched below.

Annual Email Security Budget Line Items	Annual Costs (Operating Expense)	Rationale
Staff Salaries (2 FTE @ $200K per annum)	$400,000	Team supporting day-to-day email security tasks
Contractor Fees (1 FTE @ $200K per annum)	$200,000	Reduce additional staff for day-to-day email security tasks (contracted)
Platform Expenses	$550,000	Deployed security platforms for cloud security
Fortra Cloud Security Platform	$300,000	Typical annual fee for mid-sized firm for Fortra platform
Integrated SEG Augmentation Tool	0	No need to augment with a tool for cloud email
Microsoft E3 Support (Estimated Email Proration)	$250,000	Estimated E3 license portion for email security
Service Expenses	$150,000	Security services externally contracter
On-Demand Incident Response Services	$150,000	Based on estimated response support for one incident per year
Total Annual Secure Email-Related Operating Budget	$1,300,000	Total annual email security expenditure - Using Fortra

Figure 3. Security Costs for Midsized Retail Firm After Use of the Fortra Cloud Email Platform

Analysis of the difference between the *before* and *after* use-cases of Fortra being deployed to our retail firm suggest that in this case, an expenditure of $300K for Fortra results in an overall $600K reduction in the overall budget. If we observe that this $300K increase in the budget for Fortra results in a corresponding $600K drop in expenses (to produce the $300K reduction), then we can reference the investment as having a 200% quantitative ROI.

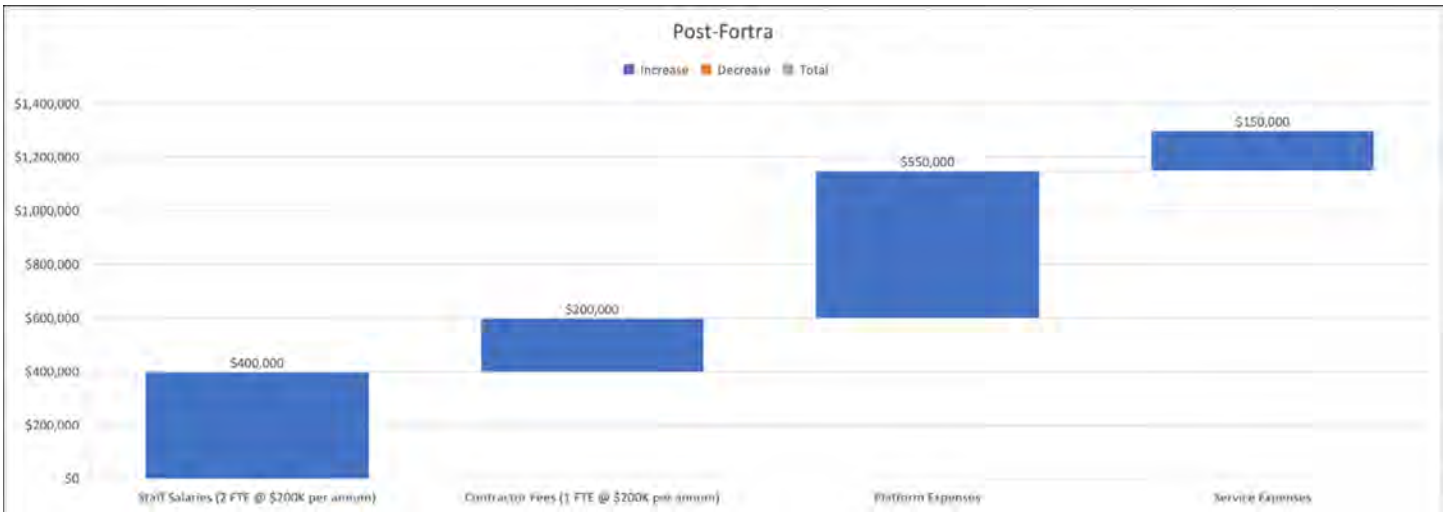

Figure 4. Waterfall View for Midsized Retail Firm Post-Fortra

CASE STUDY: LARGE FINANCIAL SERVICES COMPANY

The second use-case involves a typical large sized financial services company, one that is perhaps operating as a global entity, and that maintains a well-staffed security team. We can assume that this team engages internal email security resources and that it employs a best-in-class security architecture to deal with regulatory compliance and avoidance of serious threats such as ransomware and nation-state exploits.

If we assume that the security team includes eighty employees and twenty contractors, and that the budget for security includes Microsoft E5[12] and many additional email security-related platforms supporting governance, risk, and compliance (GRC), identity and access management (IAM),[13] and engagement in annual incident response costs with the expectation that at least two meaningful security event occurs annually.[14]

The security financials associated with such a large manufacturing company scenario would include costs for employee staff, which we assume to have an annual loaded cost per headcount (employees and contractors) of USD $200K, as well as costs in each of the three categories used in the prior use case example – namely, consulting, security services (including response), and security platforms. These costs are sketched below.

Annual Email Security Budget Line Items	Annual Costs (Operating Expense)	Rationale
Staff Salaries (4 FTE @ $200K per annum)	$800,000	Team supporting day-to-day email security tasks
Contractor Fees (4 FTE @ $200K per annum)	$800,000	Additional two staff supporting day-to-day email security tasks (contracted)
Platform Expenses	$1,400,000	Deployed security platforms for cloud security
Integrated SEG Augmentation Tool	$400,000	Common for mid-sized team to augment with a tool for cloud email
Microsoft E5 Support (Estimated Email Proration)	$1,000,000	Estimated E5 license portion for email security
Service Expenses	$600,000	Security services externally contracter
On-Demand Incident Response Services	$600,000	Based on estimated response support for two major incidents per year
Total Annual Secure Email-Related Operating Budget	$3,600,000	Total annual email security expenditure - pre-Fortra

Figure 5. Security Costs for Large Financial Services Company Before Use of Fortra

The financials associated with this large organization include $1.6M in employee and contractor expenses, which suggests that many tasks are being done by individuals perhaps using home-grown or open-source tools that would not show up on an income statement. The budget also includes $1.4M in platform and service expense which seems typical, if not a bit modest the cloud email security portion of an organization's platform allocation.

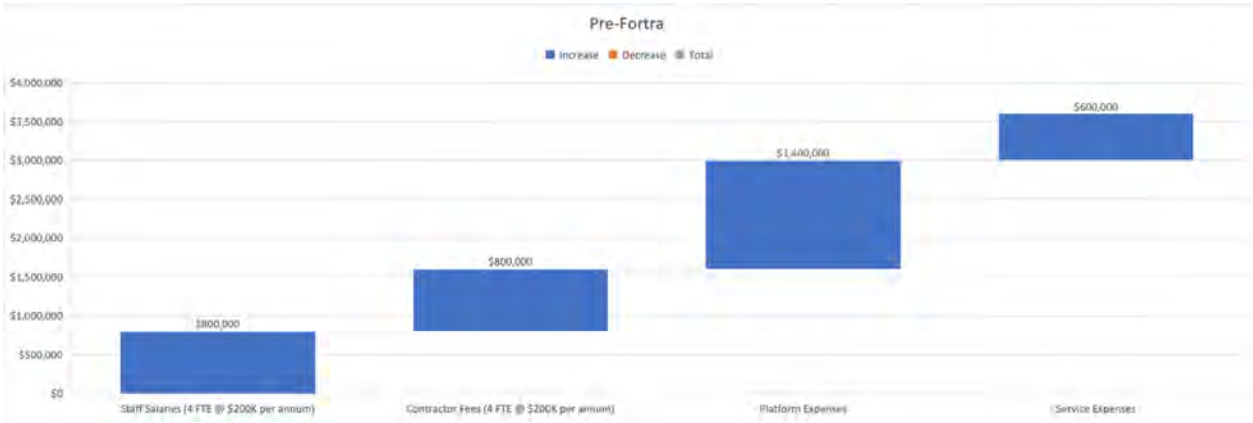

Figure 6. Waterfall View for Large Financial Services Firm Pre-Fortra[15]

If this large organization were to select Fortra for enhanced cloud email security protection, then the qualitative impact would be considerable, but the quantitative benefit will also be positive, as in our previous case study. One key benefit is reduction in the high response costs associated with the two expected annual incidents. This is done through the use of advanced technologies to reduce the risks associated with cloud email.

As in our previous case, we can adjust the company's annual email security-related financials and roughly calculate the quantitative benefit which comes from (1) the reduction in need for existing email security augmentation tools, (2) the reduction of four contractors, and (3) the reduced likelihood of two incidents to one, thus resulting reduction of security incident-related external consulting costs. These new costs are sketched below.

Annual Email Security Budget Line Items	Annual Costs (Operating Expense)	Rationale
Staff Salaries (4 FTE @ $200K per annum)	$800,000	Team supporting day-to-day email security tasks
Contractor Fees (1 FTE @ $200K per annum)	$0	No additional staff supporting day-to-day email security tasks (contracted)
Platform Expenses	$1,700,000	Deployed security platforms for cloud security
Integrated SEG Augmentation Tool	$0	No need to augment with a tool for cloud email
Fortra Cloud Security Email Platform	$700,000	Typical license for large bank
Microsoft E5 Support (Estimated Email Proration)	$1,000,000	Estimated E5 license portion for email security
Service Expenses	$300,000	Security services externally contracter
On-Demand Incident Response Services	$300,000	Based on estimated response support for one major incident per year
Total Annual Secure Email-Related Operating Budget	$2,800,000	Total annual email security expenditure - pre-Fortra

Figure 7. Security Costs for Large Financial Services Company After Use of Fortra

The use of Fortra is shown to have the following impact: First, four contractors can be removed from the budget, resulting in $800K in savings; second, the probability of incident is cut in half, thus resulting in half the expected response costs in-year which saves $300K; and third, the need for augmented email security tools also saves $0.4M in costs per year – and this is not an unusual savings given the complexity of a larger organization.

Figure 8. Waterfall View for Large Financial Services Firm Post-Fortra

The analysis of these savings is as follows: An investment of $700K in Fortra results in $800K in savings which represents a 114% ROI. The result is that the company's cybersecurity budget can be reduced from $3.6M to $2.8M based on an investment in Fortra. Obviously, this would be useful if the CISO is under pressure to reduce budget. The preference from most practitioners, obviously, would be to reinvest these savings into the program.

ACTION PLAN

The implication of our analysis is that buyers who find themselves in the pre-state described by our use-cases, and we assume this to be a common state, should review the qualitative and quantitative return estimates included in this report. We understand that an interpretation of our generalized analysis will need to be done for the local environment, but it would be worth the time for the local security team to work this task.

If the returns appear to be relevant locally, then we see no reason why steps should not be taken to contact Fortra for discussion about a proof of concept (POC) or other first steps toward selection, deployment, and use of the cloud email security platform. As always, TAG analysts are available to help Research as a Service (RaaS) customers with this and any other source selection analysis or decision process for security solutions such as from Fortra.

[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, artificial intelligence, and climate science/sustainability. TAG has been developing ROIs since 2018.

[2] Fortra is a commercial vendor, formerly known as HelpSystems, that has grown over the past decade in the cybersecurity industry through a series of major acquisitions including Agari, Clearswift, Tripwire, and other vendors. Fortra's public website is https://www.fortra.com/.

[3] Stakeholders in enterprise security will agree that rationalization is now being done commonly for CISO budgets. Here is a typical article on the topic from Boston Consulting Group (BCG): https://www.bcg.com/publications/2023/how-cisos-are-reducing-cyber-risk-on-a-tight-budget.

[4] The Fortra acquisitions of interest for this article were the 2019 acquiring of email security solution provider Clearswift (the announcement article is here: https://www.clearswift.com/resources/press-releases/help-systems-announces-clearswift-acquisition) and the 2021 acquiring of DMARC vendor Agari (the acquisition announcement article is here https://www.fortra.com/resources/press-releases/helpsystems-acquires-agari-grow-data-security-portfolio). Also, both PhishLabs and Digital Guardian were acquired by Fortra in 2021. The press releases are at https://www.phishlabs.com/resources/press-releases/helpsystems-acquires-phishlabs and https://www.fortra.com/resources/press-releases/helpsystems-welcomes-digital-guardian.

[5] Terranova, a leader in the provision of security awareness training, was acquired by Fortra in 2022. The press release describing the transaction is available at https://www.fortra.com/resources/press-releases/helpsystems-acquires-terranova-security.

[6] TAG works on an on-going and daily basis with roughly 100 different enterprise and government teams supporting the research and advisory needs for cybersecurity protection of their infrastructure. This practitioner community extends to research and advisory support at TAG for vendors which also often includes assistance to their CISO. Recent new rulings from the US Securities and Exchange Commission (SEC) have increased the need for CISOs to engage expert assistance and coaching from experts. TAG provides exactly that type of personalized assistance via former CISO practitioners team members. To that end, we are involved in the rationalization of dozens of annual security budgets including providing expert assistance in the selection of tools and platforms, as well as identification of strategies for dealing with budget cuts.

[7] It should go without saying that the vast majority of email deployments in enterprise settings include the use of Microsoft 365. This implies the usual set of dependencies for Fortra Cloud Email Protection on the underlying email service provider.

[8] Considerable debate exists in the enterprise security community about whether an ROI analysis should be designed to reflect cost per user (e.g., for 10K, 50K, or 100K users) or whether the analysis should be done based on expected budget allocation on a typical annual basis. We've made the decision here to use annualized spend, since this is how CISOs view the investment. It is easy, however, for a reader to take the numbers and do the simple math to break down costs on a per user basis using sizing assumptions that we will include the analysis regarding the typical numbers of users in mid-sized and larger enterprise settings.

[9] Note that this cost reflects the common practice we've seen where consultants are used to augment payroll staff to support deployment and use of a platform in this area. This not a managed security service providers (MSSP) cost.

[10] We first call the reader's attention to our earlier footnote that it is not reasonable to just assume a per seat license fee for Microsoft E3 since many factors will apply. That said, it is reasonable to assume that with 10K users at $25 per user that an annual expenditure would be in the $250,000 range for a typical mid-sized company.

[11] We try here to make reasonable practical assumptions regarding the typical types of cybersecurity staffing, platforms, services, and tools that would be engaged for this use-case. This lead author spent time on the board of trustees of a mid-sized university and also has served as faculty at two universities for decades. This helped to provide guidance on how a typical university would typically allocate their security resources.

[12] Again, we hesitate to generalize Microsoft E5 license cost, but a typical larger company paying $35 per user at 30K employees will be roughly $1M per year. For larger companies, this will be much higher. Nevertheless, we made the decision to keep the E5 estimate conservative in the calculations for this use-case.

[13] We mention these tools as relevant to email security but we do not factor the costs of these platforms and the teams and infrastructure required to run them into our email security use case calculation.

[14] We make this estimate based on our practical experiences with TAG Research as a Service (RaaS) customers rather than based on any external reporting metrics such as with the US Securities and Exchange Commission (SEC). We expect that with new SEC reporting rules, that research teams such as ours at TAG will be able to utilize and trust metrics for external reporting to entities such as the SEC. For now, however researchers must use their practical experience and an estimate of two meaningful cyber events per year for a large financial services company seems justifiable.

[15] One useful visual representation of the differences in the scenarios is to look carefully at the waterfall view of the two scenarios shown in the use-case examples above. We can represent the costs before and after use of the Fortra solution and buyers might use this as a baseline for understanding the impact of a purchase decision on their local budget. These visuals are important because they help with financial planning on an annualized basis.

ABOUT TAG INFOSPHERE

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: ED AMOROSO

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.