A Forrester Total Economic Impact™
Study Commissioned By IntSights
October 2019

# The Total Economic Impact™ Of The IntSights External Threat Protection Suite

## Cost Savings And Business Benefits Enabled By The External Threat Protection Suite

FORRESTER®

# Table Of Contents




**Project Directors:**
Sam Conway
Connor Maguire


ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.



FORRESTER®

## Business Benefits

Time savings from automated dark web searching:
**$1,151,723**

Security takedown efficiency:
**$196,497**

Proactive security response:
**$1,193,689**

# Executive Summary

According to Forrester's research, 55% of enterprise network security decision makers experienced at least one breach in the past 12 months. Of these breaches, approximately 41% were due to an external attack.[1] As cyberattacks become more prevalent, organizations are looking for solutions to help them get ahead of potential threats and preempt attacks.

Companies increasingly turn to external threat intelligence to gain the upper hand and defend against sophisticated and malicious threat actors. With external threat intelligence in hand, security teams are equipped with the visibility, automation, and technical controls to neutralize threats outside the wire. The visibility and rapid, automated response provided by these platforms can be used to identify more threats and greatly lower the risk that organizations face from external threats.

The IntSights External Threat Protection Suite (ETP) offers customers in-depth and customized data about the threats that their organizations face. IntSights monitors thousands of sources across the clear, deep, and dark web to identify threats that directly target their customers. IntSights also automates mitigation and takedown responses, neutralizing threats before they materialize into a successful attack.

IntSights commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying the External Threat Protection Suite. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of IntSights on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five of IntSights' current enterprise customers who all had years of experience using the External Threat Protection Suite. Prior to using IntSights, the interviewed organizations used legacy threat intelligence solutions — or completely lacked automated tools — that were unable to provide them with data customized to their needs and details. The customers felt they needed a comprehensive solution to monitor and defend against external threats; one that provided organizationally relevant threat data and enabled them to proactively find threats originating from social media and the dark web.

Since adopting IntSights, the customers' security teams increased the efficiency of their processes to search for and identify threats on the dark web. They improved their takedown response times and can now identify more potential threats thanks to IntSights. The chief information security officer for a financial services firm stated: "It would be very difficult for any security team to build the capabilities that IntSights provides internally. The visibility into where our name might be mentioned in the world or where we might be impersonated in the world is one of the biggest benefits IntSights provides."

## Key Findings

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



FORRESTER®

**ROI**
**442%**

**Benefits PV**
**$2.5 million**

**NPV**
**$2.1 million**

- **Automated dark web intelligence reduces the time security analysts spend searching for threats by 75%.** Utilizing IntSights' expertise to search for and identify threats on the dark web reduces the total time security analysts dedicate to searching for external threats and the total resources dedicated to these activities. Automating the search process saves organizations 7,500 hours across their security teams.
- **Security teams take down phishing domains, malicious mobile apps, and social media profiles 66% more efficiently.** Leveraging relationships, established by IntSights, with large domain registrars and service providers greatly reduces the time organizations spend attempting to take down fraudulent domains and social media profiles. Additionally, the information provided by IntSights allows organizations to delegate these takedowns to more junior members of security teams, allowing their senior analysts to focus on higher priority work.
- **IntSights detects harmful security events allowing customers to avoid expensive response processes.** Making use of the security data provided by IntSights allows organizations to identify a greater number of potential security threats. The increase in proactive response allows these organizations to avoid $600,000 in direct fraud and cleanup expenses annually.

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

- **IntSights will also monitor for threats targeting non-cyber assets.** Several customers described how they were able to make use of IntSights' intelligence to identify and avoid physical threats to employees.
- **Access to a data rich platform accelerates junior analyst training.** Increased exposure to security threats provides junior analysts with valuable on-the-job experience, improving the overall skill of security teams.
- **Increasing organizational security with IntSights has the potential to lower cyber insurance premiums.** Customers believed that having IntSights and improving cyberattack resilience would help lower insurance premiums in the future.
- **Assure compliance with legal and regulatory obligations.** Using IntSights strengthened organizations' ability to remain compliant with major data-related regulations such as General Data Protection Regulation (GDPR), HIPAA (Health Insurance Portability and Accountability Act), and the Payment Card Industry Data Security Standard (PCI-DSS). Remaining compliant ensures organizations' continued ability to participate in certain industries and avoid fines.
- **Preserve brand image.** IntSights aids organizations in avoiding the loss of customer records and taking down counterfeit profiles or domains — both of which pose a threat to customer trust and brand equity.

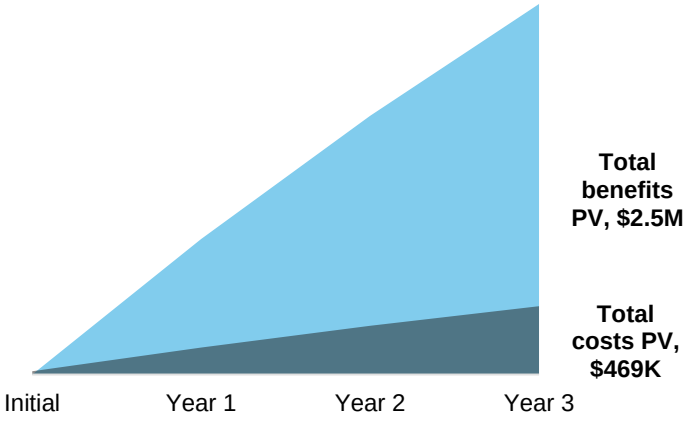
**Costs.** The interviewed organizations experienced the following risk-adjusted PV costs:

- **IntSights subscription costs**. Rather than a pricing model based on number of users, IntSights calculates an annual license fee based on the number of assets and keywords that are monitored in the platform at one time. The calculation of the licensing fees results in a three-year present value of $443,903.

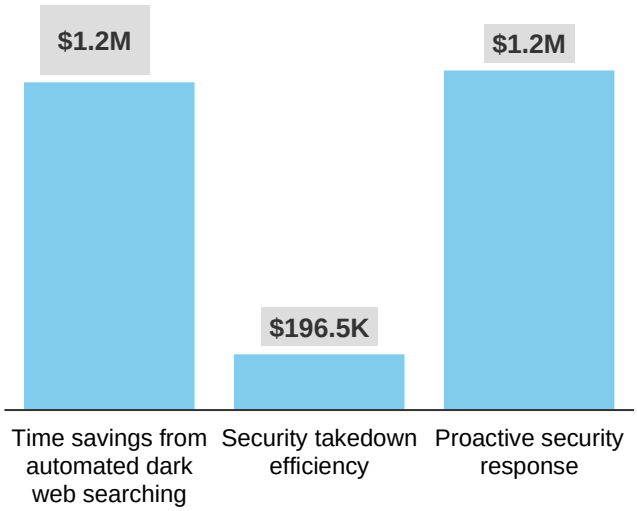
- **Cost to implement IntSights across the organization.** Users described the setup process as a simple batch upload of vendor assets, which included configuring the platform to monitor specific keywords. The conservative calculation of initial costs results in a three-year present value of $18,900.
- **The cost to train security personnel on the IntSights system.** Customers explained that the platform was very intuitive to use and required minimal training. The total three-year present value of this cost of $6,015.

Forrester's interviews with five existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $2,541,909 over three years versus costs of $468,818, adding up to a net present value (NPV) of $2,073,091 and an ROI of 442%.

**Financial Summary**




**Benefits (Three-Year)**






FORRESTER®

## TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing the IntSights External Threat Protection Suite.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that the IntSights External Threat Protection Suite can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

**DUE DILIGENCE**
Interviewed IntSights stakeholders and Forrester analysts to gather data relative to the External Threat Protection Suite.

**CUSTOMER INTERVIEWS**
Interviewed five organizations using the External Threat Protection Suite to obtain data with respect to costs, benefits, and risks.

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

**FINANCIAL MODEL FRAMEWORK**
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

**CASE STUDY**
Employed four fundamental elements of TEI in modeling the IntSights External Threat Protection Suite's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

# The External Threat Protection Suite Customer Journey

**BEFORE AND AFTER THE INTSIGHTS EXTERNAL THREAT PROTECTION SUITE INVESTMENT**

## Interviewed Organizations

For this study, Forrester conducted five interviews with customers of the IntSights External Threat Protection Suite. Interviewed customers include the following:

| INDUSTRY | REGION | ANNUAL REVENUE | SIZE OF SECURITY TEAM |
|---|---|---|---|
| Electronic manufacturing | Headquartered in EMEA | $7.3 billion | 3 security analysts |
| Energy & power | Headquartered in EMEA | $45 billion | 10 security analysts |
| Insurance | Headquartered in EMEA | $4.7 billion | 20 security analysts |
| Health insurance | Headquartered in the US | $9.9 billion | 17 security analysts |
| Financial services | Headquartered in the US | $5.9 billion | 3 security analysts |

## Key Challenges

- **Need for further protection from external attacks/threats.** Prior to investing in the IntSights External Threat Protection Suite, organizations needed an additional layer of security in their ecosystems to identify and prevent potential attacks. Some customers even stated they found evidence of compromising and potentially harmful information about their organizations that their legacy solution didn't notify them of. A cyberthreat intelligence manager stated: "We found some data online. It didn't represent a data breach, it just represented a nuance of our business, which is that sometimes confidential information is sent to an investor. This investor is a public entity, and they ended up posting that information on their website. So, it almost looks as if confidential information had been leaked."
- **Lack of visibility into the information gathered by previous solutions.** With their legacy systems, customers had little knowledge of the potential security threats their organizations faced. These solutions would often provide data across a wide swathe of verticals as opposed to catering the data to their customers' needs. Additionally, the data they provided was confusing to navigate and did not allow for high levels of customization. The head of cybersecurity for an insurance company noted: "Our legacy system didn't give us many incidents to deal with, and the things that they did give us were feeds that were publicly available. We didn't have many interactions with them and their tools, their website was very minimal, and it didn't contain a lot of features."

"We found some data online. It didn't represent a data breach, it just represented a nuance of our business, which is that sometimes confidential information is sent to an investor. This investor is a public entity, and they ended up posting that information on their website. So, it almost looks as if confidential information had been leaked."

*CISO, financial services*



FORRESTER®

- **Too much noise and unactionable data from existing security intelligence sources.** Customers stated that with their legacy threat protection systems, security analysts were required to sift through extensive amounts of information to pick out what was relevant to their job. This created immense amounts of rework for these analysts, which could have been better spent analyzing higher priority security threats. An enterprise security manager highlighted these inefficiencies by saying: "We found that there was a lot of data to go through, but the data wasn't really tailored to my company. So, I ended up having highly paid analysts spending a lot of time duplicating that information and trying to figure out what type of events were relevant to my company."
- **Difficulty reaching service providers to take down malicious content.** A common challenge all the interviewed organizations faced was the inability to take down malicious content once it was identified. Organizations needed to deal with domain registrars, social media networks, data- and file-sharing services, and mobile application stores, which were all potential channels for fraudulent and malicious content. Interviewees found the large, bureaucratic organizations difficult to work with. The head of cybersecurity for one interviewed organization expressed just how difficult this process was prior to using IntSights: "First of all, you don't know where to begin, because contacting the platform is basically impossible. You must establish a connection with them and that's difficult because I don't know how to talk to anyone at these organizations. Then you must prove that this is a fake account, which is a whole other thing."

> "We found that there was a lot of data to go through, but the data wasn't really tailored to my company. So, I ended up having highly paid analysts spending a lot of time duplicating that information and trying to figure out what type of events were relevant to my company."
>
> *Enterprise security manager, health insurance*

## Solution Requirements

The interviewed organizations searched for a solution that could:

- **Scrape and monitor dark web activity.** Organizations stated that one of the key drivers for investing in IntSights was the dark web monitoring the solution provided. This gave organizations a deeper knowledge of illicit activity and allowed them to be proactive in their threat protection practices.

## Key Results

The interviews revealed that key results from the External Threat Protection Suite investment include:

- **Faster and more efficient take down of potential security threats due to the quality of information provided by IntSights**. The established relationship between IntSights and some of the most prominent social media and domain registration websites allows organizations to remove fraudulent websites and profiles very quickly. In addition to this efficiency, security teams were able to delegate these activities to their more junior analysts, allowing their senior analysts to focus on other high priority security threats. The enterprise security manager for a large health insurance company stated: "The investigations are now done by lower level analysts. They spend a lot less time on it because we're not chasing false positives. The information is validated by IntSights. We use their analyst service and engage with them if we have questions."

> "The investigations are now done by lower level analysts. They spend a lot less time on it because we're not chasing false positives. The information is validated by IntSights. We use their analyst service and engage with them if we have questions."
>
> *Enterprise security manager, health insurance*

- **Automated dark web searches allow security analysts to dedicate their time to higher priority security threats.** Leveraging the dark web searching expertise embedded in the External Threat Protection Suite allows security analysts to use their time more efficiently. Analysts no longer spend most of their days attempting to identify and prevent external threats. The information given to them by IntSights made detection practices significantly faster, allowing analysts to spend more time looking at their internal ecosystems and analyzing potential areas of vulnerability. An enterprise security manager shared: "Our analysts would do a whole lot of searching across the dark web and were met with very little results. Now we leverage the [IntSights] information because it gives us information about the next planned attacks and what are the latest and greatest attack techniques."
- **Increased the scope of security threats that organizations can stop and avoided the costly expense of remediating these attacks.** Proactive security monitoring enabled organizations to identify and remediate more threats than they would have without IntSights. The head of cyberthreat intelligence for one organization described, "There were a few cases that we missed some, but IntSights provided alerts on time and we were able to avoid the effects of a costly breach." This benefit is invaluable to organizations as the size and scope of a security breach can vary greatly and the cost of being breached can quickly grow into the hundreds of millions of dollars.

## Composite Organization

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

**Description of composite.** The composite is a US-based, Fortune 500 financial services and insurance company, with operations and supply chain vendors worldwide. The company has an annual revenue of $8 billion. The security team is comprised of three senior security analysts and six junior security analysts.

**Deployment characteristics.** The company has input 2,000 assets into the IntSights Threat Intelligence Platform and has IntSights monitor 500 keywords with plans to expand the footprints of both over time. Prior to using IntSights the organization spent extensive time attempting to do its own dark web monitoring and takedowns.

> "When you get to an event, you need someone that lives it, that knows how to deal with these issues with the big companies, with the dark web. This is a niche specialty that we do not have here in the company, and that's why we're investing in companies like IntSights."
>
> *Head of cybersecurity, insurance*

**Key assumptions:**

- 9 security analysts
- 2,000 assets and 500 keywords protected
- Perform 200 fraudulent domains/account takedowns annually



FORRESTER®

# 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 | Time savings from automated dark web searching | $463,125 | $463,125 | $463,125 | $1,389,375 | $1,151,723 |
| Btr | Security takedown efficiency | $79,014 | $79,014 | $79,014 | $237,043 | $196,497 |
| Ctr | Proactive security response | $480,000 | $480,000 | $480,000 | $1,440,000 | $1,193,689 |
| | Total benefits (risk-adjusted) | $1,022,139 | $1,022,139 | $1,022,139 | $3,066,418 | $2,541,909 |

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $2.5 million.

### Time Savings From Automated Dark Web Searching

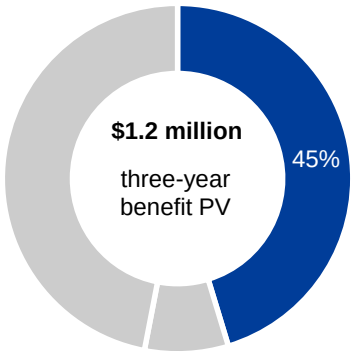
Before using the IntSights External Threat Protection Suite, organizations devoted significant resources to scrubbing dark web chatrooms/forums and searching for information on their company and attempting to learn the latest cyberattack techniques. Security analysts devoted hundreds of hours each week to these extremely manual processes, which limited their ability to search internally for potential vulnerabilities.

Organizations can offload a significant proportion of these processes by using IntSights Threat Command™. IntSights scrubs through dark web chatrooms/forums looking for information relevant to their customers and provides said information in a consolidated platform. The information that organizations receive from IntSights is used to proactively stop attacks and make security analysts aware of the most recent attack techniques so they can more easily handle a threat when one is identified. As an enterprise security manager noted, “We rely on the information from IntSights because it gives us information about the next planned attacks and what the latest and greatest attack techniques are.”

IntSights enables these organizations to greatly reduce the amount of time that analysts spend looking for external threats to their organizations. This in turn frees up analysts to look internally at their security ecosystems and make preemptive adjustments to their security profile. The enterprise security manager for a large health insurance organization said: “With IntSights our analysts are able to spend about 80% of their time doing internal hunting. With our legacy solution, they spent 70% of their time doing research and then 30% doing internal hunting.”

For the composite organization, Forrester assumes that:

- Prior to investing in IntSights, organizations devoted nine security analysts to threat searching and prevention. A significant portion of these analysts are senior members of the team who are required to oversee these searches. All analysts spent 4 hours daily on dark web searching.




Automated dark web search: **45%** of total benefits



FORRESTER®

- After implementing IntSights, the composite organization can reduce the size of the team responsible for these searches to six security analysts. These analysts can reallocate their time to perform higher priority internal hunting tasks. The remaining analysts dedicate 1 hour each day to these activities.
- The average fully loaded hourly compensation for the security analysts responsible for this searching is $65.

This benefit will vary based on the following risk factors:

- The team size and time devoted to dark web threat detection, prior to investing in IntSights.
- The speed at which assets are onboarded into IntSights platform, allowing security teams to reduce their workflows.
- The fully loaded compensation of senior and junior security analysts.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $1.2 million.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

**Time Savings From Automated Dark Web Searching: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| A1 | FTEs dedicated to dark web searching prior to IntSights | Interview | 9 | 9 | 9 |
| A2 | Time spent daily dark web searching prior to IntSights (hours) | Interview | 4 | 4 | 4 |
| A3 | Average hourly fully loaded security specialist salary | Assumption | $65 | $65 | $65 |
| A4 | Cost of dark web searching prior to IntSights | A1*A2*A3*250 | $585,000 | $585,000 | $585,000 |
| A5 | FTEs dedicated to dark web searching with IntSights | Interview | 6 | 6 | 6 |
| A6 | Daily time spent dark web searching with IntSights (hourly) | Interview | 1 | 1 | 1 |
| A7 | Average hourly fully loaded security specialist salary | Assumption | $65 | $65 | $65 |
| A8 | Cost of dark web searching with IntSights | A5*A6*A7*250 | $97,500 | $97,500 | $97,500 |
| At | Time savings from automated dark web searching | A4-A8 | $487,500 | $487,500 | $487,500 |
| | Risk adjustment | ↓5% | | | |
| Atr | Time savings from automated dark web searching (risk-adjusted) | | $463,125 | $463,125 | $463,125 |

## Security Takedown Efficiency

Organizations dedicated significant resources to taking down fraudulent domains and social media profiles impersonating their brand and executives. This proved to be a difficult task as security analysts needed to do extensive work to prove that these entities were not related to their organization. Oftentimes this included attempting to reach out to large domain registration and social media websites in order to have these entities removed. Customers all shared that connecting with the correct representative from these organizations was a labor-intensive and sometimes unachievable task.

IntSights can leverage their preexisting relationships with these domain registrars and social media organizations to efficiently take down these entities. These relationships give IntSights customers a direct communication channel to the proper representatives who can address these fraudulent domains, vastly reducing the amount of time that security analysts needed to spend trying to perform takedowns. Using IntSights to streamline the takedown process also allowed the

interviewed organizations to delegate these tasks to their more junior-level employees. This has the added benefit of increasing the amount of on-the-job experience these junior security analysts received while also making takedowns more cost efficient. The interviewed enterprise security manager highlighted this benefit by saying: "The investigations are now done by lower level analysts. They spend a lot less time on it because we're not chasing false positives. The information is validated by IntSights. We use their analyst service and engage with them if we have questions."

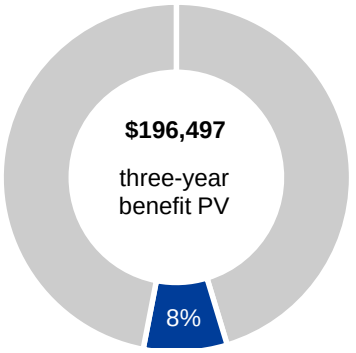
For the composite organization, Forrester assumes that:

- Prior to using IntSights, senior security analysts spent approximately 6 hours collectively each day attempting to perform takedowns on fraudulent domains and social media profiles.
- The average hourly fully loaded salary for a senior security specialist performing these takedowns is $72.
- By deploying IntSights across their organization security teams can delegate security takedown activities to their junior analysts. These analysts now collectively spend 2 hours daily performing these tasks.
- The average hourly fully loaded salary for a junior security specialist performing these takedowns is $50.

Security takedown efficiency will vary with:

- The time security analysts spend daily performing security takedowns.
- The degree to which senior security analysts can be reallocated to other value-add activities.
- The fully loaded compensation of senior and junior security analysts.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $196,497.




Security takedown efficiency: 8% of total benefits

**Security Takedown Efficiency: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| B1 | Hours spent performing daily takedowns by senior security specialist team without IntSights | Interview | 6 | 6 | 6 |
| B2 | Average hourly fully loaded senior security specialist salary | Assumption | $72 | $72 | $72 |
| B3 | Annual cost of manual takedowns without IntSights | B1*B2*250 | $108,173 | $108,173 | $108,173 |
| B4 | Hours spent daily performing takedowns by junior security specialists with IntSights | Interview | 2 | 2 | 2 |
| B5 | Average hourly fully loaded junior security specialist salary | Assumption | $50 | $50 | $50 |
| B6 | Annual cost of security takedowns with IntSights | B4*B5*250 | $25,000 | $25,000 | $25,000 |
| Bt | Security takedown efficiency | B3-B6 | $83,173 | $83,173 | $83,173 |
| | Risk adjustment | ↓5% | | | |
| Btr | Security takedown efficiency (risk-adjusted) | | $79,014 | $79,014 | $79,014 |

## Proactive Security Response

Interviewees noted that the information provided by IntSights allowed them to identify more threats that they would have otherwise missed. In some cases, these threats turned into costly breaches that required extensive resources to remediate. As the head of cyberthreat intelligence for one organization told Forrester: "There were a few cases that we



FORRESTER®

missed some of the domains, and as a result some amounts of money were, let's say, scammed or stolen. We understand that if we do not take down the domains or the fake accounts, we see the damage." These security incidents could be anything from a fake social media profile, defaming the organization online, or a phishing scam that leads to hundreds of thousands of dollars being stolen.

These events were not only costly from a financial perspective but also from a resource perspective, as they took vast amounts of person hours to ensure the organization was secure against future threats.

IntSights provided these customers a more comprehensive security solution, which was able to better identify threats before they turned into larger problems.

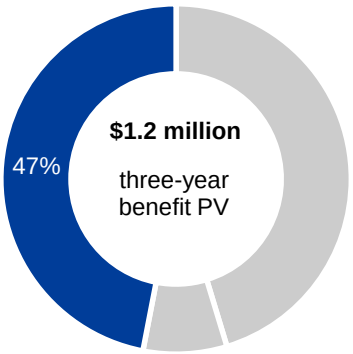
For the composite organization Forrester assumes that:

- The organization takes down 200 fraudulent domains and accounts each year. Of the domains and accounts that are taken down each year, Forrester assumes that there is a 4% probability that these fraudulent domains lead to a business compromise.
- The average direct cost to an organization of a fraudulent event is $100,000. The average cost to remediate an event (inclusive of the cost of labor) is $200,000.
- IntSights provides increased visibility into potential threats and breaches. Information provided by IntSights allows organizations to identify and prevent these attacks at a higher rate. Forrester assumes that IntSights enables organizations to avoid 25% of breaches that would have otherwise been successful.

These benefits from avoided breaches can vary based on:

- The number of domains and fraudulent profile takedowns an organization performs in a year, and the probability that one of these domains/profiles will lead to a business compromise.
- The size and scale of the business compromise will affect the direct cost an organization incurs as a result of a breach.
- Security best practices will affect the amount of labor resources that are needed to remediate a potential breach.

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.2 million.




response: **47%** of total benefits

**Proactive Security Response: Calculation Table**

| REF. | METRIC | CALC. | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|
| C1 | Fraudulent domains/accounts taken down per year | | 200 | 200 | 200 |
| C2 | Probability that domain/account would lead to business compromise | | 4% | 4% | 4% |
| C3 | Average direct value of fraudulent event | | $100,000 | $100,000 | $100,000 |
| C4 | Average value of clean up and investigation | | $200,000 | $200,000 | $200,000 |
| C5 | Combined value of compromising event | C3+C4 | $300,000 | $300,000 | $300,000 |
| C6 | Attribution of event avoidance to IntSights | | 25% | 25% | 25% |
| Ct | Proactive security response | C1*C2*C5*C6 | $600,000 | $600,000 | $600,000 |
| | Risk adjustment | ↓20% | | | |
| Ctr | Proactive security response (risk-adjusted) | | $480,000 | $480,000 | $480,000 |



FORRESTER®

## Unquantified Benefits

In addition to the quantified benefits above, the interviewees experienced additional benefits that were not able to be quantified, including:

- **IntSights can be used to protect against physical threats.** Customers stated that they were able to use information from IntSights to monitor and prevent non-cyber events, such as the potential kidnapping of an employee. The operations lead for the security operations center of one interviewed organization explained: “We had an alert for one of our employees for some non-cyber related data. There was a site that had all of their personal information posted on there like phone numbers, family details, addresses, what car he drives etc. We were able to reach out to local security to alert them of this.”
- **Access to a data rich platform augments junior analyst learning.** The customized and easily digestible data provided by the IntSights platform reduces the complexity of threat searching. This allows junior security analysts to take more responsibility for identifying and taking down potential security threats. Providing junior analysts with invaluable on-the-job experience accelerates the learning process and increases the skill sets of the overall workforce.
- **Increasing organizational security with IntSights has the potential to lower cyber insurance premiums**. Though many customers were only beginning their cyber insurance journeys they already reported that the proactive response ability provided by the platform has played a part in lowering their cyber insurance premium. As one IntSights user described, “I don’t know what percentage it was, but the fact that we use IntSights for cyberthreat intel, and to proactively deal with some dark net information and threat intelligence, was written into our new premium for our cyber insurance.”
- **Securing customer data protects against violating government and industry regulations**. Many organizations operate in heavily regulated industries with stringent customer privacy rules. Using IntSights to avoid data compromise reduces the likelihood that an organization will run afoul of regulation imposed by industry groups or governmental agencies. Noncompliance with GDPR, HIPAA, PCI-DSS, and other standards and regulations comes with stiff financial penalties.
- **Protecting brand image**. Customer data breaches, counterfeit sites, and fraudulent profiles all pose a major threat to brand image and organizational reputation. Eliminating these threats helps to maintain customer trust and brand equity.

## Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement the IntSights External Threat Protection Suite and later realize additional uses and business opportunities, including:

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the “right” or the ability to engage in future initiatives but not the obligation to do so.

- **Automated blocking of malicious domains.** Integrating IntSights across security environments allows organizations to automate the process of blocking phishing email domains and malicious IP addresses. Customers described how further assimilating the information provided by IntSights into their existing environments could further reduce the risk their organization faces. The head of cyber security for an interviewed insurance organization shared, “What we’re going to do is, we are going to connect all the feeds that IntSights will give us directly to our central security system. This way we can block certain IPs from connecting and block certain ports automatically in order to remediate vulnerabilities or reduce some risk.”

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

# Analysis Of Costs

**QUANTIFIED COST DATA AS APPLIED TO THE COMPOSITE**

## Total Costs

| REF. | COST | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 | TOTAL | PRESENT VALUE |
|---|---|---|---|---|---|---|---|
| Dtr | IntSights subscription cost | $0 | $178,500 | $178,500 | $178,500 | $535,500 | $443,903 |
| Etr | Implementation costs | $18,900 | $0 | $0 | $0 | $18,900 | $18,900 |
| Ftr | Training costs | $3,289 | $1,096 | $1,096 | $1,096 | $6,577 | $6,015 |
| | Total costs (risk-adjusted) | $22,189 | $179,596 | $179,596 | $179,596 | $560,977 | $468,818 |

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of $468,818.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

## IntSights Subscription Cost

For the composite organization, Forrester assumes that:

- It has an enterprise license where costs are based on the volume of transactions and keywords that IntSights is tasked with monitoring. Additional costs are driven through adopting additional functionalities offered by IntSights. Since IntSights is a software-as-a-service (SaaS) solution it does not require FTEs to dedicate additional time to monitoring the solution.

This cost will vary based on the following risk factors:

- Volume and other discounts can vary from organization to organization based on the assets and keywords being monitored by IntSights.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $443,903.

**IntSights Subscription Cost: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| D1 | IntSights subscription cost | Composite list price | | $170,000 | $170,000 | $170,000 |
| Dt | IntSights subscription cost | D1 | $0 | $170,000 | $170,000 | $170,000 |
| | Risk adjustment | ↑5% | | | | |
| Dtr | IntSights subscription cost (risk-adjusted) | | $0 | $178,500 | $178,500 | $178,500 |

## Implementation Costs

For the composite organization, Forrester assumes that:

- The solution takes very little time to get up and running. On Day 1, most customers were able to turn it on and immediately start seeing results. The majority of the implementation time is spent uploading key words and assets into the platform. The entire implementation took the composite organization one month to complete.
- Customers described the implementation process as intuitive and easy. Security analysts were dedicated to upload and monitor assets and keywords, but this did not make up the entirety of their time. The head of cyberthreat intelligence for one organization explained: “Basically, it’s really easy. You just go to your platform, plug it in, and that’s it. You will use all the keywords, and you play with all the other features. And everything is really easy to understand.”

**One month**
Total implementation and deployment time



FORRESTER®

- The composite organization dedicated three FTEs to implement the solution. These employees spend approximately 60% of their time implementing the IntSights platform.

Implementation costs will vary based on the following risk factors:

- The number of keywords and assets that need to be manually uploaded to the IntSights system.
- The number of FTEs dedicated to the implementation and the proportion of their time that is spent implementing IntSights.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $18,900.

**Implementation Costs: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| E1 | Time to implement solution (months) | | 1 | | | |
| E2 | FTEs needed to implement solution | | 3 | | | |
| E3 | % of FTE time spent implementing solution | | 60% | | | |
| E4 | Average monthly fully loaded security specialist salary | | $10,000 | | | |
| Et | Implementation costs | E1*E2*E3*E4 | $18,000 | $0 | $0 | $0 |
| | Risk adjustment | ↑5% | | | | |
| Etr | Implementation costs (risk-adjusted) | | $18,900 | $0 | $0 | $0 |

## Training Costs

For the composite organization, Forrester assumes:

- Very little training is needed to get employees onboarded to the IntSights platform. Security teams spend approximately 6 hours upfront, participating in online trainings and attending an onsite training where a representative from IntSights gives a live product demo.
- On an annual basis, security analysts attend approximately 2 hours of training, which are used as skill refreshers and forums to showcase new features of the platform.

Implementation costs will vary based on the following risk factors:

- Interviewees provided a wide range of training estimates, ranging from minimal training to longer sessions or multiple sessions over time.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $6,015.

**Three FTEs** spend 60% of their time on ongoing management of the IntSights External Threat Protection Suite.

**Training Costs: Calculation Table**

| REF. | METRIC | CALC. | INITIAL | YEAR 1 | YEAR 2 | YEAR 3 |
|---|---|---|---|---|---|---|
| F1 | Time spent training (hours) | | 6 | 2 | 2 | 2 |
| F2 | FTEs involved in training sessions | | 9 | 9 | 9 | 9 |
| F3 | Average hourly fully loaded security specialist salary | | $58 | $58 | $58 | $58 |
| Ft | Training costs | F1*F2*F3 | $3,132 | $1,044 | $1,044 | $1,044 |
| | Risk adjustment | ↑5% | | | | |
| Ftr | Training costs (risk-adjusted) | | $3,289 | $1,096 | $1,096 | $1,096 |

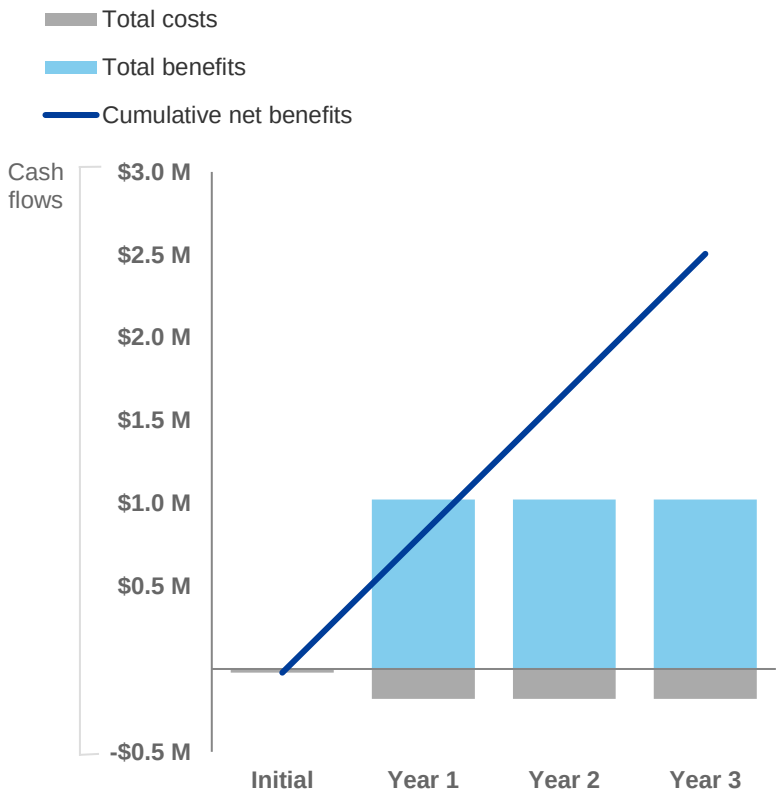


FORRESTER®

# Financial Summary

**CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS**

## Cash Flow Chart (Risk-Adjusted)




The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI and NPV 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 | ($22,189) | ($179,596) | ($179,596) | ($179,596) | ($560,977) | ($468,818) |
| Total benefits | $0 | $1,022,139 | $1,022,139 | $1,022,139 | $3,066,418 | $2,541,909 |
| Net benefits | ($22,189) | $842,543 | $842,543 | $842,543 | $2,505,441 | $2,073,091 |
| ROI | | | | | | 442% |



FORRESTER®

# IntSights External Threat Protection: Overview

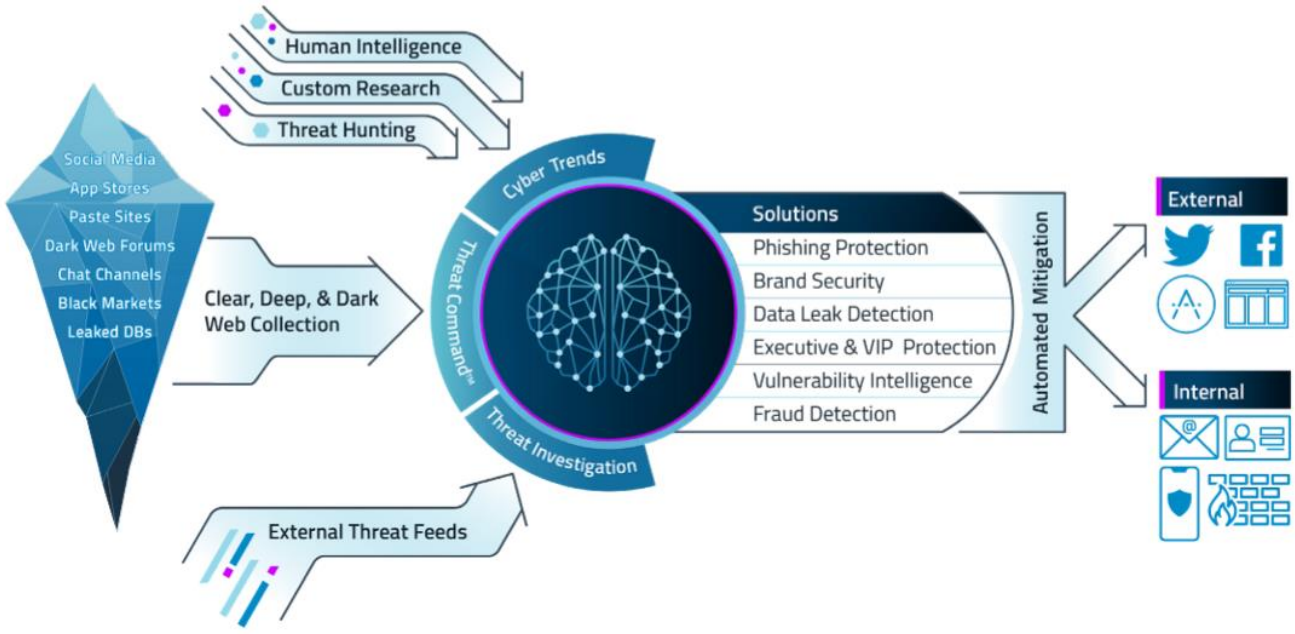
The following information is provided by IntSights. Forrester has not validated any claims and does not endorse IntSights or its offerings.

### The IntSights Advantage

The IntSights External Threat Protection (ETP) Suite monitors thousands of sources across the clear, deep, and dark web to identify threats that directly target your unique digital footprint — so threats are specific, intelligence is relevant, and action is automated. And with our broad ecosystem of integration and takedown partnerships, we enable orchestrated mitigation and automated response, so threats are neutralized before they ever cause damage.

### Turning External Intelligence Into Security Action

Defending your organization against cyberattacks requires timely intelligence and informed decision-making. IntSights positions your unique digital footprint at the center of your intelligence so you know how every threat, IOC, leaked database, and hacker interaction affects your business. Through our automated policies and broad integration ecosystem, we help you identify threats and orchestrate the threat mitigation process.




### Threat Command

IntSights Threat Command continuously discovers the critical threats targeting your business by mapping external intelligence to your unique digital assets. Threat Command delivers tailored intelligence from across the clear, deep, and dark web in the form of alerts categorized by severity, type (e.g., phishing, brand security, data leakage), and source (e.g., hacking forums, social media, black markets, etc.).

Threat Command also enables customers to fine-tune alert creation based on relevant characteristics of threats. Organizations can implement unique rule sets to define exactly what constitutes an alert based on their specific criteria and fine-tune an already tailored experience to help further increase ROI. Then, with one-click remediation, you can coordinate cross-functional response directly within alerts and operationalize the threat remediation lifecycle.



FORRESTER®

**Threat Intelligence Platform (TIP)**

The IntSights Threat Intelligence Platform (TIP) centralizes and operationalizes thousands of sources of intelligence for streamlined investigation and faster threat blocking. IOCs are enriched and correlated to your digital assets and prioritized by severity, bringing context and clarity to your threat feeds. Our visualized investigation dashboard enables you to see how new campaigns are connected to known malicious assets enabling you to coordinate your response appropriately. With our Threat Intelligence Platform you can gain visibility and enhance your ability to continuously monitor and mitigate the malicious external threats that pose the greatest danger to your organization.

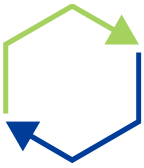
# Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

## Total Economic Impact Approach

**Benefits** represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

**Costs** consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.



**Flexibility** represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

**Risks** measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

**Present value (PV)**

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

**Net present value (NPV)**

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

**Return on investment (ROI)**

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

**Discount rate**

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

**Payback period**

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

# Appendix B: Endnotes

[1] Source: “Top Cybersecurity Threats In 2019,” Forrester Research, Inc., December 11, 2018.