FORRESTER®

The Total Economic Impact™ Of Deep Instinct Advanced Endpoint Security Solution

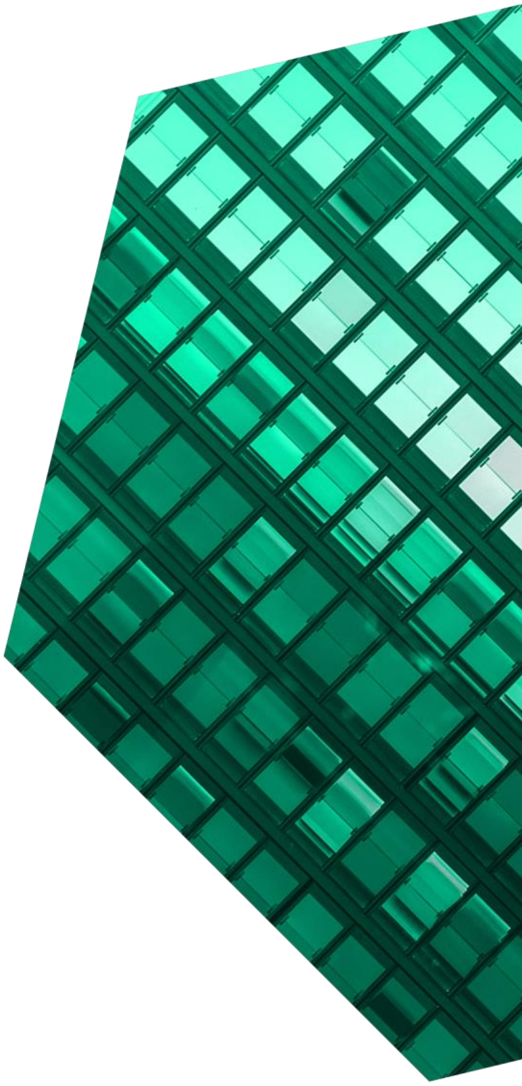
The Cost Savings And Business Benefits Enabled By Deep Instinct Advanced Endpoint Security Solution

NOVEMBER 2020

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY DEEP INSTINCT

Table Of Contents

Consulting Team: YiQin Teow
Leon Zhang



ABOUT FORRESTER CONSULTING

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

Executive Summary

Effective endpoint protection is essential for organizations operating in the new normal. Remote work is now widely prevalent with the COVID-19 pandemic, and organizations need to be ready for the growing number of endpoint threats that could amount to significant business losses. And as these attacks grow in complexity and nuance, endpoint security solutions need to shift from being merely reactive to also being proactive through more advanced prevention capabilities.

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

Deep Instinct provides endpoint security software that applies deep learning algorithms to endpoint protection. Unlike traditional detection and response-based cybersecurity solutions that wait for the execution of the attack to react, Deep Instinct's advanced predictive approach proactively keeps customers protected from both known and unknown threats while minimizing false positives. This adds resilience to customers' cybersecurity defenses.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four customers with one to three years of experience using Deep Instinct Advanced Endpoint Security Solution. For simplicity of reference, Deep Instinct Advanced Endpoint Security Solution will be referred to as "Deep Instinct" throughout the rest of this study.

KEY STATISTICS

Return on investment (ROI)
446%

Payback period
<3 months

Prior to using Deep Instinct, the customers' organizations were using a combination of endpoint detection and response (EDR) solutions and endpoint protection platforms (EPPs), including antivirus or anti-malware software. While these solutions were somewhat effective in detecting and responding to known and some zero-day endpoint threats, security operations (SecOps) employees were often inundated with time-consuming manual processes that stretched from endpoint management to alert investigation and threat hunting. In a shifting threat landscape where unknown and zero-day threats are growing more common, these organizations acknowledged that they were more vulnerable than ever at the endpoint level and that they needed enhancements to achieve proper security posture. The organizations sought a solution that could provide heightened threat prevention and analysis capabilities while relieving their SecOps teams of extraneous manual tasks and processes.

After the investment in Deep Instinct, the customers gained both quantitative and qualitative benefits against the backdrop of enhanced endpoint security. Efficacy of endpoint protection increased and efficiency on threat investigation improved, while the false positive rate drastically dropped. Early prevention through deep-learning predictive algorithms shifted work away from SecOps employees and allowed them to reallocate their time to higher-value tasks and projects. For these organizations, the investment in Deep Instinct also alleviated the difficult task of hiring additional SecOps FTEs, as many were teams were already running at 100% capacity. The COVID-19 pandemic has changed the cybersecurity paradigm: Endpoints are more important than ever, and it will stay that way for the foreseeable future. Interviewees told Forrester that shifting left with Deep Instinct on the endpoint security cycle was key to addressing security in this new remote work situation.

For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a composite organization named Deagon Bank to illustrate the quantified benefits and costs of investing in Deep Instinct. Deagon Bank is a state bank headquartered in the United States with a 6,000-person workforce and a team of 15 employees working in SecOps. The organization deploys Deep Instinct to protect a total of 7,000 endpoints across the organization. For more information, see the section titled “Composite Organization.”

Reduction in number of alerts due to false positive elimination

99%

KEY FINDINGS

Quantified benefits. The composite organization, Deagon Bank, achieves the following risk-adjusted present value (PV) quantified benefits totaling $3.5 million over a three-year period:

- **SecOps time savings in managing endpoint protection ($111,861).** This benefit focuses on the productivity gains that IT security engineers experience in managing endpoint protection. Prior to using Deep Instinct, there was a lot of management overhead due to the use of multiple endpoint products, burdensome maintenance work, and constant updates and patching required. With the use of Deep Instinct, Deagon Bank improves time spent on managing endpoint protection by 80%, as the lightweight model of Deep Instinct’s agents require only one to two updates per year. This relieves SecOps employees of these manual and mundane processes.

- **SecOps time savings in investigating endpoint threats ($1,260,019).** The deployment of Deep Instinct brings a 99% reduction in the number of false positive alerts to Deagon Bank. It also brings a 90% reduction in alerts requiring manual investigation. This results in time savings for IT security engineers around investigation of security alerts, triages, and threat hunting activities — all of which used to be time-consuming processes.

- **SecOps time savings in remediating endpoint attacks ($481,464).** Deep Instinct’s advanced preventive approach toward endpoint protection effectively safeguards Deagon Bank against both known and unknown threats, especially during the COVID-19 pandemic when interviewed customers observed a two-fold increase in the number of potential endpoint attacks. The model lays out the potential time savings for IT security engineers in remediating endpoint attacks, taking into account the likely shift in proportion of employees working from home versus those working in the office across three years, from pre-pandemic to post-pandemic.

- **Avoided financial loss due to user downtime ($477,187).** Endpoint attacks not only take up IT security engineers' time in performing remediation work, but they also prevent affected employees from doing productive work. This could result in potential financial loss for the organization. The detrimental impact is further amplified during the COVID-19 pandemic when employees are working remotely. The average user downtime per endpoint attack increases up to 12 hours due to the additional time required to deliver a loaner laptop to the affected employee and set up the laptop for proper usage.

- **Cost savings from retirement of legacy solutions ($860,665).** With the adoption of Deep Instinct, Deagon Bank retires both its legacy EDR solution and anti-malware software, yielding direct cost savings of more than $300,000 per year.
- **Decreased likelihood of material breaches ($323,840)** Weaknesses in user behavior and technology present loopholes for attackers to access confidential information, especially via endpoint devices. Data breaches represent not only financial losses, but also potential damage to an organization's customers and reputation. Deep Instinct's threat prevention capabilities across any threat, environment, and operating system enables broad attack surface protection, reducing the likelihood of a material data breach by 15%.

Reduction in likelihood of a material data breach

15%

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

- **Reduced operational disruption.** Interviewed customers shared a common experience with legacy solutions that required frequent security updates and patches. Deep Instinct's semiannual updates ensure continued security efficacy while minimizing disruption to organizational activity. This relieves organizations of these pain points.
- **Improved employee experience.** Having a single, lightweight agent enabled interviewees' organizations to deploy endpoint security across endpoints rapidly, with low overhead on end-user machines. The reduction in user downtime and the lower likelihood of breaches made possible by Deep Instinct also has a positive effect on employee experience as users are no longer disrupted due to loss of endpoint use.

Costs. The composite organization, Deagon Bank, experiences the following risk-adjusted PV costs:

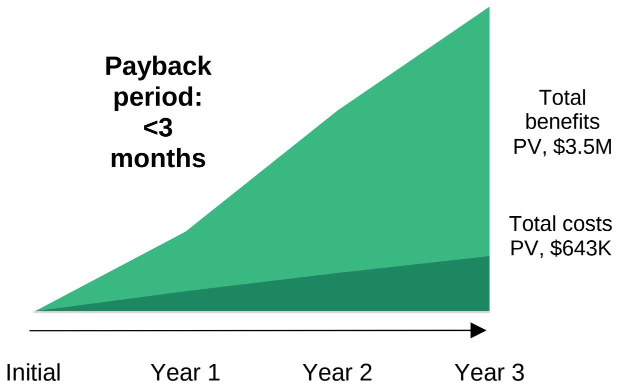
- **Deep Instinct solution cost ($569,245).** The solution cost for this study mainly consists of the license cost for 7,000 endpoints and "Premium" customer support charges. Readers are encouraged to reach out to Deep Instinct for a more tailored quote based on their company's needs and anticipated usage volume.
- **Initial setup cost ($5,654).** This cost mainly accounts for the deployment hours one IT security engineer spends rolling out Deep Instinct across the organization and getting it up to a running steady state. Key tasks accounted for in calculating the deployment hours include solution implementation, configuration optimization, and policy updates.

- **Ongoing resource cost ($68,360).** Two IT security engineers are deployed to manage endpoint protection on an ongoing basis. Each of them spends about 10% of their time managing Deep Instinct, performing maintenance work, administering security updates, and integrating Deep Instinct with other components of security stack that are added over time.

> **"Post-proof-of-value, it took us about two weeks to have everything rolled out with just one IT employee overseeing the process"**
>
> *Director, information technology, education*

Forrester's interviews and subsequent financial analysis found that Deagon Bank experiences benefits of $3.5 million over three years versus costs of about $643,000, adding up to a net present value (NPV) of $2.9 million and an ROI of 446%.

Financial Summary



ROI

446%

BENEFITS PV

$3,515,036

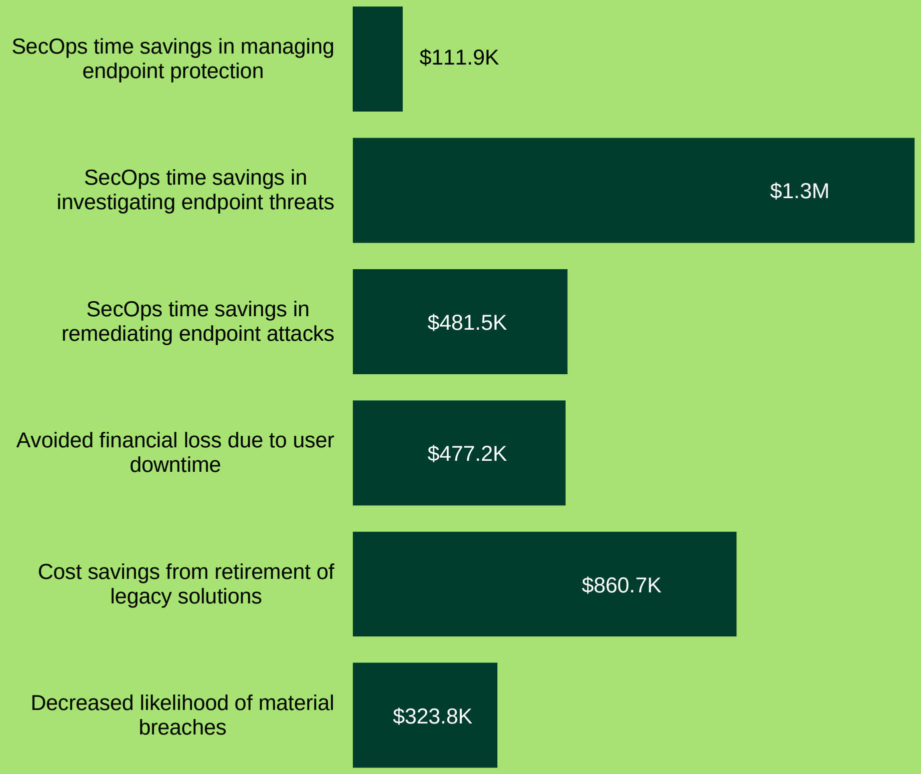
NPV

$2,871,777

PAYBACK

<3 months

Benefits (Three-Year)



> **"Having Deep Instinct running on endpoints is like having a cybersecurity analyst doing the job 24/7."**
>
> *Director, information technology, education*

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in the Deep Instinct Advanced Endpoint Security Solution.

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 Deep Instinct Advanced Endpoint Security Solution can have on an organization.

DUE DILIGENCE

Interviewed Deep Instinct stakeholders and Forrester analysts to gather data relative to the Deep Instinct Advanced Endpoint Security Solution.

CUSTOMER INTERVIEWS

Interviewed four decision-makers at organizations using the Deep Instinct Advanced Endpoint Security Solution 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 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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Deep Instinct 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 report to determine the appropriateness of an investment in the Deep Instinct Advanced Endpoint Security Solution.

Deep Instinct 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.

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

The Deep Instinct Advanced Endpoint Security Solution Customer Journey

🟩 Drivers leading to the Deep Instinct Advanced Endpoint Security Solution investment

Interviewed Organizations

Industry	Region	Interviewee	Number of endpoints
Information technology and services	USA	Chief investment officer	10,000
Education	USA	Director, information technology	7,200
Banking	USA	Vice president, information security	2,800
Education	USA	Director, information technology	5,000

KEY CHALLENGES

Before investing in Deep Instinct, the interviewees' organizations leveraged a range of EDR, antivirus and anti-malware solutions. Multiple challenges prompted the organizations to explore new endpoint security solutions. These included:

- **Increased zero-day threats and attacks.** One interviewee whose organization supports its clients in IT operations management shared that his organization has been seeing an increase in the number of zero-day threats and attacks among its clients' endpoints. As such, the organization looked for an endpoint security solution that could provide better protection against next-gen threats, given the increase in unknown threats driven by how hackers are trying to circumvent their existing AI technology.
- **Growing security stack complexity.** It was not uncommon for organizations to have multiple agents installed on their employees' endpoints to strengthen the organization's security posture. For instance, one interviewee mentioned that his legacy EDR solution required additional software to operate and to provide a more complete endpoint protection. Also, several interviewees said their legacy EDR solutions were typically designed to aid sophisticated and larger SecOps teams, where dedicated employees are required to manage endpoint protection. This was not feasible for midsize organizations like theirs.
- **Manual, time-consuming threat investigation and remediation efforts.** Interviewees mentioned that they had to spend a significant amount of time responding to endpoint threats and remediating them. One of the organizations had four to six team members spend half their time performing incident reviews.

> **"We've seen an increase in [zero-day] attacks that were being successful. There were concerns over future AI-driven threats … so we wanted to fight fire with fire."**
>
> *CIO, information technology and services*

SOLUTION REQUIREMENTS/ INVESTMENT OBJECTIVES

The interviewees' organizations searched for a single, lightweight, cloud-based solution that could:

- Enhance endpoint security to prevent more unknown threats and maintain business continuity.

- Improve endpoint threat investigation and remediation efficacy.
- Enable the redeployment of SecOps employees for higher-value tasks.
- Minimize total cost of ownership.

After a business case process evaluating multiple vendors, the interviewees' organizations eventually chose Deep Instinct and began deployment.

- Interviewed customers undertook a proof-of-value before full deployment.
- Three interviewees said their organizations replaced their legacy solutions with Deep Instinct, while the fourth interviewee's organization deployed Deep Instinct as an augmentation of its endpoint security stack.

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, Deagon Bank, is representative of the four interviewees' companies and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

DEAGON BANK

Description of composite. Deagon Bank is a regional bank headquartered in United States. The organization has a total of approximately 6,000 employees, and it serves a customer base of roughly 900,000 members with strong online and offline presence. The organization has a team of 15 employees on its SecOps team, and they handle operational tasks including IT ticket resolutions, incident management, and security operations.

Deployment characteristics. The organization deploys Deep Instinct to protect a total of 7,000 endpoints. Looking to enhance the organization's security posture against both known and unknown threats, Deagon Bank rolls out Deep Instinct across all its endpoints following a 30-day proof-of-value. The software-as-a-service (SaaS) version of the security management and monitoring console that supports the organization in advanced analysis of prevented threats is implemented as well. With the adoption of Deep Instinct, the organization retires its legacy EDR solution and anti-malware software.

Key assumptions

- **Financial services firm**
- **6,000 FTEs**
- **7,000 endpoints protected**
- **15-person SecOps team**

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	SecOps time savings in managing endpoint protection	$43,740	$45,052	$46,404	$135,196	$111,861
Btr	SecOps time savings in investigating endpoint threats	$348,554	$618,294	$575,212	$1,542,060	$1,260,019
Ctr	SecOps time savings in remediating endpoint attacks	$134,059	$233,050	$222,262	$589,371	$481,464
Dtr	Avoided financial loss due to user downtime	$13,792	$316,969	$269,782	$600,543	$477,187
Etr	Cost savings from retirement of legacy solutions	$346,086	$346,086	$346,086	$1,038,258	$860,665
Ftr	Decreased likelihood of material breaches	$130,221	$130,221	$130,221	$390,663	$323,840
	Total benefits (risk-adjusted)	$1,016,452	$1,689,672	$1,589,967	$4,296,091	$3,515,036

SECOPS TIME SAVINGS IN MANAGING ENDPOINT PROTECTION

Prior to using Deep Instinct, SecOps employees responsible for managing endpoint protection were inundated with manual processes that involved performing maintenance work, administering constant security updates and patching, and integrating their endpoint protection solutions with other parts of the organization’s security stack. With the deployment of Deep Instinct, these employees were relieved of these tedious tasks and experienced improved efficacy in endpoint management. Deep Instinct’s lightweight architecture also meant that the organizations could easily be self-sufficient and they do not need to rely on external vendors like managed service providers for support on endpoint management.

The interviewed customers shared the following information that were key in modelling this benefit category for Deagon Bank:

- Pre-Deep Instinct, two IT security engineers each spent about 50% of their time managing and administering multiple endpoint solutions.
- Post-Deep Instinct, these two employees only spent 4 hours per week managing Deep Instinct, achieving an 80% improvement in productivity. This freed up their time for more strategic initiatives.

> **“There was a lot of management overhead back then. A lot of manual work was required by my small IT security team.”**
>
> *Vice president, information security, banking*

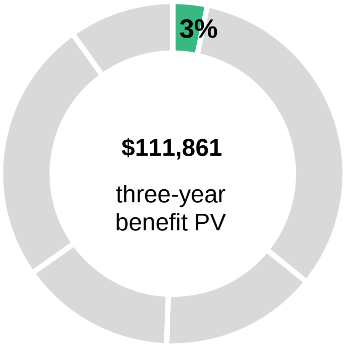
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- Average IT security engineer fully loaded salary of $121,500 with a 3% year-over-year increase during the three-year period to account for inflation.
- Productivity conversion ratio of 50%. Forrester adjusts productivity formulas with a productivity conversion ratio to be realistic and conservative in modeling. Productivity conversion considers that not every minute gained in productivity is put directly back into productive work; employees could use the time to take a longer break, leave work on time, etc.

Risks. The model accounts for the following risks that could impact the value of benefits:

- Variance in SecOps employees' time spent on managing endpoint protection pre-Deep Instinct due to differing requirement of different legacy solutions.
- Variance in salaries by role and geography.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $111,861.



SecOps time savings in managing endpoint protection: 3% of total benefits

SecOps Time Savings In Managing Endpoint Protection					
REF.	**METRIC**	**CALCULATION**	**YEAR 1**	**YEAR 2**	**YEAR 3**
A1	Number of IT security engineers involved in managing endpoint protection	Composite	2	2	2
A2	Amount of time spent on managing endpoint protection	Composite	50%	50%	50%
A3	Pre-Deep Instinct endpoint protection management time (hours)	A1*A2*2,080	2,080	2,080	2,080
A4	Post-Deep Instinct improvement in endpoint protection management time	Composite	80%	80%	80%
A5	Post-Deep Instinct endpoint protection management time (hours)	A3*(1-A4)	416	416	416
A6	Average IT security engineer fully loaded salary	Year 1: Composite Years 2 and 3: $A6_{py}$*103%	$121,500	$125,145	$128,899
A7	Productivity conversion	Assumption	50%	50%	50%
At	SecOps time savings in managing endpoint protection (showing rounded value)	(A3-A5)*(A6/2,080)*A7	$48,600	$50,058	$51,560
	Risk adjustment	↓10%			
Atr	SecOps time savings in managing endpoint protection (risk-adjusted)		$43,740	$45,052	$46,404

SECOPS TIME SAVINGS IN INVESTIGATING ENDPOINT THREATS

A large part of SecOps employees' jobs revolved around the time-consuming tasks of investigating security alerts and performing threat hunting. Furthermore, with the high false positive rate of some legacy EDR solutions, these SecOps employees often spent unnecessary time chasing down alerts that turned out not to be threats at all.

With the use of Deep Instinct, the interviewees' organizations shifted from using a reactive detection model to a proactive prevention model, where most threats are stopped before reaching the execution stage. This eliminated security trade-off as the organizations achieved high efficacy in threat prevention without a corresponding increase in false positives. As such, the lower false positive rate enabled by Deep Instinct resulted in time savings for SecOps employees.

The interviewed customers shared the following information that were key in modelling this benefit category for Deagon Bank:

- 99% reduction in the number of alerts due to false positive elimination.
- 90% reduction in daily alerts requiring manual investigation, which is attributable to the automated investigation and remediation capabilities of Deep instinct.
- Average investigation time of 3 hours for each alert requiring manual investigation.

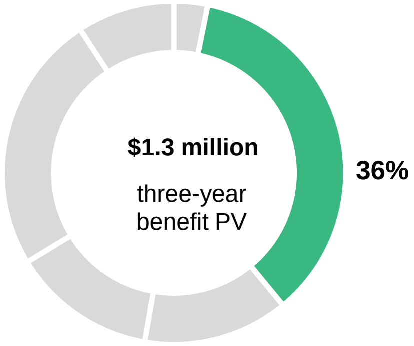
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- The number of alerts received from Year 1 to Year 3 are scaled in parallel to the number of potential endpoint attacks prevented, as the organization transitioned from a pre-COVID-19 state to a post-COVID-19 state.
- Pre-Deep Instinct false positive rate of 10%, considering that the organization deploys a combination of EDR and anti-malware solutions in the legacy state.
- Only 10% of Pre-Deep Instinct daily alerts require manual investigation because SecOps employees largely focus investigation efforts on never-seen-before threats, with the remaining alerts being self-remediated by legacy EDR solutions.
- Average IT security engineer fully loaded salary of $121,500 with a 3% year-over-year increase during the three-year period to account for inflation.
- Productivity conversion ratio of 50%.

Risks. The model accounts for the following risks that could impact the value of benefits:

- Variance in false positive elimination, depending on the suite of legacy endpoint solutions deployed.
- Variance in complexity of threats that results in variation in investigation time required.
- Variance in salaries by role and geography.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1,260,019.



SecOps time savings in investigating endpoint threats: 36% of total benefits

SecOps Time Savings In Investigating Endpoint Threats

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
B1	Pre-Deep Instinct number of alerts per day	Composite	200	338	314
B2	Pre-Deep Instinct false positive rate	Assumption	10%	10%	10%
B3	Pre-Deep Instinct number of false positives per day (showing rounded value)	B1*B2	20	34	31
B4	Post-Deep Instinct reduction in number of alerts due to false positive elimination	Composite	99%	99%	99%
B5	Post-Deep Instinct number of alerts per day (showing rounded value)	B1-(B3*B4)	180	304	283
B6	Pre-Deep Instinct proportion of alerts per day requiring manual investigation	Assumption	10%	10%	10%
B7	Post-Deep Instinct reduction in alerts per day requiring manual investigation	Composite	90%	90%	90%
B8	Post-Deep Instinct proportion of alerts per day requiring manual investigation	B6*(1-B7)	1%	1%	1%
B9	Pre-Deep Instinct number of alerts per day requiring manual investigation (showing rounded value)	B1*B6	20	34	31
B10	Post-Deep Instinct number of alerts per day requiring manual investigation (showing rounded value)	B5*B8	2	3	3
B11	Average investigation time per alert requiring manual investigation (hours)	Composite	3	3	3
B12	Pre-Deep Instinct total time spent investigating alerts per day (hours)	B9*B11	60	102	93
B13	Post-Deep Instinct total time spent investigating alerts per day (hours)	B10*B11	6	9	9
B14	Average IT security engineer fully loaded salary	A6	$121,500	$125,145	$128,899
B15	Productivity conversion	Assumption	50%	50%	50%
Bt	SecOps time savings in investigating endpoint threats (showing rounded value)	(B12-B13)*260*(B14/2,080)*B15	$410,063	$727,405	$676,720
	Risk adjustment	↓15%			
Btr	SecOps time savings in investigating endpoint threats (risk-adjusted)		$348,554	$618,294	$575,212

SECOPS TIME SAVINGS IN REMEDIATING ENDPOINT ATTACKS

Even though the majority of the interviewees' organizations did not experience any successful endpoint attacks prior to the deployment of Deep Instinct, the zero-time threat prevention and multilayer protection capabilities enabled by Deep Instinct's deep learning technology gave greater confidence in combating endpoint attacks.

This was especially critical amidst the COVID-19 pandemic, as organizations rapidly deployed remote systems and networks to support the shift to a remote workforce. This transition spurred an increase in security vulnerabilities as organizations found themselves at greater risk of potential endpoint attacks. The interviewees' organizations observed an average two-fold increase in the number of potential endpoint attacks prevented by Deep Instinct when the pandemic occurred. The successful prevention of endpoint attacks by Deep Instinct in a heightened threat environment saved SecOps employees from potential time spent on remediation of endpoint attacks.

The interviewed customers shared evidence and data that were scaled accordingly to model this benefit category for Deagon Bank:

- Average of 150 potential endpoint attacks prevented per month pre-COVID-19 (when 100% of employees are working from office).
- Average of 300 potential endpoint attacks prevented per month during peak period of COVID-19 (when 100% of employees are working from home).
- Average remediation time of 3 hours for each potential endpoint attack pre-Deep Instinct.
- Following the implementation of Deep Instinct, remediation activities involving endpoint, process, and network containment, rollbacks and reimaging, and the like are avoided by the prevention of attacks. This eliminates the traditional 3 hours needed for remediation time.

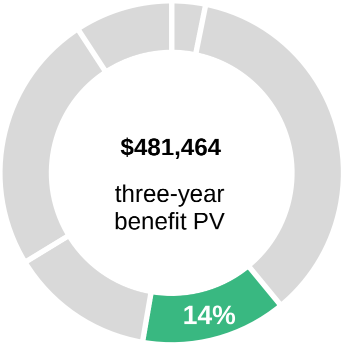
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- The full outbreak of COVID-19 (i.e., the events of 2020) occur in Year 2. Hence, Year 1 captures the organization's working model and threat landscape pre-COVID-19 while Year 3 illustrates the situation where restrictions are slowly eased as the pandemic is expected to slow down.[1]
- The shift in the proportion of employees working from office versus working from home throughout the three-year period is shown in rows C3 to C6 of the model. This reflects the estimated duration of the pandemic outbreak and organizations' corresponding office reopening protocols.
- Average IT security engineer fully loaded salary of $121,500 with a 3% year-over-year increase during the three-year period to account for inflation.
- Productivity conversion ratio of 50%.

Risks. The model accounts for the following risks that could impact the value of benefits:

- Significant changes in the pandemic situation against forecast, resulting in corresponding nuances in the organization's estimated working model in Year 3.
- Variance in severity of potential endpoint attacks that may result in variation in remediation time required.
- Variance in salaries by role and geography.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $481,464.



SecOps time savings in remediating endpoint attacks: 14% of total benefits

SecOps Time Savings In Remediating Endpoint Attacks

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
C1	Number of potential endpoint attacks prevented per month (when 100% of employees are working from office)	Composite	150	150	150
C2	Number of potential endpoint attacks prevented per month (when 100% of employees are working from home)	Composite	300	300	300
C3	Number of months where 100% of employees are working from office	Assumption	12	3	0
C4	Number of months where 100% of employees are working from home	Assumption	0	6	0
C5	Number of months when 75% of employees are working from home	Assumption	0	3	3
C6	Number of months when 50% of employees are working from home	Assumption	0	0	9
C7	Number of potential endpoint attacks prevented per year (from employees working from office) (showing rounded value)	(C1*C3)+(0.25*C1*C5)+(0.5*C1*C6)	1,800	563	788
C8	Number of potential endpoint attacks prevented per year (from employees working from home)	(C2*C4)+(0.75*C2*C5)+(0.5*C2*C6)	0	2,475	2,025
C9	Average remediation time per endpoint attack (hours)	Composite	3	3	3
C10	Average IT security engineer fully loaded salary	A6	$121,500	$125,145	$128,899
C11	Productivity conversion	Assumption	50%	50%	50%
Ct	SecOps time savings in remediating endpoint attacks (showing rounded value)	(C7+C8)*C9*(C10/2,080)*C11	$157,716	$274,176	$261,485
	Risk adjustment	↓15%			
Ctr	SecOps time savings in remediating endpoint attacks (risk-adjusted)		$134,059	$233,050	$222,262

AVOIDED FINANCIAL LOSS DUE TO USER DOWNTIME

Beyond SecOps employees' time spent on remediation, another critical implication for organizations in the event of endpoint attacks is the end user downtime.

This potential impact is further amplified during the COVID-19 pandemic, when employees are working from home. This is because unlike a working from office environment where SecOps employees can easily help to remediate the system in person or provide a loaner laptop, considerable time is required to deliver the loaner laptop to employees. Upon receiving the loaner laptop, employees also need to spend time ramping up the system for missing files and applications. The loss in productive hours for employees due to user downtime would thus result in financial loss for organizations.

The interviewed customers shared the following information that were key in modelling this benefit category for Deagon Bank:

- Average downtime of 0.75 hours per potential endpoint attack for employees working from office.
- Average downtime of 12 hours per potential endpoint attack for employees working from home, taking into account additional time spent on courier delivery as well as time spent setting up the loaner laptop.

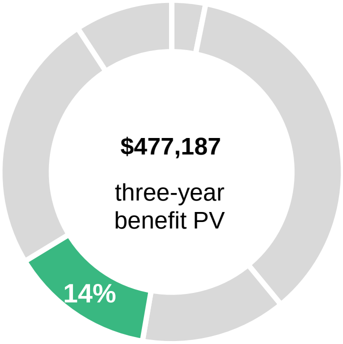
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- Average employee fully loaded salary of $50,000 with a 3% year-over-year increase during the three-year period to account for inflation.
- Productivity conversion ratio of 50%.

Risks. The model accounts for the following risks that could impact the value of benefits:

- Variances in user downtime, depending on the organization's protocol in endpoint attack remediation.
- Variance in salaries by role and geography.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $477,187.



Avoided financial loss due to user downtime: 14% of total benefits

Avoided Financial Loss Due To User Downtime

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
D1	Number of potential endpoint attacks prevented per year (from employees working from office)	C7	1,800	563	788
D2	Number of potential endpoint attacks prevented per year (from employees working from home)	C8	0	2,475	2,025
D3	Downtime per potential endpoint attack for employees working from office (hour)	Composite	0.75	0.75	0.75
D4	Downtime per potential endpoint attack for employees working from home (hour)	Composite	12	12	12
D5	Total downtime per year (hour) (showing rounded value)	(D1*D3)+(D2*D4)	1,350	30,122	24,891
D6	Average employee fully loaded salary	Year 1: Composite Years 2 and 3: $D6_{py}$*103%	$50,000	$51,500	$53,045
D7	Productivity conversion	Assumption	50%	50%	50%
Dt	Avoided financial loss due to user downtime (showing rounded value)	D5*(D6/2,080)*D7	$16,226	$372,905	$317,390
	Risk adjustment	↓15%			
Dtr	Avoided financial loss due to user downtime (risk-adjusted)		$13,792	$316,969	$269,782

COST SAVINGS FROM RETIREMENT OF LEGACY SOLUTIONS

With the deployment of Deep Instinct, the majority of the interviewed customers said their organization retired its legacy EDR solutions, antivirus software, or anti-malware software. The security stack is thus optimized towards preventing known and unknown threats with a low false positive rate at a reduced total cost of ownership.

The interviewed customers shared evidence and data that were scaled accordingly to model this benefit category for Deagon Bank:

- Annual cost of legacy solution for endpoint protection of $244,540.
- Annual cost of legacy anti-malware software of $140,000.

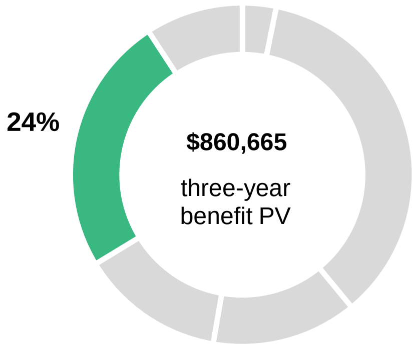
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- The legacy solutions are retired at the go-live date of Deep Instinct (i.e., the beginning of Year 1).
- There is no increase in the costs of legacy systems across the three-year period.

Risks. The model accounts for a risk that could impact the value of benefits:

- Uncertainty of avoided upgrade and maintenance costs.
- Some organizations may choose to run their legacy software in parallel to Deep Instinct for a number of months to prove the effectiveness of new versus legacy. Should this be the case, an organization may not realize savings for the entirety of the first year.

To account for this risk, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $860,665.



Cost savings from retirement of legacy solutions: 24% of total benefits

Cost Savings From Retirement Of Legacy Solutions

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
E1	Cost of legacy solution for endpoint protection	Composite	$244,540	$244,540	$244,540
E2	Cost of legacy anti-malware software	Composite	$140,000	$140,000	$140,000
Et	Cost savings from retirement of legacy solutions	E1+E2	$384,540	$384,540	$384,540
	Risk adjustment	↓10%			
Etr	Cost savings from retirement of legacy solutions (risk-adjusted)		$346,086	$346,086	$346,086

DECREASED LIKELIHOOD OF MATERIAL BREACHES

The digital landscape has resulted in scattered data and information as convenience is increasingly valued over security. Weaknesses in user behavior and technology thus present loopholes for attackers attempting to access confidential information — especially via endpoint devices, which are most susceptible to such attacks. The far-reaching impact of data breaches includes not only financial losses, but also the potential damage to an organization's reputation. This implicates its business competitiveness.

Deep Instinct's threat prevention capabilities across any threat, environment, and operating system is thus a critical piece of the interviewed customers' security stacks in preventing data breaches, as the input agnostic algorithm of its deep-learning technology provides broad attack-surface protection.

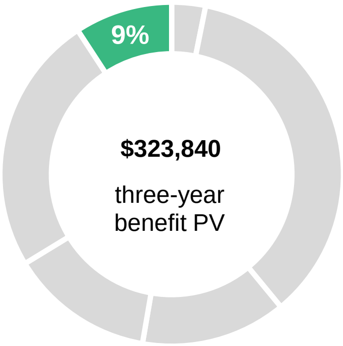
Modeling and assumptions. In modeling this benefit category, results from an internal Forrester study called "Cost Of A Security Breach," conducted in August 2020 (with a sample size of 300 organizations), were referenced and verified with the interviewed customers.[2] Forrester assumes the following for Deagon Bank in the model:

- An average of 2.6 material data breaches per year.
- The average potential cost of a data breach per endpoint is $53, taking into account reputational losses, fines, customer reacquisition costs and payouts, but excluding internal user downtime.
- The number of material breaches generally changes little with organizational size, but the breach-related costs do change, and they are reflective of different organizational sizes. This is represented by the $53 shown above.
- A 15% reduction in the likelihood of material breach, considering the fact that legacy EDR solutions were already in place prior to using Deep Instinct.

Risks. The model accounts for the following risks that could impact the value of benefits:

- The level of protection and collective effectiveness offered by the organization's previous security stack.
- The size, vertical, and region of the organization.
- The organization's diligence and maturity in security practices.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $323,840.



Decreased likelihood of material breaches: 9% of total benefits

Decreased Likelihood Of Material Breaches

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
F1	Average number of data breaches per year	Forrester Research, composite verified	2.6	2.6	2.6
F2	Number of endpoints protected	Composite	7,000	7,000	7,000
F3	Average potential cost of data breach per endpoint, exclusive of internal user downtime	Forrester Research, composite verified	$53	$53	$53
F4	Total potential cost of a breach	F2*F3	$371,000	$371,000	$371,000
F5	Reduced likelihood of a breach	Forrester Research, composite verified	15%	15%	15%
Ft	Decreased likelihood of material breaches	F1*F4*F5	$144,690	$144,690	$144,690
	Risk adjustment	↓10%			
Ftr	Decreased likelihood of material breaches (risk-adjusted)		$130,221	$130,221	$130,221

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Reduced operational disruption.** Interviewed customers shared a common experience with legacy solutions where frequent security updates and patching are required. Deep Instinct's semiannual updates ensured continued security efficacy while minimizing disruption to organizational activity. This relieved organizations of these pain points.

- **Improved employee experience.** Several factors contribute to the potential increase in employee satisfaction rate following the use of Deep Instinct. Primarily, organizations will enjoy low overhead on endpoints due to a single lightweight agent, and this results in snappier performance. Organizations can also avoid crippling downtime, causing less interruptions to employee productivity. Business end users don't have to do guess work on when laptops would be returned, reducing ambiguity on meeting deadlines. Lastly, SecOps teams are happier and are more easily retained when repetitive, ordinary tasks are largely removed from their day-to-day operations.

FLEXIBILTY

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

- **Confidence to operate in the new normal and at the cutting edge.** Semiannual updates minimize disruption to organizational activity while ensuring security efficacy — particularly around zero-day attacks. This gives organizations the confidence to pursue new technologies and operating models that might otherwise be hampered by security concerns.

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
Gtr	Deep Instinct solution cost	$0	$228,902	$228,902	$228,902	$686,706	$569,245
Htr	Initial setup cost	$5,654	$0	$0	$0	$5,654	$5,654
Itr	Ongoing resource cost	$0	$26,730	$27,532	$28,358	$82,620	$68,360
	Total costs (risk-adjusted)	$5,654	$255,632	$256,434	$257,260	$774,980	$643,259

DEEP INSTINCT SOLUTION COST

The cost of Deep Instinct Advanced Endpoint Security Solution is mainly comprised of the license cost and customer support charges. The license cost is calculated based on the number of endpoints covered while the customer support charges differ by the level of support (“Standard,” “Premium,” “Platinum”) selected by the organization.

Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- The organization leverages Deep Instinct to protect a total of 7,000 endpoints across all three years.
- The annual fee per endpoint is $25.85 after a discount that is scaled and applied for an organization with a coverage of 7,000 endpoints.
- The organization opts for “Premium” support each year.

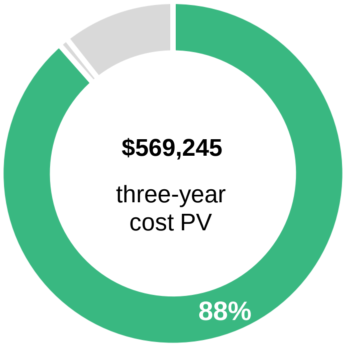
> **“[Deep Instinct’s] support has been nothing but spectacular. [The support staff is] very responsive and [they provide] good knowledge transfer.”**
>
> *Director, information technology, education*

To find out more information about the solution cost, readers are encouraged to reach out to Deep Instinct for a more tailored quote.

Risks. The model accounts for the following risks that could impact the value of costs:

- Variances in the number of endpoints protected and the associated discount rate.
- The level of support selected each year.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $569,245.



Deep Instinct solution cost: 88% of total costs

Deep Instinct Solution Cost

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	Number of endpoints protected	Composite		7,000	7,000	7,000
G2	Annual cost per endpoint protection	Composite		$25.85	$25.85	$25.85
G3	Premium support charge	Composite		15%	15%	15%
G4	Annual premium support cost (showing rounded value)	(G1*G2)*G3		$27,143	$27,143	$27,143
Gt	Deep Instinct solution cost	(G1*G2)+G4	$0	$208,093	$208,093	$208,093
	Risk adjustment	↑10%				
Gtr	Deep Instinct solution cost (risk-adjusted)		$0	$228,902	$228,902	$228,902

INITIAL SETUP COST

The initial setup cost mainly accounts for internal efforts associated with the implementation of Deep Instinct, which is typically executed after a proof-of-value of about 30 days on average. Interviewed customers said the simple, out-of-the-box configuration of Deep Instinct allowed for a quick and easy deployment across their organizations in a matter of weeks. Once they implemented Deep Instinct, they could carry out configuration optimization and policy updates to get the solution up and running in a steady state.

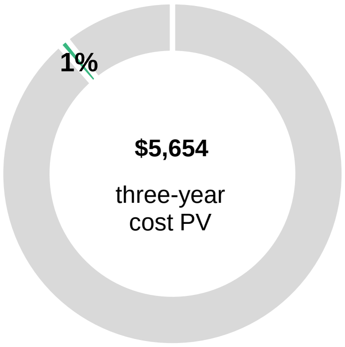
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- Only one IT security engineer oversees the implementation of Deep Instinct across two weeks, spending about 30% of their time at work.
- The same IT security engineer is also responsible for subsequent configuration optimization and policy updates across eight weeks, spending about 20% of their time at work.
- Average IT security engineer fully loaded salary of $121,500 with a 3% year-over-year increase during the three-year period to account for inflation.

Risks. The model accounts for the following risks that could impact the value of costs:

- Complexity of environment and scale of deployment.
- Variance in salaries by role and geography.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $5,654.



Initial setup cost: 1% of total costs

Initial Setup Cost

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
H1	Number of IT security engineers involved in initial setup	Composite	1			
H2	Proportion of time spent on solution implementation per IT security engineer	Composite	30%			
H3	Solution implementation duration (weeks)	Composite	2			
H4	Proportion of time spent on configuration optimization and policy update per IT security engineer	Composite	20%			
H5	Configuration optimization and policy update duration (weeks)	Composite	8			
H6	Total internal deployment hours	H1*((H2*H3)+(H4*H5))*5*8	88			
H7	Average IT security engineer fully loaded salary	Composite	$121,500			
Ht	Initial setup cost	H6*(H7/2080)	$5,140	$0	$0	$0
	Risk adjustment	↑10%				
Htr	Initial setup cost (risk-adjusted)		$5,654	$0	$0	$0

ONGOING RESOURCE COST

The ongoing resource cost primarily relates to the internal resources deployed to manage Deep Instinct on an ongoing basis. This includes performing maintenance work, administering semiannual updates, and integrating Deep Instinct with other parts of the organization’s security stack. With the lightweight architecture of Deep Instinct, ongoing resource cost is kept low as there is no need for constant security updates or burdensome maintenance.

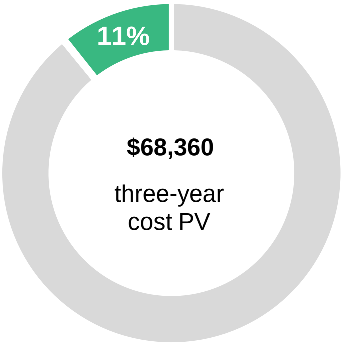
Modeling and assumptions. Forrester assumes the following for Deagon Bank in the model:

- Two IT security engineers are involved in managing endpoint protection on an ongoing basis, spending 10% of their time at work managing Deep Instinct.
- Average IT security engineer fully loaded salary of $121,500 with a 3% year-over-year increase during the three-year period to account for inflation.

Risks. The model accounts for the following risks that could impact the value of costs:

- Variance in proportion of time spent by employees managing Deep Instinct.
- Variance in salaries by role and geography.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $68,360.



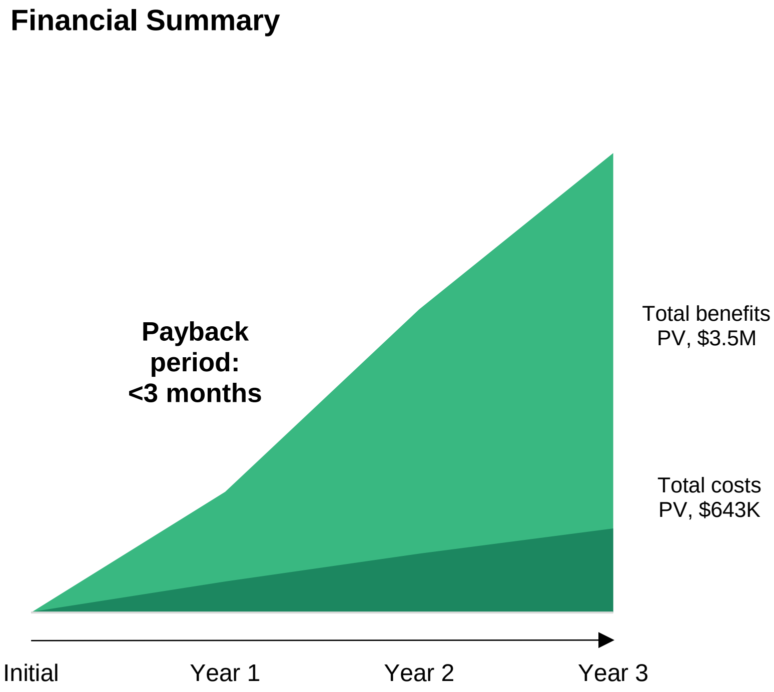
Ongoing resource cost: 11% of total costs

Ongoing Resource Cost

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
I1	Number of IT security engineers involved in managing endpoint protection	Composite		2	2	2
I2	Proportion of time spent managing Deep Instinct solution	Composite		10%	10%	10%
I3	Average IT security engineer fully loaded salary	Year 1: H7 Years 2 and 3: $I3_{py}$*103%		$121,500	$125,145	$128,899
It	Ongoing resource cost (showing rounded value)	I1*I2*I3	$0	$24,300	$25,029	$25,780
	Risk adjustment	↑10%				
Itr	Ongoing resource cost (risk-adjusted)		$0	$26,730	$27,532	$28,358

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	($5,654)	($255,632)	($256,434)	($257,260)	($774,980)	($643,259)
Total benefits	$0	$1,016,452	$1,689,672	$1,589,967	$4,296,091	$3,515,036
Net benefits	($5,654)	$760,820	$1,433,238	$1,332,707	$3,521,111	$2,871,777
ROI						446%
Payback						<3

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."

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

“Technology Best Practices To Protect Your Homeworkers' Endpoints,” Forrester Research, Inc., July 9, 2020

Appendix C: Endnotes

[1] Online Resources
“COVID-19: The CIDRAP Viewpoint”, The Center for Infectious Disease Research and Policy, April 30, 2020 (cidrap.umn.edu/covid-19/covid-19-cidrap-viewpoint)

[2] Source: “Cost Of A Security Breach,” Internal Forrester Survey Data, August 2020.

FORRESTER®