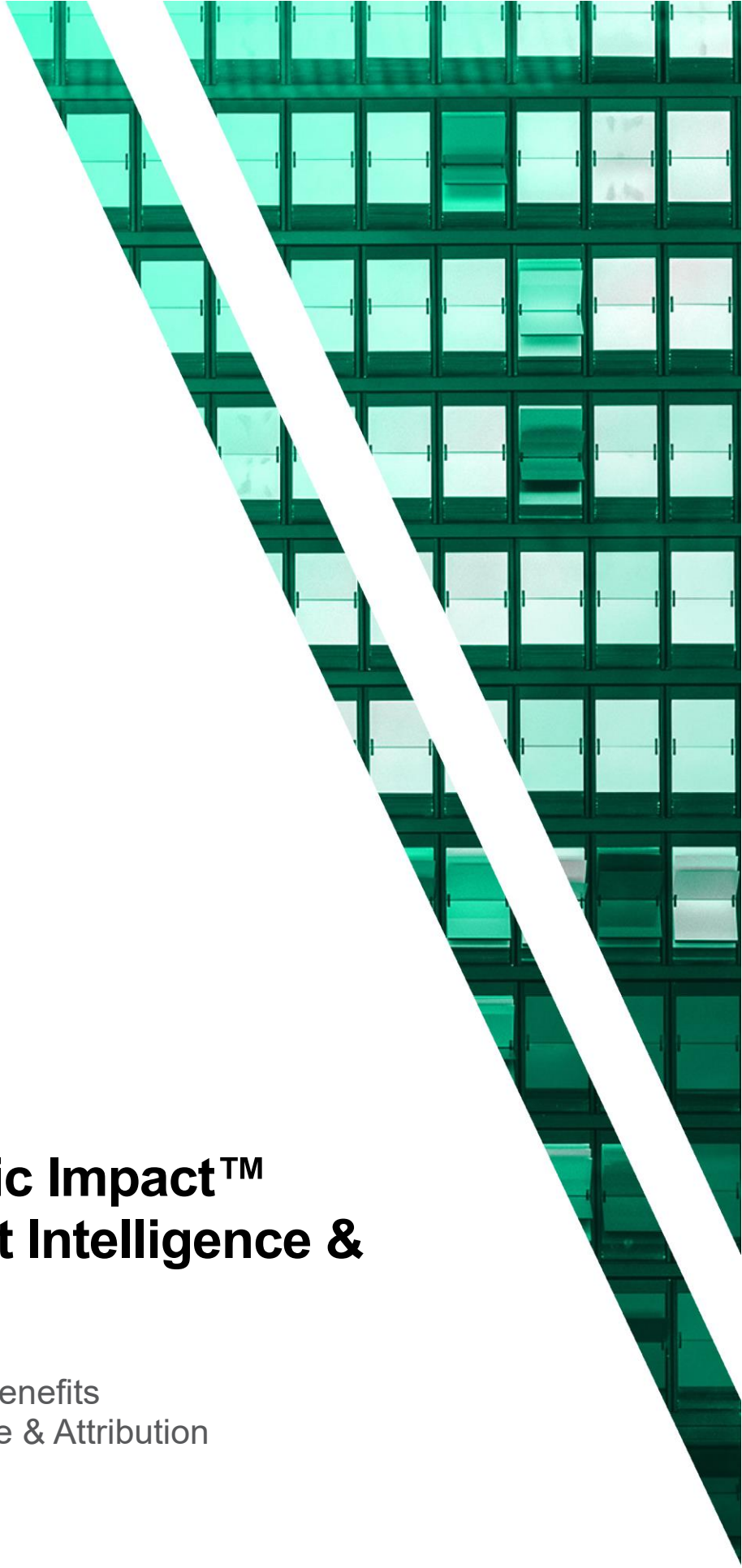
FORRESTER®



The Total Economic Impact™ Of Group-IB Threat Intelligence & Attribution

Cost Savings And Business Benefits
Enabled By Threat Intelligence & Attribution

JULY 2021

Table Of Contents

Executive Summary 1

The Group-IB Threat Intelligence & Attribution Customer Journey 6

Interviewed Organization 6

Key Challenges 6

Solution Requirements 6

Use Case Description 6

Analysis Of Benefits 8

Savings From Fraud Prevention 8

Opex Savings From Discontinuing Legacy Threat Intelligence Solutions 9

Improved Productivity And Cybersecurity Team Efficiency 10

Unquantified Benefits 11

Flexibility 12

Analysis Of Costs 13

Group-IB Threat Intelligence & Attribution Fees 13

Ongoing Management, Training Support, And Consultation 14

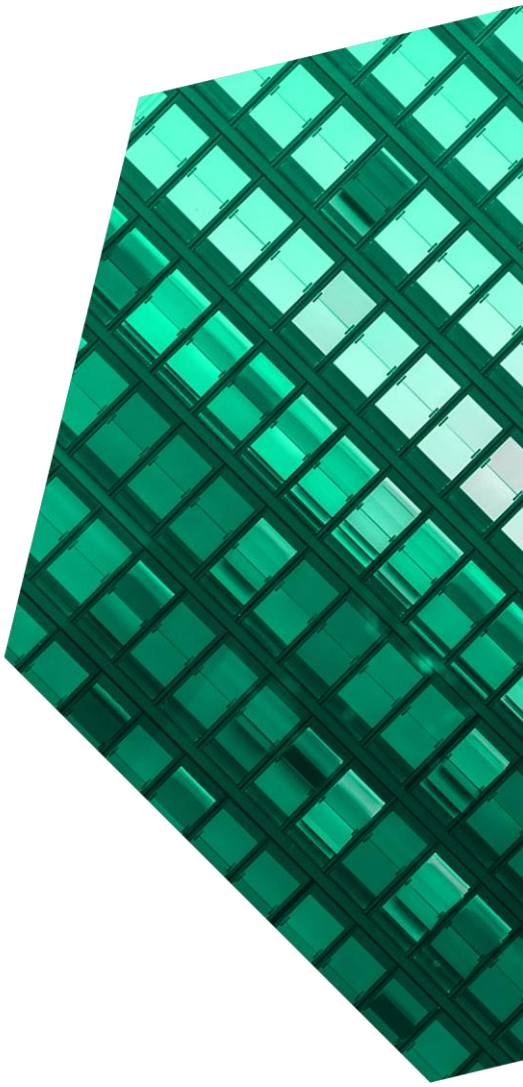
Financial Summary 15

Appendix A: Total Economic Impact 16

Appendix B: Supplemental Material 17

Appendix C: Endnotes 17

Consulting Team: Sri Prakash Gupta



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

In today's threat landscape, organizations of all sizes and types are struggling to protect their digital assets and infrastructures. At the same time, cybersecurity risks are rapidly increasing as threats become more widespread and complex and often lead to financial losses and reduced customer trust. Therefore, organizations need threat intelligence and attribution tools that enable security teams to manage cyber risks, to respond faster and more efficiently to fraudulent activities, and to build resilient security programs.

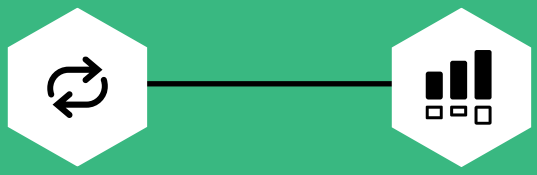
Group-IB is a global threat-hunting and adversary-centric cyberintelligence company that specializes in investigating and preventing high-tech cybercrimes. Group-IB Threat Intelligence & Attribution (TI&A) is a system for analyzing and attributing cyberattacks, proactively threat hunting, and protecting network infrastructure based on data related to adversary tactics, tools, and activity.

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 TI&A.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Threat Intelligence & Attribution on their organizations.

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

Prior to using Group-IB TI&A, it would take the customer several hours to identify compromised payment cards and to detect and analyze threats using its legacy threat intelligence solution. However, these prior attempts yielded limited success, exposed the organization to bigger cybersecurity risks and more fraud, and left it unable to stop leaks and mitigate threats.

KEY STATISTICS



Return on investment (ROI)
339%

Net present value (NPV)
$2.6 million

After the investment in Group-IB TI&A, the organization efficiently prevented fraud before threat actors could use payment card data. The organization enriched its antifraud systems with unique data, new fraud detection rules, and relevant notifications about leaked payment cards, detection, and the elimination of the source of compromises (e.g., terminal, website, or phishing resources, etc.).

> "Group-IB TI&A improved the security posture for the organization, which was much needed for our global business operations. It helped us to mitigate the risk, protect digital assets, and significantly improve vulnerability management."
>
> *Global head of cyberintelligence and threat analysis, financial services*

KEY FINDINGS

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

- **Savings from fraud prevention for compromised payment cards, resulting in $3 million in benefits over three years.** Group-IB TI&A prepared the organization to create new fraud detection rules for antifraud systems, detect threats, analyze anomalies, and set up relevant notifications about compromised payment cards. With an improved threat intelligence and fraud detection mechanism, the organization avoided fraud activity on 5,000 payment cards each year.
- **Realized opex savings by eliminating legacy threat intelligence solutions, resulting in $252,000 in benefits over three years.** Group IB TI&A provided consistent data around threat intelligence and fraud prevention that enabled the organization to discontinue software licenses and support contracts for the legacy threat intelligence solution it previously used to manage fraud prevention for compromised payment cards. Forrester estimates these tools previously cost the organization $200,000 each year and that the organization was able to discontinue them and realize these savings beginning in Year 2.
- **Improved productivity and cybersecurity team efficiency, resulting in nearly $141,000 in benefits over three years**. Group-IB TI&A helped the organization realize productivity gains and increased efficiency for its cybersecurity team by 10%. It also allowed security analysts to gather vital information about fraudulent activities, promptly stop leaks, mitigate threats, and make use of time for improvements and innovations.

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

- **Better visibility into digital security threats.** Group-IB TI&A provided better visibility into advanced digital security threats. This led to better understanding and monitoring of relevant threats, more 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 TI&A provided threat intelligence services to the organization that helped it understand the threat landscape, mitigate reputational risks, and prevent financial losses and fraud by protecting customer credentials for compromised banks cards. Leveraging Group-IB TI&A, security and cyber risk professionals became more confident about the organization's cyber risk posture.
- **Time savings from reduced false incident investigations.** Group-IB empowered the organization's security team to determine whether or not a threat was real, and security tools within the perimeter generated alerts whenever they detected something risky. Group-IB TI&A augmented this internal information with insights into external threat landscapes, and this allowed security teams to prioritize alerts based on tactics, techniques, and procedures (TTPs) that bad actors implement against the organization and its industry. Additionally, Group-IB provided detailed insights into the indicators of compromises mapped to the MITRE ATT&CK framework. This made it easier for security teams to correlate alerts from different tools during investigations.
- **Improved the security team's decision-making.** The increasing volume of sophisticated attacks and sources of cyberthreats (e.g., terminals, websites, malware on user devices, etc.) made the organization's security

architecture highly vulnerable. Group-IB TI&A improved its cyber readiness by providing threat intelligence. This created greater awareness about the threat landscape and led to better decision-making about the organization's security posture.

- **Increased collaboration.** Group-IB threat intelligence services augmented internal security data to provide the organization with the context needed for more complete, accurate, and timely remediation of new security events. This led to improved collaboration and teamwork.
- **Increased access to cyber threat intelligence.** Group-IB TI&A provided threat intelligence about phishing sites and data leak sites, it conducted investigations, and it closely monitored ransomware spaces. Moreover, Group-IB TI&A provided information and consultation about the compromised security points to law enforcement agencies.

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

- **Group-IB TI&A subscription fees of $763,000 over three years.** The Group-IB TI&A deployment cost includes an annual subscription fee, consultancy, an information-sharing community, and access to Group-IB analysts for custom analyses.
- **Ongoing management, internal training support, and consultancy costs of nearly $6,800 over three years.** Group-IB TI&A is a software-as-a-service (SaaS) solution, and it offers a plug-and-play solution that does not require an investment in extensive training. 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 $3.4 million over three years versus costs of $770,000, adding up to a net present value (NPV) of $2.6 million and an ROI of 339%.

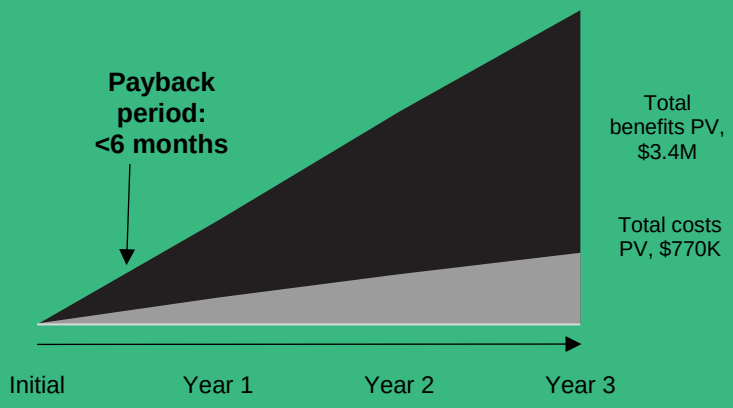
ROI
339%

BENEFITS PV
$3.4 million

NPV
$2.6 million

PAYBACK
<6 months

Financial Summary



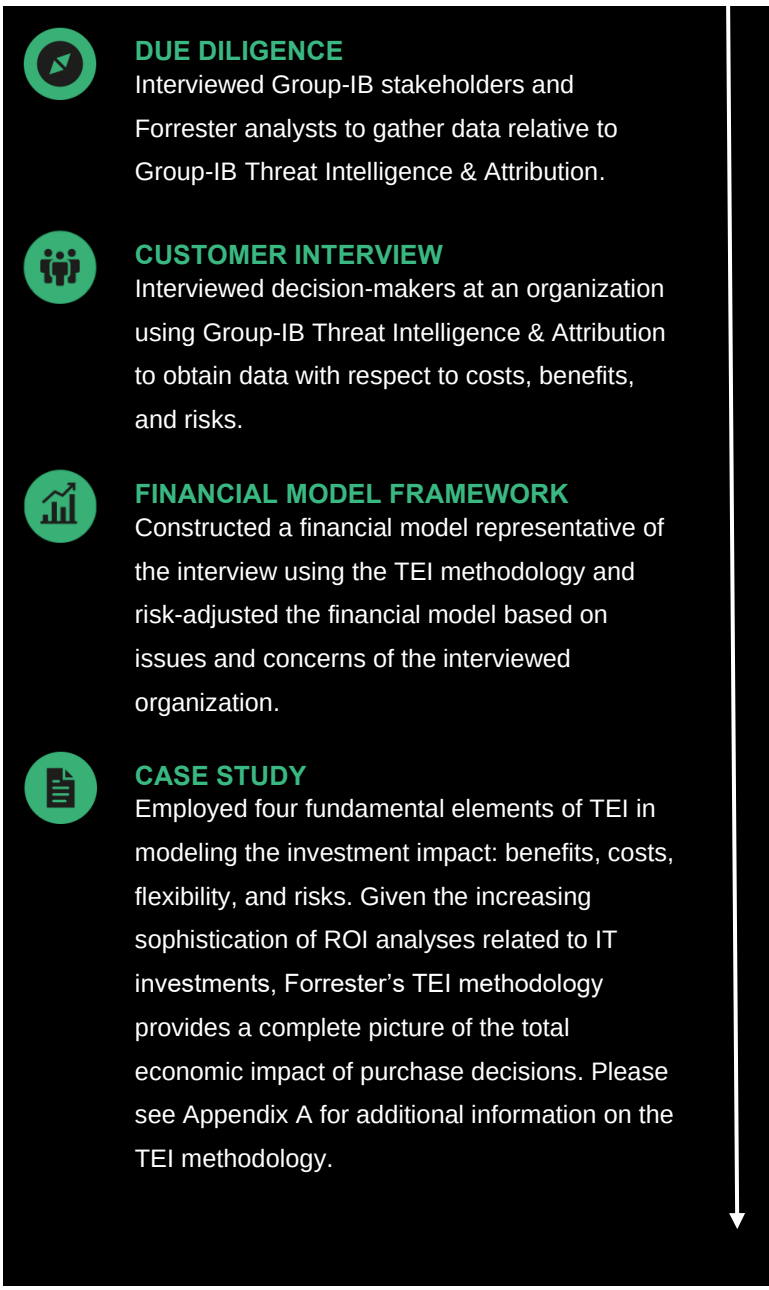
With Group-IB TI&A, fraud prevention on payment cards became available instantly, and that resulted in large savings. Before, it would not have been possible for us to replicate that effort.

— Global head of cyberintelligence and threat analysis, 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 Group-IB Threat Intelligence & Attribution.

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 Group-IB Threat Intelligence & Attribution 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 Intelligence & Attribution.

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 Intelligence & Attribution Customer Journey

Drivers leading to the Group-IB TI&A investment

INTERVIEWED ORGANIZATION

Forrester interviewed a Group-IB Threat Intelligence & Attribution customer with the following characteristics:

- The organization is a large, multinational investment bank and financial services holding company.
- It generates more than $10 billion in annual revenue, and it has more than 100,000 employees.
- It has used Group-IB TI&A for more than two years for fraud prevention on compromised payment cards.

KEY CHALLENGES

Prior to investing in Group-IB TI&A, the organization struggled with several challenges related to fraud prevention on payment cards.

- The organization struggled to prevent payment card fraud and to correlate it with the activities of specific attackers and malware.
- A rapidly evolving threat landscape and increasing cyber risks for the banking and financial services industry (BFSI) led to complex business operations.
- Fraud losses hampered the customer experience.
- The organization lacked the ability to evaluate a full list of compromised payment cards.
- The organization was unable to determine exact points of compromise, promptly stop leaks, or eliminate threats.
- The organization was unable to use bank identification numbers (BINs) to search or set up relevant notifications about leaked bank cards.

SOLUTION REQUIREMENTS

The interviewed organization searched for a solution that could:

- Collect and provide intelligence about compromised payment cards associated with its customers.
- Protect existing customers and prevent fraudulent activity.
- Enable better customer experience and more efficient business operations at an increasing scale.
- Provide the most accurate and consistent data related to adversary tactics, tools, and activity and improve visibility of advanced threats targeting this space.
- Provide intelligence about phishing sites, conduct research and investigations about data leak sites and closely monitor ransomware spaces.

USE CASE DESCRIPTION

The multinational banking and financial services company chose to take a phased approach to deploying Group-IB TI&A. The organization initially purchased a one-year subscription in 2019, but it renewed the contract for three more years in 2020. Eventually, it discontinued its legacy threat intelligence solution, and it fully leveraged Group-IB TI&A to prevent fraud on compromised payment cards and to gather threat intelligence.

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

Key metrics

- **20,000 payment cards compromised per year**
- **$600 financial loss per payment card**
- **Discontinues legacy threat intelligence tools**
- **Deploys Group-IB TI&A with no capex costs**
- **Achieves 25% fraud prevention on payment cards**

Analysis Of Benefits

Quantified benefit data

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Savings from fraud prevention	$1,200,000	$1,200,000	$1,200,000	$3,600,000	$2,984,222
Btr	Opex savings from discontinuing legacy threat intelligence solutions	$0	$160,000	$160,000	$320,000	$252,442
Ctr	Improved productivity and cybersecurity team efficiency	$28,125	$57,938	$89,513	$175,576	$140,703
	Total benefits (risk-adjusted)	$1,228,125	$1,417,938	$1,449,513	$4,095,576	$3,377,367

SAVINGS FROM FRAUD PREVENTION

Evidence and data. Group-IB TI&A enabled the organization to create new fraud detection rules for antifraud systems, detect threats, analyze anomalies, and set up relevant notifications about compromised payment cards. With an improved threat intelligence and fraud detection mechanism, the organization avoided fraud activity on 5,000 payment cards.

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

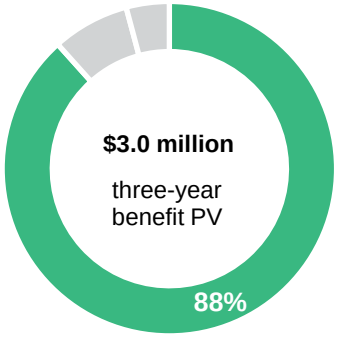
- The organization experiences fraud on 20,000 payment cards per year.
- The average loss per compromised payment card is $600.
- The average loss prevention due to Group-IB TI&A is $300.

  Group-IB TI&A reduces the fraud on payment cards by 25%.

Risks. The savings from fraud prevention could vary with:

- The total number of payment cards compromised per year.
- The total loss per compromised payment card.
- The average loss prevention due to Group-IB TI&A.
- The average percentage of fraud avoidance for payment cards.

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 $3 million.



Savings from fraud prevention: 88% of total benefits

Savings From Fraud Prevention					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Total number of payment cards compromised due to fraud activity	Interview	20,000	20,000	20,000
A2	Average loss per payment card	Interview	$600	$600	$600
A3	Average loss prevention per payment card attributed to Group-IB TI&A	Assumption	$300	$300	$300
A4	Fraud activity prevented for payment cards due to Group-IB TI&A	Assumption	5,000	5,000	5,000
At	Savings from fraud prevention	A3*A4	$1,500,000	$1,500,000	$1,500,000
	Risk adjustment	↓20%			
Atr	Savings from fraud prevention (risk-adjusted)		$1,200,000	$1,200,000	$1,200,000
	Three-year total: $3,600,000			**Three-year present value: $2,984,222**	

OPEX SAVINGS FROM DISCONTINUING LEGACY THREAT INTELLIGENCE SOLUTIONS

Evidence and data. Group-IB TI&A provided consistent data around threat intelligence and fraud prevention, and this enabled the organization to discontinue software licenses and support contracts for legacy threat intelligence solution it previously used to manage fraud prevention for compromised payment cards.

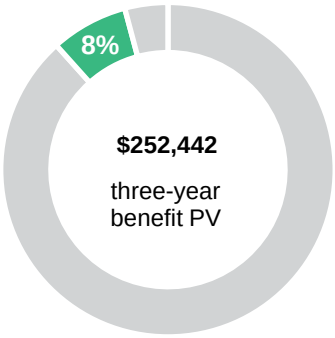
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- After the first year, when all fraud detection rules with Group-IB TI&A are in place, the organization discontinues the use of legacy tools.
- This saves the organization an estimated $200,000 in both years 2 and Year 3.

Risks. The savings from discontinued legacy tools could vary based on the following factors:

- The number and type of legacy tools discontinued.
- The contract terms and agreements of the discontinued legacy tools.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $252,000.



Savings from discontinuing of legacy threat intelligence solutions: 8% of total benefits

Opex Savings From Discontinuing Legacy Threat Intelligence Solutions					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Opex savings from discontinuing legacy threat intelligence solutions	Interview	$0	$200,000	$200,000
Bt	Opex savings from discontinuing legacy threat intelligence solutions	B1	$0	$200,000	$200,000
	Risk adjustment	↓20%			
Btr	Opex savings from discontinuing legacy threat intelligence solutions (risk-adjusted)		$0	$160,000	$160,000
	Three-year total: $320,000			**Three-year present value: $252,442**	

IMPROVED PRODUCTIVITY AND CYBERSECURITY TEAM EFFICIENCY

Evidence and data. The organization realized productivity gains and increased the efficiency of its cybersecurity team by 10% with Group-IB TI&A. The solution helped security analysts gather vital information about fraud attacks, promptly stop leaks, mitigate threats, and make use of time for improvements and innovation.

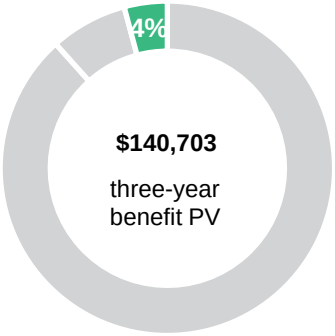
Modeling and assumptions. Forrester makes the following assumptions for the financial model:

- 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 10%, yielding a three-year, risk-adjusted total PV of nearly $141,000.



Improved productivity and efficiency gains: 4% of total benefits

Improved Productivity And Cybersecurity Team Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Security analyst FTEs	Assumption	5	5	5
C2	Average fully loaded cost of per security analyst	Assumption	125,000	128,750	132,613
C3	Efficiency enabled by Group-IB	Assumption	10%	20%	30%
C4	Productivity conversion	Assumption	50%	50%	50%
Ct	Improved productivity and cybersecurity team efficiency	C1*C2*C3*C4	$31,250	$64,375	$99,459
	Risk adjustment	↓10%			
Ctr	Improved productivity and cyber-security team efficiency (risk-adjusted)		$28,125	$57,938	$89,513
	Three-year total: $175,576			**Three-year present value: $140,703**	

UNQUANTIFIED BENEFITS

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

- **Better visibility into digital security threats.** Group-IB TI&A provided better visibility into advanced digital security threats. This led to better understanding and monitoring of relevant threats, more 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 TI&A provided threat intelligence services to the organization that helped it understand the threat landscape, mitigate reputational risks, and prevent financial losses and fraud by protecting customer credentials for compromised banks cards. Leveraging Group-IB TI&A, security and cyber risk professionals became more confident about the organization's cyber risk posture.
- **Time savings from reduced false incident investigations.** Group-IB empowered the organization's security team to determine whether or not a threat was real, and security tools within the perimeter generated alerts whenever they detected something risky. Group-IB TI&A augmented this internal information with insights into external threat landscapes, and this allowed security teams to prioritize alerts based on tactics, techniques, and procedures (TTPs) that bad actors implement against the organization and its industry. Additionally, Group-IB provided detailed insights into the indicators of compromises mapped to the MITRE ATT&CK framework. This made it easier for security teams to correlate alerts from different tools during investigations.
- **Improved the security team's decision-making.** The increasing volume of sophisticated attacks and sources of cyberthreats (e.g., terminals, websites, malware on user devices, etc.) made the organization's security architecture highly vulnerable. Group-IB TI&A improved its cyber readiness by providing threat intelligence. This created greater awareness about the threat landscape and led to better decision-making about the organization's security posture

- **Increased collaboration.** Group-IB threat intelligence services augmented internal security data to provide the organization with the context needed for more complete, accurate, and timely remediation of new security events. This led to improved collaboration and teamwork.
- **Increased access to cyber threat intelligence.** Group-IB TI&A provided threat intelligence about phishing sites and data leak sites, it conducted investigations, and it closely monitored ransomware spaces. Moreover, Group-IB TI&A provided information and consultation about the compromised security points to law enforcement agencies.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Group-IB Threat Intelligence & Attribution and later realize additional uses and business opportunities.

- As industries evolve and change, Group-IB TI&A provides a foundation of threat intelligence to help companies navigate the changes with agility, improved security postures, and increased flexibility. The interviewee said external threat intelligence is vital not only to the financial sector, but also to the business ecosystem going through digital transformation**.**
- Group-IB TI&A allows organizations to optimize security investments. As an SaaS solution, deploying Group-IB TI&A is straightforward and does not require capex costs. The interviewed organization did not have to purchase separate subscriptions for passive domain name systems (DNS) and passive secure sockets layer (SSL) data, web scanning, and malware detonation systems.

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**
Dtr	Group-IB Threat Intelligence & Attribution fees	$11,000	$302,500	$302,500	$302,500	$918,500	$763,273
Etr	Ongoing management, training support, and consultation	$0	$2,644	$2,724	$2,805	$8,173	$6,763
	Total costs (risk-adjusted)	$11,000	$305,144	$305,224	$305,305	$926,673	$770,036

GROUP-IB THREAT INTELLIGENCE & ATTRIBUTION FEES

Evidence and data. The Group-IB TI&A deployment includes subscription and training/consultation costs. The interviewed organization incurred annual subscription costs of $275,000 and it paid $10,000 in fees for up-front training and consultation services.

The training and consultation services cost is included at the beginning of the deployment because security analysts need help learning how to understand threat data. 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 $763,000.

Group-IB Threat Intelligence & Attribution Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Annual subscription cost	Interview	$0	$275,000	$275,000	$275,000
D2	Cost of up-front training/consulting	Assumption	$10,000	$0	$0	$0
Dt	Group-IB Threat Intelligence & Attribution fees	C1+C2	$10,000	$275,000	$275,000	$275,000
	Risk adjustment	↑10%				
Dtr	Group-IB Threat Intelligence & Attribution fees (risk-adjusted)		$11,000	$302,500	$302,500	$302,500
	Three-year total: $918,500			**Three-year present value: $763,273**		

ONGOING MANAGEMENT, TRAINING SUPPORT, AND CONSULTATION

Evidence and data. For the interviewed organization, Group-IB deployment was straightforward and the required resource time was minimal. Because Group-IB TI&A is a SaaS solution, the organization did not need to pay capex costs for its implementation. Furthermore, ready-made integrations with security information and event management (SIEM) and threat intelligence platforms (TIPs) automated processes with flexible APIs. However, successful deployments require due diligence and implementation tasks that include:

- Spending time with Group-IB experts to understand how Group-IB TI&A improves fraud prevention, provides access to data, and attributes threats.
- Working with Group-IB experts to generate new ideas, identify compromised customers, and resolve queries.

The organization dedicated one week per year for its five FTEs to oversee, manage, consult, and monitor the Group-IB TI&A deployment.

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 nearly $6,800.

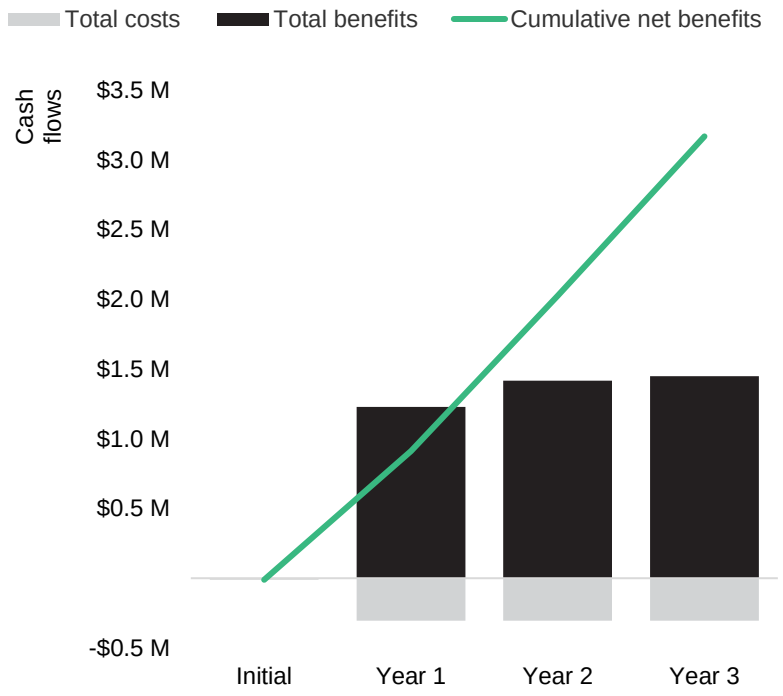
Ongoing Management, Training Support, And Consultation

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Ongoing management, training support, and consultation FTEs	Assumption	0	5	5	5
E2	Time spent annually per FTE (hours)	Assumption	0	8	8	8
E3	Average hourly cost of FTE	Assumption	$0	$60.10	$61.90	$63.76
Et	Ongoing management, training support, and consultation	E1*E2*E3	$0	$2,404	$2,476	$2,550
	Risk adjustment	↑10%				
Etr	Ongoing management, training support, and consultation (risk-adjusted)		$0	$2,644	$2,724	$2,805
	Three-year total: $8,173			**Three-year present value: $6,763**		

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	($11,000)	($305,144)	($305,224)	($305,305)	($926,673)	($770,036)
Total benefits	$0	$1,228,125	$1,417,938	$1,449,513	$4,095,576	$3,377,367
Net benefits	($11,000)	$922,981	$1,112,714	$1,144,208	$3,168,902	$2,607,331
ROI						339%
Payback						<6 months

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
"Now Tech: External Threat Intelligence Services, Q4 2020," Forrester Research, Inc., December 28, 2020

"Defend Your Digital Business From Cyberattacks," Forrester Research, Inc., June 25, 2021

Appendix C: 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


FORRESTER®