A Forrester Total Economic Impact™
Study Commissioned By Echoworx
March 2019

The Total Economic Impact™ Of Echoworx OneWorld Encryption

Cost Savings And Business Benefits Enabled By OneWorld Encryption

FORRESTER®

Table Of Contents

Project Director:
David Park

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.

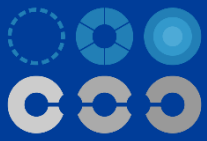
FORRESTER®

Key Benefits

Increased digital delivery of secure documents:
$1,500,751

Slashed costs of on-premises, legacy encryption solution:
$793,893

Reduction in email encryption-related call center tickets:
$318,939



Eliminated cost of custom email domain branding:
$67,145

Executive Summary

Email encryption has become one of the most popular data security technologies, thanks to compliance requirements. In fact, 41% of client security decision makers now say their firms have implemented or are implementing email encryption. More recently, however, organizations are recognizing other benefits of email encryption, including the ability to enhance security, heighten customer experience, and accelerate digital transformation. These use cases will continue to contribute to email encryption's popularity beyond compliance-driven mandates.[1]

Echoworx is a dedicated provider of email encryption services that allow organizations to encrypt both inbound and outbound emails in multiple delivery formats at scale. Echoworx commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying OneWorld Encryption. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of OneWorld Encryption on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with years of experience using OneWorld Encryption. Prior to engaging Echoworx, interviewed organizations typically relied on a combination of encryption native to their email clients and point solutions that solved for specific needs or use cases but did not scale well with increasing email volume or the growing needs of a diverse clientele. For these organizations, Echoworx provided not only the physical infrastructure and encryption features they needed, but also the support required to run an encryption program that could seamlessly integrate with users' day-to-day activities.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Increased digital delivery of secure documents by 10%.** While the delivery of secure documents digitally versus through traditional mail has continued to grow organically, organizations found that OneWorld Encryption accelerated this growth by offering a superior customer experience and by garnering traction with an increasing number of business lines within the organization. Organizations saved $1 per paper document delivered digitally instead, accumulating to a three-year cost savings PV of $1,500,751.
- **Slashed costs of on-premises, legacy encryption solutions.** By using OneWorld Encryption to replace on-premises legacy encryption solutions, organizations could retire the full software cost of their previous solutions. Because OneWorld Encryption could be hosted as a software-as-a-service (SaaS) solution within Echoworx's own data centers, organizations avoided additional physical server purchases and could forego the cost of paying for systems and security administrators to manage the encryption hardware and software. The associated three-year cost savings totaled a PV of $793,893.

FORRESTER®

ROI
155%

Benefits PV
$2.7 million

NPV
$1.6 million

Payback
7 months

- **Reduced email encryption-related call center tickets by 80%.** Both internal users and customers found OneWorld Encryption intuitive and easy to use for self-service. As a result, most tier 1 encryption-related support tickets, which made up the bulk of organizations' support requests, could be addressed without the need for a call center agent. Additionally, organizations could route more difficult support requests directly to Echoworx for remediation. The resulting three-year cost savings totaled a PV of $318,939.
- **Eliminated cost of custom email domain branding.** Organizations could avoid paying a third party for domain customization of their individual brands by engaging the Echoworx team to produce unique branding experiences for individual email domains. Over three years, the ensuing cost savings amounted to a PV of $67,145.

Unquantified benefits. The interviewed organizations experienced the following benefits from OneWorld Encryption, which are not quantified for this study:

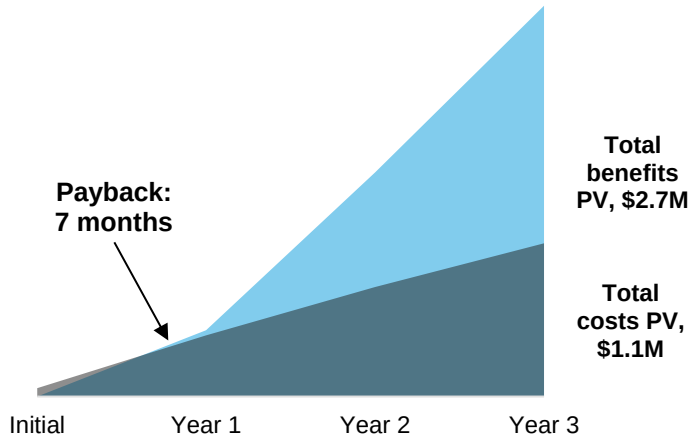
- Enhanced customer experience.
- Digital customer onboarding.
- Reduced downtime.

Costs. A composite organization, based on the combined characteristics of organizations interviewed for this study, experienced the following risk-adjusted PV costs over the three-year analysis:

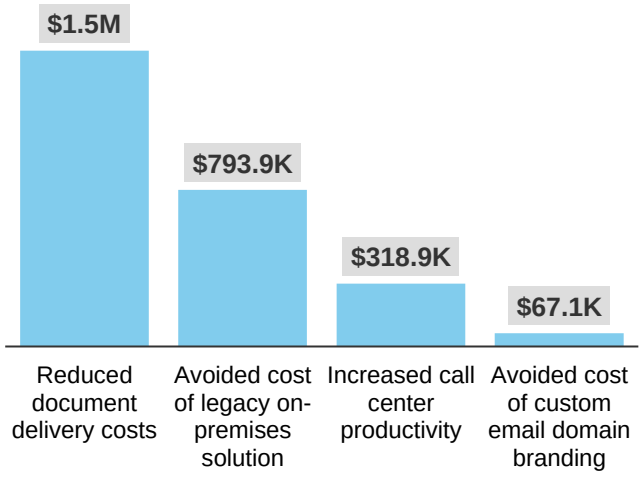
- **Echoworx fees**, including setup fees and license fees, which account for initial data migration and server setup, support and maintenance, and ongoing managed services, reached a PV of $996,241.
- **Deployment costs** as a result of labor required for planning and implementation totaled a PV of $54,912.

Forrester's interviews with three existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $2.7 million over three years versus costs of $1.1 million, adding up to a net present value (NPV) of $1.6 million and an ROI of 155%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Echoworx OneWorld Encryption.

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 Echoworx OneWorld Encryption 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 Echoworx stakeholders and Forrester analysts to gather data relative to OneWorld Encryption.

CUSTOMER INTERVIEWS
Interviewed three organizations using OneWorld Encryption to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

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 interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Echoworx OneWorld Encryption'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.

The OneWorld Encryption Customer Journey

BEFORE AND AFTER THE ONEWORLD ENCRYPTION INVESTMENT

Interviewed Organizations

For this study, Forrester conducted three interviews with Echoworx OneWorld Encryption customers. Interviewed customers include the following:

INDUSTRY	REGION	EMAILS ENCRYPTED ANNUALLY	INTERVIEWEE
Financial services	Americas	50M to 100M	Senior vice president of email engineering
Financial services	EMEA	<100K	Implementation lead
Municipality	Americas	100K to 500K	Senior systems administrator

Key Challenges

Prior to adopting OneWorld Encryption, interviewees struggled with their previous email encryption environments for the following reasons:

- **Existing encryption solutions were unable to scale with growing demands of the business.** With an ever-growing and increasingly diverse group of customers, organizations struggled to keep up with all of the requirements of these customers, including multilingual support, multiple encryption delivery methods, and increased capacity during peak volume periods. As a result, organizations used a combination of different encryption point solutions to address each unique use case yet continued to struggle with a growing backlog of mail volume across an increasingly strained and complex infrastructure.
- **Without the right support and processes, running an encryption platform became an onerous activity.** Encryption is an issue that impacts multiple groups within an organization, including IT, security, compliance, and end users. In larger enterprises, this reality manifested in multiple functions running separate components of an encryption solution. When an issue or challenge arose, these functions would then need to coordinate to resolve the issue, which would create inefficiencies and inconsistencies in approach. Furthermore, numerous tier 1 support tickets for issues such as password resets would overwhelm call centers, taking up a significant amount of call center agent time. Finally, interviewed organizations needed more than just reactive support to isolated problems; they needed a partner that could run an email encryption program with them or even for them. According to a 2019 Forrester study examining the state of endpoint security, a lack of necessary skills increasingly drives engagement with managed security service providers, with 71% of surveyed endpoint security decision makers saying that using a managed security service would be a high or critical priority for their firms over the next 12 months.[2]

> "We were using two different email encryption solutions, and the expense was tremendous. Our infrastructure was complicated, and managing and upgrading the platforms was a task that really should have been done by a set of dedicated resources."
>
> *Senior systems administrator, municipality*

> "Solving encryption issues required the support of several different groups within the organization, and nobody was willing to raise their hand to be the one to talk to all of those people and brings those groups together."
>
> *Senior vice president of email engineering, financial services*

FORRESTER®

- **Legacy solutions lacked the flexibility of a dedicated platform.** Email encryption is often found as a single feature of a standardized set of broader security solutions, and thus many third-party providers may not have the ability to customize the encryption platform outside of the "out-of-box" settings. This lack of flexibility proved to be a major point for organizations that needed their email encryption to be more tailored for purposes such as branding or multilingual support. One financial services firm interviewee recounted, "When we asked for something outside of the vendor's traditional offering, most of the time their answer would be that they couldn't do it because their platform could not support the customization."
- **Hosting email encryption on-premises required additional resources and management.** Few organizations had the internal expertise to properly manage and maintain their email encryption solutions. And without a dedicated provider, organizations had to front all of the hardware, software, support, and maintenance costs associated with email encryption internally.

"Our old security solution could only send encrypted mail to an online portal. The problem was that it never actually reached the customer's inbox, and after a certain amount of time, it would be deleted, which was extremely risky from a compliance perspective."

Implementation lead, financial services

Solution Requirements

The interviewed organizations searched for a solution that could:

- **Support all major email encryption methods.** Due to regulatory differences across industries and geographies, organizations, particularly those operating on a global or multinational scale, needed a solution that could perform both inbound and outbound encryption across all of the major encryption methods commonly used today. With OneWorld Encryption, organizations could support encryption for half a dozen methods, including PGP, Secure PDF, S/MIME, web portal, TLS, and encrypted attachment.
- **Offer customization and dedicated support.** Organizations access email encryption solutions in one of three ways: 1) as a native feature of email services; 2) as a feature of broader security solutions; or 3) through a dedicated encryption platform.[3] While some organizations may suffice with the first two methods, interviewed organizations, particularly those in highly regulated industries, required a dedicated solution that could meet both regulatory and business needs. Said one interviewee, "We had a lot of custom requests that needed to be addressed, including allowing the user to choose their own encryption method and having our encryption appear with our bank's unique branding."

"Echoworx's different encryption methods were a huge part of our decision to invest in them. If we didn't have that list of encryption methods and the user could not choose what they wanted, we probably would have needed to use multiple point solutions to have the same functionality."

Senior vice president of email engineering, financial services

Key Results

The interviews revealed that key results from the OneWorld Encryption investment include:

- **Accelerated digital transformation.** With their complex legacy email encryption solutions, organizations often struggled to grow adoption of the solution with both customers and internal stakeholders, such as other lines of businesses. Using OneWorld Encryption, organizations could increase traction with both groups by offering a frictionless experience backed by support from the Echoworx team. The increased adoption allowed organizations to gradually shift from paper-based document delivery to secure digital document delivery.

"OneWorld Encryption allowed us to reduce paper, reduce the cost of post, and, at the same time, speed up delivery of our documents."

Implementation lead, financial services

- **Simplification of encryption stack.** Because organizations often accessed email encryption as part of their native email clients or broader security solutions, organizations required point solutions to address individual needs or use cases such as a specific encryption method or multilingual support. Additionally, these solutions often ran out of numerous nondedicated, on-premises servers that required constant manual upkeep. With Echoworx, organizations found that they could meet all of their email encryption needs with a single platform powered by a small, dedicated set of Echoworx servers.
- **Greater self-sufficiency.** By simplifying their email encryption platforms, end users found that they could also better handle encryption on their own without outside support. Leveraging an intuitive user interface combined with multiple encryption options, end users could handle disparate encryption use cases through a single platform via integration with their existing email clients. Furthermore, interviewees experienced fewer tier 1 issues such as password creation and management, resulting in a reduction of encryption-related support requests.
- **Operational efficiency.** While other endpoint security platforms that offer email encryption may not have the in-house resources or expertise to deploy, maintain, and update their email encryption platforms without the help of partners and other third parties, the cost of which is passed down to organizations, Echoworx self-manages the hardware and software of the OneWorld Encryption platform on behalf of organizations without charging additional fees. As a result, organizations could redeploy or avoid onboarding additional security and systems administrators dedicated to OneWorld Encryption while having the confidence that that their email encryption is being actively managed.

> "Even though they are traditionally a SaaS provider, Echoworx worked with us to deploy OneWorld Encryption on our data centers. They built and delivered the equipment, led the testing process, worked with us to create the users, managed the environment, and provided the front-end tools to our help desk to allow them to start and manage the password reset process."
>
> *Senior vice president of email engineering, financial services*

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the three companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

- Fortune 1000-sized financial services firm with $12 billion in annual revenue and 35,000 employees, 75% of whom use Echoworx OneWorld Encryption.
- Sends between 10 million and 20 million encrypted secure documents per year for use cases such as customer onboarding and delivering monthly recurring statements.
- Runs multiple lines of businesses, including payments, lending, and asset management. Due to the nature of these businesses, the financial institution manages, sends, and receives a significant amount of data subject to regulations such as those set by the Payment Card Industry (PCI).
- Prior to adopting Echoworx OneWorld Encryption, the organization leveraged email encryption in two ways: 1) native email encryption through the existing email client and 2) as a single feature of a legacy encryption point solution that was deployed on-premises. However,

Key assumptions

- $12B in annual revenue
- 10M to 20M encrypted secure documents delivered per year
- Three distinct lines of business
- SaaS deployment of OneWorld Encryption

FORRESTER®

this legacy solution offered limited functionality in terms of different encryption options and little customization for the organization's specific business requirements, including custom email domain branding for three distinct business lines.

- The organization learned of Echoworx through an existing engagement with a security software and services vendor that provided solutions for several of the organization's other cybersecurity needs. Because of this relationship, the organization could immediately initiate meetings with Echoworx without needing to go through an in-depth request-for-proposal (RFP) process to evaluate other vendors. Ultimately, the organization opted for a SaaS deployment of OneWorld Encryption on Echoworx's data centers to achieve both cost and technology efficiencies.

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

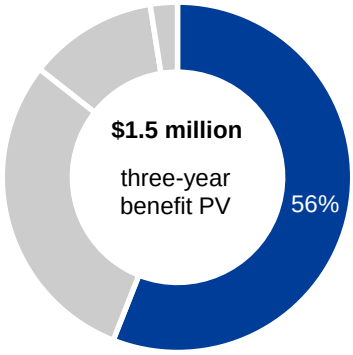
REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Reduced document delivery costs	$0	$850,000	$1,062,500	$1,912,500	$1,500,751
Btr	Avoided cost of legacy on-premises solution	$345,121	$304,321	$304,321	$953,764	$793,893
Ctr	Increased call center productivity	$128,250	$128,250	$128,250	$384,750	$318,939
Dtr	Avoided cost of custom email domain branding	$27,000	$27,000	$27,000	$81,000	$67,145
	Total benefits (risk-adjusted)	$500,371	$1,309,571	$1,522,071	$3,332,014	$2,680,728

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 composite organization expects risk-adjusted total benefits to be a PV of almost $2.7 million.

Reduced Document Delivery Costs

Organizations have naturally gravitated toward secure eStatements instead of traditional paper forms in an effort to reduce mailing costs and increase efficiencies in document processing. However, despite these efforts, many customers have been reluctant to migrate to secure eStatements due to a lack of preferred delivery methods, concerns over security, or a frustrating user experience. Organizations, too, have faced challenges reaching broad adoption of email encryption solutions internally due to hurdles such as poor scalability of legacy solutions, limited encryption methods, and a complex and labor-intensive user interface. Interviewed organizations found that OneWorld Encryption solved for the encryption challenges of both customers and internal user groups in the following ways:

- From a customer-facing perspective, OneWorld Encryption enabled organizations to offer their customers a frictionless eStatement delivery experience that integrated into the organization's existing portals and web pages without needing to redirect to alternative pages or requiring layers of additional verification steps.
- From the organization's perspective, using OneWorld Encryption meant that more business lines could leverage email encryption since the increased volume would no longer cause an email backlog or reduced performance. The senior VP of engineering at a financial services firm articulated: "More of our businesses are now able to send encrypted messages to our internal audit folks and various regulators. If we hadn't made this move, it would have had a significant impact on our ability to grow."
- Finally, across all stakeholder groups, the ability to select the method of encryption from a list of the most commonly accepted encryption formats allowed organizations, customers, partners, and other third parties to send encrypted digital documents to each other on an international scale. One financial services organization interviewee recounted, "OneWorld Encryption gave us the flexibility to talk to European regulators, the vast majority of whom require S/MIME."



Reduced document delivery costs: **56%** of total benefits

"If we hadn't made this move, it would have had a significant impact on our ability to grow."

Senior vice president of engineering, financial services

FORRESTER®

For the composite organization, Forrester assumes that:

› Encrypted secure documents grow at a flat rate of 25% each year from Year 1 to Year 3 after adopting OneWorld Encryption. OneWorld Encryption drives 40% of this growth, with the remaining 60% driven by organic growth.[4] These estimates are on the conservative side of data gathered from Forrester's interviews conducted for this study.

Actual benefits that other organizations experience from reducing document delivery costs may differ based on the following factor:

› An organization's digital maturity and previous email encryption environment will dictate the percentage of encrypted secure document growth driven by OneWorld Encryption. Less mature organizations leveraging nondedicated legacy encryption solutions with limited encryption methods and scalability may realize more pronounced growth as a result of adopting OneWorld Encryption while organizations further down the maturity curve may experience more modest growth.

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.

To account for this risk, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $1.5 million.

Reduced Document Delivery Costs: Calculation Table

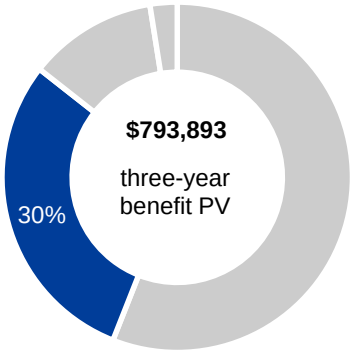
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Encrypted secure documents delivered annually	25% YoY growth	10,000,000	12,500,000	15,625,000
A2	Incremental growth of encrypted secure documents delivered	$A1_{Year\ X}$ - $A1_{Year\ X-1}$	0	2,500,000	3,125,000
A3	Percentage of encrypted secure document growth driven by OneWorld Encryption		40%	40%	40%
A4	Cost savings achieved by replacing paper document delivery with digital, per document		$1	$1	$1
At	Reduced document delivery costs	A2*A3*A4	$0	$1,000,000	$1,250,000
	Risk adjustment	↓15%			
Atr	Reduced document delivery costs (risk-adjusted)		$0	$850,000	$1,062,500

Avoided Cost Of Legacy On-Premises Solution

The composite organization opted for a cloud-based, SaaS deployment of OneWorld Encryption to replace an existing email encryption solution deployed on-premises. This previous encryption solution required hardware investments along with administration for both the software and hardware components of the platform. With a SaaS deployment of OneWorld Encryption, the organization could retire the full software cost of its previous email encryption solution, avoid the need to invest in additional servers, and streamline or eliminate administration tasks.

› By choosing a cloud-based deployment, the organization can avoid purchasing four servers that would have been needed to host OneWorld Encryption.

› Echoworx now handles server maintenance and administration; therefore, the organization can now redeploy a systems administrator who was previously dedicated to the legacy platform.



Avoided cost of legacy on-premises solution: **30%** of total benefits

FORRESTER®

- Echoworx also manages and updates OneWorld Encryption software, allowing security administrators to save time and focus on business-critical issues.
- A senior VP of email engineering for a financial services firm said, “Echoworx manages the entire email encryption environment, including the physical hardware, which means I no longer need people to go into our data center to update the servers.”

Forrester assumes:

- Each server needed to support OneWorld Encryption costs $1,000 per month.
- The fully burdened salary of a tier 4 systems administrator is $84,500.
- The fully burdened hourly salary of a security administrator is $49.

The benefit of avoiding the costs associated with a legacy email encryption solution will vary based on:

- Size and scope of the email encryption environment.

To account for this risk, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $793,893.

> “I used to spend at least 2 hours per day doing activities like whitelisting email addresses or fixing bugs in the code that would cause our email encryption solutions to decluster. I no longer have to worry about any of those things.”
>
> *Senior systems administrator, municipality*

Avoided Cost Of Legacy On-Premises Solution: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Avoided legacy encryption solution licensing costs		$262,500	$262,500	$262,500
B2	Avoided server purchases		4	0	0
B3	Price per server		$12,000	$0	$0
B4	Hardware cost avoidance	B2*B3	$48,000	$0	$0
B5	Reallocated systems administrators		1	1	1
B6	Fully burdened systems administrator annual salary		$84,500	$84,500	$84,500
B7	Security administrator hours spent managing email encryption with legacy solution, per week		10	10	10
B8	Reduction in time required to manage email encryption with OneWorld Encryption		90%	90%	90%
B9	Fully burdened security administrator hourly salary		$49	$49	$49
B10	Labor productivity recapture		50%	50%	50%
B11	Labor cost avoidance	(B5*B6)+ (B7*B8*B9*B10* 50 weeks/year)	$95,525	$95,525	$95,525
Bt	Avoided cost of legacy on-premises solution	B1+B4+B11	$406,025	$358,025	$358,025
	Risk adjustment	↓15%			
Btr	Avoided cost of legacy on-premises solution (risk-adjusted)		$345,121	$304,321	$304,321

Increased Call Center Productivity

Email encryption platforms traditionally require significant technical support, which often comes in the form of agents in a call center. These agents would be inundated with high volumes of support requests for simple tier 1 issues such as the need to reset a password to access an encrypted document. With OneWorld Encryption, interviewed organizations experienced significant reductions in encryption-related call center tickets by leveraging an intuitive user interface in conjunction with self-service features such as auto password resets.

- One interviewee described the challenge of providing tier 1 support for email encryption with the organization's previous email encryption platform: "We actually had a whole customer service team that would spend almost all their time simply resetting passwords for people who had forgotten them."
- A financial services organization experienced similar challenges, but the senior VP of email engineering spoke to the ease of use of OneWorld Encryption as a driver of reduced support calls: "Echoworx continues to make improvements to the usability of their platform, and it has come to a point where we now rarely deal with any support requests because it is so much easier for the user to just follow a set of basic instructions, click on a link, and start the password reset process by themselves."

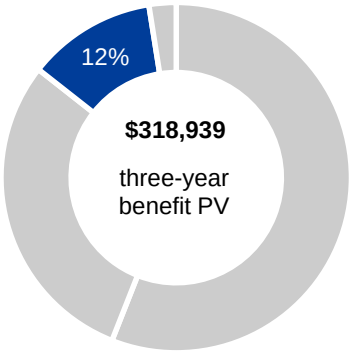
OneWorld Encryption's self-service functionality and seamless user interface drove an 80% reduction in encryption-related call center requests. The impact on subsequent labor cost savings for the composite organization is based on the following assumptions:

- The fully burdened salary of a call center agent is $45,000.
- For every hour of labor productivity saved by reducing encryption-related call center requests, 75% of time is effectively captured in equal value-added activities.

The benefit of increased call center productivity will vary based on:

- Functionality and user interface of the organization's previous email encryption solution.

To account for this risk, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $318,939.



Increased call center productivity: **12%** of total benefits

> "Echoworx continues to make improvements to the usability of their platform, and it has come to a point where we now rarely deal with any support requests because it is so much easier for the user to just follow a set of basic instructions, click on a link, and start the password reset process by themselves."
>
> *Senior vice president of email engineering, financial services*

Increased Call Center Productivity: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Number of call center agents		5	5	5
C2	Annual fully burdened call center agent salary		$45,000	$45,000	$45,000
C3	Reduction in encryption-related call center requests		80%	80%	80%
C4	Productivity capture		75%	75%	75%
Ct	Increased call center productivity	C1*C2*C3*C4	$135,000	$135,000	$135,000
	Risk adjustment	↓5%			
Ctr	Increased call center productivity (risk-adjusted)		$128,250	$128,250	$128,250

FORRESTER®

Avoided Cost Of Custom Email Domain Branding

Large enterprises will inevitably rely on a variety of external vendors to power their many business and customer-facing applications. However, some organizations have recognized the value of "white-labeling" these applications as a way of unifying the customer experience, while others may even be required under company policy to maintain specific branding standards for distinct business lines. In the past, these organizations would need to pay their email encryption vendors or other third parties to create custom branding for their web or email domains; however, Echoworx provides custom branding as a service to OneWorld Encryption customers, allowing organizations to offer their customers a native brand experience while saving on branding costs.

- Comparing the quality and functionality of branding offered by a legacy email encryption platform and Echoworx, the senior VP of email engineering at a financial services enterprise said, "Our old encryption platform offered what we could call rudimentary branding, but what Echoworx did for us was much more sophisticated and included features such as multiple language support."
- The senior systems administrator for a municipality spoke to the speed of Echoworx's custom branding: "If I needed any custom branding done, it would always be less than four days to get everything finalized."

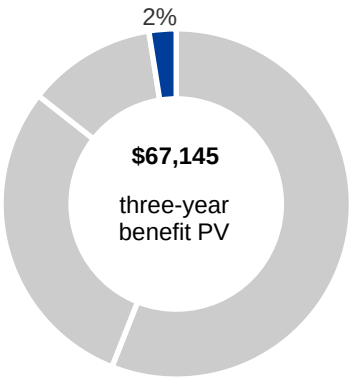
Forrester assumes:

- Each of the composite organization's three lines of business requires new and updated email domain branding annually.
- The cost to engage a third party to create custom email domain branding is $10,000 per domain.

Benefits of avoiding the cost of custom email domain branding will vary based on:

- Number of unique domains branded.
- Complexity of branding design or functionality requirements.

To account for this risk, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $67,145.



Avoided cost of custom email domain branding: **2%** of total benefits

"Our old encryption platform offered what we could call rudimentary branding, but what Echoworx did for us was much more sophisticated and included features such as multiple language support."

Senior vice president of email engineering, financial services

Avoided Cost Of Custom Email Domain Branding: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Number of custom email domains rebranded annually		3	3	3
D2	External quote for custom domain branding, per domain		$10,000	$10,000	$10,000
Dt	Avoided cost of custom email domain branding	D1*D2	$30,000	$30,000	$30,000
	Risk adjustment	↓10%			
Dtr	Avoided cost of custom email domain branding (risk-adjusted)		$27,000	$27,000	$27,000

Unquantified Benefits

Organizations experienced other benefits not included in the financial model that were significant and apparent but could not be quantified for

FORRESTER®

this study. Unquantified benefits of the Echoworx OneWorld Encryption include:

- **Enhanced customer experience.** With their legacy infrastructure, interviewed organizations struggled with a poor user experience caused by a lack of encryption delivery options, lengthy and complicated password and key management processes, and inconsistent delivery timeframes caused by the inability to handle a growing backlog of email volume. As the senior VP of email engineering at a financial institution noted: "At the end of the day, you expect to receive your statement within a certain timeframe, and before, there was no way for me to do that. Now, I can guarantee to a customer that they will receive their statement within 5 minutes."
- **Digital customer onboarding.** While the composite organization constructed for this study is mature in its digital journey and thus is already able to securely onboard customers digitally, other organizations may still be relying on traditional methods of customer onboarding using paper mail or fax. For these organizations, OneWorld Encryption reduced the time required to onboard customers from days down to minutes by enabling secure exchange of documents with multiple inbound and outbound encryption methods and features such as self-service registration and digital signatures. The implementation lead at a financial services organization mentioned, "Our onboarding process went from five days to now just 5 minutes, and we reduced our document handling costs by 90% to 95%."
- **Reduced downtime.** With on-premises legacy encryption platforms, organizations ran the risk of their administrators improperly patching, updating, or configuring software, ultimately increasing the risk of downtime. A senior systems administrator at a regional municipality recalled: "We used to have several incidences per year where something went wrong, and emails would go out clear when they should have gone out encrypted. Every time this happened, we'd have to halt our email server for at least 5 hours."

"At the end of the day, you expect to receive your statement within a certain timeframe, and before, there was no way for me to do that. Now, I can guarantee to a customer that they will receive their statement within 5 minutes."

Senior vice president of email engineering, financial services

"Our onboarding process went from 5 days to now just 5 minutes and we reduced our document handling costs by 90% to 95%."

Implementation lead, financial services

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 OneWorld Encryption and later realize additional uses and business opportunities, including:

- **Reduced risk of data breaches.** Large enterprises with sizable security budgets still fail to properly encrypt their data all the time. In fact, 9 billion records have been breached since 2013, but only 4% were encrypted. Forrester's in-depth research with enterprise security decision makers has shown that a complex legacy environment is one of the key drivers of organizations failing to encrypt all their sensitive data. These legacy environments are often minimally integrated as the result of repeated acquisitions or are run on servers or appliances that reside at a network location that makes software or firmware update impossible.[5] Interviewed organizations anticipate that Echoworx's managed services and coverage of multiple use cases may allow them to gradually reduce reliance on multiple point solutions, simplify their encryption environments, and subsequently better protect their user and customer records.

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.

- **Improved analytics.** In addition to encrypting messages, OneWorld Encryption allows organizations to actively monitor all inbound and outbound messages and reject those not in compliance with company policies. Over time, this analytics platform can provide indexed reports and summary diagrams that identify critical information such as most flagged policies, top offenders, bounces, and more.

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

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
Etr	Echoworx fees	$1,500	$400,000	$400,000	$400,000	$1,201,500	$996,241
Ftr	Deployment costs	$54,912	$0	$0	$0	$54,912	$54,912
	Total costs (risk-adjusted)	$56,412	$400,000	$400,000	$400,000	$1,256,412	$1,051,153

Echoworx Fees

Interviewed organizations found pricing for OneWorld Encryption to be simple and predictable, which not only sped up the procurement process, but also facilitated planning and budgeting for subsequent years following the initial investment. While other encryption vendors typically have distinct pricing for individual services and even features, Echoworx packages its managed services, support, product maintenance, and customization services within its licensing fees, meaning organizations can continue to engage Echoworx for these services as part of their licensing agreement. OneWorld encryption fees can be broken down into the initial setup fees and perpetual licensing fees, as described below:

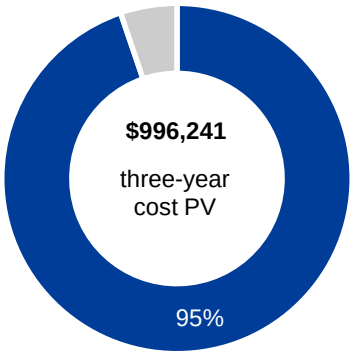
- Setup fees are charged for installing OneWorld Encryption on either Echoworx data centers or on-premises and configuring encryption on the organization's internal mailboxes.
- License fees reflect both usage of the product and the aforementioned services and are based on either the number of secure documents delivered with OneWorld Encryption per year or the number of total users of the software.

For the composite organization, Forrester assumes:

- OneWorld Encryption is deployed as a SaaS solution over Echoworx data centers.
- License fees are based on secure delivery of between 10 million and 20 million documents per year through OneWorld Encryption.

As list price was used, Forrester made no risk adjustment. The three-year risk-adjusted total PV is $996,241.

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 composite organization expects risk-adjusted total costs to be a PV of more than $1.0 million.



95% of total costs

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.

FORRESTER®

Echoworx Fees: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	OneWorld Encryption Advanced setup fees		$1,500			
E2	Echoworx OneWorld Encryption Advanced license fees			$400,000	$400,000	$400,000
Et	Echoworx fees	E1+E2	$1,500	$400,000	$400,000	$400,000
	Risk adjustment	0%				
Etr	Echoworx fees (risk-adjusted)		$1,500	$400,000	$400,000	$400,000

Deployment Costs

From a technology standpoint, deploying Echoworx is a relatively simple task and, as one interviewee described, "is really no more complicated than simply pointing to a shared mail address." However, email encryption is often adopted by organizations in heavily regulated industries, such as financial services, which require external solutions to pass numerous formal controls and reviews, ultimately lengthening time-to-deployment. For the 26,000-user composite organization, deployment is a six-month process with the following phases:

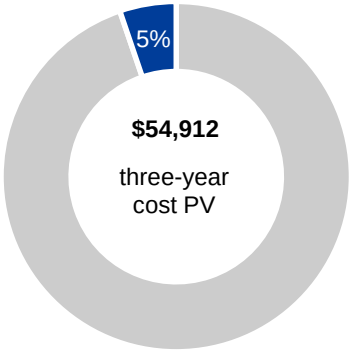
- A three-month planning phase that consists of identifying and outlining business requirements for Echoworx, obtaining sign-off from risk and legal teams, and developing custom domain branding to comply with group policies.
- A three-month implementation pilot phase that involves rolling out OneWorld Encryption to business lines and its users, testing the solution, and addressing any issues with the appropriate IT groups, such as the security or firewall teams.

For the purposes of this study, Forrester assumes the following for its composite organization:

- Planning involves one FTE from information security, two FTEs from compliance, one FTE from risk, and one FTE from procurement spending one full day each week on planning over the course of three months.
- Implementation involves three FTEs from various IT security functions spending one full day each week on implementation over the course of three months.
- The hourly, fully burdened salary of FTEs engaged for planning and implementation is $65.
- For every hour of labor productivity lost during planning and implementation activities, 50% of time is effectively recaptured in equal value-added activities.

Actual deployment costs that other organizations experience will vary based on the following factors:

- The organization's industry will dictate the number and type of resources that need to be engaged during the planning process. Highly regulated industries will typically require sign-off from functions such as risk, compliance, and sometimes the impacted line-of-business heads.



Deployment costs:
5% of total costs

Six months
Total planning and implementation time

FORRESTER®

- The size of deployment, including the number of different business lines or locations, will impact the time and resources it takes to fully roll out the solution.
- A thorough vendor selection and RFP process may add weeks or even months to the planning process and require additional resources from functions such as procurement.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a risk-adjusted total PV of $54,912.

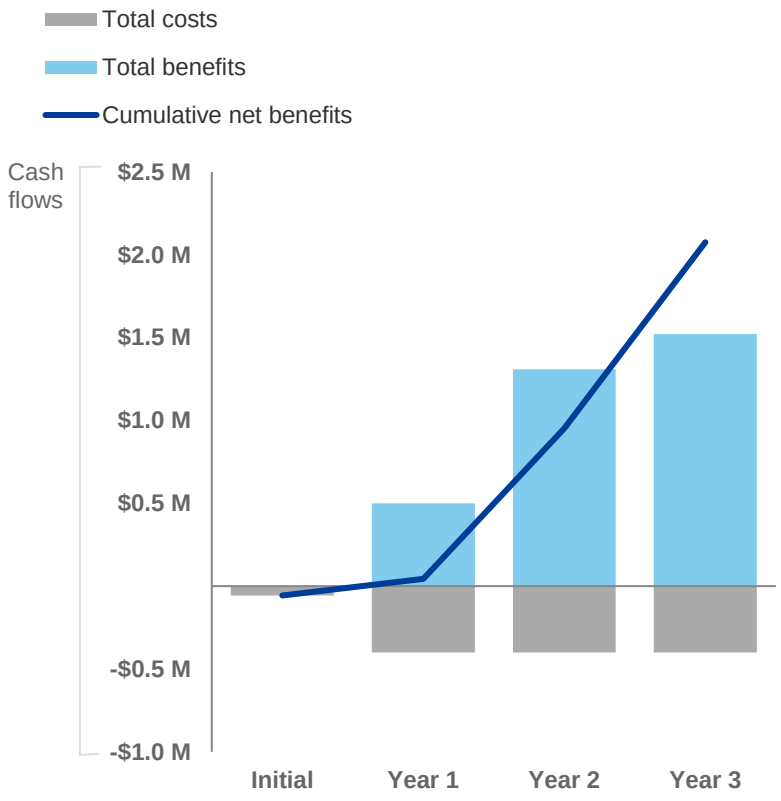
Deployment Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
F1	FTEs involved in planning and implementing OneWorld Encryption		8			
F2	Number of hours spent planning and implementing OneWorld Encryption	24 weeks* 8 hours/week	192			
F3	Hourly fully burdened salary of planning and implementation FTEs		$65			
F4	Labor productivity recapture		50%			
Ft	Deployment costs	F1*F2*F3*F4	$49,920	$0	$0	$0
	Risk adjustment	↑10%				
Ftr	Deployment costs (risk-adjusted)		$54,912	$0	$0	$0

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($56,412)	($400,000)	($400,000)	($400,000)	($1,256,412)	($1,051,153)
Total benefits	$0	$500,371	$1,309,571	$1,522,071	$3,332,014	$2,680,728
Net benefits	($56,412)	$100,371	$909,571	$1,122,071	$2,075,602	$1,629,575
ROI						155%
Payback period						7.0

FORRESTER®

Echoworx OneWorld Encryption: Overview

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

As a pure-play encryption solutions provider, Echoworx works with finance, government, healthcare, legal, and compliance professionals to tailor secure communication solutions that don't impede on customer experience. Echoworx's encryption experts take pride in transforming chaos into order for leading multinational enterprises using its SaaS encryption platform. No matter how large your organization, Echoworx can help you protect your important data by providing you with a path to secure communications. Echoworx's scalable encryption platform can address multiple uses across your organization.

Clients in 30 countries use the OneWorld encryption platform, and more than 5,000 business, public sector, and institutional deployments are serviced through Echoworx's data centers in the US, Canada, Germany, Ireland, Mexico, and the UK.

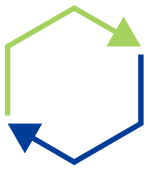
Appendix A: Total Economic Impact

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.

Appendix B: Endnotes

[1] Source: “Understand The State Of Data Security And Privacy: 2015 to 2016,” Forrester Research, Inc., January 8, 2016.
[2] Source: “The State Of Endpoint Security, 2019,” Forrester Research, Inc., January 22, 2019.
[3] Source: “TechRadar™: Data Security And Privacy, Q4 2017,” Forrester Research, Inc., October 4, 2017.
[4] Source: Koch, Bruno “E-Invoicing / E-Billing,” Billentis, May 18, 2017.
[5] Source: “Use Advanced Encryption For Data Security,” Forrester Research, Inc., January 30, 2019.