FORRESTER®

The Total Economic Impact™ Of Mimecast

Cost Savings And Business Benefits Enabled By Mimecast

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY MIMECAST, JULY 2024

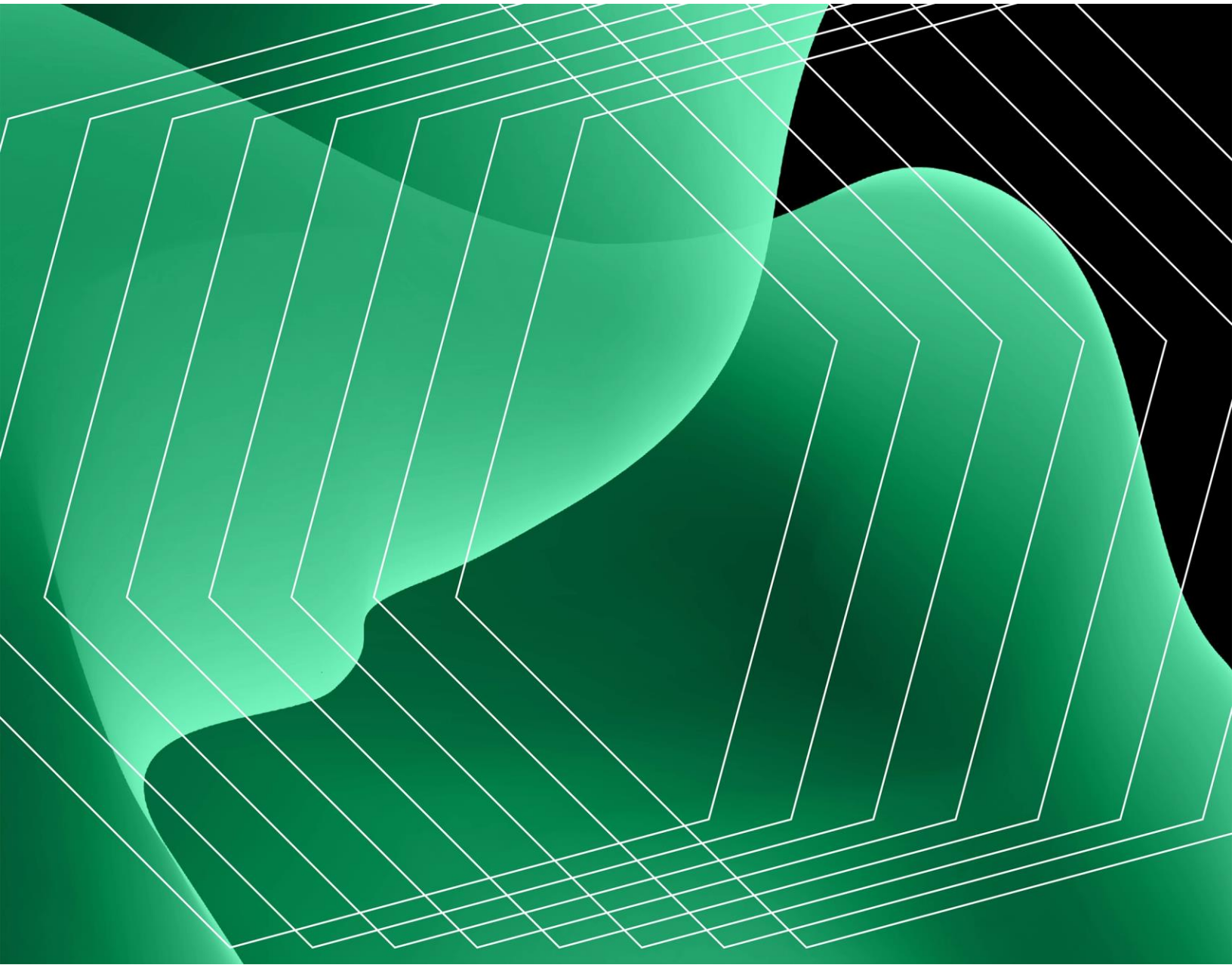


Table Of Contents

Consulting Team:

Andrew Nadler

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Organizations face an increasingly complex and uncertain cybersecurity threat landscape, with 78% of organizations experiencing at least one incident in the past 12 months and more than half of those organizations estimating the cost of an incident to exceed $1 million.[1] Email is still employees' most-used application and therefore remains a major inroad for attackers, allowing them direct access to end users.[2] Organizations using common cloud email infrastructure providers are turning to a layered approach with security solutions to protect the way they communicate and collaborate.[3] Using an enterprise email security solution such as Mimecast in tandem with native email security offerings can deliver greater efficacy and efficiencies than native-only email security alone while also reducing concentration risk and increasing reliability.[4]

Mimecast Advanced Email Security is an AI-powered, enterprise email security solution used to block email-based threats such as phishing, malware, and business email compromise (BEC) with flexible deployment methods that include Email Security Cloud Integrated, a cloud-native, API-enabled email security (CAPES) deployment; and Email Security Cloud Gateway, a secure email gateway (SEG) deployment. The Mimecast product suite also includes Email Archive and Security Awareness Training. Customers can further expand upon Advanced Email Security with support, services, and add-ons including DMARC Analyzer and Collaboration Security.

Mimecast commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Mimecast.[5] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Mimecast on their organizations.

Return on investment (ROI)
255%

Net present value
$1.53M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed seven representatives from six organizations with experience using Mimecast including both CAPES and SEG deployment methods. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. This composite is a global organization with 2,500 users it desires to protect with Mimecast as an extension of its native email infrastructure using Mimecast's Email Security Cloud Integrated deployment method.

Interviewees said that prior to using Mimecast, their organizations typically either used on-premises legacy solutions, other email security solutions, or simply native email security infrastructure. However, prior attempts yielded limited success, leaving them with challenges around email security efficacy, efficiency, and reliability.

After investing in Mimecast, the interviewees' organizations benefited from increased security efficacy, improved efficiencies for IT and security teams as well as end users, and overall business benefits from enhanced security.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Strengthened security against malicious emails.** The composite organization implements Mimecast to extend the efficacy of its native email platform and address email-based threats, including attacks designed to succeed with native email security infrastructure. Due to this increased efficacy, the composite organization avoids external attacks and the associated costs of breaches, such as fines, business disruptions, and revenue loss. Forrester used interviewee data and the 2023 Forrester Analytics Business Technographics Security Survey to calculate this value. Over three years, the strengthened security is worth $1.1 million to the composite organization.
- **Improved efficiency of security operations with 24% time savings addressing email-based attacks and 50% time savings on email platform management.** The composite organization's security and IT teams benefit from the security efficacy of Mimecast, its APIs and integrations, automation, and

> “We have had no breaches or any malicious attacks [with Mimecast].”
>
> **IT ADMINISTRATOR, HEALTHCARE**

more, allowing them to spend time on higher-value tasks. This time savings is based on the composite organization’s seven security employees and one IT employee productively reallocating 2,267 total hours per year as supported by survey and interviewee data. Over three years, this productivity benefit is worth $337,000 to the composite organization.

- **Improved efficiency of end users with 24% time savings on email-based attacks.** Given Mimecast’s efficacy, end users benefit from fewer unwanted and malicious emails in their inboxes, allowing them to use that time savings for more valuable tasks. Forrester calculates the value of this improved efficiency using survey and interviewee data with the composite organization’s 2,500 end users saving hours of productivity with each avoided incident. Over three years, this productivity benefit is worth $727,000 to the composite organization.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Business benefits, including reputation protection.** Via strengthened security with Mimecast, the composite organization reduces its chance of being compromised and therefore not only avoids the losses associated with breaches, including revenue losses, contract cancelations, and fines, but also protects its brand and reputation by avoiding unwanted email sends and negative publicity. In addition, Mimecast’s feature set, including DMARC Analyzer provides DMARC authentication monitoring for domains, helps the composite organization protect

its brand and email reputation even further by ensuring its domains are trusted, which increases customer trust and leads to potential email marketing-related benefits and revenue growth.

- **Mimecast services, support, and customer experience.** The composite organization takes advantage of Mimecast's services, enabling it to implement Mimecast more quickly. Additionally, it utilizes Mimecast's technical support to help it achieve its business outcome goals.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Licensing costs of $438,000.** In addition to paying a license fee per user per year for Mimecast, the composite organization purchases Advanced Support and Guided Implementation services; it also has the option to purchase add-ons.
- **Implementation, training, and ongoing management costs of $163,000.** After choosing to invest in Mimecast, the composite organization commits time to implement the email security solution, educate and train, and manage the solution on an ongoing basis.

The representative interviews and financial analysis found that a composite organization experiences benefits of $2.13 million over three years versus costs of $602,000, adding up to a net present value (NPV) of $1.53 million and an ROI of 255%.

Return on investment (ROI)

255%

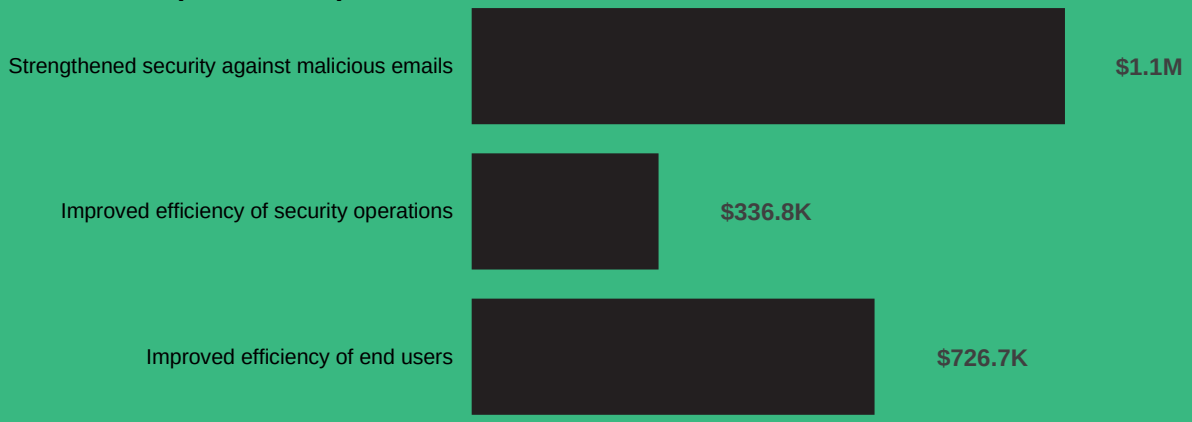
Benefits PV

$2.13M

Net present value (NPV)

$1.53M

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Mimecast.

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 Mimecast can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Mimecast and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Mimecast.

Mimecast reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Mimecast provided the customer names for the interviews but did not participate in the interviews.

1. **Due Diligence**
   Interviewed Mimecast stakeholders and Forrester analysts to gather data relative to Mimecast.
2. **Interviews**
   Interviewed seven representatives from six organizations using Mimecast to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **Financial Model Framework**
   Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.
5. **Case Study**
   Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Mimecast Customer Journey

Drivers leading to the Mimecast investment

Interviews			
Role	**Industry**	**Region**	**Users Protected**
SOC architect	Healthcare	Global	135,000
Head of infrastructure operations	Multi-industry	Middle East, Africa, and Asia	25,000
IT director, application administration	Food	Global	15,000
VP of IT	Education	North America	1,000
Infrastructure manager Security manager	Entertainment	Europe	400
IT administrator	Healthcare	North America	50

KEY CHALLENGES

Before Mimecast, interviewees' organizations typically either used an on-premises legacy solution, another email security solution, or native email security infrastructure. After facing common challenges, they chose to adopt Mimecast as an enterprise email security solution using either the SEG or CAPES deployment method, depending on their environments and needs.

The interviewees noted how their organizations struggled with common challenges, including:

- **Efficacy challenges with malicious and unwanted emails.** Interviewees told Forrester that the primary challenge they struggled with before Mimecast was the efficacy of their email security solutions. Furthermore, they said the volume of malicious and unwanted emails was only increasing. The SOC architect of a healthcare organization explained: "Phishes were a nightmare. Nothing was detected, and the phishing emails were delivered. … URL detection was not good, [either]." Similarly, the head of infrastructure operations for a multi-industry

organization said, “We had incidents that [our prior] email security solution couldn’t detect.”

> “Email is a big threat for cybersecurity.”
>
> IT DIRECTOR, APPLICATION ADMINISTRATION, FOOD

- **Security teams burdened by inefficient tools.** In addition to efficacy challenges with malicious and unwanted emails, interviewees said their organizations’ IT and security teams experienced challenges with working efficiently. They discussed excessive time spent investigating malicious and unwanted emails, inefficient email security management, insufficiently granular access for managing email and policies, inadequate integrations, and more.
- **Reliability challenges with outages, delayed emails, and a lack of support.** Furthermore, interviewees shared how their organizations faced reliability-related challenges. They told stories of outages and a lack of support in the face of them. The head of infrastructure operations for a multi-industry organization said: “We had outage issues. Sometimes we were getting emails delayed. They also lacked proactiveness and support.” Using Mimecast’s Mailbox Continuity add-on with a SEG deployment, the IT director, application administration, at a food organization added: “Email continuity is big. I now use Mimecast to continue my email flow.”

> “Email is the first vector of attack in any company. We want to have two layers to be able to do defense in depth.”
>
> SOC ARCHITECT, HEALTHCARE

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Provide effective, cloud-based, and cost-efficient security against malicious and unwanted emails in tandem with their native email security infrastructure.
- Offer both CAPES and SEG deployment methods, depending on their organizations' needs.
- Meet more than just their email security needs by offering desired features and other products for information archiving, security awareness and training (SA&T), and more.
- Offer ease-of-use and management with a single pane of glass and sufficient granularity.
- Be supported by a vendor they trusted.

> "We had a strong recommendation from our information security team. … [With our use of a common email platform], … they recommended going for a third-party solution [like Mimecast]."
>
> HEAD OF INFRASTRUCTURE OPERATIONS, MULTI-INDUSTRY

Market Overview

Enterprise Email Security

Forrester defines **enterprise email security** as technologies that protect organizations' email communications in order to mitigate and lessen the impact of email-borne attacks. These consist of on-premises or cloud-based email gateways and solutions that integrate with cloud-based email infrastructure. Capabilities include antispam, antimalware, antiphishing, data loss prevention (DLP), encryption, phishing education, business email compromise (BEC) and spoofing protection, malicious URL detection, and email authentication.[6]

Email infrastructure providers supply organizations with their core email infrastructure, along with APIs that allow other enterprise email security solutions to supplement built-in security features with additional capabilities.[7]

Secure email gateway (SEG) solutions sit in front of an email infrastructure provider or in front of on-premises email infrastructure.[8]

Cloud-native API-enabled email security (CAPES) solutions integrate with email infrastructure providers to extend their native security capabilities.[9]

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the six interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a global business with 2,500 employees. This includes seven FTEs managing security incidents and one FTE

managing email. Before Mimecast, it relied solely on native email security infrastructure and desired to add a CAPES solution to extend the functionality and security efficacy of its native email infrastructure provider. It is the customer of a cloud-based productivity platform.

Deployment characteristics. The composite organization begins using Mimecast in Year 1, following an implementation period. It chooses Mimecast's Email Security Cloud Integrated deployment method. This implementation covers 100% of all 2,500 employees across all geographies.

Key Assumptions

Mimecast Email Security Cloud Integrated deployment method

2,500 users protected with Mimecast

> "My team compared [Mimecast] with [other email security] solutions last month. They said Mimecast is still better."
>
> IT DIRECTOR, APPLICATION ADMINISTRATION, FOOD

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Strengthened security against malicious emails	$430,166	$430,166	$430,166	$1,290,499	$1,069,760
Btr	Improved efficiency of security operations	$135,443	$135,443	$135,443	$406,328	$336,826
Ctr	Improved efficiency of end users	$292,205	$292,205	$292,205	$876,616	$726,671
	Total benefits (risk-adjusted)	$857,814	$857,814	$857,814	$2,573,443	$2,133,257

STRENGTHENED SECURITY AGAINST MALICIOUS EMAILS

Evidence and data. Interviewees confidently told Forrester that using Mimecast along with their native email security infrastructure strengthened their organizations' security against malicious emails as compared to their prior environments. With email as a key threat vector, they said Mimecast is a first line of defense (in conjunction with their native email security infrastructure) to block external attacks.

- Interviewees said the likelihood of experiencing a breach was high and increasing. Furthermore, they explained how breaches were costly. For example, the SOC architect of a healthcare organization detailed the cost of BEC specifically: "We are doing a great job with impersonation protection [with Mimecast], which is [valuable] to our company because we have seen cases in the past where it costs us several thousand euros." They added: "If we speak about bad attachments, that's where the more massive impact [of a potential breach] could be. We leverage Mimecast to ban a lot of extensions." They also explained the further impacts of a potential breach, saying: "[It could] impact production, delivery, and pharmacovigilance, which is one of our core activities. We need to be available and reachable by hospitals and truck deliveries 24/7 in

case there is a problem. We migrated all our pharmacovigilance activity to Mimecast to ensure the continuity of this activity because this activity can never stop."

- When considering their organizations' primary threat vectors for attacks, interviewees pointed to email. The security manager of an entertainment organization said: "The main surface for attack is email. The initial way [external attackers] approach organizations is always email now." Similarly, the VP of IT for an education organization said, "[Email] is our biggest point of contact internally and with vendors."

> "Social engineering is the number one way that attackers get in. Mimecast is critical to preventing social engineering."
>
> **VP OF IT, EDUCATION**

- Furthermore, interviewees highlighted how their use of common email platforms could increase their threat vector, too. The SOC architect of a healthcare organization added: "We want defense in depth. We need two solutions [including our native email security infrastructure]. Mimecast is doing a wonderful first layer of filtering."
- Interviewees also discussed how Mimecast achieved efficacy as an email security solution given the substantial risk of email-based external attacks and common email platforms. They highlighted phishing protection, defense against BEC, malware protection, and more. The VP of IT for an education organization explained: "They're that first outside line of defense, stripping malware, blocking phishing attempts, catching [content] coming in or going out, and correcting bad behavior. Mimecast automates the vast majority of it and yet gives us control

over the pieces that we care about to be able to have a second set of eyes review them. It's that first line of defense."

- The SOC architect of a healthcare organization emphasized the customizability of Mimecast as a key reason for increased efficacy, saying, "Mimecast filters threats at several detection layers and allows a lot of customization."

> "Mimecast [and native email security infrastructure together] is better."
>
> SECURITY MANAGER, ENTERTAINMENT

- Overall, interviewees spoke highly of Mimecast's efficacy. The IT director, application administration, at a food organization said, "We have not had a breach because of email." The SOC architect of a healthcare organization said, "We have seen a huge decrease in bad URLs delivered to inboxes." The security manager of an entertainment organization said, "We don't see any evidence of malware coming in by email at all [with Mimecast], and we do look." The head of infrastructure operations for a multi-industry organization said: "[Mimecast] is giving a lot of value because it is protecting from a lot of malicious attacks and malware. ... It is better than our previous solution." They added: "Blocking is almost 100%."
- The IT administrator of a healthcare organization said: "The value has been the control of malicious communication coming into my environment. … I've had zero attacks come through."
- Furthermore, interviewees said that Mimecast's efficacy, powered by AI, has only improved over time. The IT administrator of a healthcare organization explained:

"These definitions become better and better. The environment is getting stronger every day. … It has provided us with a safety net. We've had zero breaches."

> "The value of Mimecast is less administrative hassles and more protection."
>
> HEAD OF INFRASTRUCTURE OPERATIONS, MULTI-INDUSTRY

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization's likelihood of experiencing one or more breaches per year is 72%.[10]
- The composite organization's mean cumulative cost of breaches is $2,892,000.[11]
- The percentage of breaches involving external attacks is 49%.[12]
- The portion of external attacks addressable with email, such as phishing and social engineering, is 50%.
- The composite organization reduces its risk of an external attack, addressable with email, by 99% due to Mimecast's efficacy as detailed by interviewees.

Risks. This benefit may vary based on:

- The likelihood of a breach and the mean cumulative cost of breaches. This may vary by industry, geography, organization size, prior environment, and other factors.
- The sophistication and efficacy of solutions and processes in an organization's prior environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.1 million.

99%

Efficacy of Mimecast on external attacks

"Ninety-nine percent of [malicious and unwanted emails] are caught right away. … I am sure it is even higher than 99%."

VP OF IT, EDUCATION

Strengthened Security Against Malicious Emails					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Likelihood of experiencing one or more breaches per year	Forrester's Security Survey, 2023 Base: 335	72%	72%	72%
A2	Mean cumulative cost of breaches	Forrester's Security Survey, 2023 Base: 237	$2,892,000	$2,892,000	$2,892,000
A3	Percentage of breaches involving external attacks	Forrester's Security Survey, 2023 Base: 830	49%	49%	49%
A4	Addressable portion of external attacks with email	Forrester research	50%	50%	50%
A5	**Subtotal: Annual risk exposure addressable with Mimecast**	**A1*A2*A3*A4**	**$511,190**	**$511,190**	**$511,190**
A6	Efficacy of Mimecast on external attacks	Interviews	99%	99%	99%
At	Strengthened security against malicious emails	A5*A6	$506,078	$506,078	$506,078
	Risk adjustment	↓15%			
Atr	Strengthened security against malicious emails (risk-adjusted)		$430,166	$430,166	$430,166
	Three-year total: $1,290,499		**Three-year present value: $1,069,760**		

IMPROVED EFFICIENCY OF SECURITY OPERATIONS

Evidence and data. Interviewees told Forrester how Mimecast helped improve the efficiency of their organizations' security and IT functions. They explained how Mimecast's automation and the strengthened security against malicious emails saved time reviewing emails and addressing email-based external attacks. Security team members could then use this time savings addressing other risks. For IT teams, interviewees said Mimecast's integrations and APIs, automation, and overall design led to fewer support needs, fewer administrative tasks, and general email management efficiency gains, which allowed teams to spend time on higher-value IT tasks.

- The security manager of an entertainment organization said: "We don't have to expend any time on email issues. If we do, it's a 5-minute check in Mimecast, and we're done. The old process would have been much more manual, relying on the user to inform and report, staff to pick that ticket up, check the content, do research on the email, and then manually add it to a block list." They continued:

"Having the low-level stuff all automatically dealt with by Mimecast leaves the higher-level stuff for us to deal with. ... Mimecast has done all that in the background, and all it will do is alert the user."

- The head of infrastructure operations for a multi-industry organization detailed how their team gained productivity with Mimecast: "[First], Mimecast is doing proactive checks in terms of availability. Second, there are not many email incidents, so you don't have to get into any P1 or P2 issues. ... There is a lot of time [we're] saving on administrative tasks, which is much easier on Mimecast compared to [before]."

> "We spent a lot of time administering [previously], but after one year of Mimecast, I do not see a lot of issues. [We are] completely streamlined."
>
> **IT DIRECTOR, APPLICATION ADMINISTRATION, FOOD**

- The SOC architect of a healthcare organization noted how Mimecast's APIs and integrations led to greater efficiency: "[With Mimecast's APIs] our analysts ... can act directly from the source to restrict users, restrict partners, and change file types. … All these operations have eased with Mimecast. We have done a lot of integration to ease the lives of my colleagues, saving their time. We also have shared services that do the incident response at night and on weekends, for example, and they are not necessarily familiar with the Mimecast console itself. So [the integrations] are abstracting all these layers of complexity."
- The security manager of an entertainment organization discussed the value of this productivity gain: "We are a tech company. We do bleeding-edge

development, and we need time spent supporting [our developers] and not worrying about [email]."

> "We see a reduced necessity for our team's time [because of Mimecast]."
>
> SECURITY MANAGER, ENTERTAINMENT

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization has seven security FTEs who manage security incidents and one IT FTE who manages email platforms.
- Due to the efficacy of Mimecast on email-based external attacks, the security FTEs save time addressing email-based attacks.
- The IT FTE saves time managing Mimecast compared to the composite organization's prior environment.
- The fully burdened annual salary for a security analyst is $141,750, and the fully burdened annual salary for an IT manager is $125,688.
- Fifty percent of the time saved by both roles is recaptured in productive work.

Risks. This benefit may vary based on:

- The time an organization's security FTEs save on email-based external attacks given an organization's characteristics, prior environment, and risk profile.
- The number of team members engaged in this work, their roles and associated fully burdened annual salaries, and the ability of the team members to reallocate any time savings to productive work.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $337,000.

50%

Time saved on email platform management due to Mimecast

"Most of [our email platform management] in [Mimecast] can be done in less than a quarter of the time it would take [previously]."

VP OF IT, EDUCATION

Improved Efficiency Of Security Operations					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Security FTEs managing security incidents	Composite	7	7	7
B2	SecOps time saved addressing email-based attacks due to Mimecast	A3*A4*A6	24%	24%	24%
B3	Security operations analyst fully burdened salary	TEI standard	$141,750	$141,750	$141,750
B4	Productivity recapture rate	TEI standard	50%	50%	50%
B5	**Subtotal: Avoided email-based incident investigation and remediation cost**	**B1*B2*B3*B4**	**$119,070**	**$119,070**	**$119,070**
B6	FTEs managing email	Composite	1	1	1
B7	Time saved on email platform management due to Mimecast	Interviews	50%	50%	50%
B8	IT manager fully burdened salary	TEI standard	$125,688	$125,688	$125,688
B9	Productivity recapture rate	TEI standard	50%	50%	50%
B10	**Subtotal: Email administration productivity gain**	**B6*B7*B8*B9**	**$31,422**	**$31,422**	**$31,422**
Bt	Improved efficiency of security operations	B5+B10	$150,492	$150,492	$150,492
	Risk adjustment	↓10%			
Btr	Improved efficiency of security operations (risk-adjusted)		$135,443	$135,443	$135,443
	Three-year total: $406,328			**Three-year present value: $336,826**	

IMPROVED EFFICIENCY OF END USERS

Evidence and data. Besides improving the efficiency of their organizations' security operations, interviewees also told Forrester how Mimecast helped improve end-user efficiency. Interviewees explained how end users received fewer malicious emails and thereby experienced fewer incidents, avoiding stretches of unproductive time. Additionally, end users received fewer unwanted emails, enabling email management time savings. Interviewees also noted how end users could self-release emails with Mimecast and how they submitted fewer tickets with Mimecast, saving time for all parties. For end users, all these time savings meant more time spent on relevant business-outcome-related emails or other productive work.

- The IT director, application administration, at a food organization said: "[Our end users] have the capability to release emails. They don't need to create a ticket."

Relatedly, the head of infrastructure operations for a multi-industry organization said, “Altogether related to email archival or security, we’ve reduced our tickets by more than 50% to 60%.”

- The VP of IT of an education organization said: “From an end-user standpoint, their email volume has been cut by at least 40%. ... Whatever time they’re spending going through their inbox, 40% of that time has been recouped.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization has 48,987 security incidents per year.[13]
- End users lose 3.4 hours of productivity per incident due to email attacks.[14]
- Due to the efficacy of Mimecast on email-based external attacks, end users avoid hours of lost productivity.
- The average fully burdened hourly rate for an average end user is $43.[15]
- The composite’s end users reallocate 20% of any time savings to productive work.

Risks. This benefit may vary based on:

- The number of security incidents per year depending on the size of an organization, its industry, its risk profile, and other factors.
- The amount of lost productive time per end user.
- The proportion of incidents that are external attacks and/or are addressable via email security solutions.
- The fully burdened hourly rates of the end users and their ability to reallocate any time savings to productive work.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $727,000.

24%

End-user time savings on email-based specific attacks

"Whether they're junk advertisements or whether they're malicious, [Mimecast] is stopping [them]. … Every one of those emails represents [time]."

SECURITY MANAGER, ENTERTAINMENT

Improved Efficiency Of End Users					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Security incidents at the composite organization per year	Forrester custom research	48,987	48,987	48,987
C2	Lost end-user productivity per year, per incident due to email attacks (hours)	Forrester custom research	3.4	3.4	3.4
C3	Time savings on email-based specific attacks	A3*A4*A6	24%	24%	24%
C4	Average end-user fully burdened cost per hour	US Bureau of Labor Statistics, December 2023	$43	$43	$43
C5	Productivity recapture rate	TEI standard	20%	20%	20%
Ct	Improved efficiency of end users	C1*C2*C3*C4*C5	$343,771	$343,771	$343,771
	Risk adjustment	↓15%			
Ctr	Improved efficiency of end users (risk-adjusted)		$292,205	$292,205	$292,205
	Three-year total: $876,616			**Three-year present value: $726,671**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Business benefits, including reputation protection.** Driven by strengthened security and Mimecast's feature set, including DMARC Analyzer, interviewees told Forrester about broader business benefits, including brand and reputation protection, even if they couldn't quantify the value. Overall, cybersecurity contributes to firms' abilities to generate revenue.[16] The IT director, application administration, at a food organization detailed, "If somebody sends an email with our name ... it's a reputation problem." They added: "[Mimecast] protects our brand by not sending that email because we interact with millions of customers. It gives us the reputation of securing our outgoing email."

  The SOC architect of a healthcare organization explained the customer trust benefits of DMARC and BIMI: "Thanks to Mimecast, we have implemented DMARC and BIMI [Brand Indicators for Message Identification]. … [BIMI's verified logo or graphic] will engage our customers to open more emails."[17]

- **Mimecast services, support, and customer experience.** Interviewees highlighted the value of Mimecast's professional and managed services, support offerings, and its commitment to customer experience. The SOC architect of a healthcare organization said, "They are listening to our feedback." The security manager of an entertainment organization said: "The support is good. You have to make sure you use them." The IT administrator of a healthcare organization added, "They went out of their way, customer service-wise."

> "[Mimecast's] support is excellent. They are ready to go anytime for anything."
>
> IT DIRECTOR, APPLICATION ADMINISTRATION, FOOD

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Mimecast and later realize additional uses and business opportunities, including:

- **Driving greater security efficacy across products with threat sharing.** Not only did interviewees discuss strengthened security but they also described using Mimecast's APIs and integrations to share threat knowledge between Mimecast and other security solutions. By easily sharing data between solutions, interviewees said their organizations could realize greater security efficacy than using solutions individually, further reducing risk while deriving greater value from all their security investments. In addition to increased efficacy, Mimecast's integrations could drive increased efficiency across solutions, too.

> "I feed information or alerts from Mimecast to my security and my SIEM solution, and vice versa, so my SIEM solution can see the information coming from Mimecast and use it when it's deciding if an activity is malicious."
>
> SECURITY MANAGER, ENTERTAINMENT

- **Expanded functionality protecting people and data.** Interviewees told Forrester about how their organizations could also mitigate human risk and safeguard data in addition to protecting email and collaboration.

  Using Mimecast as an information archiving platform with Email Archive helped interviewees' organizations preserve email data in the long term and enable efficiencies in conducting e-discovery and other investigations.[18] For e-discovery, the VP of IT for an education organization shared, "What would have been 4 to 6 hours for a single person, we can do in 15 minutes." Relatedly, the SOC architect for a healthcare organization said, "Mimecast is much faster to retrieve end-user messages and mailboxes." The IT director, application administration, at a food organization noted, "I have strong protection that nobody is deleting email without my consent."

  Interviewees also discussed using Mimecast as a human risk management (HRM) solution with Security Awareness Training. HRM solutions can help organizations detect human security behaviors and the risks they pose, protect humans at scale, and integrate human risk into total cyber risk while breaking down silos.[19] The VP of IT for an education organization said, "The cyber awareness has been a huge benefit." They continued, "For those that have taken the training, we've seen very positive feedback and acknowledgment that they have changed some of their behaviors based on those trainings."

- **The ability to scale quickly.** Interviewees from organizations ranging from small businesses to enterprises expressed confidence in Mimecast's ability to scale with them as their organizations expanded, regardless of deployment method. The IT administrator of a healthcare organization explained that as their business grows, "I'm going to be able to onboard as many people to [Mimecast] as [I need to]."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> "[Mimecast] scales easily."
>
> SECURITY MANAGER, ENTERTAINMENT

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Licensing	$1,650	$175,533	$175,533	$175,533	$528,248	$438,173
Etr	Implementation, training, and ongoing management	$6,732	$63,015	$63,015	$63,015	$195,776	$163,440
	Total costs (risk-adjusted)	$8,382	$238,547	$238,547	$238,547	$724,023	$601,613

LICENSING

Evidence and data. The primary cost for interviewees' organizations was the fee for Mimecast. It was based on the number of users and the selected plan's cost per user, in addition to any purchased add-ons, professional or managed services, and support.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization selects Mimecast's Comprehensive Defense Plan for its 2,500 users.
- It purchases a Guided Implementation service initially and then purchases Advanced Support for all three years.

Risks. This cost may vary based on:

- The number of users an organization desires to protect with Mimecast.
- The selected plan and the associated cost per user.
- The add-ons, services, and support an organization chooses to purchase.
- Pricing may vary. Contact Mimecast for additional details.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $438,000.

> "[Mimecast's support] is brilliant value."
>
> INFRASTRUCTURE MANAGER, ENTERTAINMENT

Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Licensing	Mimecast	$1,500	$159,575	$159,575	$159,575
Dt	Licensing	D1	$1,500	$159,575	$159,575	$159,575
	Risk adjustment	↑10%				
Dtr	Licensing (risk-adjusted)		$1,650	$175,533	$175,533	$175,533
	Three-year total: $528,248			**Three-year present value: $438,173**		

IMPLEMENTATION, TRAINING, AND ONGOING MANAGEMENT

Evidence and data. Some interviewees said their organizations could implement Mimecast in as little as one day or one week with the Email Security Cloud Integrated deployment method. The implementation length depended on their organization's scale and complexity, prior states, chosen deployment methods, and purchased add-ons. Other interviewees, including those using the Email Security Cloud Gateway deployment method, described multimonth proofs of concept (POCs) and ramp-up periods as their organizations methodically migrated domains and user groups. Regardless of organization size and complexity, interviewees described the

implementation process as smooth and easy, particularly with Mimecast's support and services.

Post-implementation, interviewees said ongoing labor requirements were minimal. They discussed training, planning sessions with Mimecast, and general administration, which could include troubleshooting and threat and policy management.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization initially allots 90 hours to implement Mimecast, train the team, and prepare training materials for end users.
- After implementation, the composite organization's team averages 1 hour per week on Mimecast administration, threat and policy management, ongoing training, troubleshooting, and planning.
- The composite company chooses to educate its end users on email security best practices. It averages 30 minutes per user per year.
- The average fully burdened hourly rate for a security operations analyst is $68.
- The average fully burdened hourly rate for an end user is $43.

Risks. This cost may vary based on:

- The duration of the implementation, the activities involved, the hours required, the number of team members involved, and the associated roles and fully burdened hourly rates of those team members.
- The activities an organization engages in post-implementation, the hours required for those activities, the number of team members required, and the associated roles and fully burdened hourly rates of those team members.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $163,440.

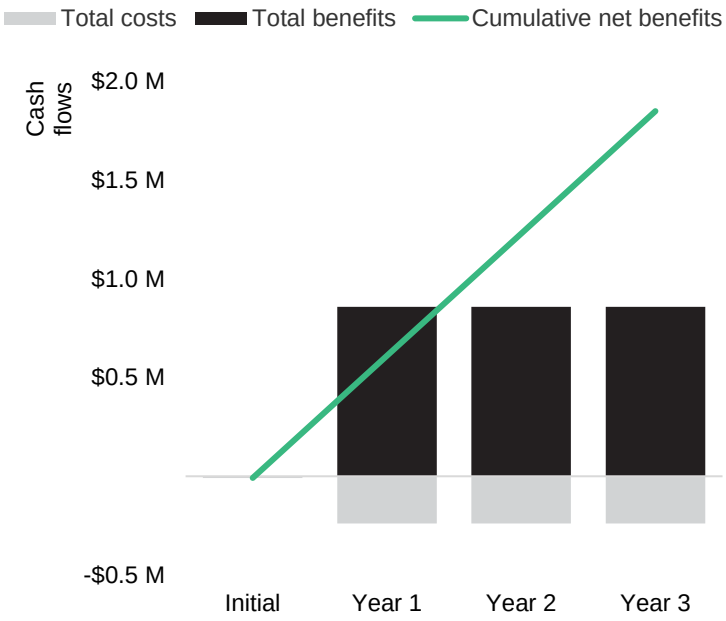
> "[Implementing Mimecast] was a very smooth process."
>
> IT DIRECTOR, APPLICATION ADMINISTRATION, FOOD

Implementation, Training, And Ongoing Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Implementation and initial training (hours)	Interviews	90	0	0	0
E2	Administration, threat and policy management, ongoing training, troubleshooting, and planning (hours)	Interviews	0	52	52	52
E3	End-user best practice training and education (hours)	Composite	0	1,250	1,250	1,250
E4	Security operations analyst fully burdened cost per hour	TEI standard	$68	$68	$68	$68
E5	Average end-user fully burdened cost per hour	C4	$43	$43	$43	$43
Et	Implementation, training, and ongoing management	((E1+E2)*E4)+(E3*E5)	$6,120	$57,286	$57,286	$57,286
	Risk adjustment	↑10%				
Etr	Implementation, training, and ongoing management (risk-adjusted)		$6,732	$63,015	$63,015	$63,015
	Three-year total: $195,776			**Three-year present value: $163,440**		

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 composite 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)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($8,382)	($238,547)	($238,547)	($238,547)	($724,023)	($601,613)
Total benefits	$0	$857,814	$857,814	$857,814	$2,573,443	$2,133,257
Net benefits	($8,382)	$619,267	$619,267	$619,267	$1,849,420	$1,531,644
ROI						255%

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."

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.

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.

APPENDIX B: SUPPLEMENTAL MATERIAL

Related Forrester Research

What 2023's Most Notable Breaches Mean For Tech Execs, Forrester Research, Inc., May 31, 2024

Collaborate With Security To Select Trustworthy Tech, Forrester Research, Inc., March 1, 2024

Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2023, Forrester Research, Inc., February 28, 2024

The Tech Exec's Guide To The Top Cyberthreats, 2023, Forrester Research, Inc., November 28, 2023

The Forrester Wave™: Security Awareness And Training Solutions, Q1 2022, Forrester Research, Inc., March 16, 2022

The Business Case For Privacy And Data Protection, Forrester Research, Inc., August 2, 2021

APPENDIX C: ENDNOTES

[1] Source: Top Cybersecurity Threats In 2024, Forrester Research, Inc., April 5, 2024.

[2] Source: The Enterprise Email Security Landscape, Q1 2023, Forrester Research, Inc., February 3, 2023.

[3] Source: The Forrester Wave™: Enterprise Email Security, Q2 2023, Forrester Research, Inc., June 12, 2023.

[4] Source: The CISO's Guide To Microsoft Investments, Forrester Research, Inc., September 28, 2023.

[5] 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.

[6] Source: Forrester Glossary, Forrester Research, Inc.

[7] Source: Now Tech: Enterprise Email Security Providers, Q3 2020, Forrester Research, Inc., July 14, 2020

[8] Ibid.

[9] Ibid.

[10] Source: Security Survey, 2023, Forrester Research, Inc., October 2023.

[11] Ibid.

[12] Ibid.

[13] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[14] Ibid.

[15] Source: US Bureau of Labor Statistics, December 2023

[16] Source: Top Recommendations For Your Security Program, 2024, Forrester Research, Inc., March 4, 2024.

[17] Source: Bolster Brand Resilience With DMARC, Forrester Research, Inc., August 27, 2021; Jess Burn, Apple's BIMI Support = Time To Get Serious About DMARC Enforcement, Forrester Blogs, September 19, 2022.

[18] Source: The Information Archiving Platforms Landscape, Q2 2024, Forrester Research, Inc., April 3, 2024.

[19] Source: The Human Risk Management Solutions Landscape, Q1 2024, Forrester Research, Inc., March 18, 2024.

FORRESTER®