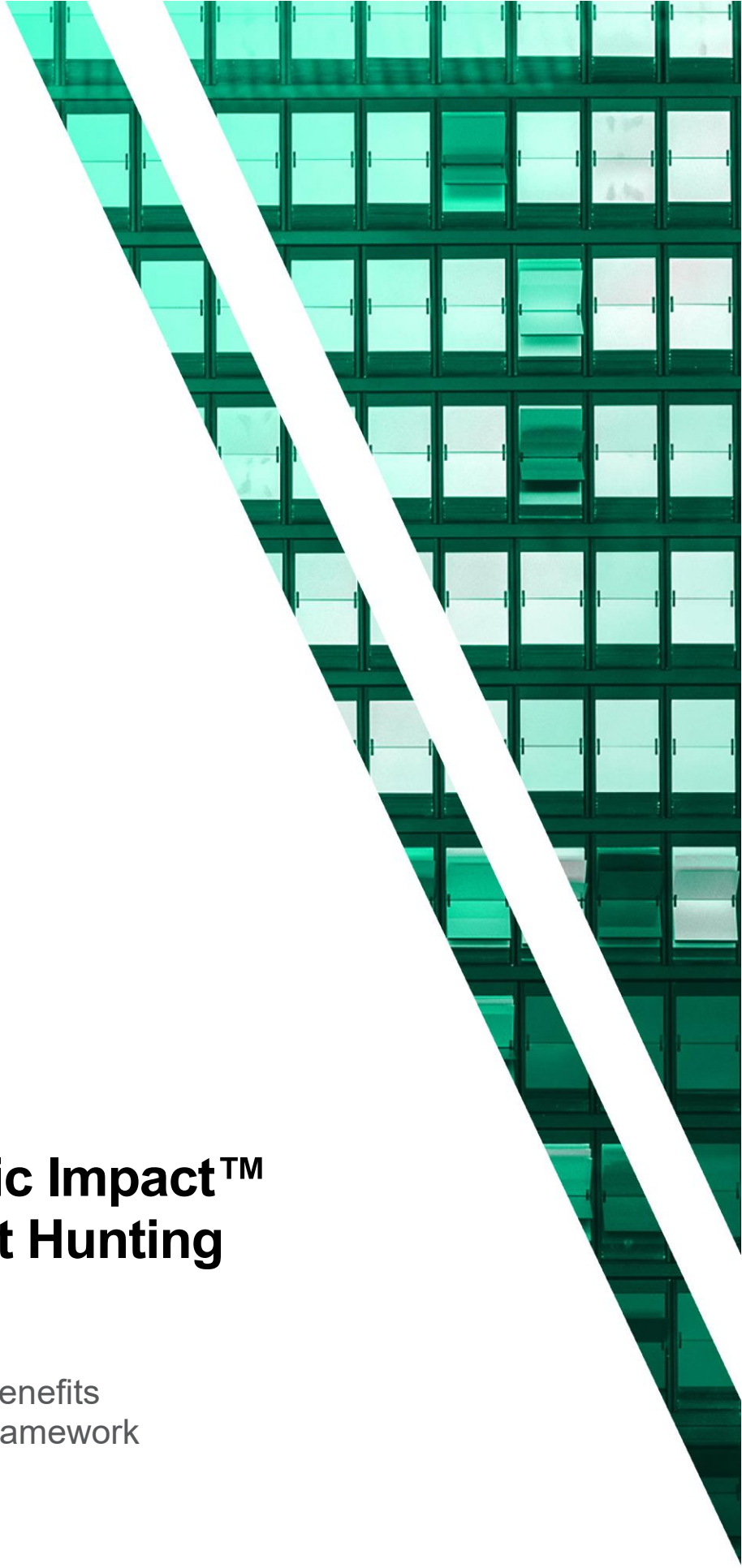
FORRESTER®



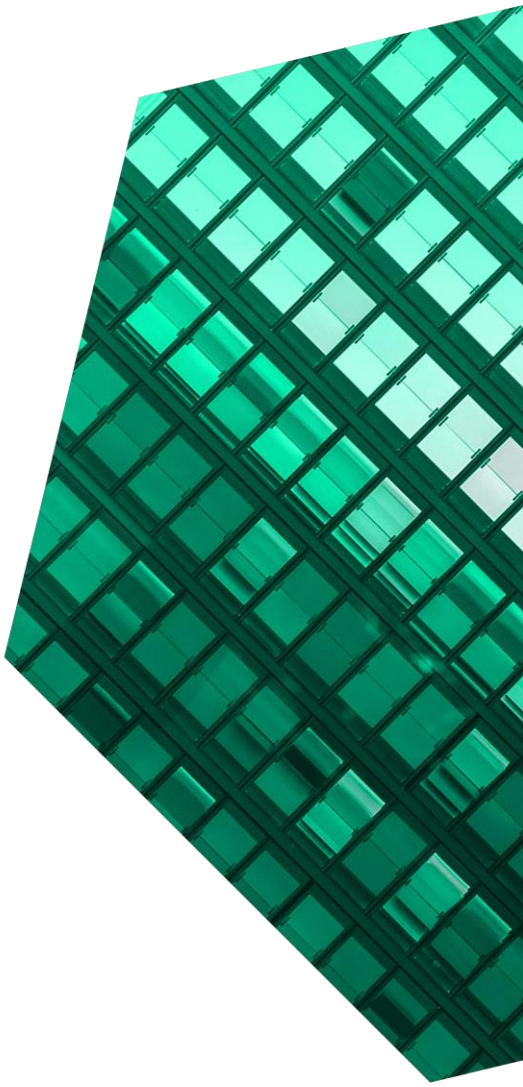
The Total Economic Impact™ Of Group-IB Threat Hunting Framework

Cost Savings And Business Benefits Enabled By Threat Hunting Framework

AUGUST 2021

Table Of Contents

Consulting Team: Sri Prakash Gupta



Executive Summary

Organizations that continually accelerate their performance in threat detection and response capabilities are far more likely to win, serve, and retain customers. However, sophisticated cyberthreats continue to rise and easily evade through standard security tools. Therefore, organizations need advanced threat-hunting and analysis tools that enable security teams to manage cyber risks, detect threats within protected perimeter and beyond, and efficiently manage security incidents.

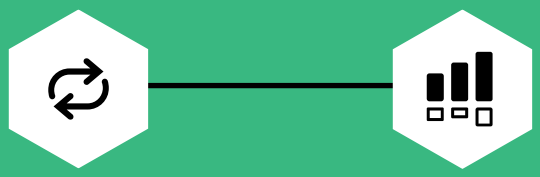
Group-IB is a global threat-hunting and adversary-centric cyberintelligence company that specializes in investigating and preventing high-tech cybercrimes. Group-IB Threat Hunting Framework (THF) is a comprehensive solution that identifies targeted attacks and unknown threats, hunts for threats, and performs incident response and investigation. In addition, Group-IB's ability to use threat-intelligence data to attribute detected threats to cybercriminals and hacker groups powers the overall Threat Hunting Framework.

Group-IB commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Group-IB THF. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Threat Hunting Framework on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed an organization with experience using Threat Hunting Framework. Forrester used this experience to project a three-year financial analysis.

> "Group-IB THF allows us to be much more strategic about how we manage our security environment. It is vital for business success to promptly detect threats and effectively manage security incidents."
>
> *Information security leader, financial services*

KEY STATISTICS



Return on investment (ROI)
272%

Net present value (NPV)
$1.4 million

Prior to using Group-IB THF, it would take the customer several hours to detect and analyze threats using a legacy sandbox tool and manual processes. However, these prior attempts yielded limited success. The organization was vulnerable to bigger cyberthreats, ransomware outbreaks, attacks on digital bank infrastructure using social-engineering techniques, and other unknown malicious objects that remain undetected by antivirus and signature-based systems.

- The rapidly evolving threat landscape and increasing cyber risks needed advanced security methods.
- The organization struggled to prevent malware attacks and threats involving email as an entry point. Email is a vital medium for communicating with customers, suppliers, partners, and prospects. Malicious actors

often targeted email due to its ubiquitous nature and the trusted relationship between senders and recipients.

- A lack of visibility and security monitoring tools impacted business operations with haphazard incident response and investigation methods.

The customer decided to focus on a layered defense involving several sandboxes to improve its detection capabilities. After testing many products, the customer decided to use Group-IB THF.

After the investment in Group-IB THF, the organization efficiently identified threats within protected perimeter and beyond, and performed incident response and investigation. The organization gained better visibility of cyberthreats, detonating files in isolated environments, and extracting indicators of compromise that typical security tools usually overlook (e.g., antivirus software, firewalls, intrusion prevention systems, etc.).

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Savings from improved email protection, resulting in over $907,000 in benefits over three years.** Emails are the most common attack vector cybercriminals use. Group-IB THF provided accurate assessment of threat levels based on the organization's typical work scenarios, IT landscape, and variety of information processed. In addition, the solution conducted a behavioral analysis of files and links in isolated environments, correlated the events, and effectively identified previously unknown vectors of hacker attack. With improved email protection, the organization achieved an efficiency increase of 20% in three years.
- **Cost savings from avoidance of data breaches, resulting in nearly $448,000 in benefits over three years.** Group-IB THF protects endpoint devices and performs dynamic analysis of malware on virtual machines. It also performs fully executable codes and extracts indicators of compromise. Real-time analysis of data and improved monitoring of endpoints devices helped the customer organization to avoid breaches. Forrester estimates that the average probability of a breach is about 10% and, with prompt response to mitigate threats due to THF, the risk of data breach reduces by 50%.

50% reduced risk of a data breach with Group-IB THF.

- **Improved productivity and security team efficiency, resulting in nearly $384,000 in benefits over three years**. Automatic incident investigation saves time on routine tasks. The organization realized productivity gains with Group-IB THF and increased efficiency for its security team by 20%. It also allowed security analysts to gather vital information about cyberattacks, gain a higher visibility of network traffic, promptly mitigate threats, and make use of time for improvements and innovations.

20% improvement in tier one and tier two security incident response times.

- **Increased efficiency of prioritization and resolution of security incidents, resulting in almost $129,000 in benefits over three years.** The organization saw a 20% improvement in tier one security incident response efficiency. It also realized a 20% efficiency increase related to managing tier two and higher security incidents that require coordination across multiple IT and security resources. These efficiencies are gained by automating workflows that span security and IT teams, prioritizing security incidents based on

business criticality, and tracking incidents and assigning tasks using Group-IB THF.

Unquantified benefits. Benefits that are not quantified for this study include:

- **Better visibility into digital security threats, malware attacks.** Group-IB THF provided better visibility into advanced digital security threats and cyberattacks. This led to a better understanding and improved monitoring of relevant threats, increased focus on specific threat vectors and other activities to identify gaps, and an improved security posture for the organization.
- **Reduced cyber risks and potential reputational damage.** Group-IB THF provided threat-hunting capabilities to the organization that helped it understand the threat landscape, mitigate reputational risks, and prevent financial losses. Leveraging Group-IB THF, security and IT professionals became more confident about the organization's cyber risk posture**.**
- **Business operations continuity with low false rates.** Proactive threat hunting in network traffic within and outside the perimeter, as well as analysis of threats, has enabled the organization's security team to determine whether or not a threat is real. Low false positive rates prevented business disruptions.
- **Improved collaboration.** Group-IB THF provides a shared environment, remote incident response, digital forensics, and access to analyst community and experts. This led to improved collaboration and teamwork.

Costs. Risk-adjusted PV costs for the interviewee's organization, include:

- **Group-IB THF subscription fees of over $306,000 over three years.** The Group-IB THF deployment cost includes an annual subscription fee, consultancy, an information-sharing community, and access to Group-IB analysts for custom analyses.
- **Planning, ongoing management, internal training support, and consultancy costs of nearly $196,000 over three years.** Group-IB THF is straightforward and the required resource time was minimal. Analysts can become proficient with the platform with a minimal amount of on-the-job learning and consultation with the Group-IB team.

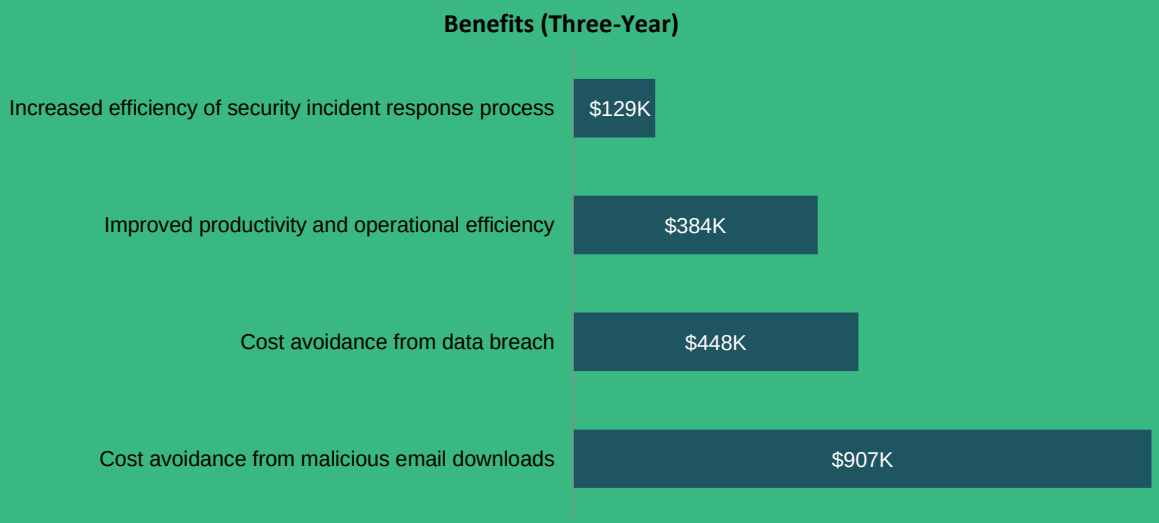
The interview and financial analysis found that this customer experiences benefits of almost $1.9 million over three years versus costs of over $502,000, adding up to a net present value (NPV) of nearly $1.4 million and an ROI of 272%.

ROI
272%

BENEFITS PV
$1.9 million

NPV
$1.4 million

PAYBACK
<6 months



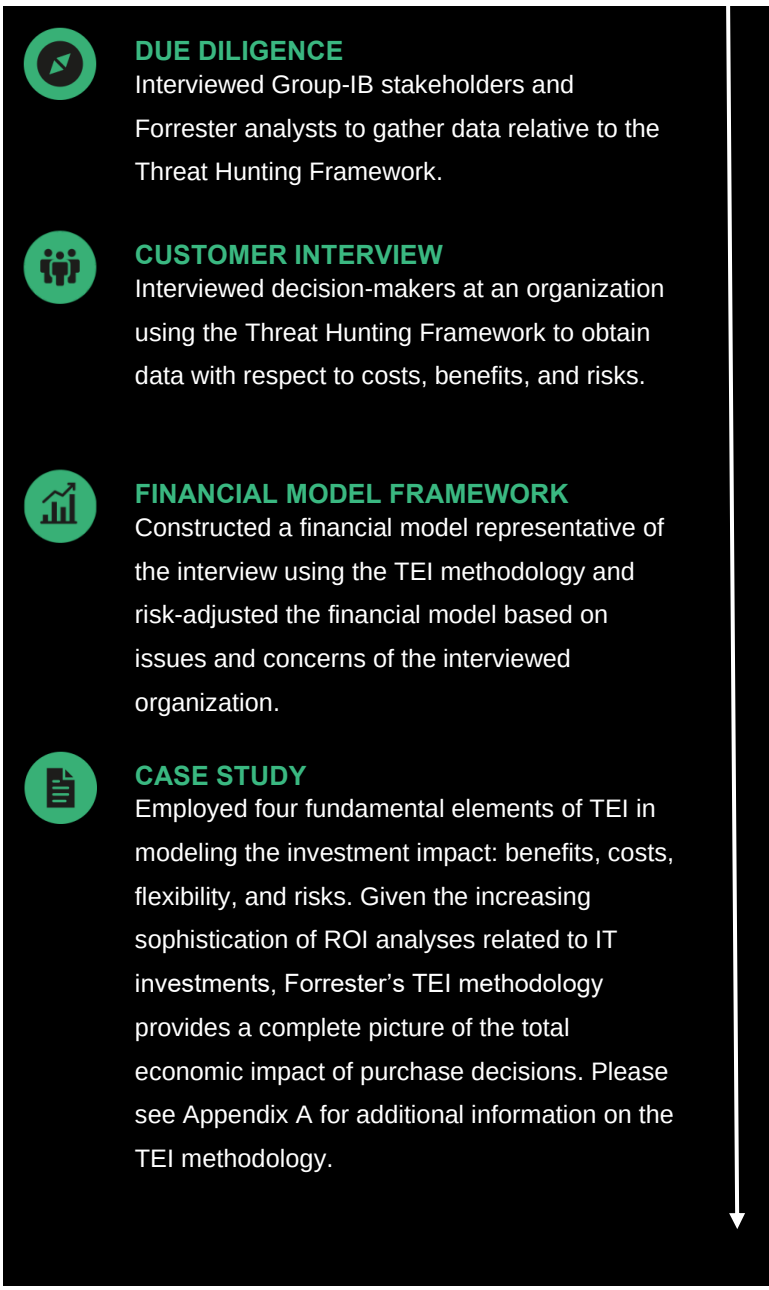
The perimeter of the infrastructure requires special attention from the information security department, thus modern technological security devices as THF at this point are needed.

— Information security leader, financial services

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 the Threat Hunting Framework.

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 the Threat Hunting Framework can have on an organization.



DISCLOSURES

Readers should be aware of the following:

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

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

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

Group-IB provided the customer name for the interview but did not participate in the interview.

The Group-IB Threat Hunting Framework Customer Journey

Drivers leading to the Threat Hunting Framework investment

INTERVIEWED ORGANIZATION

Forrester interviewed a Group-IB Threat Hunting Framework customer with the following characteristics:

- The organization is a large digital bank and financial services holding company.
- It generates more than $1 billion in annual revenue, and it has more than 100,000 employees.
- It has more than 10 million customers.
- It has used Group-IB THF for more than two years for email protection and security incident management. More specifically, to detect malicious code in email attachments, file downloads, links, and targeted attacks.
    - Email attachment: Malicious files sent to users via email as a part of social engineering and targeted attacks.
    - File download: Documents or objects downloaded by users and their devices during attacks on browsers.
    - Links: Suspicious links extracted from email, documents, and archives.
    - Targeted attacks: Malware configured to disrupt the business operations and infrastructure.

KEY CHALLENGES

Prior to investing in Group-IB THF, the organization struggled with several challenges related to threat hunting and the management of complex security incidents.

- The rapidly evolving threat landscape and increasing cyber risks needed advanced security methods.
- The organization was vulnerable to bigger cyberthreats, ransomware outbreaks, more fraud and attacks on digital banking infrastructure using social engineering techniques, and other unknown malicious objects that remain undetected by antivirus and signature-based systems.
- The organization struggled to prevent malware attacks and threats involving email as an entry point. Email is a vital medium for communicating with customers, suppliers, partners, and prospects. Malicious actors often targeted email due to its ubiquitous nature and the trusted relationship between senders and recipients.
- A lack of visibility and security monitoring tools impacted business operations with haphazard incident response and investigation methods.

SOLUTION REQUIREMENTS

The interviewed organization searched for a solution that could:

- Efficiently administer email traffic and augment email protection regardless of physical servers, cloud servers, or hybrid configuration.
- Provide behavioral analysis of files, email attachments, and links in isolated environment.
- Protect corporate emails from targeted phishing and malware attacks.
- Provide in-depth analysis of network traffic to detect traffic and provide more visibility of potential threats and malicious traffic. Faster

detection of anomalies and perform malware analysis.

- Protect end-user devices and servers from unwanted apps and untrustworthy devices.

USE CASE DESCRIPTION

The digital banking and financial services company serves 10 million customers remotely through online channels and a contact center. The bank's unique structure imposes high requirements on the level of information security for both internal systems and financial product and services. Therefore, the topmost priorities for the organization were twofold: 1) uninterrupted business operations and 2) proactive threat management against a wide range of cyberthreats that might impact business continuity.

The organization found that antivirus software wasn't effective against targeted cyberattacks, ransomware outbreaks, and attacks on digital bank infrastructure using social engineering techniques, and other unknown malicious objects that remain undetected by antivirus and signature-based systems.

It decided to focus on a layered defense with several sandboxes to improve its detection capabilities. After testing many products, the customer decided to use Group-IB THF.

For this use case, Forrester has modeled benefits and costs over three years.

Key assumptions

- **$1 billion annual revenue**
- **10 million customers**
- **10,000 employees**
- **10,000 endpoints**
- **1,000 emails detected with malicious code per year**
- **20% efficiency enabled by Group-IB THF**

Analysis Of Benefits

Quantified benefit data

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Cost avoidance from malicious email downloads	$240,000	$370,800	$509,200	$1,120,000	$907,198
Btr	Cost avoidance from data breach	$180,000	$180,000	$180,000	$540,000	$447,633
Ctr	Improved productivity and operational efficiency	$150,000	$154,500	$159,135	$463,635	$383,610
Dtr	Increased efficiency of security incident response process	$50,400	$51,912	$53,466	$155,778	$128,890
	Total benefits (risk-adjusted)	$620,400	$757,212	$901,801	$2,279,413	$1,867,331

COST AVOIDANCE FROM MALICIOUS EMAIL DOWNLOADS

Evidence and data. Email is the most common attack vector cybercriminals use. Threats involving email as entry point evolve continuously as new tactics, techniques, and tools develop. While standard tools, such as antispam systems and antivirus software, protect against certain threats, sophisticated target attacks require more advanced security methods. Group-IB THF enables email protection regardless of whether the company uses physical servers, cloud servers, or a hybrid configuration.

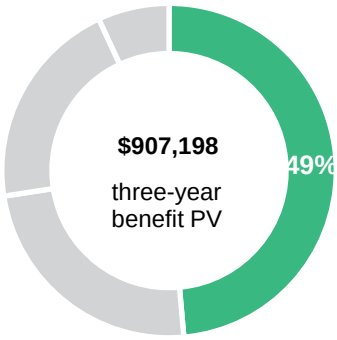
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- The composite organization experiences malicious downloads on 1,000 emails per year.
- The Group-IB THF improves the email protection by 20%.
- The Group-IB THF reduces the email threat mitigation time by 10% in Year 1. Further time savings for security teams are estimated for Year 2 and Year 3.

Risks. The savings from email protection could vary with:

- The total number of emails identified with malicious downloads per year.
- The average percentage of efficiency gain from email protection could vary depending on the type of business environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of nearly $907,000.



Cost avoidance from malicious email downloads: 49% of total benefits

Cost Avoidance From Malicious Email Downloads					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Average number of malicious emails downloads annually	Interview	1,000	1,000	1,000
A2	Improvement with Group-IB (attribution)	Interview	20%	20%	20%
A3	Average number of man-hours spent to remediate malicious email downloads (annually)	Interview	250	250	250
A4	Improved efficiency to remediate emails	Interview	10%	15%	20%
A5	Average hourly fully burdened rate of FTE	Assumption	$60.00	$61.80	$63.65
At	Cost avoidance from malicious email downloads	A1*A2*A3*A4*A5	$300,000	$463,500	$636,500
	Risk adjustment	↓20%			
Atr	Cost avoidance from malicious email downloads (risk-adjusted)		$240,000	$370,800	$509,200
	Three-year total: $1,120,000			**Three-year present value: $907,198**	

COST AVOIDANCE FROM DATA BREACH

Evidence and data. Group-IB THF protects endpoint devices and performs a dynamic analysis of malware on virtual machines. It also performs fully executable codes and extracts indicators of compromise. Real-time analysis of data and improved monitoring of endpoints devices helped the customer organization to avoid breaches.

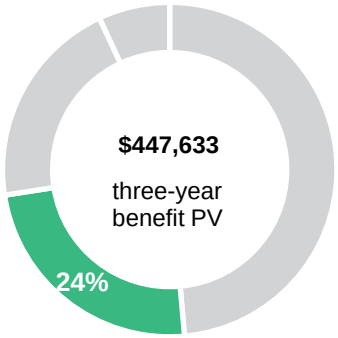
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- The average cost of data breach per endpoint is estimated $450 per year.[1]
- The average probability of breach is 10%.
- The risk avoidance of 50% is attributed to Group-IB THF.

Risks. The savings from data breach avoidance could vary with:

- The average cost of data breach per endpoint.
- The average probability of breach.
- The risk avoidance attributed to Group-IB THF could vary depending on the type of business environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of nearly $447,000.



Cost avoidance from data breach: 24% of total benefits

Cost Avoidance From Data Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Total number of endpoints to be protected	Interview	10,000	10,000	10,000
B2	Average cost of breach per end point	Ponemon	$450	$450	$450
B3	Average probability of breach	Assumption	10%	10%	10%
B4	Risk avoidance attributed to Group-IB	Assumption	50%	50%	50%
Bt	Cost avoidance from data breach	B1*B2*B3*B4	$225,000	$225,000	$225,000
	Risk adjustment	↓20%			
Btr	Cost avoidance from data breach (risk-adjusted)		$180,000	$180,000	$180,000
	Three-year total: $540,000			**Three-year present value: $447,633**	

IMPROVED PRODUCTIVITY AND OPERATIONAL EFFICIENCY

Evidence and data. Automatic incident investigation saves time on routine tasks. Group-IB THF helped the organization realize productivity gains and increased security team efficiency. It also allowed security analysts to gather vital information about cyberattacks, gain a higher visibility of network traffic, promptly mitigate threats, and make use of time for improvements and innovations.

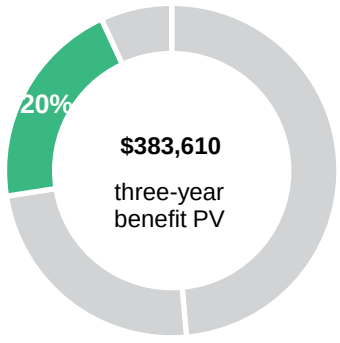
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- In Year 1, the average salary for a security analyst is $125,000. The salary then increases by 3% each year.
- To be realistic and conservative with the model, Forrester adjusted the productivity formulas with a productivity conversion ratio. Productivity conversion assumes that not every minute gained in productivity is put directly back into productive work. Staff could use that time to take longer breaks, leave work on time, etc. Forrester set the productivity conversion ratio for this study at 50%.

Risks. The savings from productivity gains and cybersecurity team efficiency could vary based on following factors:

- The salary of a security analyst.
- The productivity gain per security analyst.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of nearly $383,000.



Improved productivity and operational efficiency: 20% of total benefits

Improved Productivity And Operational Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Total FTEs	Interview	15	15	15
C2	Average annual fully loaded salary for security analyst	Assumption	$125,000	$128,750	$132,613
C3	Efficiency enabled by Group-IB	Assumption	20%	20%	20%
C4	Productivity conversion	Assumption	50%	50%	50%
Ct	Improved productivity and operational efficiency	C1*C2*C3*C4	$187,500	$193,125	$198,919
	Risk adjustment	↓20%			
Ctr	Improved productivity and operational efficiency (risk-adjusted)		$150,000	$154,500	$159,135
	Three-year total: $463,635			**Three-year present value: $383,610**	

INCREASED EFFICIENCY OF SECURITY INCIDENT RESPONSE PROCESS

Evidence and data. Group-IB THF eases the management of complex security incidents. Efficiencies are gained by automating workflows that span security and IT teams, prioritizing security incidents based on business criticality, and tracking incidents and assigning tasks using Group-IB THF.

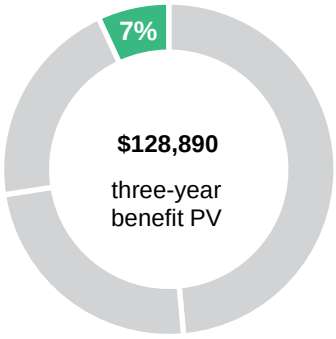
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- The organization deals with 1,000 qualified security incidents each month that require responses.
- On average, 95% of these incidents are classified as tier one, which are less complex incidents that frontline security analysts can handle and resolve.
- Prior to using Group-IB THF, the composite organization's frontline analysts spends approximately 15 minutes responding to each tier one incident.
- By implementing Group-IB THF, the organization estimates that response times for these incidents improves by 20%. Automating responses to recurring incidents allows security analysts to focus on investigating and remediating more complex threats.
- Resolving the remaining 5% of security incidents, which are considered tier two incidents, requires greater coordination across IT and security teams.

Risks. Forrester considered the following potential risks when assigning a risk adjustment:

- The number of security threats affecting an organization.
- The types of security threats affecting an organization.
- The skill sets of IT and security resources.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of over $128,000.



Increased efficiency of security incident response process: 7% of total benefits

Increased Efficiency Of Security Incident Response Process					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Average number of qualified monthly security incidents	Interview	1,000	1,000	1,000
D2	Average annual number of qualified security incidents	D1*12	12,000	12,000	12,000
D3	Percentage of qualified security incidents that are tier one	Interview	95%	95%	95%
D4	Percentage of qualified security incidents that are tier two and above	Interview	5%	5%	5%
D5	Number of annual tier one security incidents per year	D2*D3	11,400	11,400	11,400
D6	Average man-hours to remediate tier one security incidents prior to THF	Interview	0.25	0.25	0.25
D7	Improved efficiency to manage tier one security incidents after implementing THF	Interview	20%	20%	20%
D8	Number of tier two and higher security incidents per year	D2*D4	600	600	600
D9	Average man-hours to remediate tier two security incidents prior to THF	Interview	4	4	4
D10	Improved efficiency to manage tier two security incidents after implementing THF	Interview	20%	20%	20%
D11	Average hourly fully burdened rate of security FTE	Assumption	$60.00	$61.80	$63.65
Dt	Increased efficiency of security incident response process	(D5*D6*D7*D11)+(D8*D9*D10*D11)	$63,000	$64,890	$66,833
	Risk adjustment	↓20%			
Dtr	Increased efficiency of security incident response process (risk-adjusted)		$50,400	$51,912	$53,466
	Three-year total: $155,778			**Three-year present value: $128,890**	

UNQUANTIFIED BENEFITS

Additional benefits that the customer experienced but was not able to quantify include:

- **Better visibility into digital security threats, malware attacks.** Group-IB THF provided better visibility into advanced digital security threats and cyberattacks. This led to a better understanding and improved monitoring of relevant threats, increased focus on specific threat vectors and other activities to identify gaps, and an improved security posture for the organization.
- **Access to threat intelligence data.** Group-IB Threat Intelligence & Attribution (TI&A) strengthen the cybersecurity posture with accurate threat intelligence. It provides threat intelligence driven services and attributes scattered events to specific malware types and families or certain cybercriminal groups for efficient attack termination.
- **Reduced cyber risks and potential reputational damage.** Group-IB THF provided threat-hunting capabilities to the organization that helped it understand the threat landscape, mitigate reputational risks, and prevent financial losses. Leveraging Group-IB THF, security and IT professionals became more confident about the organization's cyber risk posture**.**
- **Business operations continuity with low false rates.** Proactive threat hunting in network traffic within and outside the perimeter, as well as analysis of threats, has enabled the organization's security team to determine whether or not a threat is real. Low false positive rates prevented business disruptions.
- **Improved collaboration.** Group-IB THF provides a shared environment, remote incident response, digital forensics, and access to analyst community and experts. This led to improved collaboration and teamwork.

FLEXIBILITY

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

- **Integrability and scalability.** Group-IB THF allows organizations to optimize security investments and integrate the THF module with other security solutions regardless of whether the company has a cloud, physical, or hybrid email configuration.
- **Increased business agility.** As industries evolve and change, Group-IB provides a foundation of threat intelligence to help companies navigate the changes with agility, security posture improvements, and increased flexibility. Group-IB TI&A provides threat intelligence to boost cyber readiness. It improves the awareness level of the threat landscape and facilitates better decision-making for the organization's security posture

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

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Group-IB Threat Hunting Framework fees	$33,000	$110,000	$110,000	$110,000	$363,000	$306,554
Ftr	Planning, ongoing management, training support, and consultation	$13,222	$71,399	$73,537	$75,747	$233,905	$195,814
	Total costs (risk-adjusted)	$46,222	$181,399	$183,537	$185,747	$596,905	$502,368

GROUP-IB THREAT HUNTING FRAMEWORK FEES

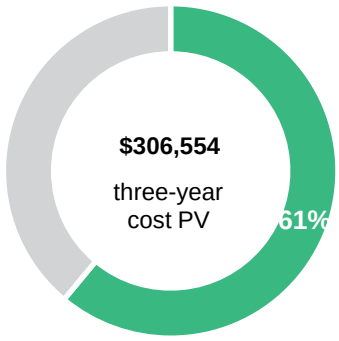
Evidence and data. The Group-IB THF deployment includes subscription and support/consultation costs. The customer organization incurred annual subscription costs of $100,000, and it paid $30,000 in fees for upfront support and consultation services.

The support and consultation services cost is included at the beginning of the deployment because security analysts need to learn how to understand threat data, run tests, and review the results. This includes training support, phone consultations, analysis and modeling, and testing.

Modeling and assumptions. Forrester modeled these costs based on high-level estimates. For a more detailed business-case estimate, request a quote from Group-IB.

Risks. Implementation costs could vary depending on the size and scope of the implementation.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of over $306,000.



Group-IB Threat Hunting Framework fees: 61% of total costs

Group-IB Threat Hunting Framework Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Annual subscription cost	Interview	$0	$100,000	$100,000	$100,000
E2	Other costs (consultation/support fees)	Assumption	$30,000	$0	$0	$0
Et	Group-IB Threat Hunting Framework fees	E1+E2	$30,000	$100,000	$100,000	$100,000
	Risk adjustment	↑10%				
Etr	Group-IB Threat Hunting Framework fees (risk-adjusted)		$33,000	$110,000	$110,000	$110,000
	Three-year total: $363,000			**Three-year present value: $306,554**		

PLANNING, ONGOING MANAGEMENT, TRAINING SUPPORT, AND CONSULTATION

Evidence and data. For the customer organization, Group-IB deployment was straightforward and the required resource time was minimal. However, successful deployments require due diligence and implementation tasks that include:

- Spending time with Group-IB experts to understand how Group-IB THF improves email protection, detect threats, performs behavioral analysis for software and users, and creates event correlation.
- Working with Group-IB experts to generate new ideas, identify compromised customers, and resolve queries.

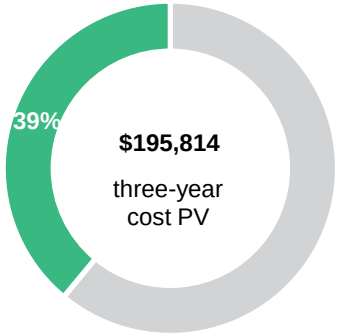
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- Five FTES spent about one week to plan the Group-IB THF deployment.
- The organization dedicated 50% time of one FTE per year to oversee, manage, consult, and monitor the Group-IB THF.

Risks. These costs could vary depending on:

- The salaries and costs of resources.
- The complexity of the deployment.
- The size and scope of the implementation.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of over $195,000.



Planning, ongoing management, training support, and consultation: 39% of total costs

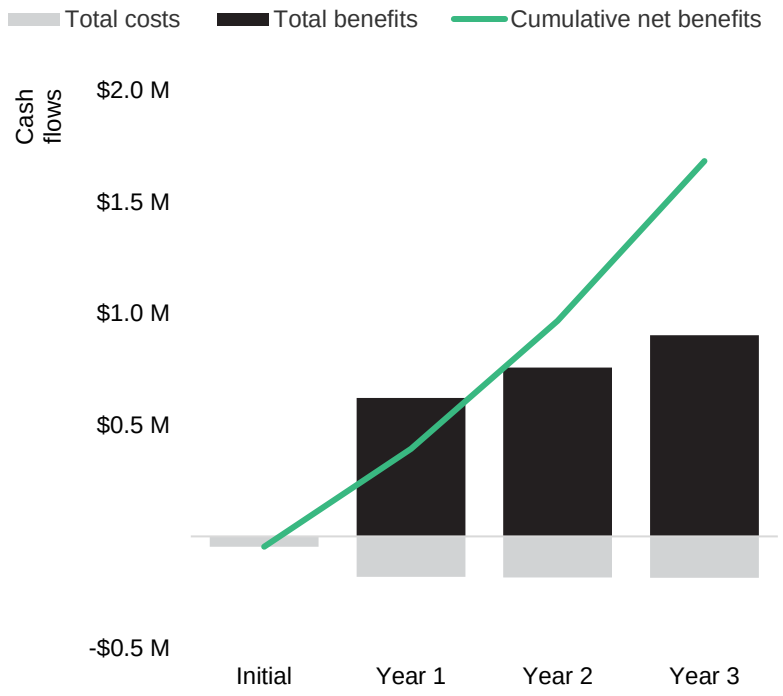
Planning, Ongoing Management, Training Support, And Consultation

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	FTEs required for planning, testing, and implementations	Assumption	5	0	0	0
F2	Ongoing management, training support, and consultation	Assumption	0	1	1	1
F3	Time spent per FTE (hours)	Assumption	40	1,080	1,080	1,080
F4	Average hourly cost of FTE	Assumption	$60.10	$60.10	$61.90	$63.76
Ft	Planning, ongoing management, training support, and consultation	(F1*F3*F4) + (F2*F3*F4)	$12,020	$64,908	$66,852	$68,861
	Risk adjustment	↑10%				
Ftr	Planning, ongoing management, training support, and consultation (risk-adjusted)		$13,222	$71,399	$73,537	$75,747
	Three-year total: $233,905			**Three-year present value: $195,814**		

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 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	($46,222)	($181,399)	($183,537)	($185,747)	($596,905)	($502,368)
Total benefits	$0	$620,400	$757,212	$901,801	$2,279,413	$1,867,331
Net benefits	($46,222)	$439,001	$573,675	$716,054	$1,682,508	$1,364,963
ROI						272%
Payback						<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: Supplemental Material

Related Forrester Research

“The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q2 2021,” Forrester Research, Inc., May 7, 2021.

“Modernize Your Approach To Endpoint Governance,” Forrester Research, Inc., April 6, 2021.

“Best Practices: Mitigating Insider Threat,” Forrester Research, Inc., March 18, 2021.

“Defend Your Digital Business From Advanced Cyberattacks Using Forrester’s Zero Trust Model,” Forrester Research, Inc., July 2, 2021.

Appendix C: Endnotes

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


FORRESTER®