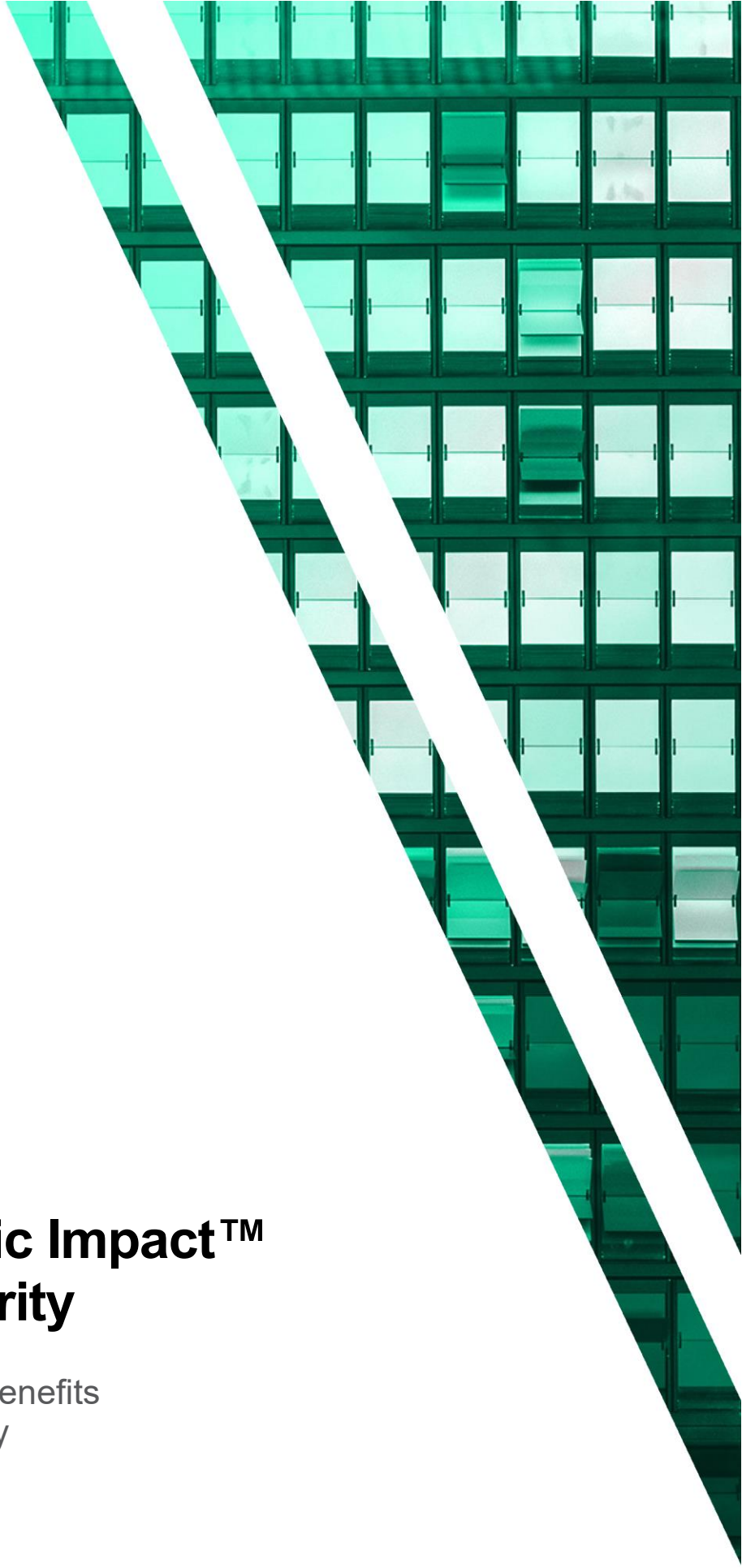
FORRESTER®



The Total Economic Impact™ Of Abnormal Security

Cost Savings And Business Benefits Enabled By Abnormal Security

DECEMBER 2022

Table Of Contents

Executive Summary 1

The Abnormal Security Customer Journey 6

Key Challenges 6

Security Context 7

Solution Requirements 8

Phishing: A Top Security Threat 8

Why Abnormal Security? 9

Composite Organization 10

Analysis Of Benefits 11

Avoided Severe Data Breaches 11

Reduced Invoice Fraud 15

Prevented Phishing 18

Streamlined Security Operations 20

Unquantified Benefits 23

Flexibility 23

Analysis Of Costs 24

Abnormal Security Fees 24

Deployment And Implementation Costs 26

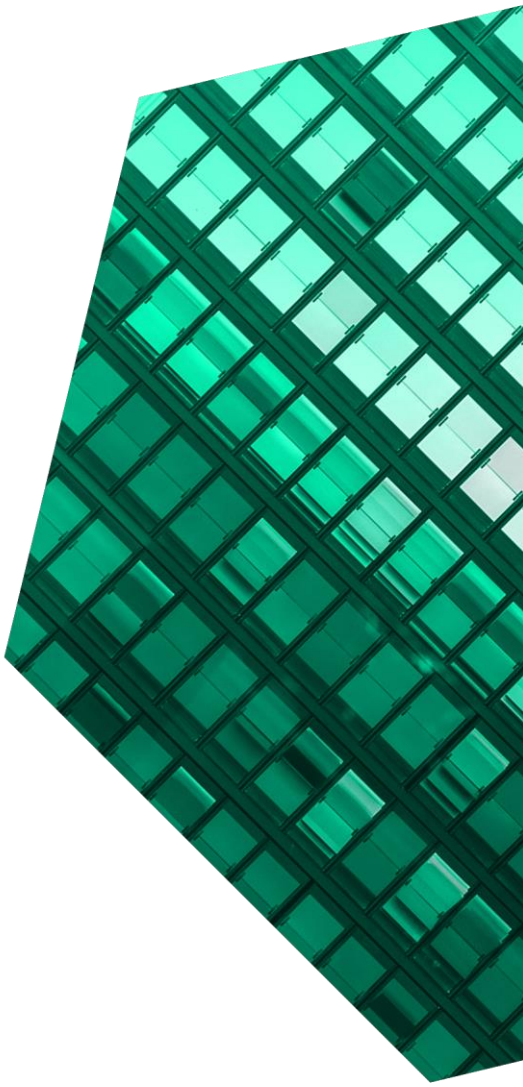
Channel Partner And Roadmap Costs 28

Financial Summary 30

Appendix A: Total Economic Impact 31

Appendix B: Endnotes 32

Consulting Team: Courtenay O'Connor
Nahida Nisa



ABOUT FORRESTER CONSULTING

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

Executive Summary

Email persists as the most mission-critical channel for business communications and marketing. Because of its importance, email is also highly vulnerable to compromise with mounting downside costs of sophisticated, high-volume, email-based attacks. Cloud-based email filtering has emerged as a more advanced approach than traditional, rules-based email security programs to safeguard email against a constantly changing and increasingly vulnerable threat surface.

Abnormal Security is an enterprise email security provider offering cloud-native, API-enabled email security (CAPES). Abnormal Security's Inbound Email Security learns the behavior of an organization's email environment to stop email attacks, including business email compromise, account takeovers, and supply chain and invoice fraud. Abnormal Security's email protection may also supplement or replace an organization's secure email gateway (SEG).

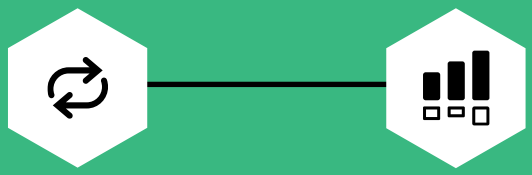
Abnormal Security commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Abnormal Security.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Abnormal Security on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Abnormal Security. Forrester aggregated the interviewees' experiences into a single composite organization with a global reach and $1 billion in annual revenues. It protects 10,000 mailboxes, receives 100 million emails annually, and is at a high risk of malicious emails and financial fraud.

Prior to using Abnormal Security, interviewees noted business email compromise (BEC) as their top security concern. Monitoring user-reported phishing emails often required fully dedicated resources. Interviewees also reported struggles with high incident caseloads and email security rule-making. These organizations suffered direct and indirect financial losses from disruptive breaches, sophisticated invoice fraud, and socially-engineered, high-frequency phishing attacks.

Interviewees quickly tested Abnormal Security and deployed with minimal effort. With Abnormal Security, interviewees reported no major BEC incidents and significantly reduced email security-related labor. By blocking inbound malicious emails, Abnormal Security helped interviewees minimize their risk exposure, simplify their email security environment, prevent wasted labor, and focus on higher-value security efforts.

KEY STATISTICS



Return on investment (ROI)
278%

Net present value (NPV)
$3.20M

KEY FINDINGS

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

- **Averting approximately five breaches caused by BEC, which avoids over 50,000 hours of breach-related end-user downtime.** Abnormal Security blocks 99.97% of messages that the composite organization's existing, upstream email security systems did not filter. This avoids significant effort to contain and remediate email security incidents; external costs, such as fines, damages, and lost revenues; and internal costs to finance, legal, and customer experience labor resources.
- **Saving over 1,400 hours of invoice fraud investigation by blocking over 500 fraudulent invoices delivered via email.** After the investment in Abnormal Security, the composite organization effectively blocks 60 emails containing highly sophisticated fraudulent invoices that upstream email filters could not block. It also avoids significant effort from security and finance resources to monitor and investigate invoice fraud.
- **Blocking 1,800 phishing emails over three years, preventing prevented losses of $1.3 million over three years.** Phishing, once the composite organization's main threat vector, is effectively neutralized with Abnormal Security Inbound Email Security. In preventing thousands of phishing attacks, the composite organization avoids other, indirect financial losses due to labor associated with investigations and internal and public response.
- **Simplifying the email security environment with displacement of the SEG and around 5,000 avoided hours of phishing mailbox monitoring.** The composite organization works with Abnormal Security to decrease the complexity of its email security environment over time. Across the three-year period, it achieves this by deploying Abnormal Security's Abuse Mailbox Automation and Email Account Takeover Protection. It also achieves savings from displacing its secure email gateway with Abnormal Security, decommissioning the associated hardware, software, and maintenance costs.

Unquantified benefits. Benefits that provide value but are not quantified in this study include:

- **Improved insight into the email threat landscape**. Interviewees gained advanced intelligence on email attack vectors, improving their understanding of their threat landscape.
- **Confidence in email security posture.** Interviewees reported an a newly gained peace of mind and confidence in their security posture. This allowed them to refocus their efforts on other security concerns.

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

- **Abnormal Security fees of $971,000.** The composite fees align with the growth trajectory of Abnormal Security's product roadmap. These fees include mailbox protection, Abuse Mailbox automation, and Account Takeover protection.
- **Deployment and implementation costs totaling $15,000.** The composite's initial deployment phase, including the proof of concept (POC), is four months. In Years 2 and 3, the composite automates phishing mailbox monitoring and further remediates account takeovers with Abnormal Security. SecOps resources safeguard product integration and deployment of Abnormal Security functionalities deployed over time.
- **Channel partner and roadmap costs totaling $167,000.** The composite organization experiences channel partner costs equaling 15%

of total annual Abnormal Security fees (although, not all organizations will). Its email security manager also engages with Abnormal Security on a quarterly basis to continually advance the email security strategy according to Abnormal Security features and offerings.

The representative interviews and financial analysis found that a composite organization experiences benefits of $4.36M over three years versus costs of $1.15M, adding up to a net present value (NPV) of $3.20M and an ROI of 278%.

Email Security Trends

Email is invaluable. It is also vulnerable.

Email is a vital tool used to communicate with customers and partners. Attackers know this and often impersonate trusted brands and domains in phishing.

> ***Business email compromise (BEC):*** *Attacks that convince unwitting users to take actions like wiring money, granting access to payment accounts, or sharing sensitive financial documents.*

Cloud-based email filtering augments email security. Security professionals know that, despite best efforts, malicious emails inevitably get through, so they need a layered approach that includes both prevention and response measures.

Email security solutions filter out unwanted and/or malicious inbound content, leading to direct cost savings and operational efficiencies, and protect organizations from phishing attacks that may lead to more destructive ransomware or BEC attacks.

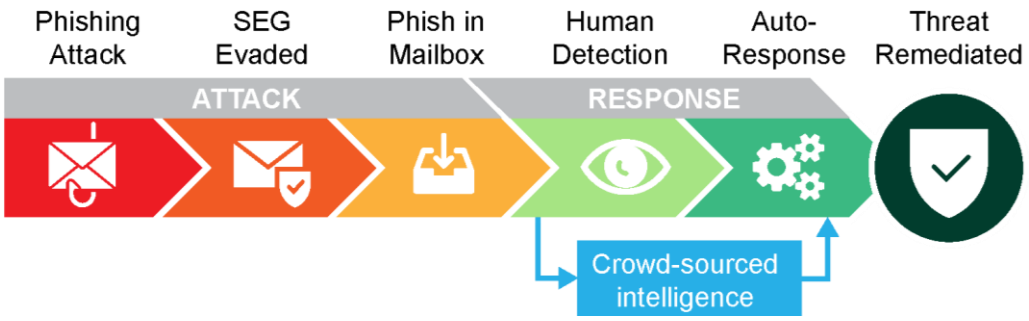


Figure 1. Anatomy Of A BEC Attack: *New abilities to prevent phishing attacks drive security pros to replace incumbent vendors and stay ahead of a rapidly shifting threat environment.*

Source: “Bolster Brand Resilience With DMARC,” Forrester Research, Inc., August 27, 2021.

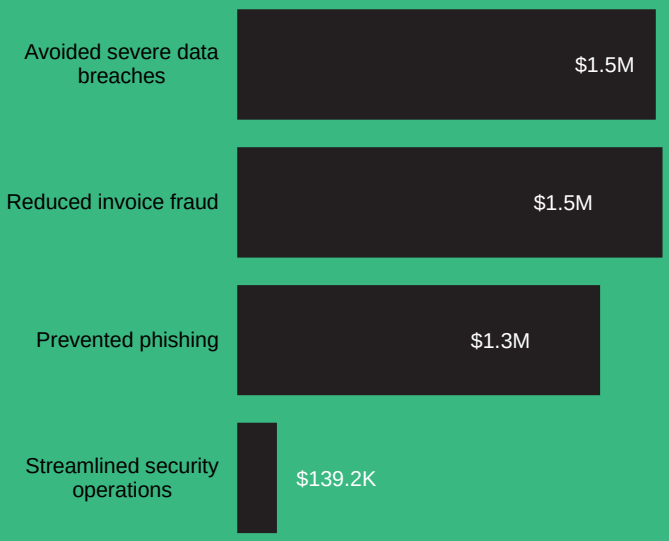
ROI
278%

BENEFITS PV
$4.36M

NPV
$3.20M

PAYBACK
<6 months

Benefits (Three-Year)



Abnormal Security **blocks inbound malicious emails** that upstream email security systems do not filter.

This helps the composite organization **avoid over $4 million in losses** and **thousands of hours of labor effort** from business email compromise.

“I couldn’t unsee what I saw since launching Abnormal Security. It has captured 152,535 attacks in eight months, automatically, with no human involvement!”

— Global technology services director, commodities

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 Abnormal Security.

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 Abnormal Security can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DUE DILIGENCE

Interviewed Abnormal Security stakeholders and Forrester analysts to gather data relative to Abnormal Security.

INTERVIEWS

Interviewed four representatives at organizations using Abnormal Security to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' 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 interviewees.

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 Abnormal Security Customer Journey

Drivers leading to the Abnormal Security investment

Interviews			
Role	**Industry**	**Region**	**Mailboxes**
Global technology services director	Commodities	United Kingdom headquarters, global reach	5,000
Chief information officer	Fintech	Australia headquarters and reach	600
Cybersecurity Manager	Manufacturing	United States headquarters, global reach	23,500 + SEG
Manager of corporate email	Insurance	United States headquarters, global reach	90,000

KEY CHALLENGES

Prior to investing in Abnormal Security, interviewees described untenable security environments in which BEC loomed as the most sigsnificant challenge.

Interviewees reported growth in inbound email volumes, rising security concerns from all vectors, and increases in the frequency and severity of email incidents writ large.

- The global technology services director in the commodities sector described a context of broader, denial of service (DOS) attacks with email being the most significant cause. They stated: “We were getting a large quantity of email and [other] attacks. The email attacks in particular have gotten worse over the last few years, including identity theft, phishing, viruses, spam spyware, and adware.”
- The manager of corporate email in the insurance industry reported a significant international attack with the senior vice president via email in the past five years, prompting the search for a better email security filtering solution.
- The cybersecurity manager in the manufacturing sector described their organization’s limited experience with business email compromise: “We really couldn’t detect BEC before, but we weren’t as proactive as we should have been. It was very difficult for us because we didn’t have a good way of bringing those to the surface.”

“We saw significant increases in everything bad you can think of from an email security perspective.”

Cybersecurity manager, manufacturing

Interviewees noted the challenges of keeping up with phishing reporting, incident caseloads, and email security rule-making and updating in a dramatically shifting security environment.

- The cybersecurity manager in the manufacturing sector noted: “It was a big negative for IT when our users started seeing significant increases of unwanted email messages. But then on the cybersecurity side, we saw the significant increase in our caseloads, as well.”
- The manager of corporate email in the insurance industry described the general email security environment and response to threats, “It was a game of whack-a-mole: Find an issue, make a

configuration change, find an issue, make a configuration change."

- The global technology services director in the commodities sector shared, "We spent a lot of time and effort updating rules trying to keep ahead of the bad guys."

Direct financial losses resulting from malicious emails were costly to interviewees' organizations.

- The chief information officer at the fintech organization shared how threat actors targeted sensitive areas of the organization. They said: "We were seeing sophisticated spam and phishing emails. In particular, we are seeing spear-phishing attacks that had been generally targeting our C-suite or related to financial matters."
- The cybersecurity manager in the manufacturing sector described an emergent pattern of sophisticated, fraudulent invoices designed to evade scrutiny. They said: "The attackers tried little things that would be a lot easier to push through. Other than that, we had a few fraudulent invoices in the $50,000 to $60,000 range."

"Before, the process was quite manual, cumbersome, and required a lot of human involvement which — to be brutally honest — is flawed. Human beings make mistakes."

Global technology services director, commodities

SECURITY CONTEXT

The Greater Value Of Data, The Greater Likelihood Of Compromise

Breaches are not just about attackers targeting obvious high-value data. A lapse in process controls or a simple error can be all it takes for a data breach.[2] Forrester research indicates that:

- 63% of organizations were breached in the past year.3
- In the past 12 months, organizations were breached an average of three times.4
- 59% more organizations were breached globally than in the previous year.5
- Enterprises spend a median of 37 days and a mean of $2.4 million to find and recover from a breach.6
- Globally, organizations took a median of 27 days to find an adversary and eradicate an attack.7
- Organizations took a median of 10 days to recover from a breach.8
- It also cost organizations a global mean of $2.4 million in total per breach.9

In an environment where threats continue to evolve, risks to data morph, and business needs expand, organizations must adapt both today and in the future.[10] Forrester's 2021 data shows that of enterprise security decision-makers whose organizations experienced a breach in the past 12 months:

- 46% reported personally identifiable information was involved.[11]
- 36% reported breaches of authentication credentials.[12]
- 36% reported compromises in protected health information.[13]

SOLUTION REQUIREMENTS

The interviewees' organizations searched for an advanced, automated email security solution that could address the mounting pressure from BEC frequency and severity

- The manager of corporate email in the insurance industry described their organization's requirements for a new email security solution: "Block every unwanted email in the organization, whether it's spam, marketing, malicious, suspicious malware or viruses. Our goal is to not deliver those messages."
- The cybersecurity manager in the manufacturing sector shared that their organization sought a solution that was streamlined, automated, and hands-off to minimize the rising phishing caseload. They explained, "We were looking for a way to minimize the phishing mailbox monitoring and drive phishing down as much as we possibly could."
- The global technology services director in the commodities sector described criteria including breadth of defenses, quality of results, time to value, and a lack of granular email security rule-making.
- According to the interviewee at the fintech company, his organization sought an artificial intelligence (AI)-based email security system that could provide advanced detection capabilities that rules-based solutions could not offer.

"Email seems to be the number-one attack vector we're seeing at the moment."

Global technology services director, commodities

PHISHING: A TOP SECURITY THREAT

BEC, and phishing in particular, pose mounting challenges for organizations.

Despite the many security technologies and education in place, phishing and BEC remain two of the biggest threats for organizations everywhere.

- **Phishing.** Phishing emails are crafted by bad actors seeking to defraud users with messages that look like they are from you. Made to look legitimate, spoofed emails appear to come from known and trusted senders, and attackers dwelling in enterprises insert themselves into email threads at just the right moment to reroute financial transactions. Attackers use stolen credentials to access your sensitive systems, appearing as if they're legitimate users. This maligns a brand's reputation, deteriorates customer trust, and inflicts financial losses.[14]
- **Malware and ransomware.** Malicious files and URLs lead to malware and ransomware outbreaks. Attackers responsible for advanced persistent threats (APTs) also use phishing to spread malware that can lead to sensitive data theft, encryption, or both. Fortify email infrastructure with enterprise email security.[15]
- **Invoice payment/fraud.** Fraud has always been a headache, and the COVID-19 pandemic has exacerbated fraud risks. Businesses increasingly require robust fraud and risk management capabilities to avoid fraud losses, retain customer loyalty, and improve buyer and supplier experiences and relationships.[16]

WHY ABNORMAL SECURITY?

The interviewees noted Abnormal Security could better meet their mounting email security needs. They noted Abnormal Security's various differentiators, including:

- **Proof of efficacy.** The manager of corporate email in the insurance industry described the value of Abnormal Security's POC. They said, "Abnormal Security was finding stuff that was still being delivered that should not have been."
- **AI-based, not rules-based, approach.** The global technology services director in the commodities sector noted: "Abnormal Security avoided the need for granular rule-making that is subject to human error and becomes quickly outdated. Once I saw the POC, I didn't have plausible deniability. I needed to act to make that go away. I stopped sleeping at night until we'd implemented Abnormal Security because they showed us so many active threats."

  The cybersecurity manager in the manufacturing sector noted, "Abnormal Security uses the behavior of machine learning to be very effective at what they do, which is what sold it for me."
- **Peer confidence.** The chief information officer in the fintech industry learned about Abnormal Security from word of mouth. They shared: "My colleague at a security company was just over the moon with this product. I wasn't even ready to buy a new solution, but I was really surprised at the power of their product and where it could fit in in our organization."

"I kept hearing that I had to check out this product."

Cybersecurity manager, manufacturing

Customer Journey: Chief Information Officer, Fintech

This interviewee described how Abnormal Security's email security functionalities met their organization's criteria for advanced message filtering:

> *"A lot of standard products are looking for risky domains or they're looking more in attachments.*
>
> *Abnormal Security does it differently. They look at mailboxes across the entire organization, cataloging that into what's normal and what's abnormal messaging.*
>
> *Over time, it can see things and immediately say 'That's a bit strange. I'm going to look at that more,' and then flag it as dangerous and block it.*
>
> *It's just really intelligent the way it does things. It can pick up zero-day and new attack vectors and mailbox compromises. With these, it can pick up when the behavior is off, which I find really interesting.*
>
> *On top of that, they have a mailbox compromise remediation feature, so if a user within our organization started sending compromised emails, especially internally to other staff, Abnormal Security would tell us that mailbox is compromised, and it can actually lock it and log the user out."*

"Abnormal Security is a *real* AI-based mailbox protection product. It has solutions for things that were painful for us."

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 four interviewees, 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 is a global organization headquartered in North America. It has $1 billion in annual revenues, a portion of which comes from a high-volume financial product. This subjects the composite organization to a higher risk of malicious emails and financial fraud.

The composite manages 10,000 mailboxes and twenty domains with 100 million inbound emails annually. Before Abnormal Security, the composite organization had deployed an email security message-filtering feature within its enterprise email client, as well as the SEG. These served as a first — and only — line of email security defense prior to the Abnormal Security investment.

Well over 100,000 malicious emails delivered in the prior environment added a significant strain on the composite organization's email, incident response, finance, legal, and customer experience teams.

The composite organization is exposed to an average of 1.8 material breaches annually with a 31% likelihood that a breach is launched via email. A breach is defined as an incident resulting in the loss or compromise of data, accompanied by material remediation costs. Breaches at the composite cost over $850,000 each on average.[17]

Deployment characteristics. The composite organization fully deploys Abnormal Security's Inbound Email Security product in Year 1.

In addition, the composite organization seeks to decrease the complexity of its email security environment. To achieve this goal, it opts to engage with Abnormal Security on a quarterly basis, above and beyond its regular product administration, to review the solution's product roadmap and potential fit for its own security strategy.

From the quarterly roadmap meetings, the composite organization adopts new Abnormal Security features into the email environment, seeking to progressively decrease email security complexity by:

- Deploying Abnormal Security's Abuse Mailbox Automation product in Year 2.
- Deploying Abnormal Security's Email Account Takeover Protection product in Year 3.
- Displacing the existing SEG product in Year 3.

Key Assumptions

- **$1 billion annual revenue**
- **100 million inbound emails**
- **20 domains**

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	Avoided severe data breaches	$526,938	$526,938	$729,449	$1,783,325	$1,462,566
Btr	Reduced invoice fraud	$597,975	$597,975	$597,975	$1,793,925	$1,487,075
Ctr	Prevented phishing	$509,847	$509,847	$509,847	$1,529,541	$1,267,914
Dtr	Streamlined security operations	$23,400	$44,460	$107,998	$175,858	$139,157
	Total benefits (risk-adjusted)	$1,658,160	$1,679,220	$1,945,269	$5,282,649	$4,356,712

AVOIDED SEVERE DATA BREACHES

Evidence and data. Interviewees noted a substantial reduction in email-related data breaches and decreased remediation costs.

Interviewees reported on Abnormal Security's high level of efficacy in blocking malicious emails that could lead to a severe data breach.

- The chief information officer in the fintech industry reported on the added value of having Abnormal Security integrated into its existing message filtering service. They said, "Abnormal Security is still catching about 100 emails a month on top of that, which doesn't sound like much, but it is the scarier stuff."
- The cybersecurity manager in the manufacturing sector said, "We really have not had a major email-related incident since Abnormal Security."
- The manager of corporate email in the insurance industry stated: "There hasn't been an incident in over five years. That's quite an effective fence of protection in our environment."
- The global technology services director in the commodities sector said: "Our rule-based email security product was never going to be good at protecting against the threats that you can't write rules for. Abnormal Security plugs a huge gap for us."

Interviewees further reported cascading organizational time savings and diminished impacts of a breach caused by BEC.

- The cybersecurity manager in the manufacturing sector stated: "We have an ever-increasing amount of data that my analysts are expected to work through. We are very much resource-constrained with remediating incidents."
- The manager of corporate email in the insurance industry stated how Abnormal Security avoided postbreach costs related to incident identification, mitigation, response, and communication. They shared: "Dependent on the volume, it would take at least 6 to 10 hours. But now that we have Abnormal Security and [another security product] on our desktops, postbreach reviews are prevented because, again, knock on wood, we haven't had an incident since we had the two products deployed."

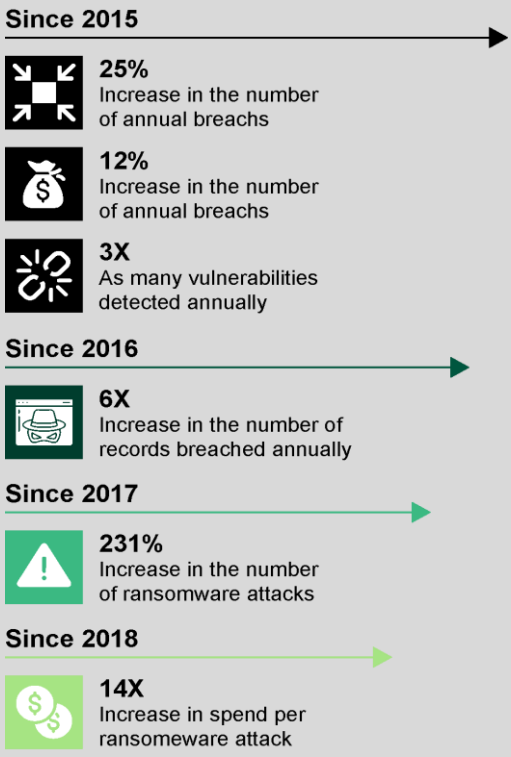
Modeling and assumptions. With Abnormal Security deployed as part of a multipronged cybersecurity strategy, the composite organization avoids external and internal costs, losses, and labor of a data breach.

- Before Abnormal Security, the composite organization experiences 1.8 breaches per year with 31% of those caused by a malicious email.[18]
- In the prior environment, annualized risk exposure to significant material breaches averages $854,192 per breach.[19] This included:
  - **Direct, external costs, and business losses.** At $654,846 per breach, this category comprises of fines, damages, compliance costs, and customer compensation; lost business revenues; and additional costs to acquire customers per material breach.
  - **Indirect labor costs**. To recover from a severe data breach in the prior environment, the composite organization deploys a range of finance, legal, and customer experience resources. Those total 3,437 labor hours or $199,346 assuming an average fully burdened salary of $58 per hour across the following categories: 837 hours for security operations, 871 hours for IT/network operations, 895 hours for development operations, and 835 hours for external resources (rounded).
  - **End-user downtime.** In the prior environment, each breach causes 3.6 hours of downtime per end-user mailbox per breach. The composite organization protects 10,000 mailboxes.

FACTORS INCLUENCING THE COST OF A DATA BREACH

Breaches will happen and they sometimes go unnoticed. Forrester defines a breach as an incident resulting in the loss or compromise of data, accompanied by material remediation costs. These costs are influenced by:

- An organization's annual revenue.
- The type of data compromised and the cause of the breach or privacy violation.
- An organization's level of cyberinsurance.
- If personal data, number of records and individuals affected, and whether the data was encrypted.
- The nature and timing of public disclosures, an incident response plan, and the quality of customer-facing breach response.



- With Abnormal Security, the composite organization blocks 99.97% of malicious emails that would have been delivered in the prior environment.
    - Considering the presence of additional upstream email security measures in Years 1 and 2, Forrester attributes half of the material impact to Abnormal Security.
    - As the composite organization displaces the SEG in favor of Abnormal Security in Year 3 (see Benefit D), Forrester fully attributes this benefit to Abnormal Security.
- In addition, Forrester applies a 50% productivity recapture to time savings, indicating that resources repurpose 50% of the time saved to value-add activities.

Risks. With Abnormal Security, the extent to which an organization may reduce the cost of a material breach caused by email depends on an array of factors. These may include:

- The number, size, and cost of successful breaches the company experiences before deploying Abnormal Security.[20]
- The presence and efficacy of upstream email security systems.[21]
- The sophistication of incoming malicious emails, which will impact the likelihood of users interacting with them. An organization should use its own metrics for the likelihood and individualized internal and external costs of a material breach.
- Internal security processes and systems, impacting how quickly issues and incidents can be investigated and remediated.
- The nature of any resulting breach, which will further impact realized financial costs.

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 $1.5 million.

“I’m comfortable saying Abnormal Security is blocking 99.999% of all that bad email.”

Chief information officer, fintech

“Once we switched on Abnormal Security, it looked back over ninety days and found 46,230 active threats inside my mailboxes that [the incumbent solution] hadn’t filtered.”

Global technology services director, commodities

Avoided Severe Data Breaches

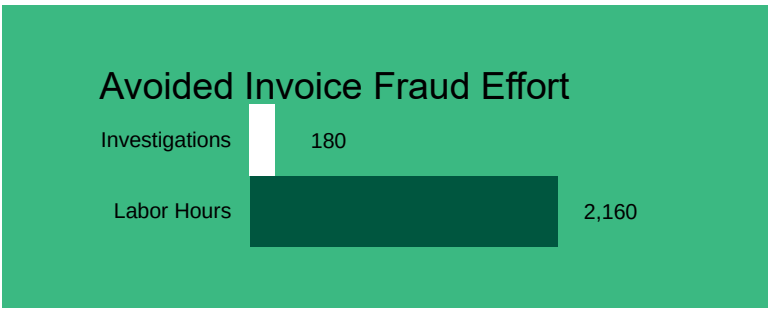
Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average incidence of significant material breaches per year in prior environment	Forrester CDB survey data	1.8	1.8	1.8
A2	Likelihood of a breach launched via phishing	Forrester 2021 Technographics	31%	31%	31%
A3	Average cost of security breach	Forrester CDB survey data	$854,192	$854,192	$854,192
A4	Percent of malicious emails blocked by Abnormal Security	Interviews	99.97%	99.97%	99.97%
A5	Attribution to Abnormal Security	Forrester Assumption	50%	50%	100%
A6	Subtotal: Avoided external cost of a data breach	A1*A2*A3*A4*A5	$238,248	$238,248	$476,496
A7	Hours of security labor for triage, investigation, and remediation per breach in prior environment	Forrester CDB survey data	7.5	7.5	7.5
A8	Average incident response analyst fully burdened hourly rate	Composite	$58	$58	$58
A9	Hours of lost user productivity per breach	Forrester CDB survey data	36,000	36,000	36,000
A10	Average fully burdened hourly salary for end user FTEs	BLS, March 2022	$38	$38	$38
A11	Productivity recapture rate	Forrester	50%	50%	50%
A12	Subtotal: Avoided internal cost of a data breach	A1*A2*A4*((A7* A8)+(A9*A10)) *A11	$381,679	$381,679	$381,679
At	Avoided severe data breaches	A6+A12	$619,927	$619,927	$858,175
	Risk adjustment	↓15%			
Atr	Avoided severe data breaches (risk-adjusted)		$526,938	$526,938	$729,449
	Three-year total: $1,783,325			**Three-year present value: $1,462,566**	

REDUCED INVOICE FRAUD

Evidence and data. Invoice fraud was a significant problem in interviewees' prior email security environment. For those who leveraged it, Abnormal Security's VendorBase functionality analyzed vendors based on past email communications and other risk signals. It then recognized when vendor behavior deviated from the norm and blocked all suspicious emails from the sender, preventing further invoice fraud.

Abnormal Security's message filtering blocked sophisticated and costly fraudulent requests for payment from reaching their recipients' mailboxes.

- The global technology services director in the commodities sector described their organization's experience with invoice fraud in the prior email environment. They shared that the organization paid three false invoices in the last three years totaling more than a half-million dollars. They admitted: "The risk is immense, as our invoices can be in the hundreds of millions. We've had instances where members of staff salaries have been paid to the wrong account."
- The manager of corporate email in the insurance industry shared: "We benefited from VendorBase, their capability for claims, fraud, and invoice fraud. After it's passed through the other tools, Abnormal Security is finding an additional 6,000 to 8,000 emails that aren't legitimate business emails, which it removes from a user's mailbox."
- The cybersecurity manager in the manufacturing sector reported up to five fraudulent invoices being paid monthly with most of them under $10,000. Furthermore, they described which roles would save time from blocking invoice fraud-related emails with Abnormal Security. They said, "A lot of the people involved would be accounting and purchasing resources, the corporate office, senior people in that department to prevent that from being processed."
- The chief information officer in the fintech industry shared false invoices sent to their organization averaged around $20,000. They expanded: "It's probably 5% of 6,000 malicious emails getting past without being caught by other tools, but those are the most critical that you want to stop. Abnormal has just totally removed it from our list of things we're concerned about."



Modeling and assumptions. By effectively blocking anomalous emails, the composite avoids significant direct costs related to payouts of fraudulent invoices. It also avoids significant labor costs associated with invoice fraud investigation and remediation, which occurs with high frequency in the prior environment. Of all delivered malicious emails:

- Five percent are related to invoice fraud at a typical cost of $10,000.
- Three percent of users are likely to click through on a fraudulent invoice.
- Twenty-five percent of those who click act on the fraudulent invoice.
- For every single correctly identified malicious email, there are two incorrectly identified as fraud. These emails entail investigation effort but no direct payout to fraudsters.
- Prior to Abnormal Security, 180 emails require investigation, each entailing:
    - Four hours of security investigation at a fully burdened hourly rate of $58.
    - Eight hours of finance investigation at a fully burdened hourly rate of $43.

- Over three years, the composite organization avoids nearly $1.8 million in fraudulent invoices. It further avoids over $311,000 over three years in internal security and finance investigation resource hours. Forrester applies a 50% productivity recapture to time savings, indicating that resources repurpose 50% of the time saved to value-add activities.

Risks. The extent to which Abnormal Security may reduce an organization's exposure to invoice fraud depends on a variety of factors. These may include:

- The number, size, and cost of successful payments to fraudulent invoices the company experiences before deploying Abnormal Security.[22]
- The presence and efficacy of upstream email security systems.[23]
- The volume and nature of sensitive information that end users can access resulting from a breach, which will impact realized financial costs.
- The sophistication of incoming fraudulent invoices, which will impact the likelihood of users interacting with them. End-user awareness of and adherence to policies around invoice fraud can counteract this risk.
- Average costs of invoice fraud, considering both the low likelihood of larger attacks and higher likelihood of lower-level attacks, as well as any other internal or external business disruption caused by payment of a fraudulent invoice.
- Other controls in place to identify and prevent invoice fraud, as well as internal security processes and systems, impacting how quickly issues and incidents can be investigated and remediated.
- Salary and seniority level of analysts to monitor and act on invoice fraud, which may vary. Action taken against any given fraudulent invoice may involve more or less finance and analyst time.

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

Reduced Invoice Fraud

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of invoice fraud-related emails delivered in prior environment	Composite	8,000	8,000	8,000
B2	Typical clickthrough rate for invoice fraud emails reaching inboxes	Verizon	3%	3%	3%
B3	Likelihood of a successful email-related invoice fraud attack once clicked through	Composite	25%	25%	25%
B4	Number of malicious emails resulting in invoice-fraud in prior environment	B1*B2*B3	60	60	60
B5	Reduction in malicious emails blocked by Abnormal Security	A4	99.97%	99.97%	99.97%
B6	Average cost of invoice fraud	Interviews	$10,000	$10,000	$10,000
B7	Subtotal: Avoided external costs of invoice fraud attacks	B4*B5*B6	$599,820	$599,820	$599,820
B8	Percent of invoice fraud email false positives in prior environment for every truly fraudulent invoice emailed	Composite	200%	200%	200%
B9	Number of invoice-fraud related emails requiring investigation in prior environment	B4+(B4*B8)	180	180	180
B10	Security team hours to monitor and investigate invoice fraud in prior environment	Composite	4	4	4
B11	Average incident response analyst fully burdened hourly rate	A8	$58	$58	$58
B12	Finance team hours to monitor and investigate invoice fraud	Composite	8	8	8
B13	Finance resource fully burdened hourly salary	Composite	$43	$43	$43
B14	Subtotal: Avoided internal costs of invoice fraud attacks	B9*((B10*B11) +(B12*B13))	$103,680	$103,680	$103,680
Bt	Reduced invoice fraud	B7+B14	$703,500	$703,500	$703,500
	Risk adjustment	↓15%			
Btr	Reduced invoice fraud (risk-adjusted)		$597,975	$597,975	$597,975
	Three-year total: $1,793,925			**Three-year present value: $1,487,075**	

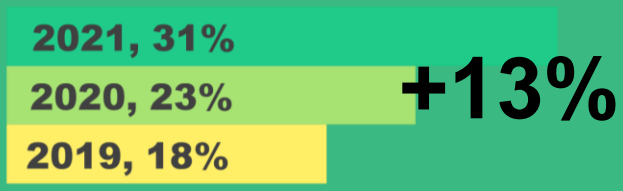
PREVENTED PHISHING

Evidence and data. Phishing, once the main security concern many interviewees reported, was effectively neutralized with Abnormal Security.

- The chief information officer in the fintech industry shared their users' experience with phishing emails. They said: "I was still getting 10% of people, so 60 staff, clicking every time. That's the need for Abnormal. We had a bad incident when a legitimate vendor had a mailbox compromised with malware. Abnormal proved that it would have been able to prevent that. It's blocking around 100 phishing emails a month, but the important thing is not the volume. For Abnormal Security, it's the intelligence."
- The cybersecurity manager in manufacturing shared how their organization's security posture changed with Abnormal Security. Speaking of phishing emails, they noted: "Either they don't make it through at all or we can very clearly tell when that sort of activity is happening. We can then alert our contacts and be very proactive about what has happened."

Phishing As An Attack Vector

Over the past three years of the Forrester's Analytics Business Technographics® Security Survey, 2021, respondents of who suffered an external attack increasingly cited phishing as the attack vector.



Source: Forrester Analytics Business Technographics® Security Survey, 2021

Modeling and assumptions. Abnormal Security's ability to block malicious emails helps the composite organization avoid the escalating costs of phishing as follows.

- Of all delivered malicious emails delivered in the prior environment:
  - Fifteen percent are related to phishing at an average cost of $1,000 per successful phishing attempt. From that portion of email traffic, 24,000 emails pass through upstream message filtering.
  - Ten percent of users are likely to click through on a phishing email reaching their inboxes.
  - Twenty-five percent of those who clicked would have actioned on the phishing attempt.
- Of the 24,000 phishing emails delivered in the prior environment, 600 phishing emails would have been actioned by users, entailing external costs and internal security resources. Per-incident response costs are tabulated here with further operational costs and related savings associated with monitoring user-reported suspicious emails tabulated in Benefit D.

Risks. The extent to which Abnormal Security may reduce an organization's exposure to phishing depends on a variety of factors. These may include:

- The number, size, and cost of successful phishing attempts the company experiences before deploying Abnormal Security.[24]
- The presence and efficacy of upstream email security systems.[25]
- The sophistication of incoming phishing attempts, which will impact the likelihood of users interacting with them. End-user awareness of and adherence to policies around phishing can counteract this risk.

- The effectiveness of the company's email provider or of any security control already in place and, hence, the incrementality of the solution Abnormal Security provides.
- The volume and nature of sensitive information that end users can access resulting from a breach, which will impact realized financial costs.
- Internal security processes and systems, impacting how quickly issues and incidents can be investigated and remediated.
- The nature of any resulting breach, which will impact realized financial costs.
- Average costs of phishing, considering both the low likelihood of larger attacks and higher likelihood of lower-level attacks, as well as any other internal or external business disruption caused by phishing.
- Other controls in place to identify and prevent phishing, as well as internal security processes and systems, impacting how quickly issues and incidents can be investigated and remediated.
- Salary and seniority level of analysts to monitor and act on invoice fraud, which may vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.3 million.

"I was afraid that the system wasn't working because I wasn't seeing anything.

In reality, it was doing exactly what we wanted it to do."

Cybersecurity manager, manufacturing

Prevented Phishing

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of phishing-related emails delivered in prior environment	Composite	24,000	24,000	24,000
C2	Typical clickthrough rate for phishing emails reaching inboxes	Interviews	10%	10%	10%
C3	Likelihood of a successful email-related attack after clicking through	B3	25%	25%	25%
C4	Number of emails resulting in successful phishing attacks in prior environment	C1*C2*C3	600	600	600
C5	Reduction in invoice fraud emails with by Abnormal Security	B5	99.97%	99.97%	99.97%
C6	Average cost of successful phishing attacks	Composite	$1,000	$1,000	$1,000
Ct	Prevented phishing	C4*C5*C6	$599,820	$599,820	$599,820
	Risk adjustment	↓15%			
Ctr	Prevented phishing (risk-adjusted)		$509,847	$509,847	$509,847
	Three-year total: $1,529,541			**Three-year present value: $1,267,914**	

STREAMLINED SECURITY OPERATIONS

Evidence and data. Interviewees communicated several ways in which their organizations saved money from simplifying their email environment with Abnormal Security. These included:

Cost consolidation from legacy email environment.

- The cybersecurity manager in the manufacturing sector shared: "We actually did a five-year deal with Abnormal Security. It was related to costs, but it was also just how efficient and effective the service was for us."
- With Abnormal Security, the chief information officer in the fintech industry reported legacy savings from downsizing email security licenses.

Time savings in phishing reporting mailbox monitoring, reallocated to higher-value activities.

- The cybersecurity manager in the manufacturing sector shared how their organization had an analyst dedicated to email security. They explained: "I felt really bad because they were really good at it, but you can only take that so much before you get really burned out."
- The manager of corporate email in the insurance industry shared how Abnormal Security impacted their organization's phishing mailbox monitoring program. They shared: "It's still the same process for the end user, except now the analysis is done in real time versus previously someone having to wait 24 hours to get a message back from the security team. Abnormal Security will automatically send a communication and remove the message from the mailbox. It's quite effective and efficient from that perspective."

Reduction in mailbox takeover remediation, reallocated to higher-value activities.

- The chief information officer in the fintech industry shared how their organization reduced the number of phishing emails delivered and the effort involved with neutralizing them.
- The cybersecurity manager in the manufacturing sector also shared how Abnormal Security's Account Takeover feature helped their organization. They said: "We had around 15 phishing attacks last year, and two that the sales engineer from Abnormal escalated to us during our POC. Prior to Abnormal Security, that could have gone on for days, weeks, before the attacker did something that would have flagged something in our system, versus we had that completely remediated within two hours of it happening."

Displacement of the prior SEG and associated reduction in hardware, software, and internal and external maintenance costs.

- The global technology services director in the commodities sector opted to displace the incumbent SEG with Abnormal Security's continuous email monitoring. They said: "I didn't see the value that a SEG would provide on top of [our enterprise email] and Abnormal Security. We haven't noticed any loss by not having a SEG , we just noticed gain. So, I basically redeployed the budget I used to spend on the SEG to Abnormal Security."
- The cybersecurity manager in the manufacturing sector also reported displacing the incumbent SEG. They noted: "We still rely on [our email client for] basic configuration for exchange online, bulk spam, and the like, and then Abnormal Security handles everything else first."

"Account takeovers have been completely remediated with Abnormal Security."

Chief information officer, fintech

Modeling and assumptions. In addition to deploying its inbound email security protection throughout the entire investment period, the composite organization takes a multiyear approach to simplifying its email security environment.

- **Phishing monitoring.** In the prior environment, the composite organization fully dedicates one email security resource to monitoring and triaging messages reported to the company's phishing mailbox.
    - With Abnormal Security's inbound email protection, the composite organization reduces this time by half in Year 1. The remainder of the time is used to monitor safe emails that employees report for further investigation.
    - In Year 2, the composite organization switches on the Abuse Mailbox Automation from Abnormal Security. This centralizes all user-reported messages and automatically analyzes, classifies, remediates, and responds to them, reducing the effort the email security resource requires by 95%.
- **Account takeover.** In the prior environment, 30 successful phishing attacks (5% of all successful attacks) require incident response teams to secure an infected mailbox, resulting in thirty attacks, each involving 6.5 hours of investigation and remediation from the incident response team.
    - In Year 3, the composite organization further decreases complexity in its email security environment by turning on Abnormal Security's Account Takeover Protection (see Costs E). With Account Takeover Protection deployed, Abnormal Security detects when employee accounts have been compromised, automatically remediates any messages sent from them, and disarms the account before further damage can occur. This nearly eliminates the incident response team effort, avoiding 99% of the time to remediate infected mailboxes.
    - Forrester applies a 50% productivity recapture to time savings, indicating that resources repurpose 50% of the time saved to value-add activities.
- **SEG displacement.** In Year 3, the composite also decommissions the incumbent SEG. This helps the composite organization save on hardware and ongoing software, maintenance, and other related costs.

Risks. The extent to which Abnormal Security may streamline an organization's security operations depends on a variety of factors. These may include:

- The number, size, and cost related to managing malicious emails that the company experiences before deploying Abnormal Security.[26]
- The presence and efficacy of upstream email security systems.[27]
- The sophistication of incoming phishing attempts, which will impact the likelihood of users interacting with them. End-user awareness of and adherence to policies around phishing can counteract this risk.
- Internal security processes and systems, impacting how quickly issues and incidents can be investigated and remediated.

- Other controls in place to identify and prevent delivery of malicious emails, as well as internal security processes and systems, impacting how quickly issues and incidents can be investigated and remediated.
- Salary and seniority level of analysts to monitor and act on malicious emails, which may vary.
- Whether a customer chooses to displace its SEG with Abnormal Security.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $139,000.

Streamlined Security Operations

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Hours of phishing email box monitoring and investigation in prior environment	Composite	2,080	2,080	2,080
D2	Reduction in hours of phishing email box monitoring and investigation in prior environment	Interviews	50%	95%	95%
D3	Email security analyst fully burdened hourly salary	Composite	$50	$50	$50
D4	Productivity recapture rate	Forrester	50%	50%	50%
D5	Subtotal: Reduction in phishing mailbox monitoring with Abnormal Security	D1*D2*D3*D4	$26,000	$49,400	$49,400
D6	Percent of successful phishing attack requiring account takeover in prior environment	Composite	5%	5%	5%
D7	Number of successful phishing attacks requiring account takeover in prior environment	C4*D6	30	30	30
D8	Hours of account takeover remediation from successful phishing attacks	Composite	6.5	6.5	6.5
D9	Reduction in hours of account takeover remediation from successful phishing attacks	Interviews	0%	0%	99%
D10	Average incident response analyst fully burdened hourly rate	Composite	$58	$58	$58
D11	Productivity recapture rate	Forrester	50%	50%	50%
D12	Subtotal: Avoided account takeover costs	D7*D8*D9*D10*D1 1	$0	$0	$5,598
D13	Savings from decommissioning SEG hardware with Abnormal Security	Interviews	$0	$0	$20,000
D14	Savings from decommissioning SEG software and maintenance with Abnormal Security	Interviews	$0	$0	$45,000
Dt	Streamlined security operations	D5+D12+D13+D14	$26,000	$49,400	$119,998
	Risk adjustment	↓10%			
Dtr	Streamlined security operations (risk-adjusted)		$23,400	$44,460	$107,998
	Three-year total: $175,858			**Three-year present value: $139,157**	

UNQUANTIFIED BENEFITS

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

- **Improved insight into the email threat landscape.** The cybersecurity manager in the manufacturing sector noted that Abnormal Security provided better insight into the threat landscape: "I like having a very easy-to-understand interface where I can see how the product is making the decision to block an email. I can go into the platform and see exactly what in the email caused them to be suspicious about it."

  The global technology services director in the commodities sector said: "If [a malicious email] was sent, we were able to get it corrected before there was an exposure. It would then show exactly how their technology was successful in detecting that this was a true attack."
- **Confidence in email security posture.** The chief information officer in the fintech industry admitted: "Their mailbox threat protection is really good. Furthermore, if we did have a mailbox compromised, I'm pretty confident that Abnormal's Account Takeover Protection would automatically remediate it for us. That's something that has made me sleep better at night."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Abnormal Security and later realize additional uses and business opportunities, including optimizing the use of the solution's out-of-the-box features.

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

"At the end of the day, we can take a good chunk of our focus off what we consider to be a major attack vector for us and put it to other avenues."

Cybersecurity manager, manufacturing

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	Abnormal security fees	$0	$315,000	$399,000	$472,500	$1,186,500	$971,112
Ftr	Deployment and implementation costs	$4,910	$3,296	$3,296	$6,046	$17,547	$15,172
Gtr	Channel partner and roadmap costs	$278	$54,278	$68,678	$81,278	$204,514	$167,447
	Total costs (risk-adjusted)	$5,189	$372,574	$470,974	$559,824	$1,408,561	$1,153,731

ABNORMAL SECURITY FEES

Evidence and data. Interviewees' organizations experienced costs related to their Inbound Email Protection service. Several organizations experienced subscription fees for Abuse Mailbox Automation and Account Takeover Protection. Fees were based on the number of mailboxes Abnormal Security covered.

Modeling and assumptions. The composite organization's fees align with the growth trajectory of Abnormal Security's product roadmap.

- In Year 1, Abnormal Security fees for the composite organization comport with standard pricing for an organization with 10,000 inboxes protected with inbound email security.
- The composite organization activates Abnormal Security's Abuse Mailbox Automation in Year 2.
- In Year 3, the composite organization further subscribes to Abnormal Security's Account Takeover Protection service.

Risks. Forrester recognizes that these results may not be representative of all experiences and the cost will vary depending on:

- The number of inboxes protected.
- The number and type of modules deployed.
- Potential for future changes to pricing, capabilities, or packaging.
- Deployment and implementation.
- Pricing may vary. Contact Abnormal Security for additional details.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $971,000.

Abnormal Security Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Abnormal Security fees	Composite		$300,000	$380,000	$450,000
Et	Abnormal security fees	E1	$0	$300,000	$380,000	$450,000
	Risk adjustment	↑5%				
Etr	Abnormal security fees (risk-adjusted)		$0	$315,000	$399,000	$472,500
	Three-year total: $1,186,500			**Three-year present value: $971,112**		

DEPLOYMENT AND IMPLEMENTATION COSTS

Evidence and data. Interviewees described an implementation period which included a proof of concept. In this phase, the interviewees permitted Abnormal Security read-only analysis of a subset of mailboxes to demonstrate the efficacy of its threat detection.

The global technology services director in the commodities sector described their organization's experience from POC to implementation: "Once I'd seen the report on how it did, we signed the purchase order, and then we implemented it within four weeks. We got it working and fully integrated pretty quickly. It took us about eight weeks to fully ramp up because we migrated across 212 email domains."

Modeling and assumptions. The composite organization launches Abnormal Security's inbound email security protection first as POC. The initial deployment phase for activating inbound mailbox protection is four calendar months.

- This includes 80 hours of initial technical implementation and 1 hour a month of ongoing systems administration. Such efforts include scoping, running the POC, conducting testing and reviewing feedback, conducting security and governance reviews, installations, and initial custom rules configuration. The fully burdened hourly rate of an email security analyst is $50.
- This period also entails 8 hours of security oversight to secure system administration and updates, as well as other security checks and group management. The fully burdened hourly rate of a security analyst is $58.
- The composite organization adds Abnormal Security's Abuse Mailbox Automation in Year 2 and Account Takeover Protection in Year 3, both requiring ten additional hours of implementation to deploy.
- In Year 3, it also displaces the SEG and decommissions legacy SEG hardware, software, and services. The effort to migrate its 20 domains results in another deployment push of 60 hours in Year 3.
- In addition to basic product administration, two email security resources spend 1 hour a month meeting with Abnormal Security for regular business reviews regarding threat management and planning, including analysis of threat trends, behavioral patterns, and high-risk groups and subsequent updates to improve email security and minimize risk.

Risks. Forrester recognizes that these results may not be representative of all experiences. The costs will vary depending on:

- The presence and efficacy of upstream email security systems, which will impact the number of emails screened by Abnormal Security.
- Internal security processes, impacting how quickly new systems can be implemented.
- Internal requirements for security and governance reviews.
- The modules being deployed and the level of customization implemented.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $15,000.

> **"We effectively rolled right from POC into production. It was immensely easy for us because we didn't have to change [domain name system] (DNS) records."**
>
> *Cybersecurity manager, manufacturing*

Deployment And Implementation Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Hours of technical implementation	Composite	80	10	10	60
F2	Hours of system administration	Composite	0	12	12	12
F3	Hours of threat management, policy rightsizing, and planning leveraging Abnormal Security	Composite	0	24	24	24
F4	Email security analyst fully burdened hourly salary	Composite	$50	$50	$50	$50
F5	Subtotal: hours of technical implementation and administration	(F1+F2+F3)*F4	$4,000	$2,300	$2,300	$4,800
F6	Hours of SecOps cloud perimeter oversight	Composite	8	12	12	12
F7	Security analyst fully burdened hourly salary	Composite	$58	$58	$58	$58
F8	Subtotal: hours of security oversight	F6*F7	$464	$696	$696	$696
Ft	Deployment and implementation costs	F5+F8	$4,464	$2,996	$2,996	$5,496
	Risk adjustment	↑10%				
Ftr	Deployment and implementation costs (risk-adjusted)		$4,910	$3,296	$3,296	$6,046
	Three-year total: $17,547			**Three-year present value: $15,172**		

CHANNEL PARTNER AND ROADMAP COSTS

Evidence and data. Some interviewees experienced costs associated with channel partners. Multiple interviewees also reported spending additional time with Abnormal Security, above and beyond the regular threat monitoring noted in Cost F. This additional time was spent planning the customer email security roadmap around Abnormal Security.

- The manager of corporate email in the insurance industry described their relationship with Abnormal Security: "We meet with them quarterly as part of their business review, and they provide information-based analysis on the previous quarter's experience with phishing credentials, extortion, invoice payment, and other fraud."
- The global technology services director in the commodities sector noted that, as a manager, they participated in quarterly meetings with their team and Abnormal Security. This was in addition to the 1-hour monthly meeting with Abnormal Security that their direct reports attended (see Cost F).
- Of its more involved relationship with Abnormal Security, the cybersecurity manager in the manufacturing sector discusses their more involved relationship with Abnormal Security: "The leadership team saw this as an opportunity to establish a new kind of relationship with one of our key security vendors. We are watching the roadmap to leverage their monitoring, detection and remediation offerings."

Modeling and assumptions. The composite organization experiences 15% channel partner fees on top of Abnormal Security subscription fees.

It also opts for a higher level of engagement with Abnormal Security to continually advance its own email security strategy to align with Abnormal Security offerings.

In addition to the monthly security review meetings with Abnormal Security (noted in Cost F), the email security manager joins these 1-hour meetings on a quarterly basis. The fully burdened hourly rate for the email security manager is $58.

Risks. Forrester recognizes that these results may not be representative of all experiences. The costs will vary depending on:

- Whether a channel partner is engaged and the rate of their partnership fees.
- The depth of roadmap planning performed directly with Abnormal Security above and beyond regular security reviews.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $167,000.

> **"I've been very impressed with their roadmap, their support, and the effectiveness of the product."**
>
> *Cybersecurity manager, manufacturing*

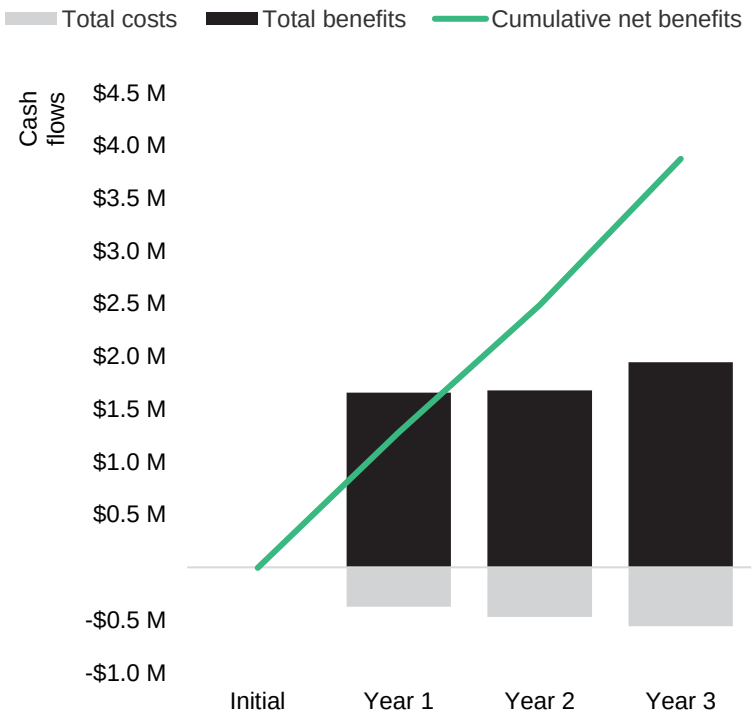
Channel Partner And Roadmap Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Channel partner pass through paid by composite	Et*15%		$45,000	$57,000	$67,500
G2	Additional threat management and planning leveraging Abnormal roadmap	Composite	4	4	4	4
G3	Hourly rate per email security manager	Composite	$58	$58	$58	$58
Gt	Channel partner and roadmap costs	G1+(G2*G3)	$232	$45,232	$57,232	$67,732
	Risk adjustment	↑20%				
Gtr	Channel partner and roadmap costs (risk-adjusted)		$278	$54,278	$68,678	$81,278
	Three-year total: $204,514			**Three-year present value: $167,447**		

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 Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($5,189)	($372,574)	($470,974)	($559,824)	($1,408,561)	($1,153,731)
Total benefits	$0	$1,658,160	$1,679,220	$1,945,269	$5,282,649	$4,356,712
Net benefits	($5,189)	$1,285,586	$1,208,246	$1,385,445	$3,874,088	$3,202,981
ROI						278%
Payback period (months)						<6

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] 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.

[2] Source: "The State Of Data Security, 2022," Forrester Research, Inc., September 20, 2022.

[3] Source: "The 2021 State Of Enterprise Breaches," Forrester Research, Inc., April 8, 2022.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Ibid.

[9] Ibid.

[10] Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[11] Source: "The State Of Data Security, 2022," Forrester Research, Inc., September 20, 2022.

[12] Ibid.

[13] Ibid.

[14] Source: "Best Practices: Phishing Prevention," Forrester Research, Inc., November 18, 2021.

[15] Ibid.

[16] Source: "The Forrester Tech Tide™: B2B Payment Augmentation, Q1 2022," Forrester Research, Inc., March 23, 2022.

[17] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

[18] Source: Ibid; Forrester Analytics Business Technographics® Security Survey, 2021

[19] Ibid.

[20] Breaches and privacy incidents vary in size and reach, so the consequences of data exposure or misuse can vary greatly. The same applies to quantifying benefits, as the value of data will depend on value derived from its use. The number and of attacks directed at the organization may vary by industry, e.g., malicious actors tend to target financial services firms more than some other industries. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[21] The effectiveness of the company's email provider or of any security control already in place will impact the number of emails screened by Abnormal Security and, hence, the incrementality of the solution Abnormal Security provides. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[22] Breaches and privacy incidents vary in size and reach, so the consequences of data exposure or misuse can vary greatly. The same applies to quantifying benefits, as the value of data will depend on value derived from its use. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[23] The effectiveness of the company's email provider or of any security control already in place will impact the number of emails screened by Abnormal Security and, hence, the incrementality of the solution Abnormal Security provides. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[24] Breaches and privacy incidents vary in size and reach, so the consequences of data exposure or misuse can vary greatly. The same applies to quantifying benefits, as the value of data will depend on value derived from its use. The number and of attacks directed at the organization may vary by industry, e.g., malicious actors tend to target financial services firms more than some other industries. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[25] The effectiveness of the company's email provider or of any security control already in place will impact the number of emails screened by Abnormal Security and, hence, the incrementality of the solution Abnormal Security provides. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[26] Breaches and privacy incidents vary in size and reach, so the consequences of data exposure or misuse can vary greatly. The same applies to quantifying benefits, as the value of data will depend on value derived from its use. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.

[27] The effectiveness of the company's email provider or of any security control already in place will impact the number of emails screened by Abnormal Security and, hence, the incrementality of the solution Abnormal Security provides. Source: "The Business Case For Privacy And Data Protection," Forrester Research, Inc., August 2, 2021.


FORRESTER®