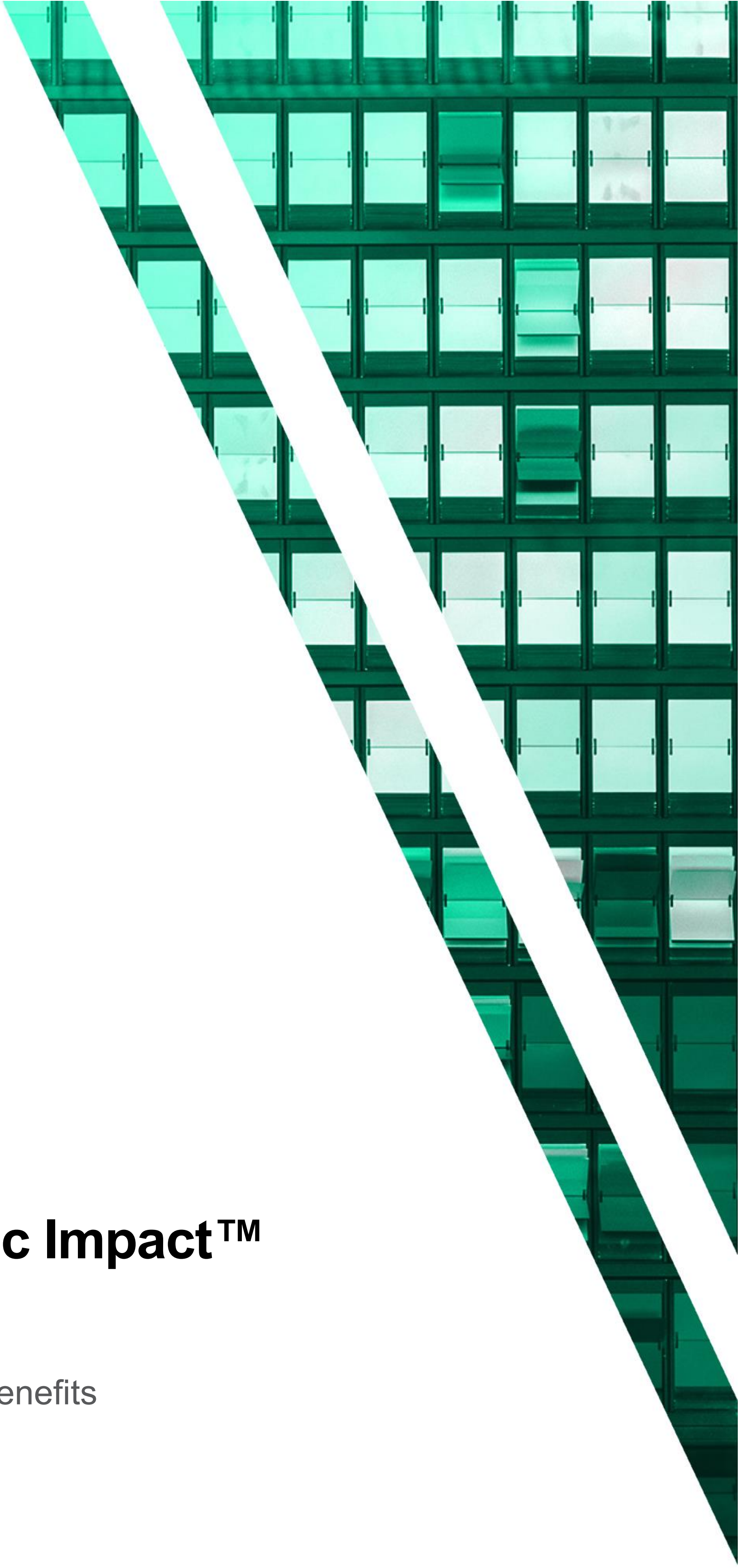
FORRESTER®



The Total Economic Impact™ Of Code42 Incydr

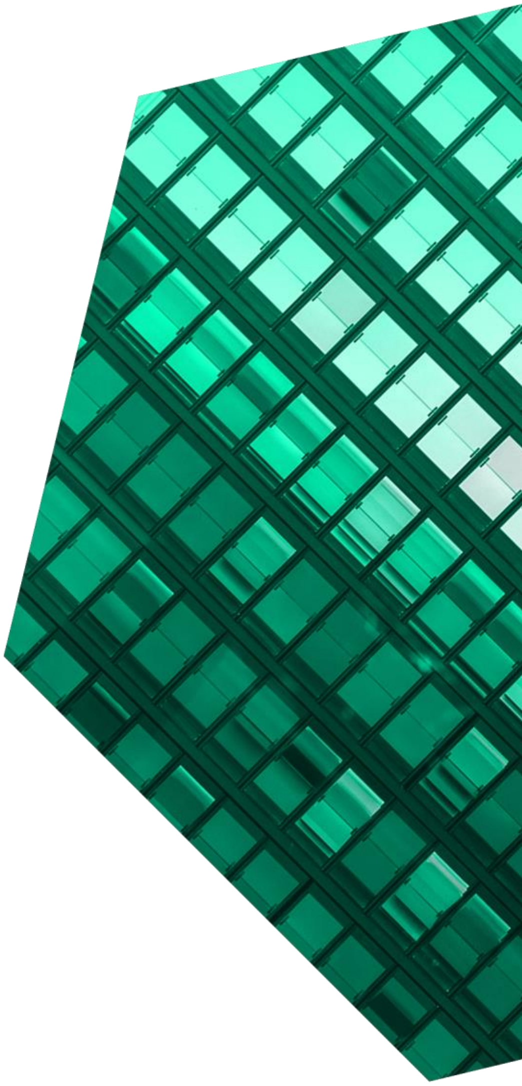
Cost Savings And Business Benefits Enabled By Incydr

NOVEMBER 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY CODE42

Table Of Contents

Consulting Team: Sanitra Desai
Zahra Azzaoui



ABOUT FORRESTER CONSULTING

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

Executive Summary

Although insider incidents make up 22% of data breaches, many security teams don’t prioritize insiders as a threat vector.[1,2] Organizations need the ability to identify suspicious behaviors and take appropriate action to reduce data theft in today’s constantly evolving business environment.[3] Code42 Incydr provides the context-driven detection and the wide array of response controls needed to see and stop data leaks and IP theft across an organization's data landscape while improving efficiencies for internal resources.

The Code42 Incydr data protection solution rapidly detects data exposure, loss, leak, and theft and speeds incident response without lengthy deployments, complex policy management, or disrupting employee productivity. With Incydr, security professionals can protect corporate data and reduce exfiltration while fostering an open and collaborative culture for employees.

Code42 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Incydr.[4] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Incydr on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives with experience using Incydr. For the purposes of this study, Forrester aggregated the interviewees’ experiences and combined the results into a single composite organization.

KEY STATISTICS

Return on investment (ROI)
172%

Net present value (NPV)
$1.30M

Reduction in low-risk events through Instructor microtrainings embedded in Incydr

40%

Prior to using Incydr, interviewees' organizations used a mix of security solutions to manage and monitor their data environment. However, as data loss from insiders grew due to digital, cloud, workforce, and cultural business transformations, existing solutions fell short of protecting sensitive data. Organizations had limited visibility into data movement, which resulted in time consuming security workflows and an inability to focus on what matters.

Once implementing Incydr, organizations had full visibility into file activity across computers, cloud, and email to accurately assess data exposure. With optimized investigation workflows, organizations could streamline the threat resolution process, reduce the need for manual forensic investigations, and reduce losses related to breaches caused by data exfiltration. Organizations also highlighted the ease of use and deployment of the solution. Implementing Incydr resulted in efficiencies across IT, security, legal, and compliance teams, while reducing overall end-user downtime as well.

KEY FINDINGS

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

- **A 35% reduction in manual investigations and a 50% reduction in mean time to investigate medium- and high-risk incidents.** Incydr reduces the noise from alerts and enables security teams to focus on what really matters using Incydr's prioritization model and the Forensic Search feature. This saves the composite organization $462,000 over three years.

- **A 40% reduction in low-risk events with Instructor.** Microtrainings sent through Code42 Incydr drive secure work habits, reducing the number of low-risk events with the organization. For the composite organization, this results in $63,000 in savings over three years.

- **An 80% reduction in endpoint devices that require manual forensic investigation services.** Incydr's extensive visibility into file movement meant organizations could avoid sending devices for manual forensic investigations, resulting in time savings for those who conduct forensic investigations and cost savings related to shipping fees. The composite organization saves $268,000 in forensic search costs over three years.

- **More than 19,000 hours of end user downtime avoided over three years.** The composite organization sees a reduction in security events and investigations related to data exfiltration and a reduction in devices needing forensic investigations. Additionally, all investigations with Incydr can be performed while users still have full use of their device. These efficiencies result in fewer interruptions and less downtime for end users, saving the composite organization $570,000 over three years.

- **A 40% reduction in loss per major data exfiltration incident.** Faster threat detection and improved visibility into data movement with Incydr means the composite organization can reduce the extent of data theft through insider incidents and stop data loss before it happens. The composite organization avoids $686,000 in losses due to data exfiltration over three years.

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

- **Legal efficiencies.** Clear visibility into data movement across the landscape accelerates the incident investigation process and provides legal teams with the evidence they needed for a case faster. This saved legal fees for interviewees' organizations.

- **Unexpected cost savings.** Incydr saved the interviewees' organizations money in many unexpected ways, such through avoiding investments into other security solutions and identifying insiders that are risky in nontraditional ways.

- **Compliance efficiencies.** Incydr's secure data collection and monitoring across a variety of vectors eased interviewees' organizations' ability to comply to industry requirements.

- **Data infiltration efficiencies.** Alongside streamlined data exfiltration processes, data infiltration incident resolution processes were optimized as well.

- **Great provider support.** Interviewees' organizations found a partner in Code42 that was hands-on, helpful, and willing to be an active partner to mitigate insider-driven data loss for an organization.

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

- **Fees to Code42.** Subscription fees for Incydr are based on size and scope of the implementation in terms of the number of employees covered and the subscription package in use. The composite organization also pays a one-time fee for Code42 professional services during the initial deployment period. Based on the composite organization's size and usage, this totals $696,000 over three years.
- **Internal fees.** IT and engineering team members are involved in Incydr implementation and deployment and continue to manage the solution on an ongoing basis. The composite organization experiences ease of use and deployment of the solution. All users of the platform, consisting of engineers and SOC team members, are trained on the platform. Internal fees cost the organization $57,000 over three years.

The representative interviews and financial analysis found that a composite organization experiences benefits of $2.05 million over three years versus costs of $753,000, adding up to a net present value (NPV) of $1.30 million and an ROI of 172%.

Security terms to know, as defined by Forrester:*

- **Breach/major incident**: An event in which someone has intentionally or unintentionally leaked an organization’s sensitive information and the data has left the organization.
- **High risk**: An insider with risk indicators or exhibiting risky behavior is preparing to move sensitive data/is already moving the data.
- **Medium risk**: An insider has risk indicators or is exhibiting risky behavior and has sensitive data access.
- **Low risk**: An insider accidentally moves or deletes sensitive data or data is shared outside policy.

***Definitions listed here inform the benefits outlined in the study.**

> **Without Incydr, we would need to double the security folks dedicated to insider risk events to figure out what events to focus on at the scale we are growing. Everything would just be harder and more time-consuming to investigate and resolve.**
>
> — Senior director, information security, cybersecurity technology

ROI
172%

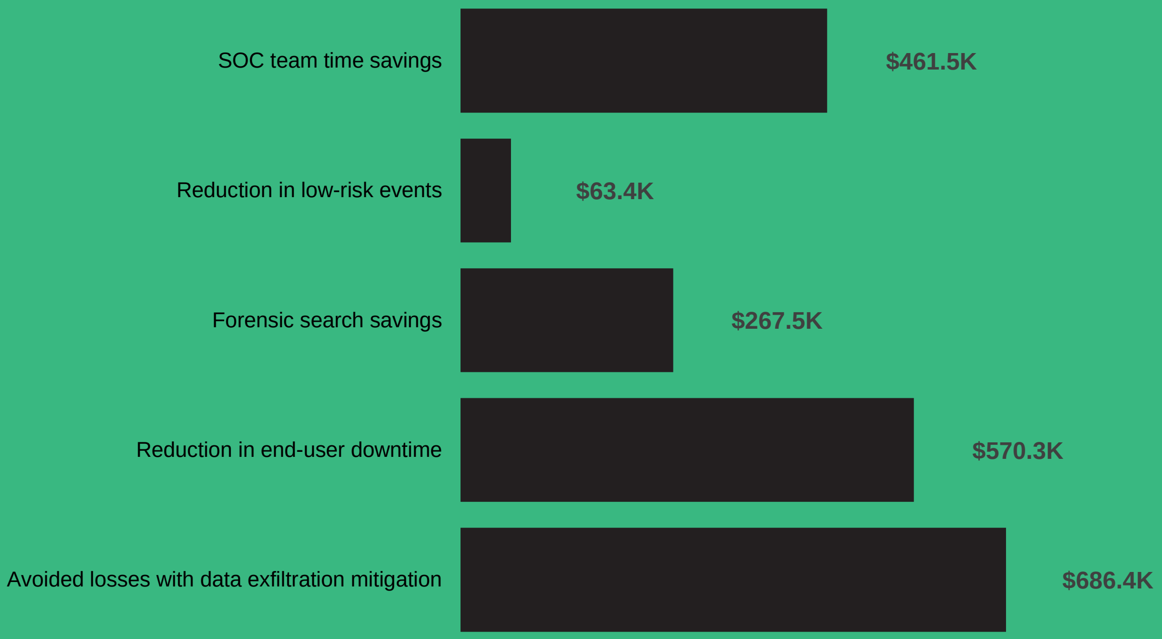
BENEFITS PV
$2.05M

NPV
$1.30M

PAYBACK
<6 months

C

Benefits (Three-Year)



> **“Incydr has decreased the company’s overall risk profile by giving us enhanced visibility and enabling us to keep persistent watch on things we had never seen before.”**

— Enterprise security architect, industrial equipment supplier

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 Incydr.

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 Incydr 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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Code42 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 Incydr.

Code42 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.

Code42 provided the customer names for the interviews but did not participate in the interviews.

DUE DILIGENCE

Interviewed Code42 stakeholders and Forrester analysts to gather data relative to Incydr.

INTERVIEWS

Interviewed five representatives at organizations using Incydr 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 Code42 Incydr Customer Journey

🟩 Drivers leading to the Incydr investment

Interviews

Role	Industry	Geography	Number Of Employees And Endpoints	Data Landscape
Manager	Software	Global	8,000 employees, 9,500 endpoints	OS: Windows, Mac, Linux Data: Cloud, on- and off-network computers, shared drives
Senior director, information security	Cybersecurity technology	Global	7,000 employees	Data: Cloud
Enterprise security architect	Industrial equipment	Global	6,000 employees, 6,000 endpoints	OS: Windows, Mac, Linux Data: Cloud, USB, airdrop
Information security architect	Security	Global	2,500 employees, 3,100 endpoints	OS: Windows, Mac, Linux Data: Cloud, on- and off-network computers, shared drives, USB, airdrop
Manager, information security	Life sciences technology	Global	3,000 employees, 4,500 endpoints	OS: Windows, Mac Data: Cloud

KEY CHALLENGES

Prior to implementing Code42 Incydr, interviewees' organizations used a mix of security systems, consisting of security information and event management (SIEM), cloud access security broker (CASB), endpoint detection and response (EDR), and/or data loss prevention (DLP) solutions. However, they lacked a comprehensive solution to see and stop data loss and insider threat.

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

- **An increase in risk to data due to business transformation.** According to Forrester's Security Survey, 2023, "the changing and evolving nature of IT threats (internal and external)" is one of the biggest IT/security challenge for 21% of the participating enterprise security decision-makers' organizations.[5] Urgent business requirements, such as the rapid shift to the cloud and adoption of anywhere work, has compounded cybersecurity challenges.[6] These business transformations have increased the variety and volume of employee-driven data exposure events, and the legacy policies and controls in place at the interviewees' organizations could not keep up. Additionally, while existing security solutions were effective in safeguarding regulated data, they fell short of protecting sensitive data. In turn, these solutions were sometimes unable to prevent IP from falling into the wrong hands. The enterprise security architect at an industrial equipment supplier explained, "With the influx of remote workers, we had no idea where data was going, regardless of whether the movement was with nefarious intent or not."

- **Limited visibility into data movement.** The interviewees' organizations had invested in multiple security solutions but still saw gaps at the insider risk level and were unable to see how files were moved and shared across the organization. The manager at a software organization said: "We just didn't have any data on file movement. We knew insider risk was a thing, but we couldn't quantify the problem. We could only retroactively dive in by collecting a laptop, imaging it, and sending it to our forensic lab. At that point, the IP is already leaked."

> **"Are they bringing data in? Taking data out? What are the vectors in which they're doing that? What is the scale? What are they taking? We had no insight and had to retroactively dive in if we thought there was something we needed to investigate. But again, we could only see the individual tree, not the forest."**
>
> *Manager, software*

- **Inefficient security workflows.** Interviewees reported that their security workflows were extremely time-consuming in their organizations' legacy environments, largely due to limited visibility and an overabundance of security alerts and false positives hindering threat detection coupled with mostly manual investigation and response processes. The enterprise security architect at an industrial equipment supplier stated: "We were getting 30 alerts a day, and our security team was constantly frustrated because most of the alerts we would get were false positives. There were so many alerts that our small team couldn't possibly sift through them all. We had no way of knowing what we actually needed to investigate."
- **Lack of an effective security education program.** Interviewees' organizations received a lot of low-risk alerts related to uploading and moving data to the wrong place and other accidental data leaks. However, once IT resolved the issue for an employee, the employee would often make the same mistake again. Interviewees stated that their organizations had no way to promote and ensure data use policy compliance and enable and empower a more risk-aware workforce.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Enhance visibility into data movement.
- Increase confidence in alert/threat decisions.
- Optimize investigation workflows.
- Reduce the need for manual forensic investigations.
- Be easily deployed and easily integrated with other security tools.
- Improve security education practices.
- Help preserve brand reputation in the marketplace.

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 five interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Why Incydr?

- Full visibility into file activity across computers, cloud, and email to accurately assess data exposure.
- OS agnostic.
- Breadth and depth of event file metadata.
- Alert prioritization to ensure fast, informed responses.
- Ease of deployment and management.

Key Assumptions

- **3,000 employees**
- **4,000 endpoints**
- **Widespread organization with distributed workforces**
- **Windows, Mac, and Linux OS**
- **6 FTEs with access to Incydr**
- **2 FTEs who manage Incydr part time**

Description of composite. The composite organization is a global, IT/source code-driven company with $800 million in annual revenue. The organization has a total of 4,000 endpoints for its 3,000 employees, which include remote workers and those distributed across numerous locations. Employees use Windows, Mac, and Linux operating systems.

Deployment characteristics. The organization previously deployed a cloud access security broker, an endpoint detection and response product, and a SIEM solution. With this setup in place, the organization experienced 300 low-risk events per month and 200 medium- and high-risk security incidents and alerts requiring investigation per month.

Overall, the organization struggled to gain full visibility into data movement across its full data landscape, from corporate computers to the cloud and email systems, and across Windows, Mac, and Linux operating systems. This, in turn, created inefficiencies for security teams and increased risk to the organizations' intellectual property. Recognizing these vulnerabilities, the organization formulated the need for a more effective data loss protection solution.

As a result, the organization deploys Code42 Incydr to all employees and endpoints to increase transparency into the data landscape. The organization utilizes features such as Instructor and 90-day historical visibility into data events to gain maximum value from the solution for its organization.

> **"With Incydr, we have ease of usability, visibility, and confidence in the fact that we're getting as much data as we can in order to make informed decisions."**
>
> *Senior director, information security, cybersecurity technology*

It also deploys an Incydr Flow to initiate technical response control between Incydr and existing systems in the security tech stack. Of its employees, six actively use Incydr, and users consist of members from the SOC, IT, and engineering teams, with some users being forensic search enabled.

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	SOC team time savings	$178,875	$186,030	$193,185	$558,090	$461,500
Btr	Reduction in low-risk events	$22,059	$25,736	$29,412	$77,207	$63,420
Ctr	Forensic search savings	$107,580	$107,580	$107,580	$322,739	$267,534
Dtr	Reduction in end-user downtime	$219,600	$229,968	$240,336	$689,904	$570,261
Etr	Avoided losses with data exfiltration mitigation	$276,005	$276,005	$276,005	$828,014	$686,383
	Total benefits (risk-adjusted)	$804,118	$825,318	$846,517	$2,475,953	$2,049,098

SOC TEAM TIME SAVINGS

Evidence and data. With Incydr in place, interviewees' organizations gained the visibility, context, and control needed to substantially decrease the number of insider-driven incidents requiring investigation, while also cutting down the time to investigate those alerts.

Before deploying Incydr, the security solutions in place at the interviewees' organizations left gaps in data visibility across computer, cloud, and email systems across Windows, Mac, and Linux OSes. Additionally, other security tools flooded security analysts with alerts, many of which were benign or false positives. These issues lengthened the remediation process, as it required significant analyst effort to sift through all alerts and validate whether or not an event was a true data security threat, and if it was, decide how to adequately resolve the threat.

Conversely, Incydr prioritized file activity based on Incydr Risk Indicators at the interviewees' organizations, which prioritized the risks that needed immediate attention through contextual risk scoring based on file, destination, source, and user characteristics and behaviors. The organizations could then further investigate event details using the Forensic Search feature, which allowed them to query file and event metadata. They could also use watchlists to programmatically protect data from employees who are most likely to leak or steal files, such as departing employees. Overall, Incydr

> **"With Code42, the alerts are the tip of the iceberg. When you can dig into the level of detail that you can using the Forensic Search tool, that's been the biggest help. I have caught a few things in Code42 that even our SIEM has not caught. So, we've noticed a few things in some alerts in Code42 that then triggered much deeper looks into all of our other platforms."**
>
> *Manager, software*

reduced the noise and allowed teams to focus on what really matters.

Interviewees spoke at length about the improved visibility and subsequent time savings they experienced with the Code42 investment:

- The enterprise security architect at an industrial equipment supplier explained: “Code42 forensically dictates where it moved and the value of what moved, so investigations are shorter. Also, there was no way previously to see movement in unsanctioned cloud destinations, but now we can.”
- The senior director, information security’s cybersecurity organization previously had to manually investigate thousands of alerts per month only investigated hundreds with Incydr, a reduction in its number of investigated alerts by more than 30%. The interviewee said, “We have been able to reduce the number more over time depending on how we mark the alerts in order to tune the alerts to focus on what actually needs investigating.
- The same interviewee described a recent incident related to torrent activity. The senior director said: “With our other tool, we saw the activity as data theft by threat actor. But with Incydr, we could view it as an employee torrenting activity, and understand what the person was doing and how frequently they were doing this activity. Code42 brought this event to focus faster than our previous setup would have, and, with added context, allowed us to investigate the incident 50% faster.”
- Incydr allowed the life sciences technology organization in this study to respond faster and reduce its SOC workload. The manager, information security said: “Incydr investigations were 10% of the team’s workload three years ago, now it’s 3%. So it's no longer a case where someone does not have the capacity to investigate and rolls the investigation over to another engineer.”
- In its previous environment, 90% of data exfiltration investigations at the software organization involved USBs. According to the manager, “That has now tanked, and we’ve been able to reallocate our focus to higher-level problems where you’re actually catching people with malicious intent because you’re removing the ability to accidentally do something wrong.”

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite investigated 200 security incidents and serious alerts related to sensitive data per month in its legacy environment. Of these, 75% are of medium risk and 25% are of high risk.
- With Incydr in place, the organization reduces investigations for medium- and high-risk alerts related to sensitive data by 25% in Year 1. This increases to 35% by Year 3 as increased automation and rules are added to Incydr to mark alerts more effectively.
- In the legacy setup, it took 2 hours to investigate medium-risk incidents and alerts and 4 hours to investigate high-risk incidents and alerts.
- With Incydr and improved visibility, the mean time to investigate these incidents and alerts reduced by 50%
- The engineering/SOC analyst blended fully burdened hourly salary is $53.

Risks. SOC team time savings may vary depending on the following:

- The total number and complexity of security incidents and serious alerts requiring manual investigation.
- The time spent on each investigation process prior to Incydr.

- The speed of adopting Incydr.
- The skill level, efficiency, and salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $462,000.

SOC Team Time Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of medium- and high-risk security incidents and serious alerts related to sensitive data requiring manual investigation in legacy environment per year	Composite	2,400	2,400	2,400
A2	Number of security incidents and serious alerts related to sensitive data requiring manual investigation in legacy environment per year: Medium risk	A1*75%	1,800	1,800	1,800
A3	Number of security incidents and serious alerts related to sensitive data requiring manual investigation in legacy environment per year: High risk	A1*25%	600	600	600
A4	Reduction in security incidents and serious alerts requiring manual investigation once implementing Incydr	Interviews	25%	30%	35%
A5	Number security incidents and serious alerts requiring manual investigation avoided once implementing Incydr: Medium risk	A2*A4	450	540	630
A6	Mean time to investigate a security incident and serious alert with legacy setup: Medium risk (hours)	Interviews	2	2	2
A7	Number security incidents and serious alerts requiring manual investigation avoided once implementing Incydr: High risk	A3*A4	150	180	210
A8	Mean time to investigate a security incident and serious alert with legacy setup: High risk (hours)	Interviews	4	4	4
A9	Subtotal: Avoided investigation hours due to a reduction in medium and high risk security incidents and serious alerts	A5*A6+A7*A8	1,500	1,800	2,100
A10	Reduction in mean time to investigate a medium- and high-risk security incident or serious alert once implementing Incydr	Interviews	50%	50%	50%
A11	Subtotal: Reduction in investigation hours on remaining security incidents and serious alerts: Medium risk	(A2-A5)*A6*A10	1,350	1,260	1,170
A12	Subtotal: Reduction in investigation hours on remaining security incidents and serious alerts: High risk	(A3-A7)*A8*A10	900	840	780
A13	Engineering/SOC analyst FTE blended hourly salary (fully burdened)	TEI standard	$53	$53	$53
At	SOC team time savings	(A9+A11+A12)*A13	$198,750	$206,700	$214,650
	Risk adjustment	↓10%			
Atr	SOC team time savings (risk-adjusted)		$178,875	$186,030	$193,185
	Three-year total: $558,090		**Three-year present value: $461,500**		

REDUCTION IN LOW-RISK EVENTS

Evidence and data. Interviewees reported that Code42 Instructor microtrainings were embedded inside Incydr. They could be used to educate their organizations' workforces and drive secure work habits while reducing alert fatigue for SOC teams and mitigating overall future risk to data.

- The senior director, information security's cybersecurity organization used to receive thousands of alerts related to low-risk events, such as accidental unsanctioned file movement. Once it implemented Instructor, the organization saw a 15% drop in events related to file sharing and a more than 30% reduction in low-risk events overall.

Modeling and assumptions. For the composite organization, Forrester assumes:

- The composite organization experienced 300 low-risk events per month in the legacy environment.
- In the legacy environment, it took 30 minutes to remediate a low-risk event.
- The organization reduces the number of low-risk events by 30% in Year 1 of implementing Instructor. This increases to 40% by Year 3 as the organization expands its investment in Instructor and adds more use cases for automatic microtraining.
- The SOC analyst fully burdened hourly salary is $43.

> **"Instructor allows our SOC team to reallocate time to more high-risk events."**
>
> *Senior director, information security, cybersecurity technology*

Risks. Reduction in low-risk events may vary depending on the following:

- The number of low-risk events in legacy environments and time spent remediating each low-risk event.
- The speed of adopting Incydr.
- The skill level, efficiency, and salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $63,000.

Reduction In Low-Risk Events

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of low-risk events per year in legacy environment	Composite	3,600	3,600	3,600
B2	Time spent remediating a low-risk event (hours)	Interviews	0.50	0.50	0.50
B3	Reduction in low-risk events once implementing Instructor	Interviews	30%	35%	40%
B4	SOC analyst FTE hourly salary (fully burdened)	TEI standard	$43	$43	$43
Bt	Reduction in low-risk events	B1*B2*B3*B4	$23,220	$27,090	$30,960
	Risk adjustment	↓5%			
Btr	Reduction in low-risk events (risk-adjusted)		$22,059	$25,736	$29,412
	Three-year total: $77,207		**Three-year present value: $63,420**		

FORENSIC SEARCH SAVINGS

Evidence and data. Prior to implementing Incydr, IT and security staff at interviewees' organizations had little visibility into the file movement on the endpoints, whether it was from the endpoints to external devices or to external cloud storage. The companies sometimes suspected both existing and departed employees of taking sensitive information to competitors but had no solid proof and no means of preventing the use of this information by the competition. The investigation process was reactive, required involvement from multiple IT and security resources, took a long time, and frequently yielded limited or no results. Interviewees with multiple locations around the globe faced additional challenges and fees related to physically obtaining devices for investigation due to varied legislation.

Organizations could drastically reduce the number endpoints requiring forensic investigations with Incydr due to increased visibility into file movement and the ability to be proactive rather than reactive.

- When suspecting someone of wrongdoing, the life sciences technology organization had to have that person's laptop shipped to an on-site staff forensic examiner to perform a disc carving. Pre-Incydr, the organization was conducting three forensic investigations per month and each one would take about 10 days. In the past year since implementing Incydr, they have only had to do two. The manager, information security said, "We have been able to avoid forensic investigations for 95% of our cases."
- For the software organization, traditional dead box forensic analysis took multiple days and 24 people hours to conduct. Overall, issues would take weeks to be resolved. The same issues could be resolved in hours with Incydr. The manager explained: "Incydr acts like a barometer. You can tell right away if a person is as clean as a whistle or if there is something we need to go deeper on. And if we do need to go deeper, we can pull relevant artifacts right out of the tool. Now before we even approach the person of interest and start investigating, we have all the answers."
- The software industry interviewee also discussed the value of having to deal with customs less frequently. They said: "Shipping a Mac from Argentina would cost us $5,000 every time due to taxes and other fees. Now, it doesn't matter where in the world someone is, I can investigate using Incydr from anywhere and I can take action from anywhere as well. We rarely have to deal with customs anymore."
- When examining files of departing employees for a legal case, the security organization was able to recover evidence on a file status within a week with Incydr. If they had had to ship the laptop and then attempt to recover the data, it would have taken a month. According to the organization's information security architect, "It would have been a very ambiguous month, because we don't know for sure whether or not we would have been able to recover the file."

> **"We have been able to reallocate 2.5 FTEs by reducing the need to run forensics manually."**
>
> *Manager, information security, life sciences technology*

Modeling and assumptions. For the composite organization, Forrester assumes:

- Every year, 0.15% of endpoint devices require forensic investigation services. This includes devices for existing and departing employees.

- On average, it takes an IT security architect 24 hours of active work to perform a forensic investigation.
- The number of endpoint devices requiring forensic investigation services reduces by 80% once implementing Incydr.
- The IT security architect fully burdened hourly salary is $72.
- About 70% of the endpoints that needed forensic investigation were not located in the same places as where the services were being performed in the legacy environment. It cost the organization $500 to ship one device to the IT team for investigation on average.

Risks. Forensic search savings may vary depending on the following:

- The size of the organization, number of endpoints, and the level of suspicious activity or perceived risk to IP within an organization.
- Detection and investigation capabilities available to the organization prior to Incydr
- Shipping costs (domestic vs. international) and associated fees.
- The salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $268,000.

> **If we didn’t have Incydr, we would need at least 3 more people just doing forensics, and we wouldn’t have been able to transition our security team to adopt a more generalist model where everybody can do everything.**
>
> — Manager, software

Forensic Search Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of endpoints devices	Composite	4,000	4,000	4,000
C2	Number of endpoint devices requiring forensic investigation services per year in legacy environment	C1*0.15%	72	72	72
C3	Time spent performing a forensic investigation per device (hours)	Interviews	24	24	24
C4	Reduction in number of endpoint devices requiring forensic investigation services once implementing Incydr	Interviews	80%	80%	80%
C5	IT security architect FTE hourly salary (fully burdened)	TEI standard	$72	$72	$72
C6	Subtotal: Time savings performing forensic investigations	C2*C3*C4*C5	$99,533	$99,533	$99,533
C7	Number of endpoints shipped for forensic investigation in legacy environment	C2*70%	50	50	50
C8	Reduction in number of endpoints shipped for forensic investigation once implementing Incydr	C7*C4	40	40	40
C9	Cost of sending an endpoint device for reimaging (shipping and processing fees, taxes)	Interviews	$500	$500	$500
C10	Subtotal: Shipping cost savings	C8*C9	$20,000	$20,000	$20,000
Ct	Forensic search savings	C6+C10	$119,533	$119,533	$119,533
	Risk adjustment	↓10%			
Ctr	Forensic search savings (risk-adjusted)		$107,580	$107,580	$107,580
	Three-year total: $322,739			**Three-year present value: $267,534**	

REDUCTION IN END-USER DOWNTIME

Evidence and data. A reduction in the number and duration of investigations for medium- and high-risk security incidents and serious alerts, the number of endpoint devices requiring forensic investigation services, and the number of low-risk events, resulted in a reduction of end-user downtime as well. With Incydr, end users are less likely to be unable to access their organization's systems, as IT and security teams have better visibility into the data movement issues at hand.

- The interviewed information security architect's security organization was able to reduce the incidences of wrongful blocking of employees that would occur with false positives. The interviewee said, "With visibility into files and seeing what is being flagged by the system, we have a better ability to tune the solution to fit our needs and reduce unnecessary blocking." Downtime for these types of incidents was anywhere from four to eight hours.
- The interviewee at a cybersecurity technology organization agreed that that Incydr uplifted the end-user experience. The senior director,

information security explained: “When we detected someone moving data when they shouldn’t be, they weren’t allowed to work until we finished our investigation. For high-risk cases, that could be days.” The organization saw 25 to 30 high-risk cases per year. Now the organization locks out 50% less end users than they used to.”

- When conducting manual forensic investigations, end users at the software organization would be down from the system anywhere from one to three weeks. They were not provided with a replacement laptop as their status as a trustworthy employee was in question.

End-user downtime avoided in Year 1

6100 hours

Modeling and assumptions. For the composite organization, Forrester assumes:

- End users are impacted by 30% of the data-related investigations the SOC team completes (expressed in Benefit A).
- The end-user downtime per investigated security incident in the legacy environment was 6 hours. Once implementing Incydr, this reduces by 50% (in accordance with A10).
- End users are impacted by 50% of the manual forensic investigation requests. The remaining 50% are for departing employees, who would not experience downtime once sending their endpoint for investigation.
- End users experience 80 hours of downtime per manual forensic investigation.
- End users experience 1 hour of downtime per low-risk event.

Risks. Reduction in end-user downtime may vary depending on the following:

- The number of investigations that would materially impact an end user.
- The amount of downtime experienced due to investigations and events in the prior environment.
- The salaries of affected FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $570,000.

Reduction In End-User Downtime

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of security incidents and serious alerts requiring manual investigation avoided once implementing Incydr	A5+A7	600	720	840
D2	Percent of investigations that would materially impact an end user	Interviews	30%	30%	30%
D3	Number of avoided investigations that would materially impact an end user	D1*D2	180	216	252
D4	End-user downtime per investigated security incident in legacy environment (hours)	Interviews	6	6	6
D5	Subtotal: Avoided investigation impact to end users due to avoided security incidents (hours)	D3*D4	1,080	1,296	1,512
D6	Number of security incidents and serious alerts impacting end users once implementing Incydr	(A1-D1)*D2	540	504	468
D7	Reduction in end-user downtime for remediation activities once implementing Incydr	Interviews	50%	50%	50%
D8	Subtotal: Avoided investigation impact to end users due to a reduction in mean time to remediate (hours)	D6*D4*D7	1,620	1,512	1,404
D9	Reduction in number of endpoint devices requiring forensic investigation services with Incydr	C2*C4	58	58	58
D10	Percent of endpoint devices requiring forensic investigations affecting end-user downtime	Composite	50%	50%	50%
D11	End-user downtime per forensic investigation in legacy environment (hours)	Interviews	80	80	80
D12	Subtotal: Avoided end-user downtime for forensic investigations (hours)	D9*D10*D11	2,320	2,320	2,320
D13	Avoided low risk events once implementing Instructor	B1*B3	1,080	1,260	1,440
D14	End-user downtime per low-risk event (hours)	Interviews	1	1	1
D15	Subtotal: Avoided end-user downtime for low-risk events (hours)	Composite	1,080	1,260	1,440
D16	Business user FTE hourly salary (fully burdened)	TEI standard	$40	$40	$40
Dt	Reduction in end-user downtime	(D5+D8+D12+D15) *D16	$244,000	$255,520	$267,040
	Risk adjustment	↓10%			
Dtr	Reduction in end-user downtime (risk-adjusted)		$219,600	$229,968	$240,336
	Three-year total: $689,904		Three-year present value: $570,261		

AVOIDED LOSSES WITH DATA EXFILTRATION MITIGATION

Evidence and data. According to Forrester research, insiders represent risk to organizations. In fact, almost one-quarter of breaches security decision-makers responding to Forrester's Security Survey, 2023 noted their organizations faced in the past 12 months were the result of insider incidents.[7] Whether accidental or malicious, insider incidents can result in financial fraud, privacy abuses, intellectual property theft, or damage to infrastructure.[8]

By using Incydr, interviewees' organizations reduced the extent of data theft through insider incidents. Incydr detected suspicious employee behavior and data exfiltration actions as they happened, which allowed SOC teams to stop data loss before a competitor or nation-state actor can get it.

- According to the enterprise security architect at the industrial equipment supplier: "Every trade secret or manufacturer part we have has its own unique rule set. If there was any movement on any of those, I can see it with Incydr. If those products and recipes got out, it would destroy our business."
- The manager, information security at the life sciences organization stated: "We have multiple watchlists within Incydr. Somebody high on that watchlist came up as someone who was sending data to a competitor. We were able to reach out to the endpoint and quarantine the asset right away. It turned out that he had begun sending out IP but hadn't sent the bulk of the data yet. Legal had a field day! Our organization is currently seeking eight figures in relief, and this tool gives us all the data we need to do that at our fingertips."
- The manager at the software company explained how they have better control over their data environment: "We're now able to say, 'Hey, this piece of IP would've left the company if we didn't have the controls through Incydr in place."

Damage From Data Loss From Insiders Comes In Several Different Forms.*

- **Fraud and financial gain:** Insiders can use their privileged access to modify records, take sensitive data, or steal/transfer money for financial gain.
- **Intellectual property theft:** Insiders steal intellectual property such as proprietary formulas, source code, blueprints, or M&A documentation to sell or use outside the company.
- **Sabotage and destruction:** Insiders perform acts of sabotage such as corrupting data, breaking equipment, or damaging infrastructure maliciously.
- **Snooping, leaking, and doxing:** Insiders can abuse their access to invade the privacy of others or access secrets to which they shouldn't be privy.

*Source: "Best Practices: Insider Risk Management," Forrester Research, Inc., June 30, 2023.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Forrester models the cost of a breach by employee count at organizations. According to Forrester data, the cost of a major breach due to data exfiltration is $181,582 for an organization with 3,000 employees.[9] This cost does not consider the loss of data productivity, but includes the following:

  - Fines to regulatory bodies.
  - Customer reimbursement/lawsuits.
  - Incident response and remediation.
  - Lost revenues.
  - Brand equity rebuild costs.
  - Cost of customer reacquisition.

- With Incydr, the organization reduces the loss per major data exfiltration incident by 40% due to faster detection with enhanced visibility through the solution.
- The organization experiences four major data exfiltration incidents per year.

Security breaches due to data exfiltration can cost anywhere from **tens of thousands to millions of US dollars in labor, direct costs, and lost business** depending on the severity of the breach and volume and type of data exfiltrated. And, according to Forrester's Security Survey, 2023, the cumulative cost of breaches annually can total $10 million or more for an enterprise organization of 1,000 or more employees.

While this TEI analysis assumes a $181,582 cost per major breach for an organization of 3,000 employees, readers are encouraged to consider their own situation.

> **"We could lose massive amounts of revenue if the wrong type of IP got out there but, more importantly, our whole company would go up in smoke."**
>
> *Information security architect, security*

Risks. Avoided losses with data exfiltration mitigation may vary depending on the following:

- The volume and severity of breaches.
- The characteristics of the organization, in terms of size, industry, maturity, and security measures in place.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $686,000.

Avoided Losses With Data Exfiltration Mitigation

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Number of employees	Composite	3,000	3,000	3,000
E2	Cost of a major breach due to data exfiltration	Forrester research	$181,582	$181,582	$181,582
E3	Reduction in loss per major data exfiltration incident due to faster threat detection and enhanced visibility with Incydr	Interviews	40%	40%	40%
E4	Subtotal: Reduction in loss per major data exfiltration incident with Incydr	E2*E3	$72,633	$72,633	$72,633
E5	Number of major data exfiltration incidents per year	Interviews	4	4	4
Et	Avoided losses with data exfiltration mitigation	E4*E5	$290,531	$290,531	$290,531
	Risk adjustment	↓5%			
Etr	Avoided losses with data exfiltration mitigation (risk-adjusted)		$276,005	$276,005	$276,005
	Three-year total: $828,014			**Three-year present value: $686,383**	

UNQUANTIFIED BENEFITS

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

- **Legal efficiencies.** Legal teams faced challenges around effectively investigating suspected insider threat activity related to data exfiltration and being able to gather sufficient evidence to take action.

  With Incydr, legal teams gained access to a solution that provided clear visibility into where and how data is accessed and stored, 90-day historical visibility to review suspicious activity, and a saved copy of all exfiltrated data. In turn, organizations could accelerate the forensic investigation process and provide legal teams with the evidence necessary for litigation or prosecution, which saved legal fees.

  - For the manager, information security's life sciences technology company, it would take at least two weeks for someone in incident response to understand file movement and send the data over to legal prior to implementing Incydr. Now it takes an hour or less for legal to gain access to the necessary information. This enhanced visibility enabled the organization to win more events and stop 10 to 12 cases from going to court per year.

  - For the software organization, whenever a case escalated to court, outside counsel was involved, costing thousands of dollars per day. With Incydr, they could catch issues while they were smaller, before they escalated into a full data breach. This way, they handled the situation in-house instead and avoided outside counsel fees. The manager said: "The average case duration is five business days from the alert being fired to legal

> **“It’s easier for legal teams to take a position on a case when everything is forensically served up in a bowl versus working with a bunch of abstract pieces of information that they’re cobbling together to try and make a point.”**
>
> *Enterprise security architect, industrial equipment supplier*

taking the appropriate action. Before Incydr, it could sometimes take a week to just do the investigation aspect. And then you had to tack on time for conducting more off-the-wall investigatory methods and bringing legal up to speed." The organization was able to avoid using outside counsel for at least 60% of their cases.

- **Unexpected cost savings.** Interviewees mentioned several examples in which Incydr led to unexpected cost saving situations for their organizations.
  - The enterprise security architect at the industrial equipment supplier shared: "Two weeks after we deployed Incydr, we uncovered that one of our employees happened to be employed by half a dozen employers and had tools in place to make his device appear as though it was online when he wasn't. Incydr wrapped up that entire matter with a bow, saving our organization up to half a million dollars in terms of his payroll and his failure to make decisions to advance his intellectual contribution to the company."
  - The cybersecurity organization was able to stop investing in more security solutions because of the visibility they had with Incydr. The senior director, information security said, "I've been able to deny vendors that come in trying to sell us their security product because none of their products seem to add any additional visibility to what we have anymore."
  - The life sciences technology organization was able to save on paying unemployment costs by proving that some employees that were involuntarily dismissed were actually terminated with cause using the increased visibility Incydr provided. The manager, information security stated: "When you let somebody go, if they disagree, sometimes you pay unemployment because it's cheaper than going through the litigation process. Now, we can say, 'No, this is a slam dunk issue, we're not paying you anything because you stole from the company, and here's the proof.'" This would previously cost the organization $50,000 to $150,000 per employee in terms of stock and severance packages.

> **“There have been five events in the past year where legal was able to change an employee’s unemployment status from ‘severance package’ to ‘terminate with cause’ based off Incydr data.”**
>
> *Manager, information security, life sciences technology*

- **Compliance efficiencies.** Incydr's secure data collection, data monitoring, end-to-end encryption, and visibility into data exfiltration across a variety of vectors enabled organizations to adhere to compliance standards. The manager at the software organization exclaimed: "We're able to prove that we have good robust controls, and we take these issues very seriously. From a customer trust standpoint, being able to demonstrate that we have these controls and that they actually work upholds our relationship with them. From a regulations standpoint, Incydr ensures we comply with our industry's requirements.”

  The same interviewee spoke to the value of data segmentation with Incydr: “Now our EU data stays in the EU, my APAC data stays in APAC, and the US data stays within the US. This makes it even easier to stay compliant because you can find what you need fast.”

- **Data infiltration efficiencies.** Organizations were able to streamline their data infiltration incident resolution process as well. For instance, when the software organization learned of a potential data infiltration scenario through an external complaint, it used to take them half a day to look in each respective tool to find the files and IP that was deemed stolen. Now the organization can just plug in the file name or serial number of a hard drive and find the data in question in 10 minutes.

- **Great provider support.** Interviewees spoke highly of the level of support and guidance the Code42 team provided since their organizations decided to implement the Incydr solution. They described the Code42 team as hands on, helpful, and a group that ensured the solution added benefit to its customers’ organizations. The manager, information security, at the life sciences technology organization explained: "I’m used to sales drones. Once they make the sale, they’re gone. And that’s not really something I’ve observed with Code42's account team and this customer service group. They want to be active partners rather than it be a transactional relationship. And so, when situations arise, they’re like, 'Hey, let’s talk about the problems you’re experiencing and maybe we have a fit and maybe we don’t. Maybe we know somebody, maybe we don’t.' But they're transparent and always willing to try and help find a solution."

> **“One of the key differentiators for the product is the Code42 account team. They are always accessible and that really makes us feel like we have a partner as opposed to just a vendor. Knowing that Code42 is behind us, and that they want to help, really this speaks to their vision, execution, and their customer obsession.”**
>
> *Manager, software*

FLEXIBILITY

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

- **Further increase integrations.** Organizations looked to increase SOAR integrations to further reduce time to resolution for data leaks. They also aimed to increase integrations with collaboration and messaging tools to increase SOC efficiency. The information security architect at the security organization explained, “We want our SOC team to access alerts through our collaboration tool rather than email so they're able to gain efficiencies in processing alerts using channels and automations."

- **Expanding Incydr capabilities.** Interviewees from organizations that did not take advantage of or take full advantage of all the features associated with Incydr expressed interest in doing so in the future. For instance, organizations not using Instructor looked forward to implementing it in the next year and those with Instructor deployed looked to add additional microtrainings to their stack to further educate employees and reduce the number of low risk events.

  Organizations also looked to deploy Incydr's real-time blocking capabilities, which would allow them to block unacceptable data movement without the management burden, inaccuracy, and endpoint impact of content-based policies.

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

> **"We're constantly looking for the right risk use case for which if we deploy a new Instructor microtraining, it will have the biggest impact for employees."**
>
> *Senior director, information security, cybersecurity technology*

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
Ftr	Fees to Code42	$12,000	$275,000	$275,000	$275,000	$837,000	$695,884
Gtr	Internal fees	$22,239	$13,936	$13,936	$13,936	$64,046	$56,895
	Total costs (risk-adjusted)	$34,239	$288,936	$288,936	$288,936	$901,046	$752,779

FEES TO CODE42

Evidence and data. The interviewees' organizations paid annual fees to Code42 based on the size and scope of the implementation in terms of the number of employees covered and the subscription package in use. They also paid a one-time fee for Code42 professional services during the initial deployment period for assisting with implementation.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Annual fees for Incydr are $275,000 for 3,000 employees using the Incydr Professional subscription. It includes Instructor and a cloud storage connector, among other capabilities. The organization also deployed the 90-day retention feature.
- The composite organization pays $12,000 for Code42 professional services over the initial implementation period.
- Pricing may vary. Contact Code42 for additional details.

Risks. Fees to Code42 may vary depending on the following:

- Number of employees covered using Incydr.
- Incydr subscription package and capabilities in use.

> **"Code42 has a tremendous training and support staff from prepurchase through postpurchase."**
>
> *Senior director, information security, cybersecurity technology*

Results. As the composite organization was priced directly with Code42, this cost has not been adjusted for risk, yielding a three-year total PV (discounted at 10%) of $696,000.

Fees To Code42

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Code42 professional services fee	Composite	$12,000			
F2	Code42 annual subscription fees	Composite		$275,000	$275,000	$275,000
Ft	Fees to Code42	F1+F2	$12,000	$275,000	$275,000	$275,000
	Risk adjustment	0%				
Ftr	Fees to Code42 (risk-adjusted)		$12,000	$275,000	$275,000	$275,000
	Three-year total: $837,000			**Three-year present value: $695,884**		

INTERNAL FEES

Evidence and data. Interviewees described the implementation, training, and ongoing management of Incydr as simple and a relatively minimal time investment that required:

- Initial involvement from both IT and engineering staff for embedding the solution within an organization's environment and rollout. Roles involved in implementation included security architects, platform engineers, and deployment administrators, among others. Organizations typically rolled out the solution in groups, starting with a pilot with test users and then expanding across all departments during the implementation period. The information security architect at the security organization said, "We go by department and try to fix issues as we roll out."
- IT/engineering FTEs who provided ongoing upkeep of the solution and worked on upgrades and deploying new features. The senior director, information security at the cybersecurity organization explained, "A lot of the updates are around increased visibility, increased capabilities, and maybe adding another dashboard, but they can mostly be deployed in the background as the feature rolls in."

> **"We never have a problem with Incydr, it just works."**
>
> *Manager, software*

- Training for primary users, which typically included security and engineering resources. Training exercises were provided by Code42, but interviewees also mentioned that trying and testing the environment with Incydr helped users become proficient with the solution. The information security architect at the security organization stated: "Training was really easy. If you've worked in IT before, you should be able to pick it up pretty quick."

Organizations took an average of two months to implement Incydr, integrate it into their environment, and roll it out to different teams and departments.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Three IT/engineering FTEs dedicate 30% of their time during the initial two-month implementation period.
- After the initial period, two IT/engineering FTE spend 5% of their time per year managing Incydr.
- The blended fully burdened salary for IT and engineering FTE is $120,000.
- All six users on Incydr take part in 10 hours of training in the initial period to understand how the solution works. They are involved in training for four hours every year thereafter. This training includes refreshers and reminders on how to fully utilize the platform's capabilities.
- The blended fully burdened hourly salary for engineering and SOC analyst FTE is $53.

Risks. Internal fees may vary depending on the following:

- The size and scope of Incydr deployment.
- The skillset of internal FTEs involved in implementation, training, and management and their associated salaries.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $57,000.

> **"Deploying Incydr to a new environment and having it be fully operational took a matter of days. And then once you deploy, you have visibility into data movement in just a matter of hours."**
>
> *Senior director, information security, cybersecurity technology*

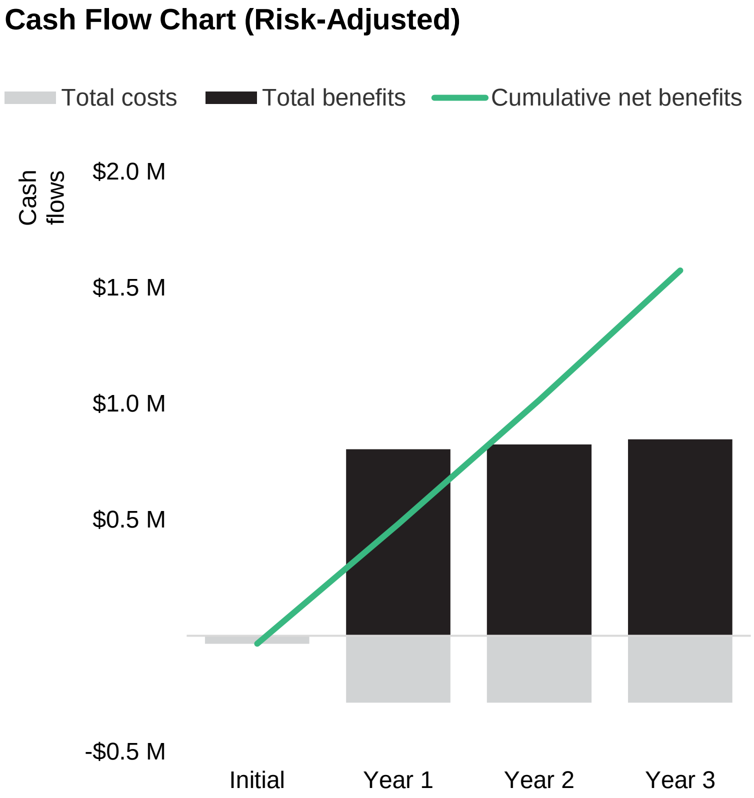
Internal Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	IT/engineering FTE involved in implementation and ongoing management	Composite	3	2	2	2
G2	Time dedicated by FTEs (months)	Interviews	2	12	12	12
G3	Percentage of FTEs' time dedicated to implementation and ongoing management	Interviews	30%	5%	5%	5%
G4	IT/engineering FTE blended annual salary (fully burdened)	TEI standard	$120,000	$120,000	$120,000	$120,000
G5	Subtotal: Implementation and ongoing management fees	G1*G2*G3*(G4/12 months	$18,000	$12,000	$12,000	$12,000
G6	FTEs trained on Code42	Interviews	6	6	6	6
G7	Training hours per FTE	Interviews	10	4	4	4
G8	Engineering/SOC analyst FTE blended hourly salary (fully burdened)	TEI standard	$53	$53	$53	$53
G9	Subtotal: Training fees	G6*G7*G8	$3,180	$1,272	$1,272	$1,272
Gt	Internal fees	G5+G9	$21,180	$13,272	$13,272	$13,272
	Risk adjustment	↑5%				
Gtr	Internal fees(risk-adjusted)		$22,239	$13,936	$13,936	$13,936

Three-year total: $64,046 **Three-year present value: $56,895**

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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	($34,239)	($288,936)	($288,936)	($288,936)	($901,046)	($752,779)
Total benefits	$0	$804,118	$825,318	$846,517	$2,475,953	$2,049,098
Net benefits	($34,239)	$515,183	$536,382	$557,582	$1,574,907	$1,296,319
ROI						172%
Payback period						<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

"Internal Incidents Cause Roughly A Quarter Of Breaches, With More Than Half Intentional," Forrester Research, Inc., July 28, 2023.

"The Insider Risk Management Team Charter," Forrester Research, Inc., June 20, 2023.

Appendix C: Endnotes

[1] Source: Forrester's Security Survey, 2023.

[2] Source: "Manage Insider Risk With Zero Trust," Forrester Research, Inc., July 6, 2023.

[3] Source: Joseph Blankenship, Heidi Shey, Jeff Pollard, "Prevent Data Turnovers With Insider Risk Management," Forrester Blogs.

[4] 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.

[5] Source: Forrester's Security Survey, 2023.

[6] Source: "The State Of Privacy And Cybersecurity, 2023," Forrester Research, Inc., September 5, 2023.

[7] Source: Forrester's Security Survey, 2023.

[8] Source: "Best Practices: Insider Risk Management," Forrester Research, Inc., June 30, 2023.

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

FORRESTER®