FORRESTER®

The Total Economic Impact™ Of CrowdStrike Falcon Identity Protection

Cost Savings And Business Benefits Enabled By Falcon Identity Protection

A Forrester Total Economic Impact™ Study
Commissioned By CrowdStrike, January 2025

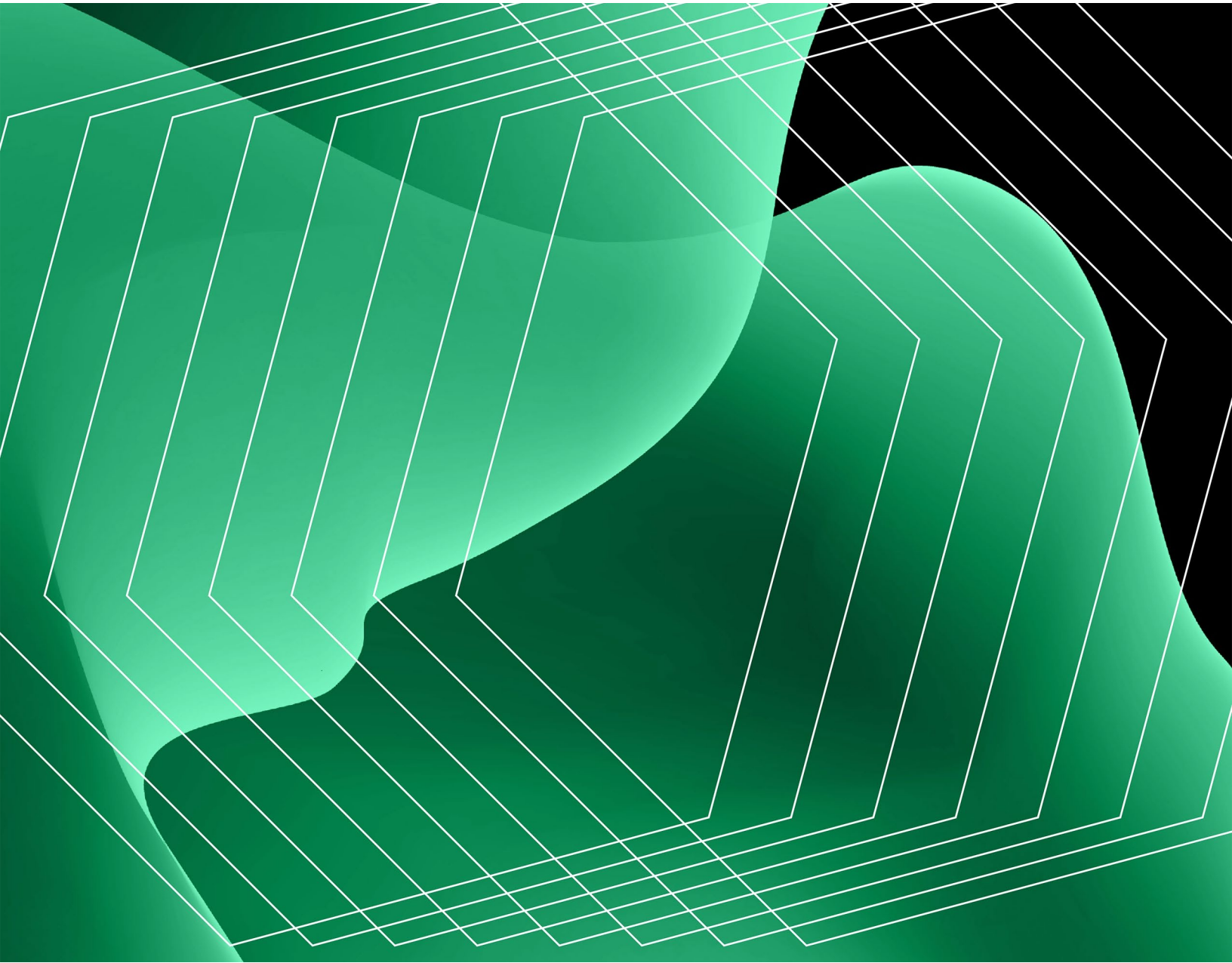


Table Of Contents

Executive Summary	3
The CrowdStrike Falcon Identity Protection Customer Journey	9
Analysis Of Benefits	13
Analysis Of Costs	29
Financial Summary	32

Consulting Team:

Eric Hall

ABOUT FORRESTER CONSULTING

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

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

Executive Summary

Identity is a major factor in most cybersecurity incidents, and it's a growing concern for organizations. In a Forrester survey, 22% of respondents said prevention and protection against identity-based attacks is a top strategic IT security priority.[1] Using Falcon Identity Protection can dramatically reduce the risk of identity-based attacks, especially high-risk incidents. And with rapid detection of incidents that do occur — including automatic response actions to high-risk activity (e.g., revoking a user session) — the solution can further reduce the risk of a successful attack.

As an identity security solution, Falcon Identity Protection provides advanced capabilities, including identity threat intelligence functionalities, to help prevent identity-related cybersecurity attacks, quickly detect threats that arise, and rapidly respond to incidents when they occur.[2] Falcon Identity Protection's threat analysis includes both direct identity-related threats as well as threats across attack paths to identify lateral movement that impacts security areas beyond identity to focus on protecting critical assets. Falcon Identity Protection's identity detection capabilities are effective in near-real time, and they can take preventative action such as blocking access if an incident is considered high risk while also minimizing false positives.

CrowdStrike commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Falcon Identity Protection.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Falcon Identity Protection on their organizations.



Return on investment (ROI)
310%



Net present value (NPV)
$955K

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Falcon Identity Protection. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global organization with 7,500 identities and a security operations center (SOC) team of five analysts. It makes two acquisitions per year.

Interviewees said that prior to using Falcon Identity Protection, their organizations had suboptimal security postures. Some described having costly breaches, and each said their organization had experienced preventable, time-consuming incidents. There were weaknesses in the SOC organizations to identify preventable risks, rank and prioritize risk, and group the prevention activities to improve efficiency and effectiveness. Incidents occurred frequently and required a lot of overtime from SOC team members, including on-call hours in the middle of the night. Some interviewees said employee demands were so bad that it led to turnover.

The interviewees said that after the investment in Falcon Identity Protection, their organizations' security postures became far better. None said their organization has experienced a breach since acquiring Falcon Identity Protection. They explained that the solution's threat-prevention analyses, including direct identity analyses and lateral attack pathway analyses, identify and score both suspected and completely unimagined threats. They also said incident alert occurrence is down significantly due both to successful prevention activities and reductions in false positives. SOC team members now work normal hours, business growth occurs without expanding security teams, and the organizations were able to negotiate lower cybersecurity insurance rates due to the improvements in their identity postures.

KEY FINDINGS

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

- **Breach reduction through better identity vulnerability prevention, incident detection, and remediation, saving $696,000 over three years.** Falcon Identity Protection identifies numerous vulnerabilities for the composite organization and effectively scores them based on risk. In addition to identifying account issues, the solution identifies and ranks risk across pathways, focusing on critical assets. Detection capabilities include real-time use of CrowdStrike's threat intelligence engine, a cloud-based repository that is updated as new threats are identified.
- **Cost reduction by eliminating legacy tools and reducing labor for SOC administration and prevention activities, saving $167,000 over three years.** By adopting Falcon Identity Protection, the composite organization reduces the use of other cybersecurity solutions. Prevention activities are more efficient due to Falcon Identity Protection's central dashboard, which is unified with the Falcon platform, integrates with

other internal systems, and has policy management and analysis capabilities the composite finds easy to use.

- **A reduction in managed security service provider (MSSP) and detection labor, saving $145,000 over three years.** The combination of effective prevention facilitated by Falcon Identity Protection's identification of threats and a significant reduction in false-positive alerts leads to a significant reduction in the volume of incidents the composite organization experiences.
- **Cost savings associated with acquisitions, saving $115,000 over three years.** With the use of Falcon Identity Protection, the composite organization foregoes paying an outside firm to do identity risk analyses. There is also no need for it to add software or resources when a typical sized acquisition occurs.
- **A cyber insurance cost reduction, saving $141,000 over three years.** The composite organization reduces its cyber insurance premiums because Falcon Identity Protection helps significant risk, ensure the proper controls are in place, and protect critical assets.

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

- **Having a strategic partner in CrowdStrike.** Interviewees shared that CrowdStrike is the core of their organizations' cybersecurity defenses. When selecting other cybersecurity products, they frequently consider whether it will integrate across the Falcon platform.
- **Labor-related savings within SOC and beyond.** Interviewees said using Falcon Identity Protection led to labor savings within the SOC, IT operations employees, and the IT help desk. They explained that employee satisfaction has improved within the SOC since implementing the solution, and some stated that employee turnover has been reduced because of multiple factors, including better work-life balance and the ability to completely prevent attacks.
- **Improved compliance, audits, and cyber insurance.** Interviewees noted labor reductions and shortened timeframes for both compliance and audit processes, as well as improvements in meeting expectations. They shared that peers from other organizations said their premiums were rising while their organizations' premiums had gone down.

- **Having a single dashboard with cybersecurity data integration and centralized policy management.** Interviewees said the centralized prevention, detection, response, and management capabilities of the solution are extremely significant, saving time for SOC and MSSP teams. They explained that these capabilities make them more confident their organizations can handle the demands placed on them.

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

- **Implementation, administration, and training costs of $19,000 over three years.** The composite completes implementation of Falcon Identity Protection in six weeks, requiring the effort of 0.5 FTE over that time. Ongoing administration is minimal, and the ease of use of the solution leads to low training costs.
- **Falcon Identity Protection Licensing costs of $289,000 over three years.** Licensing is based upon identity counts, and the composite organization has 2.5% year-over-year identity growth and adds an additional 200 identities per year from acquisitions.

The representative interviews and financial analysis found that a composite organization experiences benefits of $1.26 million over three years versus costs of $308,000, adding up to a net present value (NPV) of $955,000 and an ROI of 310%.

> “This tool gives us a good work-life balance. There used to be a lot of burnout. Analysts frequently had to work 10- to 12-hour work days due to incident response requirements. Unfortunately, we did lose top talent. We lost two senior analysts just because of burnout. We have grown by a third since bringing in CrowdStrike, have had no turnover, and have not had to increase the size of our security team. The automation is key; we have automated flows that basically disable accounts and endpoints that are identified to be risky. Integrating several platforms to a single platform simplifies the actions that they must take.”
>
> **DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY**

Return on investment (ROI)

310%

Benefits PV

$1.26M

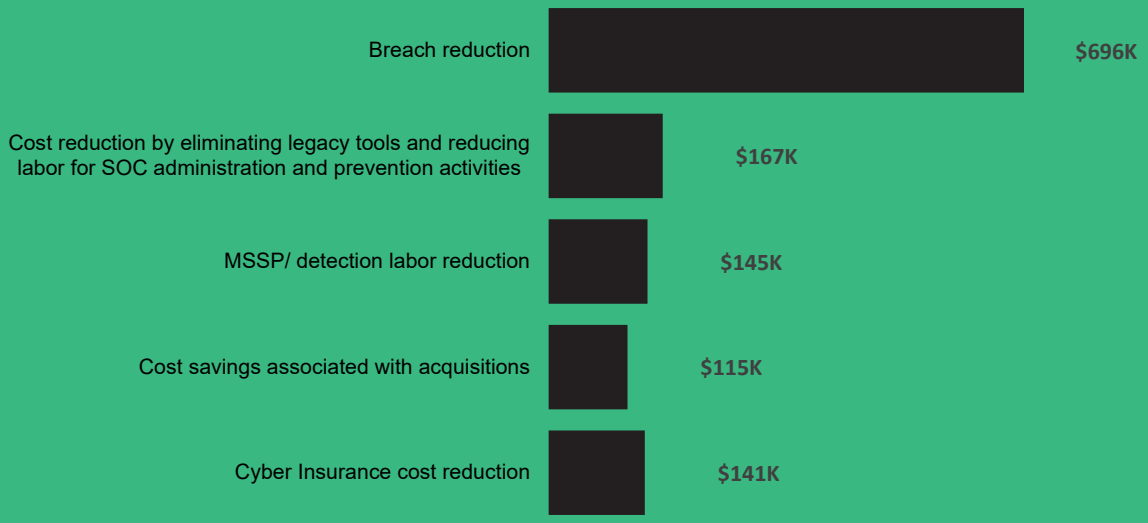
Net present value (NPV)

$955K

Payback

<6 months

Benefits (Three-Year)



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 Falcon Identity Protection.

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 Falcon Identity Protection can have on an organization.

DISCLOSURES

Readers should be aware of the following:

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

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

CrowdStrike 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.

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

1. Due Diligence
Interviewed CrowdStrike stakeholders and Forrester analysts to gather data relative to Falcon Identity Protection.

2. Interviews
Interviewed four representatives at four different organizations using Falcon Identity Protection to obtain data about costs, benefits, and risks.

3. Composite Organization
Designed a composite organization based on characteristics of the interviewees' organizations.

4. Financial Model Framework
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

5. Case Study
Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The CrowdStrike Falcon Identity Protection Customer Journey

Drivers leading to the Falcon Identity Protection investment

Interviews			
Role	**Industry**	**Region**	**Identity Count**
Cyber security director	Electronics manufacturing	Global	70,000
Director of cyber security risk and compliance	Hospitality	Global	150,000
VP of security architecture and operations	Mortgage	United States	13,000
VP of information security	Pharmaceutical	Global	750

KEY CHALLENGES

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

- **Breaches or near breaches.** A common reason the organizations looked to improve their identity security postures was because they had experienced a breach with significant costs or there was a scare that required major effort or outside assistance to ensure the incident did not escalate to become a costly breach.
- **A lack of tools to effectively identify and prioritize security gaps.** Interviewees shared that although their organizations were aware of security gaps in certain areas, they lacked the ability to identify them. And if they were able to identify them, they lacked the knowledge to effectively prioritize and address them.
- **Not knowing what they didn't know.** Interviewees said they were constantly reading about new attack methods, but they knew their organization couldn't keep up with all the

known identity-based threats that could be addressed or keep up with its identity security posture.

- **A negative effect on work-life balance due to the volume, timing, and quality of incident actions.** Interviewees shared that members of their organization's SOC team frequently had to work long hours to deal with identity-related incidents or they would get called in the middle of the night. False positives were common, and it had an even more negative effect on employee morale. Some interviewees felt that turnover within their organization was directly related to these factors in their work environment.

> "We realized that we needed the people, the process, and the technologies to effectively protect ourselves. And [Falcon Identity Protection] … offered the right technology to close our security gaps, addressing our lack of visibility."
>
> DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

> "My local sales team convinced me [of the value of Falcon Identity Protection]. [CrowdStrike] spoke the same language and made it very easy to trial. [There were] no big hurdles. I didn't have a good experience with other vendors."
>
> CYBER SECURITY DIRECTOR, ELECTRONICS MANUFACTURING

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The organization has a global presence with an initial identity count of 7,500. Year-over-year identity growth is 2.5%, with two acquisitions per year adding 200 additional identities per year. The organization utilizes an MSSP to cover 24/7 basic monitoring and alert detection.

Deployment characteristics. The composite organization completes the full implementation in 45 days. It includes all geographies and integrates numerous cybersecurity tools and data sources for display an analysis within its central CrowdStrike dashboard.

Key Assumptions

Global organization
7,500 identities
SOC team includes 5 FTEs
2 acquisitions per year

Interview Spotlight

Initial Customer Experiences

"When we switched to [Falcon Identity Protection], we got all sorts of signals from CrowdStrike about an active incident that [our legacy solution] hadn't detected. The perpetrator is now in prison."

CYBER SECURITY DIRECTOR, ELECTRONICS MANUFACTURING

"I certainly saw plenty of vulnerabilities once we put [Falcon Identity Protection] in place. It caught a couple of compromised accounts that none of our other tools had caught. Also, I knew of some areas where there were issues, but it turned out that there were a lot of other things that weren't on my radar that became priorities to fix."

VP OF INFORMATION SECURITY, PHARMACEUTICAL

"When we deployed Falcon Identity Protection, we faced a flood of vulnerability detections — things like accounts being overprivileged, misconfigured, or abused. We were also presented with resulting attack paths and were able to prioritize on major vulnerabilities, like admin accounts, and on protecting key assets."

DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

"Our introduction to Falcon Identity Protection was as part of a major incident response. It helped us with containment procedures. We followed up by doing extensive Red Team testing, as well as external and internal penetration testing. Its ability to prevent lateral movement, credential abuse, and account takeovers made it clear that it was worth keeping."

VP OF SECURITY ARCHITECTURE AND OPERATIONS, MORTGAGE

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	Breach reduction	$279,816	$279,816	$279,816	$839,448	$695,861
Btr	Cost reduction by eliminating legacy tools and reducing labor for SOC administration and prevention activities	$51,000	$76,500	$76,500	$204,000	$167,062
Ctr	MSSP/detection labor reduction	$48,000	$64,000	$64,000	$176,000	$144,613
Dtr	Cost savings associated with acquisitions	$46,400	$46,400	$46,400	$139,200	$115,390
Etr	Cyber Insurance cost reduction	$54,000	$56,756	$59,575	$170,331	$140,756
	Total benefits (risk-adjusted)	$479,216	$523,472	$526,291	$1,528,979	$1,263,682

BREACH REDUCTION

Evidence and data. The interviewees shared that Falcon Identity Protection was a major contributor toward turning around their organizations' historical breach and incident volumes. Each interviewee said their organization has not had a breach since implementing Falcon Identity Protection. More than one said a breach led their organization to look for an identity protection solution, and others said they were aware that direct competitors had experienced a breach. Interviewees also spoke of high incident rates and said Falcon Identity Protection dramatically reduced the need for remediation activities.

- Each interviewee described how Falcon Identity Protection identified significant vulnerabilities their organization's other tools had not identified. Several said they knew their organization had some areas of weakness and that Falcon Identity Protection found additional areas that needed attention.
- Interviewees shared that Falcon Identity Protection prevention capabilities went well beyond just identifying account issues, such as misconfigured or overprivileged accounts, and that it also provided lateral attack path analysis. With risk scoring heavily

weighted by a combination of administrative accounts and critical assets, SOC teams were able to both dramatically reduce the probability of a breach occurring and dramatically reduce the level of harm if a breach did occur.

- Interviewees also spoke highly of the monitoring and detection capabilities of Falcon Identity Protection. First, they noted that Falcon Identity Protection is a cloud-based solution and that CrowdStrike updates the detection rules as it identifies new malware, etc. Second, each interviewee said the speed of detection times exceeded their expectations.
- Not only did interviewees say the speed of detections is significant, but they also called out having the ability to identify high-risk incidents and lockout devices.
- Interviewees also noted they understand that identity factors play a role in the vast majority of current breaches. Some said it's up to 90% of the reason.

> "We had a penetration test done. Falcon Identity Protection was first in detecting the attack, and it did it within 10 minutes. That was remarkable."
>
> **VP OF INFORMATION SECURITY, PHARMACEUTICAL**

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- Before using Falcon Identity Protection, the composite organization had a 61% chance of experiencing one or more breach per year.
- The composite's mean cumulative cost of total breaches per year totals $2.65 million.[4]
- More than 57% of the composite's breaches originate from external sources.[5]
- Falcon Identity Protection can address 75% of the external attacks.

- The composite organization reduces its risk of breaches from external sources by 50% with Falcon Identity Protection.

Risks. Factors that could affect the impact of this benefit for organizations include the following:

- Threats will vary based upon region, industry, and organization size.
- The sophistication of attacks and the ability to prevent, detect, and remediate attacks will vary.
- Cybersecurity team maturity, the breadth of data-capture tools, and the integration and functional capabilities of other cybersecurity software will vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $696,000.

> "It helps us harden our Active Directory. Therefore, we're less likely to have lateral movement during a breach, which means our worst case is more likely to be a single pop 10 point versus enterprise ransomware."
>
> VP OF INFORMATION SECURITY, PHARMACEUTICAL

> "Breaches nowadays don't have just one component, which is malware. They always have an identity component. Falcon Identity Protection is the icing on the cake, just in case you missed anything. If a bad guy ends up on an endpoint and is trying to exfiltrate or run malware, that machine is automatically isolated."
>
> DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

> "Intrusions are almost always caught in the execution phase through identity monitoring, probably more than 70% of the time. In the scope of prevention, it's becoming more and more useful."
>
> VP OF SECURITY ARCHITECTURE AND OPERATIONS, MORTGAGE

Breach Reduction					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Likelihood of experiencing one or more breach	Forrester research	61%	61%	61%
A2	Mean cumulative cost of breaches	Forrester research	$2,650,000	$2,650,000	$2,650,000
A3	Percent of breaches originating from external sources	Forrester research	57.7%	57.7%	57.7%
A4	Percent of external attacks addressable with Falcon Identity Protection	Interviews	75%	75%	75%
A5	Risk exposure addressable with Falcon Identity Protection	A1*A2*A3*A4	$699,540	$699,540	$699,540
A6	Reduced risk	Interviews	50%	50%	50%
At	Breach reduction	A5*A6	$349,770	$349,770	$349,770
	Risk adjustment	↓20%			
Atr	Breach reduction (risk-adjusted)		$279,816	$279,816	$279,816
	Three-year total: $839,448			**Three-year present value: $695,861**	

COST REDUCTION BY ELIMINATING LEGACY TOOLS AND REDUCING LABOR FOR SOC ADMINISTRATION AND PREVENTION ACTIVITIES

Evidence and data. Interviewees' organizations varied in their maturity levels and in their use of cybersecurity tools and labor. Each organization was able to eliminate or reduce the use of various cybersecurity toolsets, and those with a formal SOC were able to reduce the effort to accomplish cybersecurity prevention while dramatically improving prevention position.

- Software reduction included not only toolsets, but also targeted tools such as Active Directory password analysis. This included both existing tools and tools under consideration.
- Interviewees said the central dashboard, integration across the Falcon platform and other existing solutions, policy management, and built-in analyses enabled much more efficient and effective prevention activities than they had before.

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- Forrester created the model for the composite organization with only existing tools in mind; not tools under consideration.
- The composite organization has a blended cost for cybersecurity software, software administration, and SOC-related prevention analysis of $120,000 per year.
- The composite organization reduces the cost of cybersecurity software, software administration, and SOC-related prevention analysis by 50% in Year 1 and by 75% in years 2 and 3.

Risks. Factors that could affect the impact of this benefit for organizations include the following:

- The ability to sunset other cybersecurity solutions or portions thereof will vary based upon the solution capabilities.
- The prevention maturity of the organization will affect prevention activities, especially in the short term.
- The efficiency and effectiveness of existing security team processes will vary.
- The skills of the SOC team in administration and prevention activities will affect reassignment opportunities.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $167,000.

> “We run an organization that’s highly distributed. We have over 1,000 locations around the globe, both franchises and managed. [Falcon Identity Protection] protects all of it.”
>
> DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

> “We’ve implemented a lot of lateral movement rules within Falcon Identity Protection to block things like RDPing [using Remote Desktop Protocol] from one server to another server. We’re using it more and more also to help us with device posture, which what weren’t aware of when we bought it.”
>
> VP OF SECURITY ARCHITECTURE AND OPERATIONS, MORTGAGE

Cost Reduction By Eliminating Legacy Tools And Reducing Labor For SOC Administration And Prevention Activities					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Blended cost of legacy tools and SOC team administration and prevention labor	Composite	$120,000	$120,000	$120,000
B2	Reduction in legacy tools and in SOC team administration and prevention labor	Composite	50%	75%	75%
Bt	Cost reduction by eliminating legacy tools and reducing labor for SOC administration and prevention activities	B1*B2	$60,000	$90,000	$90,000
	Risk adjustment	↓15%			
Btr	Cost reduction by eliminating legacy tools and reducing labor for SOC administration and prevention activities (risk-adjusted)		$51,000	$76,500	$76,500
	Three-year total: $204,000			**Three-year present value: $167,062**	

MSSP/DETECTION LABOR REDUCTION

Evidence and data. Interviewees said the effectiveness of Falcon Identity Protection's prevention management became obvious in the incident detection changes that occurred and that they were all for the better. Interviewees described incident volume declining significantly, sometimes more than 90%. They said some of this is related to the prevention actions taken and some is related to a dramatic reduction in false positives.

The director of cyber security risk and compliance at the hospitality organization said: "Prior to [Falcon Identity Protection], there were hundreds of detections per month and approximately one potential event a week needing immediate action. Now, there may be 100 detections that the MSSP handles by itself and two events annually that need immediate action by an analyst."

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- The composite organization pays $400,000 per year for MSSP support and SOC-related detection labor.
- The composite organization reduces the cost of MSSP support and SOC-related detection labor by 15% in Year 1 and by 20% in years 2 and year 3.

Risks. Factors that could affect the impact of this benefit for organizations include the following:

- The detection capabilities of existing solutions will vary.
- The efficiency and effectiveness of the processes of the existing security team and MSSP will vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $145,000.

> "The alerts are near-real time, are more actionable, and don't have a lot of false positives. Previously, it sometimes took 4 hours when now we know in less than 10 minutes. To go from alert to triage to close usually takes less than an hour."
>
> VP OF INFORMATION SECURITY, PHARMACEUTICAL

> "Falcon Identity Protection has given us the ability to be able to cut the time to identify incidents, create an action plan, and mitigate the incidents. It's now down to a science. … We have an MSSP that basically provides 24/7 coverage, running L1 for our 1,000 locations. They see detection in 30 seconds after it takes place, know what to do within about 5 minutes, and route a ticket to the right stakeholders. An additional benefit we have seen is a MSSP cost reduction due to a reduction in analyst actions. With the integrated dashboard, the incident prevention that it facilitated, and reduced false positives, our annual cost has been cut significantly, even with our growth."
>
> DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

> "When we implemented some rules to automatically block certain admin activity, we reduced related investigations from around 50 per month to less than five."
>
> VP OF SECURITY ARCHITECTURE AND OPERATIONS, MORTGAGE

MSSP/Detection Labor Reduction					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Combined cost of MSSP and SOC team detection labor	Interviews	$400,000	$400,000	$400,000
C2	SOC labor and MSSP cost reduction due to reduced detection actions	Composite	15%	20%	20%
Ct	MSSP/detection labor reduction	C1*C2	$60,000	$80,000	$80,000
	Risk adjustment	↓20%			
Ctr	MSSP/detection labor reduction (risk-adjusted)		$48,000	$64,000	$64,000
	Three-year total: $176,000		**Three-year present value: $144,613**		

COST SAVINGS ASSOCIATED WITH ACQUISITIONS

Evidence and data. Interviewees' organizations varied in the frequency and size of acquisitions occurred. One thing they had in common was that for small acquisitions, their organizations switched from having outside evaluations identity the security postures of prospective acquisitions to using Falcon Identity Protection. Another commonality was that they absorbed the identity security responsibilities for the acquired organizations without adding software capabilities or expanding their SOC teams.

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- The composite organization acquires two companies per year with an average of 100 identities per acquisition.

- For each acquisition, the composite organization avoids paying $4,000 for an external cybersecurity evaluation of the acquired company's environment.
- With Falcon Identity Protection, the composite organization completely absorbs an acquired company's security software and labor costs, avoiding $25,000 per acquisition.

Risks. Factors that could affect the impact of this benefit for organizations include the following:

- The frequency and size of acquisitions will vary.
- The risk will vary based upon geography, size, and industry of the acquired organization.
- The current state of the acquired organization's cybersecurity software, security team, and infrastructure's cybersecurity maturity will vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $115,000.

> "Prior to a prospective acquisition, we do a compromise assessment that includes Falcon Identity Protection. This gives us a picture of what it will take to clean up that environment or if we'll even clean it up. [Due to large acquisitions,] we would have needed three to four additional analysts if we hadn't had [Falcon Identity Protection]. I associate that with the real-time data analysis and reporting."
>
> DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

Cost Savings Associated With Acquisitions					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Acquisitions	Composite	2	2	2
D2	Avoided cost for external evaluation of acquired company's environment	Composite	$4,000	$4,000	$4,000
D3	Cost avoidance by completely absorbing acquired company's security costs	Composite	$25,000	$25,000	$25,000
Dt	Cost savings associated with acquisitions	D1*(D2+D3)	$58,000	$58,000	$58,000
	Risk adjustment	↓20%			
Dtr	Cost savings associated with acquisitions (risk-adjusted)		$46,400	$46,400	$46,400
	Three-year total: $139,200			**Three-year present value: $115,390**	

CYBER INSURANCE COST REDUCTION

Evidence and data. Interviewees shared that their organizations have more confidence going into discussions with cyber insurances companies and that they have seen cost reductions associated with improvements they have made with key identities and with critical assets — the latter being safer due to Falcon Identity Protection's lateral movement pathway vulnerability tracking capability. Interviewees noted that the reporting capabilities help their organizations easily show that their security postures have improved.

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- The composite organization's cyber insurance costs (including annual identity growth due to natural growth and acquisitions) are $1,350,000 in Year 1, $1,418,903 in Year 2, and $1,489,384 in Year 3.
- The use of Falcon Identity Protection reduces the composite's cybersecurity insurance costs by 5% per year.

Risks. Factors that could affect the impact of this benefit for organizations include the following:

- Cybersecurity insurance rates will vary by provider, coverage agreements, and industry, among many other factors.
- The ability to negotiate rates will vary.

- The contrast between the current state and future state of cybersecurity defenses will vary.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $141,000.

> "Cyber insurance costs have gone down significantly. Insurance companies have a very strong emphasis on privileged account monitoring and protection, which [Falcon] Identity Protection covers for us. We provide visibility in what they're being used for and show that we have controls that ensure that they are not being exploited or abused."
>
> DIRECTOR OF CYBER SECURITY RISK AND COMPLIANCE, HOSPITALITY

> "Cyber insurance is lower, and having Falcon Identity Protection is part of that. I'm sure we would have had something bad happen over the years if it wasn't for what we're using. We haven't had anything to report [since implementing Falcon Identity Protection]."
>
> CYBER SECURITY DIRECTOR, ELECTRONICS MANUFACTURER

Cyber Insurance Cost Reduction					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Cyber insurance cost prior to using Falcon Identity Protection	Composite	$1,350,000	$1,418,903	$1,489,384
E2	Cyber insurance cost reduction due to Falcon Identity Protection	Interviews	5.0%	5.0%	5.0%
Et	Cyber insurance cost reduction	E1*E2	$67,500	$70,945	$74,469
	Risk adjustment	↓20%			
Etr	Cyber insurance cost reduction (risk-adjusted)		$54,000	$56,756	$59,575
	Three-year total: $170,331			**Three-year present value: $140,756**	

UNQUANTIFIED BENEFITS

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

- **Having a strategic partner in CrowdStrike.** The cyber security director for the electronics manufacturer mentioned a common theme: “CrowdStrike is a critical partner at this point.” Interviewees shared that whether they’re working with CrowdStrike account teams or support teams, their organization’s needs are being met or exceeded with CrowdStrike at the core of their cybersecurity defenses.

> “CrowdStrike really is the primary strategic vendor for us. At this point, we talk to other vendors about how they work with CrowdStrike.”
>
> VP OF INFORMATION SECURITY, PHARMACEUTICAL

- **Labor-related savings within SOC and beyond.** Interviewees said their organizations increased employee satisfaction, which they associated with improvements to employee loyalty and retention. They said that IT operations requires less time for prevention-

related activities, work only on priority fixes, and are able to group activities into sprints. They also said IT operations requires less time with remediation activities in large part due to the success of prevention activities; automatic actions taken by Falcon Identity Protection; and clear, specific instructions on required remediation actions. They also said help deck activity is reduced or proactively triggered by Falcon Identity Protection with specific instructions at a high rate of speed.

> "Occasionally, we detect account lockouts before users report them. We then reach out to the help desk so that they can proactively help them."
>
> VP OF INFORMATION SECURITY, PHARMACEUTICAL

- **Improved compliance, audits, and cyber insurance.** Although interviewees could not measure labor savings, they noted both labor reductions and shortened time cycles for both compliance and audit processes along with improvements in meeting expectations. In addition to sharing that their organizations' cyber insurance premiums had gone down, interviewees also said peers from other organizations told them premiums are rising.

> "Falcon Identity Protection ticks a lot of the boxes out of the 113 [compliance] controls."
>
> CYBER SECURITY DIRECTOR, ELECTRONICS MANUFACTURING

- **Having a single dashboard with cybersecurity data integration and centralized policy management.** Interviewees described the centralized prevention, detection, response, and management capabilities of Falcon Identity Protection as extremely significant and that they save time for SOC and MSSP teams. They explained that these capabilities also save their organizations money by reducing the use of other tools. Interviewees noted this makes them more confident that their organizations will be able to handle the demands placed upon them.

> "We moved to [CrowdStrike's security information and event management (SIEM) solution], and the Falcon [Identity Protection] suite capabilities and the integration made that possible. The amount of vulnerability analysis we do now would have cost us a king's ransom with our prior SIEM solution."
>
> **CYBER SECURITY DIRECTOR, ELECTRONICS MANUFACTURING**

> "One of the headlines for Falcon Identity Protection is just visibility. It brings Active Directory to life for me. It shows me not just the configuration of Active Directory itself, but what's going on with these accounts. Being able to get things like passwords that are known to be compromised is super helpful. We almost spent money to buy a specific tool for that purpose."
>
> **VP OF INFORMATION SECURITY, PHARMACEUTICAL**

FLEXIBILITY

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

- **Grouping prevention activities, which allows for sprints.** Interviewees shared that their organizations gained the ability to group threat prevention activities by location and type of prevention activity, which led to more efficient and effective remediation.
- **Lockouts, which prevents the need for immediate responses.** Interviewees said Falcon Identity Protection blocks access or isolates devices with potentially serious risks and that this allows remediation responses to be timely, but not immediate.

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**
Ftr	Implementation, administration, and training costs	$12,100	$5,363	$1,403	$1,403	$20,268	$19,188
Gtr	Falcon Identity Protection Licensing	$0	$110,880	$116,539	$122,328	$349,747	$289,020
	Total costs (risk-adjusted)	$12,100	$116,243	$117,942	$123,731	$370,015	$308,208

IMPLEMENTATION, ADMINISTRATION, AND TRAINING COSTS

Evidence and data. The interviewees revealed the following about the implementation, administration, and training costs associated with their organizations' use of Falcon Identity Protection:

- Because it's a cloud-based solution, interviewees described the implementation as relatively short. Integration and sensor deployment was typically completed in four to six weeks, and no professional services were required.
- Time for ongoing administration and new SOC team-related prevention activities tapered off over time.
- Interviewees described the solution as easy to use and requiring only a small amount of training.

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- The composite completes its original implementation in six weeks and utilizes half an FTE during that period. Ongoing discussions, implementation of new features, etc. required little effort, 5 hours per year.

- Ongoing administration and time for new SOC team-related prevention activities taper off over time. The composite spends 60 hours on this in Year 1 and then 12 hours annually after that.
- The fully loaded hourly rate for an SOC team member is $75 per hour.
- The composite organization's training costs are $2,000.

Risks. Factors that could affect the impact of this cost for organizations include the following:

- The complexity and number of software integrations may vary.
- Labor costs may vary.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $19,000.

Implementation, Administration, And Training Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Implementation time (hours)	Interviews	120	5	5	5
F2	Time for ongoing administration and new prevention actions (hours)	Interviews	0	60	12	12
F3	Hourly cost for a security analyst	TEI standard	$75	$75	$75	$75
F4	One-time training costs	Interviews	$2,000			
Ft	Implementation, administration, and training costs	(F1+F2)*F3+F4	$11,000	$4,875	$1,275	$1,275
	Risk adjustment	↑10%				
Ftr	Implementation, administration, and training costs (risk-adjusted)		$12,100	$5,363	$1,403	$1,403
	Three-year total: $20,268		**Three-year present value: $19,188**			

FALCON IDENTITY PROTECTION LICENSING

Evidence and data. The interviewees shared that licensing costs for Falcon Identity Protection are based on the number of identities covered by the solution.

Pricing may vary. Contact CrowdStrike for additional details.

Modeling and assumptions. For the financial analysis, Forrester assumes the following about the composite organization:

- The composite organization's identity growth is due to a natural 2.5% year-over-year growth and growth due to acquisitions of 200 identities per year.
- The cost for Falcon Identity Protection is $12 per year per identity.

Risks. An organization's identity growth could affect the impact of this cost.

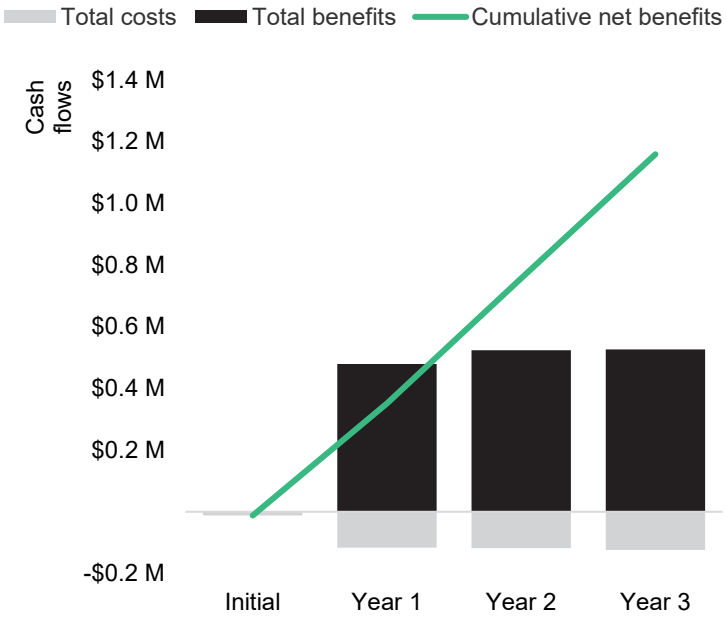
Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $289,000.

Falcon Identity Protection Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Identities (base)	Interviews		7,500	7,700	8,093
G2	Identity growth due to organizational growth	Interviews			193	202
G3	Identity growth per acquisition	Interviews		200	200	200
G4	Total identity count	G1+G2+G3		7,700	8,093	8,495
G5	Cost per identity	Composite		$12	$12	$12
Gt	Falcon Identity Protection licensing	G4*G5	$0	$92,400	$97,116	$101,940
	Risk adjustment	↑20%				
Gtr	Falcon Identity Protection licensing (risk-adjusted)		$0	$110,880	$116,539	$122,328
	Three-year total: $349,747			**Three-year present value: $289,020**		

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, 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	($12,100)	($116,243)	($117,942)	($123,731)	($370,015)	($308,208)
Total benefits	$0	$479,216	$523,472	$526,291	$1,528,979	$1,263,682
Net benefits	($12,100)	$362,974	$405,530	$402,561	$1,158,965	$955,474
ROI						310%
Payback						<6 months

APPENDIX A: TOTAL ECONOMIC IMPACT

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

Total Economic Impact Approach

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

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

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

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

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.

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.

APPENDIX B: ENDNOTES

[1] Source: Forrester's Security Survey, 2024. Base: 2,801 security decision-makers at their organizations. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[2] Source: The Forrester Tech Tide™: Identity And Access Management, Q3 2024.

[3] 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.

[4] Source: Forrester's Security Survey, 2023. Base 1,542 security decision-makers from organizations that have experienced a breach in the past 12 months. Forrester annually assesses cybersecurity metrics through interviews, surveys, and expertise in the field. Analyses are provided with information rooted with specific data sets most accurately applied to the situations that have been collected in the study.

[5] Ibid.

FORRESTER®