A Forrester Total Economic Impact™ Study
Commissioned By Agari
February 2020

The Total Economic Impact™ Of Agari Phishing Defense™

Increased Email Security And Lower Total Cost Of Ownership

agari
by HelpSystems

Table Of Contents

Project Director:
Jonathan Lipsitz

Project Contributor:
Jon Erickson

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

agari
by HelpSystems

Benefits And Costs

Reduction in time to better security realization:
36%

Reduction in internal and external solution deployment costs:
59%

Total external expenditure:
$209,448

Executive Summary

Agari provides an email security solution that helps prevent malicious emails that may make it past other defenses from reaching users' inboxes. Agari commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Agari Phishing Defense™. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Agari Phishing Defense solution on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed one customer with experience using Agari Phishing Defense, which is used in conjunction with other solutions as part of a defense-in-depth approach to IT security.

Prior to using Agari Phishing Defense, the interviewed customer had other vendor solutions to prevent phishing and other email-based attacks. However, prior attempts yielded limited success, leaving the customer with a higher than acceptable level of vulnerability. These limitations generated too much manual effort by the IT security team and increased costs and the risk of a breach.

Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **The organization improved IT security and reduced the level of effort to provide better protection.** Most importantly, the organization improved email security. This reduced the risk of leaking sensitive company or customer information, inappropriately transferring money out of the company, or ransomware attacks being successful. This was achieved while the IT security department spent less time on email security. Employees could focus on other risk areas and the company could avoid additional hires. The organization avoided hiring one FTE, which is worth $270,297 over the three years. For the financial model, Forrester includes only the avoided additional hires component.
- **Agari Phishing Defense delivered results one-third faster than the other considered solutions.** Other solutions would have taken nearly one year to implement and would have required a larger deployment team. Faster deployment means that better security is in place sooner and deployment costs are lower. The avoided deployment costs of the other solution were $519,545 for internal and external resources — 2.4x more than what Agari Phishing Defense cost to deploy.
- **Without Agari Phishing Defense, the company would've needed to roll out a full threat intelligence program.** Agari Phishing Defense streamlines and automates threat detection management. Other solutions would have required building out a threat intelligence program to integrate threat data from multiple sources. The avoided solution costs and ongoing maintenance total $230,781 over the life of the study.

agari by HelpSystems

ROI
97%

Benefits PV
$1.0 million

NPV
$502,000

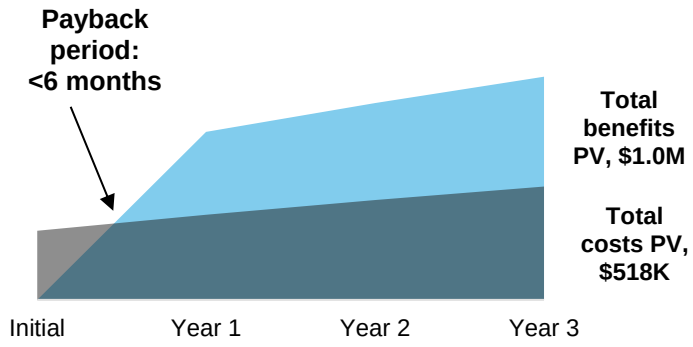
Payback
<6 months

Costs. The interviewed organization experienced the following risk-adjusted PV costs:

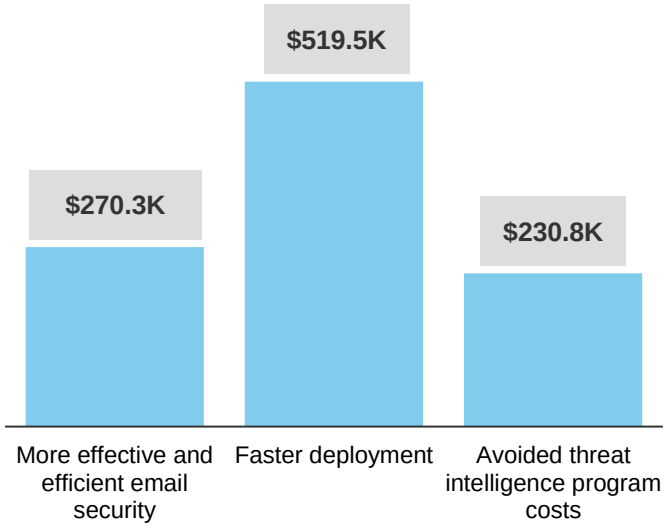
- **The internal effort for deployment, end user training, and ongoing solution management cost $308,789.** The deployment effort lasted seven months, which included two months of building use cases and policies in order to realize the solution's full potential. Each end user receives one hour of email-related security training per year. Ongoing solution management is 0.5 days per week.
- **External professional services and license costs totaled $209,448.** The company used professional services during the two-month deployment into production phase to assist with best practices and use case definition. License costs are $40,000 per year.

Forrester's interview with an existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $1.02 over three years versus costs of $518,000, adding up to a net present value (NPV) of $502,000 and an ROI of 97%.

Financial Summary



Benefits (Three-Year)



agari
by HelpSystems

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Agari Phishing Defense.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Agari Phishing Defense can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed Agari stakeholders and Forrester analysts to gather data relative to Agari Phishing Defense.

CUSTOMER INTERVIEW
Interviewed one organization using Agari Phishing Defense to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organization.

CASE STUDY
Employed four fundamental elements of TEI in modeling Agari Phishing Defense's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

agari by HelpSystems

The Agari Phishing Defense Customer Journey

BEFORE AND AFTER THE AGARI PHISHING DEFENSE INVESTMENT

Interviewed Organization

For this study, Forrester interviewed an Agari Phishing Defense customer. Key facts about the organization include:

- It's an international commercial bank with a US subsidiary.
- The organization has approximately 650 employees and 1,000 email accounts.
- The interviewee is the chief information security officer (CISO) of financial services.

Key Challenges

- **Prior solutions let too many malicious emails slip through.** Too many malicious emails were getting into end users inboxes with the previous solutions, some of which are still in place as part of a defense-in-depth strategy. Each additional email that gets through is a potential breach, and emails targeting C-level executives are especially dangerous.
- **Previous solutions did not integrate well enough with each other for an effective defense-in-depth solution.** Ease of integration was one of the biggest requirements for a new solution. Lack of integration made the previous solutions less effective, resulting in higher deployment and ongoing management costs.
- **The organization spent too much time manually investigating possible threats.** Previous solutions required two FTEs to monitor email, network, and workstation channels with email being the most labor-intensive. The team would have needed one additional FTE to manage the increasing workload.

> "We needed to build out a better defense-in-depth solution set for the email channel. Beyond better security, the most important things were ease of deployment, total cost of ownership (TCO), and integration with existing solutions."
>
> *CISO, financial services*

Key Results

The interview revealed that key results from the Agari Phishing Defense investment include:

- **Email-related security is better, which reduces the likelihood of a successful malicious attack.** Fewer malicious emails make it into an end user's inbox, which means fewer opportunities for user action to result in a breach. According to the Ponemon Institute, the average cost of a successful malicious attack was $4.45 million in 2019.[1]
- **The total cost of ownership is lower compared to both previous and other considered solutions.** The cost and effort to deploy Agari Phishing Defense (as well as the ongoing management) is considerably less than the other solutions considered. This frees up valuable resources — both time and money — to use on defending other attack vectors.

> "Agari blocks attacks based on the policies we have created. It is blocking things that were not blocked before by our other solutions."
>
> *CISO, financial services*

agari
by HelpSystems

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	More effective and efficient email security	$66,500	$133,000	$133,000	$332,500	$270,297
Btr	Faster deployment	$571,500	$0	$0	$571,500	$519,545
Ctr	Avoided threat intelligence program costs	$207,000	$27,000	$27,000	$261,000	$230,781
	Total benefits (risk-adjusted)	$845,000	$160,000	$160,000	$1,165,000	$1,020,623

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of more than $1.0 million.

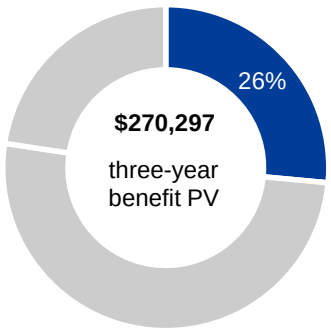
More Effective And Efficient Email Security

Improved email-related security was the most important benefit for the interviewed organization. The two critical measures were customer or employee data leakage and money being inappropriately transferred out of the bank. Agari Phishing Defense helps protect against these two threats. The interviewee said the following about improved security:

- "We have improved email security and policies, especially [against threats] around C-level impostors, which are particularly dangerous."
- "Agari helps manage security as well as compliance. We can develop our own policies based on compliance points. The cybersecurity landscape is evolving, and we need to evolve with it. Agari provides the agility to create new policies."
- "With Agari, we have a solution that helps us test each system we have in place. I test my own systems by sending malicious emails to myself. It's a red team approach."
- "If an email is blocked, it goes into a folder that the user is responsible for checking. We no longer receive complaints asking why something is blocked or [the location of an] email. We used to get complaints about our old solutions."

As discussed earlier, the average cost of a security breach due to a malicious attack was $4.45 million in 2019. The likelihood of a breach in any given year was 14.8%. Applying this likelihood makes the expected cost of a breach $658,600 per year in terms of lost business and remediation costs. These potential savings are not included in the financial analysis because it is not possible to say with certainty that a breach would be avoided and how much Agari Phishing Defense would contribute out of the entire security stack. Readers should take this benefit into consideration when calculating the possible total economic value of Agari Phishing Defense to their organizations.

Agari Phishing Defense also reduces the amount of security effort because companies can set custom policies, increase automation, and apply AI. With regards to less effort, the interviewed CISO said:



More effective and efficient email security: 26% of total benefits

agari
by HelpSystems

- "It takes less effort to look into suspicious activities and false positives. I previously had two FTEs monitoring email, network, and workstation channels. Most of their effort was around email. Now those resources can focus more of their time on networks and workstations."
- "If we hadn't adopted Agari, we would have had to hire someone else onto the team."
- "Previously, we spent a lot of time searching for emails when something was blocked. There was no tracking in place to find all instances."

For the financial analysis, Forrester makes the following assumptions:

- Only the efficiencies portion of the benefit are included.
- One additional FTE does not need to be hired halfway through the first year of the study.

This benefit will vary depending on the previous team size and spare capacity, as well as the level of automation and previous solutions in place. To account for these risks, Forrester adjusts this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $270,297.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

More Effective And Efficient Email Security: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
A1	Avoided additional hires	1 FTE*$140,000 [50% in Year 1]	$70,000	$140,000	$140,000
At	More effective and efficient email security	=A1	$70,000	$140,000	$140,000
	Risk adjustment	↓5%			
Atr	More effective and efficient email security (risk-adjusted)		$66,500	$133,000	$133,000

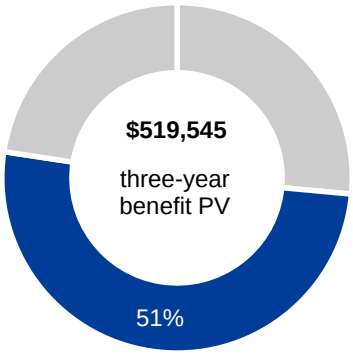
Faster Deployment

Implementing Agari Phishing Defense was easier because it easily integrates into other security solutions and email infrastructure. This saves effort and cost and, more importantly, it means that enhanced security solutions are up and running sooner. The interviewee said:

- "This took less time and effort than the other solutions we considered. The Agari project manager was very helpful in making sure this went smoothly and that we implemented and deployed properly."
- "Other solutions would have been challenging to implement because integration was very hard. The monitoring tool was natively integrated into anything. If I had to develop a separate API, it would have doubled the effort."

For the interviewed organization, Forrester assumes that:

- Implementing the other considered solutions would have required three FTEs and 11 months to complete.
- Implementation would have required $250,000 in external professional services.



Faster deployment: 51% of total benefits

agari by HelpSystems

This benefit will vary based on the considered solutions as well as how much professional services are required. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $519,545.

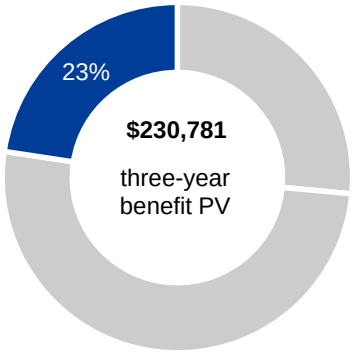
Faster Deployment: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
B1	Number of months		11		
B2	Number of FTEs		3.0		
B3	Monthly fully burdened cost	$140,000/12 months	$11,667		
B4	Internal effort	B1*B2*B3	$385,000		
B5	Professional services		$250,000		
Bt	Faster deployment	B4+B5	$635,000		
	Risk adjustment	↓10%			
Btr	Faster deployment (risk-adjusted)		$571,500		

Avoided Threat Intelligence Program Costs

The interviewee explained that with other solutions, the company would have needed to build a threat intelligence program that aggregated data from different sources. This would also have required added workflows and automation to achieve the same efficiencies. Instead, all of this is included in Agari Phishing Defense. It is estimated that solution components would cost $200,000 to $300,000 to build this with an annual maintenance of 15%. For the financial analysis, Forrester includes the low end of the range as well as the 15% annual maintenance cost.

This benefit will vary based on which solutions were already in place and what the company needed to add to replicate the capabilities built into Agari Phishing Defense. To account for these risks, Forrester adjusts this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $230,781.



Avoided threat intelligence program costs: 23% of total benefits

agari by HelpSystems

Avoided Threat Intelligence Program Costs: Calculation Table					
REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
C1	Avoided threat protection solution		$200,000		
C2	Maintenance	C1*15%	$30,000	$30,000	$30,000
Ct	Avoided threat intelligence program costs	C1+C2	$230,000	$30,000	$30,000
	Risk adjustment	↓10%			
Ctr	Avoided threat intelligence program costs (risk-adjusted)		$207,000	$27,000	$27,000

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Agari Phishing Defense and later realize additional uses and business opportunities. These can include rolling out Agari Phishing Defense to other lines of business and/or geographies and the ongoing definition of new policies to protect against different threat types.

Another possible benefit is integrating Agari Phishing Defense with other Agari solutions to achieve even better security. The interviewed organization is also using Agari's Domain-based Message Authentication, Reporting, and Conformance (DMARC) solution: Agari Brand Protection. The CISO said:

- "Even if a fraudulent email gets through, outgoing emails will be blocked. That's where Agari's demarcation solution kicks in."
- "Having demarcation and advanced threat protection from the same vendor is good. Agari has access to threat intelligence from approved domains such as Google. The more information sharing, the better the security."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A). These potential future benefits are not included in the financial analysis.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Dtr	Internal effort	$210,873	$39,373	$39,373	$39,373	$328,994	$308,789
Etr	External costs	$105,000	$42,000	$42,000	$42,000	$231,000	$209,448
	Total costs (risk-adjusted)	$315,873	$81,373	$81,373	$81,373	$559,994	$518,237

Internal Effort

The Agari Phishing Defense deployment consisted of the following phases, duration, and internal effort:

- POC: three months and two FTEs
- Moving to production and rolling out: two months and two FTEs
- Use case and policy refinement: two months and two FTEs

The Agari project manager cost was included in licenses that are covered in the next section.

Each user was provided with one hour of training on how to handle suspicious emails, and related training is repeated each year. The ongoing effort also includes 0.5 days per week managing the solution and refining use cases and policies. Costs will vary based on the size and complexity of the deployment and the required training. To account for these risks, Forrester adjusts this cost upward by 5%, yielding a three-year risk-adjusted total PV of $308,789.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of more than $518 thousand.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Internal Effort: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	POC	3 months*2 FTEs*$10,833	$70,000			
D2	Rollout	2 months*2 FTEs*$10,833	$46,667			
D3	Use case and policy refinement	2 months*2 FTEs*$10,833	$46,667			
D4	Training	1 hour*650 employees*$57.69	$37,499	$37,499	$37,499	$37,499
D5	Ongoing solution management	0.5 days*52 weeks*$538.46		$14,000	$14,000	$14,000
Dt	Internal effort	D1*D2*D3*D4	$200,832	$37,499	$37,499	$37,499
	Risk adjustment	↑5%				
Dtr	Internal effort (risk-adjusted)		$210,873	$39,373	$39,373	$39,373

agari by HelpSystems

External Costs

External costs included professional services during deployment (in addition to the Agari project manager described above) and license fees. The professional services helped ensure that the organization put best practices in place and accurately defined the initial use cases and policies.

License costs are based on the number of email accounts. Readers are encouraged to work with their Agari account managers to understand what their license costs would be.

These costs will vary based on the number of email accounts and how many professional services are required because of deployment complexity or lack of internal resources. To account for these risks, Forrester adjusts this cost upward by 5%, yielding a three-year risk-adjusted total PV of $209,448.

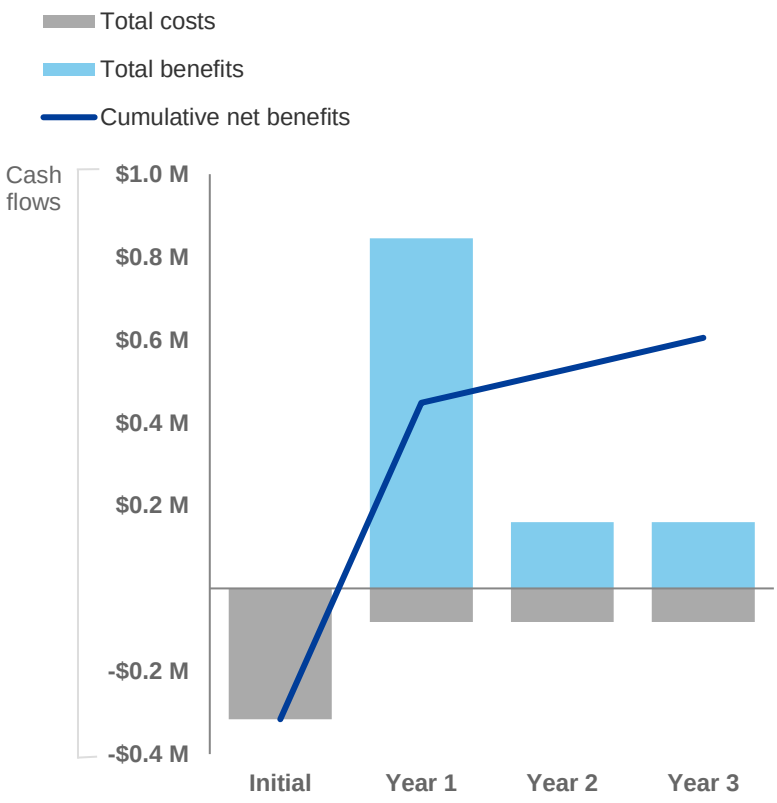
External Costs: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Professional services	1FTE*2 months*$50,000	$100,000			
E2	License fees			$40,000	$40,000	$40,000
Et	External costs	E1+E2	$100,000	$40,000	$40,000	$40,000
	Risk adjustment	↑5%				
Etr	External costs (risk-adjusted)		$105,000	$42,000	$42,000	$42,000

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the interviewed organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (risk-adjusted estimates)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($315,873)	($81,373)	($81,373)	($81,373)	($559,994)	($518,237)
Total benefits	$0	$845,000	$160,000	$160,000	$1,165,000	$1,020,623
Net benefits	($315,873)	$763,627	$78,627	$78,627	$605,006	$502,386
ROI						97%
Payback period (months)						<6

agari by HelpSystems

Agari Phishing Defense: Overview

The following information is provided by Agari. Forrester has not validated any claims and does not endorse Agari or its offerings.

Secure Your Employee Inboxes

Criminals continuously evolve their identity deception techniques, morphing from using display name deception to leveraging account takeovers. Today, more attacks involve compromised accounts, where cybercriminals can easily impersonate a trusted sender and evade perimeter controls.

Agari stops the email attacks that your existing secure email gateway misses. With over 100 million advanced attacks stopped, Agari Phishing Defense is the most effective and accurate phishing protection solution available today.

Depend On Trusted AI

Agari Phishing Defense takes a new approach to stopping email attacks, with the Agari Identity Graph at its core.

By using advanced machine learning techniques, internet-scale telemetry, and real-time data pipelines focusing on identity, behavior, and trust, the Agari Identity Graph continuously learns to stay ahead of emerging threats. By focusing on trust relationships to model the good, rather than searching for the bad, the Agari Identity Graph can block malicious emails — no matter where they originate.

Protect Against Insider Threats

With new insider impersonation protection technology, Agari Phishing Defense even protects against the threats that are hardest to detect: those originating from inside your organization. This new technology inspects all emails flowing from employee-to-employee as well as employee-to-external receiver for clues that an internal email account has been compromised for unauthorized use by a cybercriminal.

By inspecting internal email flow, Agari Phishing Defense prevents the spread of malicious emails from affected internal accounts laterally within a company and notifies the security operations center (SOC) of threats against customers or partners from employee inboxes.

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

agari by HelpSystems

Appendix B: Endnotes

[1] Source: “Cost of a Data Breach Report — 2019,” Ponemon Institute, August 2019.