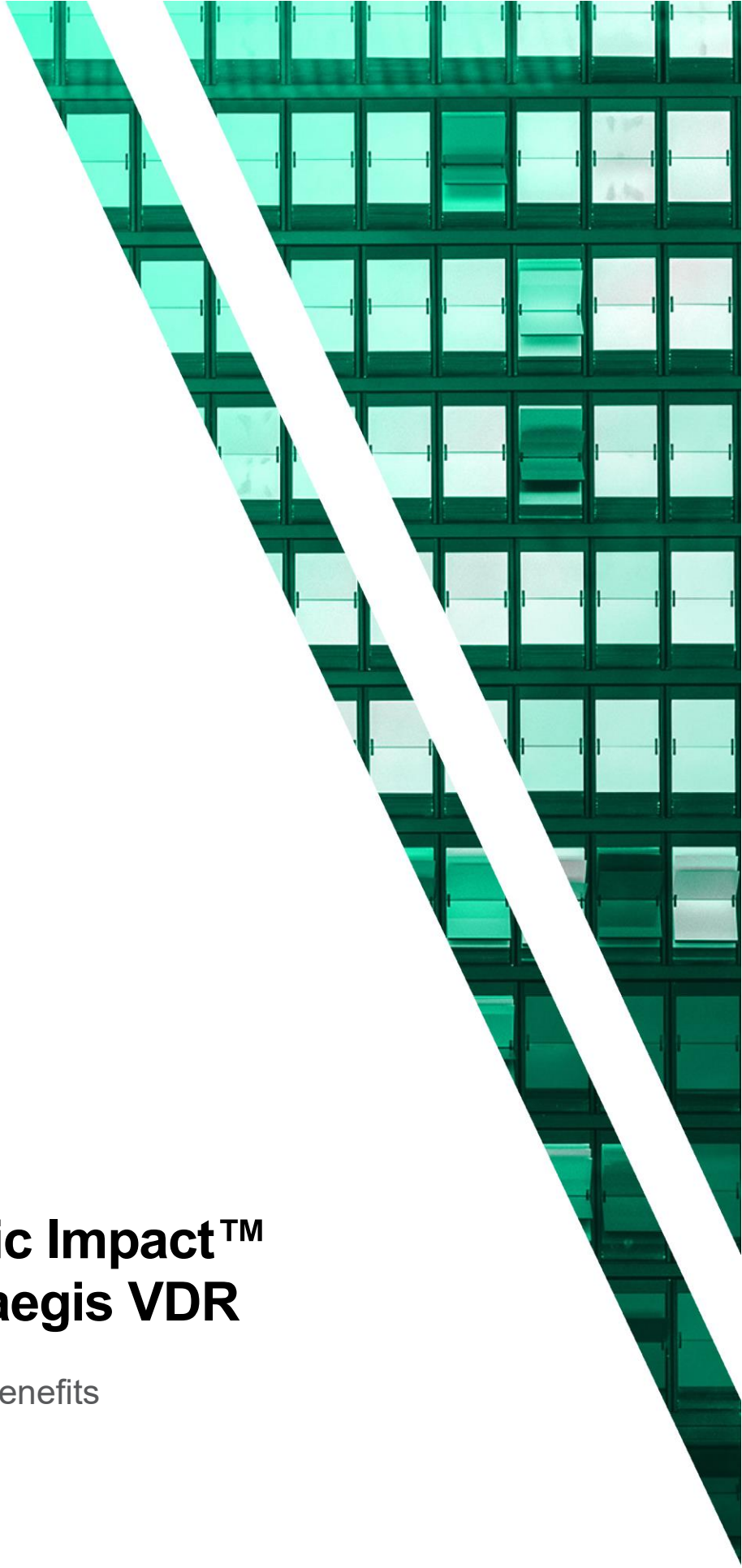
FORRESTER®



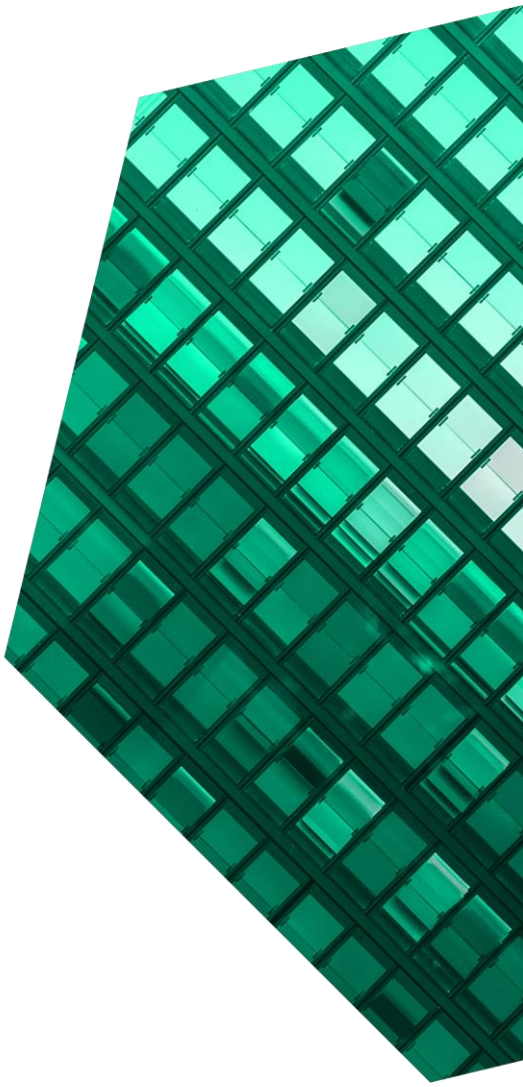
The Total Economic Impact™ Of Secureworks Taegis VDR

Cost Savings And Business Benefits Enabled By Taegis VDR

APRIL 2023

Table Of Contents

Consulting Team: Eric Hall



Executive Summary

Cybersecurity risk is growing rapidly due to bad actors continuously getting more sophisticated and acting more frequently. Cybersecurity teams, overwhelmed by reactive activities, are recognizing that more proactive processes are required to both reduce risk and to reduce cybersecurity labor efforts. Vulnerability management has expanded beyond individual asset risk identification and infrequent, costly infrastructure penetration testing to solutions like Taegis VDR, which also provide critical path vulnerabilities.

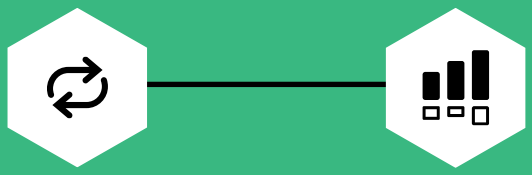
The Secureworks Taegis Vulnerability Detect and Response (VDR) solution is a vulnerability-management solution that utilizes machine learning to identify not only the vulnerabilities of individual endpoints, web applications, and network devices, but also the vulnerability relationships between these assets.

Taegis VDR provides a prioritized list of assets to patch and remediate that includes the reasoning behind the ratings, and this allows cybersecurity organizations to change patching priorities based on their organization's needs. Reports and dashboards are valuable to cybersecurity teams, IT operations, IT management, and corporate leadership, and they provide trust and confidence in the effort to reduce the risk of breaches and the significance of breaches that may occur.

Secureworks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Taegis VDR.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Taegis VDR on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Taegis VDR. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that generates $250 million per year and has 3,000 endpoints across multiple locations.

KEY STATISTICS



Return on investment (ROI)
352%

Net present value (NPV)
$404K

Prior to using Taegis VDR, the interviewees' organizations either utilized a managed security service provider (MSSP) or had security analysts utilize some combination of cybersecurity tools to perform vulnerability-management activities. Vulnerabilities were limited to endpoint vulnerabilities only, not including critical-path vulnerabilities. Those responsible for vulnerability management were not able to keep up with literature nor what the right tools should be. Neither the cybersecurity teams nor IT operations teams responsible for patching and remediation had confidence that the patching lists optimized risk reduction.

The interviewees shared that after investing in Taegis VDR, they saw confidence in their organizations' vulnerability management processes increase organization wide, from cybersecurity teams and IT operations to corporate executives. Interviewees said

Taegis VDR identifies not only individual endpoint vulnerabilities, but also critical path vulnerabilities by keeping current on the relationships of assets across the infrastructures. They said key results from the investment include a significant reduction in the probability of breaches, a significant reduction in the likely cost of a breach, and various labor and asset productivities.

KEY FINDINGS

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

- **Avoided costs associated with data breaches of $285,600 over three years.** The composite organization reduces the frequency and severity of cybersecurity attacks by utilizing Taegis VDR to identify security exposures and prioritize patching and remediation activities based on the exposure to critical assets.
- **Cost savings of $46,000 by deprecating other security software over three years.** The composite organization obtains an overall lower licensing cost for vulnerability management by eliminating related software and services.
- **Security-team labor cost reduction of $69,200 over three years.** The composite organization spends less time researching the security vulnerability landscape, identifying vulnerabilities within itsi infrastructure, studying identified vulnerabilities, prioritizing patching and remediation efforts, and communicating to IT operations (IT ops) requirements for patching and remediation.
- **IT ops labor cost reduction of $106,300 over three years.** The composite organization spends less time on vulnerability-related patching and remediation activities by focusing on exposures to critical assets and critical pathways.
- **Resource cost reductions of $11,900 over three years.** The composite organization identifies assets that were not previously tracked, and it identifies resources that can be deprecated or reduced in size.

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

- **Improved team comfort level and employee satisfaction.** Members of both the composite's cybersecurity and IT ops team members are happier because they recognize they are doing value-add work related to breach-reduction activities.
- **Increased confidence to the corporate board level.** Interviewees shared that interest in cybersecurity has risen to the board level and that Taegis VDR's role in cybersecurity protection is well-known throughout their organizations.
- **Reduction in penetration testing (pen testing).** Interviewees shared that their organizations are considering the reduction of pen testing.
- **Reduction in remediation that is disruptive to the business.** Interviewees shared that Taegis VDR's prioritizations led to a reduction in patching and remediation activities and also enabled timing flexibility.
- **Merger and acquisition evaluation.** Interviewees shared that their organizations implemented Taegis VDR on acquired organizations' networks and remediated vulnerabilities before integrations occurred.
- **Having a business partner.** Interviewees shared that their organizations' Secureworks teams are there for them. They said the teams hold monthly advisory meetings and typically provide knowledgeable feedback to questions in less than an hour. An IT manager at a construction services organization said, "[Secureworks team members] are customer-service-focused and consistently engage with us

effectively." A global IT director at a manufacturing organization shared, "We have our monthly reviews and quarterly deeper dives into the threat landscape that we're in."

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

- **Implementation and licensing costs of $115,000.** Interviewees said implementation and training at their organizations was fast, simple, and informative. Employees understood licensing, and it generally was less expensive than deprecated components.

The representative interviews and financial analysis found that a composite organization experiences benefits of $519,000 over three years versus costs of $115,000, adding up to a net present value (NPV) of $404,000 and an ROI of 352%.

ROI
352%

BENEFITS PV
$519K

NPV
$404K

PAYBACK
<6 months

Benefits (Three-Year)

“You can’t protect it if you can’t see it. I need visibility to vulnerabilities more frequently than an annual pen test. Secureworks provides those much-needed vulnerability scans for us.”

– Information security officer, pharmaceutical

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 Secureworks Taegis VDR.

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 Taegis VDR can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DUE DILIGENCE
Interviewed Secureworks stakeholders and Forrester analysts to gather data relative to Taegis VDR.

INTERVIEWS
Interviewed four representatives at organizations using Secureworks Taegis VDR to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewees' organizations.

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

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

The Secureworks Taegis VDR Customer Journey

Drivers leading to the Taegis VDR investment

Interviews			
Role	**Industry**	**Region**	**Annual revenue**
Security analyst	Manufacturing and retail	Global	$750 million
Information security officer	Pharmaceutical	Global	$500 million
IT manager	Construction services	Europe	$400 million
Global IT director	Manufacturing	Global	$200 million

KEY CHALLENGES

Interviewees shared that their organizations' vulnerability management processes were putting their companies at risk for significant cybersecurity attacks. Some organizations utilized an MSSP while others depended on their security analysts to use an incomplete set of cybersecurity tools to identify vulnerabilities and prioritize patching and remediation activities.

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

- **Chasing vulnerability-management best practices.** Interviewees shared that their organizations' security teams, IT leadership, and corporate leadership were all aware that the cybercriminals are getting better at cyberattacks and that their organizations' defenses were not keeping up. None of the interviewees felt that their organization's processes went beyond endpoint vulnerabilities to include crucial vulnerability pathways. Interviewees also noted that the frequency of endpoint-vulnerability analyses were not where they wanted them to be.
- **Cybersecurity teams being unable to keep up with active risks and apply them to their organizations' environments.** The organizations' cybersecurity teams were relatively small and didn't have anyone focused on vulnerability management. Understanding and prioritizing risks — whether identified by existing tools or MSSPs — was inefficient and imperfect, and security teams were not confident with their own prioritizations.
- **IT operations did not accepting patching-action lists.** Interviewees said their organizations' IT operations teams were skeptical with the patching and remediation lists provided by cybersecurity teams because there were not good explanations of the reason to act. Frequently the IT operations teams would not complete the actions required due to other priorities. This was even more significant because the organizations did not have timely processes to confirm that patching and remediation activities were completed successfully.

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.

Description of composite. The $250 million company historically had incomplete vulnerability coverage whether from using some software tools or a managed security service. The composite organization has 1,500 employees and 3,000 endpoints across multiple locations. There is no dedicated security analyst(s) for vulnerability management. The cybersecurity team may include part-time IT resources.

Key Assumptions

- **$250 million annual revenue**
- **3,000 endpoints**
- **1,500 employees**
- **Partial vulnerability coverage**

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	Data breach risk reduction	$114,847	$114,847	$114,847	$344,542	$285,608
Btr	Deprecated security software savings and associated service and support	$18,525	$18,525	$18,525	$55,575	$46,069
Ctr	Security team labor savings due to reduced vulnerability tracking, monitoring, and research	$27,838	$27,838	$27,838	$83,513	$69,228
Dtr	IT ops labor savings due to prioritized patching	$42,750	$42,750	$42,750	$128,250	$106,313
Etr	Resource cost savings due to finding unused assets	$4,000	$4,800	$5,760	$14,560	$11,931
	Total benefits (risk-adjusted)	$207,960	$208,760	$209,720	$626,439	$519,149

DATA BREACH RISK REDUCTION

Evidence and data. The interviewees' organizations were able to address critical security vulnerabilities far better than they could previously, which reduced both the frequency and damages due to breaches (e.g., remediation, outages, fines, revenues loss, and brand rebuilding). Taegis VDR provides their organizations with continuous monitoring of the entire threat landscape, and this includes identifying vulnerabilities within individual devices as well as vulnerabilities within network pathways.

- Interviewees said their organizations continuously monitor devices and pathways and cycle across their entire infrastructures approximately every week. Taegis VDR identifies vulnerabilities and makes recommendations for patching and remediation based on the risk associated with the vulnerabilities and the criticality of the devices or pathways affected. New vulnerabilities are quickly identified, and this enables fast remediation responses.

"Our cybersecurity posture has moved from reactive to proactive. We are identifying potential threats before they become active threats."

Security analyst, manufacturing and retail

- Interviewees shared that Taegis VDR goes beyond identifying the need to patch devices; they said it also identifies adjustments to default applications and settings. The global IT director at a manufacturer shared: "There's an assumption that everything is fine if you are fully patched, but that isn't true. [Taegis VDR] identifies vulnerabilities that are resolved by uninstalling stuff or taking stuff away that is inherent in the OS. [Taegis] VDR picks up the

need to deprecate components of patches that cause vulnerabilities."

Modeling and assumptions. To calculate the value of this benefit for the composite organization, Forrester assumes the following:

- The composite organization experiences an average of 2.6 breaches per year.[2] This data is used for the number of breaches per year at a typical maturity level, and the average cost per data breach is $151,319 exclusive of internal user downtime.
- Using Taegis VDR reduces the composite organization's likelihood of a breach by 60%.
- The average fully burdened hourly rate per end-user employee is $40.
- The average downtime per employee for each breach is 3.6 hours, and the average percentage of employees affected by a breach is 20% of the composite organization's 1,500 employees.[3]
- Each end user sees an 85% productivity recapture rate.

Risks. Risks that could impact the realization of this benefit include:

- The maturity of the organization's cybersecurity team and its existing vulnerability management capabilities.
- The organization's industry and global regions, which will lead to different levels of threats.
- The number of employees likely affected by a breach and the average recapture percentage.
- The average annual cost of employees.

"Taegis VDR is linking device vulnerabilities to other devices [and] effectively prioritizing based upon key pathways versus just device issues."

Security analyst, manufacturing and retail

"[Taegis] VDR helped us move to a more secure attack vector to avoid being noticed, scanned, and attacked. Now, we understand the risks and the mitigation requirements a lot better."

Global IT director, manufacturing

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $285,600.

Data Breach Risk Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average number of data breaches per year	Forrester research	1.6	1.6	1.6
A2	Average potential cost of data breach exclusive of end-user downtime	Forrester research	$90,791	$90,791	$90,791
A3	Percentage of breaches that benefit from vulnerability management solutions	Forrester research	79%	79%	79%
A4	Reduced likelihood and significance of a breach	Interviews	60%	60%	60%
A5	**Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs**	**A1*A2*A3*A4**	**$68,856**	**$68,856**	**$68,856**
A6	Number of employees	Composite	1,500	1,500	1,500
A7	Average salary of a business user (hourly)	TEI standard	$40	$40	$40
A8	Diminished/eliminated user productivity hours per breach	Forrester research	3.6	3.6	3.6
A9	Average percentage of employees affected per breach	Forrester research	20%	20%	20%
A10	Productivity recapture	Interviews	85%	85%	85%
A11	**Cost of reduced end-user productivity**	**A1*A6*A7*A8*A9*A10**	**$58,752**	**$58,752**	**$58,752**
At	Data breach risk reduction	A5+A11	$127,608	$127,608	$127,608
	Risk adjustment	↓10%			
Atr	Data breach risk reduction (risk-adjusted)		$114,847	$114,847	$114,847
	Three-year total: $344,542			**Three-year present value: $285,608**	

DEPRECATED SECURITY SOFTWARE SAVINGS AND ASSOCIATED SERVICE AND SUPPORT

Evidence and data. Interviewees shared that their organizations eliminated vulnerability management tools when they implemented Taegis VDR.

Modeling and assumptions. To calculate the value of this benefit for the composite organization, Forrester assumes the following the cost of its previous software was 10% higher than the cost of licensing Taegis VDR.

Risks. Risks that could impact the realization of this benefit include the amount of cybersecurity software the organization can eliminate for cost savings.

"Our previous solution provided inconsistent results and would bombard us with security information. [Taegis VDR] provides us with what we need to know about the threat landscape. We are more confident with [Secureworks] as our security partner."

IT manager, construction services

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $46,000.

Deprecated Security Software Savings And Associated Service And Support					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Licensing reduction of eliminated software and associated service and support	Interviews	$19,500	$19,500	$19,500
Bt	Deprecated security software savings and associated service and support	B1	$19,500	$19,500	$19,500
	Risk adjustment	↓5%			
Btr	Deprecated security software savings and associated service and support (risk-adjusted)		$18,525	$18,525	$18,525
	Three-year total: $55,575		**Three-year present value: $46,069**		

SECURITY TEAM LABOR SAVINGS DUE TO REDUCED VULNERABILITY TRACKING, MONITORING, AND RESEARCH

Evidence and data. Interviewees shared that their organizations' cybersecurity teams now spend less time researching the security-vulnerability landscape, identifying vulnerabilities within their infrastructures, studying identified vulnerabilities, prioritizing patching and remediation efforts, and communicating requirements for patching and remediation to IT ops. The global IT director at a manufacturer shared: "We no longer have to spend days reading about stuff, researching potential impact, and doing additional work. [Taegis] VDR provides a risk-based assessment of our organization, not a generic one."

Modeling and assumptions. To calculate the value of this benefit for the composite organization, Forrester assumes the following:

- The vulnerability tracking, monitoring, and research labor savings for the composite's cybersecurity team totals 25% of an FTE.
- The fully burdened labor cost of a security team member is $131,000 per year.

Risks. Risks that could impact the realization of this benefit include:

- The maturity of the organization's existing security architecture and capabilities.
- The size and cost of the organization's security team.
- The maturity of the organization's security team.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $69,200.

Security Team Labor Savings Due To Reduced Vulnerability Tracking, Monitoring, And Research					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	FTE labor savings per day due to reduced vulnerability tracking, monitoring and research	Interviews	25%	25%	25%
C2	Average annual fully loaded security analyst cost	TEI standard	$131,000	$131,000	$131,000
Ct	Security team labor savings due to reduced vulnerability tracking, monitoring, and research	C1*C2	$32,750	$32,750	$32,750
	Risk adjustment	↓15%			
Ctr	Security team labor savings due to reduced vulnerability tracking, monitoring, and research (risk-adjusted)		$27,838	$27,838	$27,838
	Three-year total: $83,513			**Three-year present value: $69,228**	

IT OPS LABOR SAVINGS DUE TO PRIORITIZED PATCHING

Evidence and data. Interviewees shared that Taegis VDR allowed their organizations to focus on higher-risk vulnerabilities that threaten critical pathways.

- Interviewees said their organization save time on patching activities because Taegis VDR identifies vulnerabilities and provides explanations of the severity so that only vulnerabilities of significance are prioritized to be patched and remediated. The information security offer at a pharmaceutical organization shared: "We only provide the IT admins with a remediation list [of items] that we have identified as important. We share the issues and the explanation of the criticality. The workload is less while our protection is better."
- Interviewees said post-patching scans validate that an issue is resolved without requiring manual validation effort.

Modeling and assumptions. To calculate the value of this benefit for the composite organization, Forrester assumes the following:

- The IT ops labor savings due to prioritized patching totals 50% of an FTE.
- The fully burdened labor cost of a security team member is $90,000 per year.

Risks. Risks that could impact the realization of this benefit include:

- The amount of patching the organization requires for nonsecurity-related purposes.
- Labor costs, which may vary.

> **"Secureworks provides justification for taking remediation actions, including showing what the possible impact would be if we don't fix an issue. It even provides links to articles on vulnerabilities. It saves us time on getting the information that you need to decide what to do."**
>
> *Security analyst, manufacturing and retail*

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $106,300.

IT Ops Labor Savings Due To Prioritized Patching

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	FTE labor savings from reduced patching due to Taegis VDR prioritization	Interviews	50%	50%	50%
D2	Average annual fully loaded cost of an IT ops FTE	TEI standard	$90,000	$90,000	$90,000
Dt	IT ops labor savings due to prioritized patching	D1*D2	$45,000	$45,000	$45,000
	Risk adjustment	↓5%			
Dtr	IT ops labor savings due to prioritized patching (risk-adjusted)		$42,750	$42,750	$42,750
	Three-year total: $128,250			**Three-year present value: $106,313**	

RESOURCE COST SAVINGS DUE TO FINDING UNUSED ASSETS

Evidence and data. Interviewees shared that their organizations identified untracked assets by using Taegis VDR's asset-discovery capabilities and that they were able to retire or repurpose resources that were not used. The information security offer at a pharmaceutical organization shared: "You can't address asset vulnerability if you don't even know it is there. Secureworks identified assets that we weren't aware of — 10% more than we had known [about] before."

Modeling and assumptions. To calculate the value of this benefit for the composite organization, Forrester assumes the composite reduces resource costs by $5,000 in Year 1, by $6,000 in Year 2, and by $7,200 in Year 3.

Risks. Risks that could impact the realization of this benefit include the state of the organization's inventory tracking and discovery prior to using Taegis VDR.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $11,900.

Resource Cost Savings Due To Finding Unused Assets

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Deprecating unused assets identified via asset-discovery activities	Interviews	$5,000	$6,000	$7,200
Et	Resource cost savings due to finding unused assets	E1	$5,000	$6,000	$7,200
	Risk adjustment	↓20%			
Etr	Resource cost savings due to finding unused assets (risk-adjusted)		$4,000	$4,800	$5,760
	Three-year total: $14,560			**Three-year present value: $11,931**	

UNQUANTIFIED BENEFITS

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

- **Improved team comfort level and employee satisfaction.** Members of cybersecurity teams are confident that they are very effective at reducing the likelihood of a breach and the cost of a breach if one were to occur. IT ops team members are happier because they recognize that the patching assignments reduce the likelihood of a breach.
- **Increased confidence to the corporate board level.** Interviewees shared that interest in cybersecurity has risen to the board level. They said they present Taegis VDR dashboards and reports to their corporate boards and even explain risk gaps and risk mitigation activities to them.
- **Reduction in penetration testing.** Interviewees from organizations that do penetration testing said they are evaluating whether they can do less penetration testing while meeting regulatory and internal audit requirements and without increasing risk.
- **Reduction in remediation that is disruptive to the business.** Interviewees shared that Taegis VDR provides prioritization and explanations that support making better timing decisions about patching activities. The organizations can schedule less-critical patching at less-disruptive times.
- **Merger and acquisition evaluation.** Interviewees shared that their organizations implemented Taegis VDR on acquired organizations' networks and remediated vulnerabilities before integrations occurred.
- **Having a business partner.** Interviewees shared that their organizations' Secureworks teams are there for them. They said the teams hold monthly advisory meetings and typically provide knowledgeable feedback to questions in less than an hour.

> **"With Secureworks we built a complete asset inventory including device type, model ID, firmware, etc. We now control virtual machine creep [and identify] servers in our cloud environment that aren't used."**
>
> *Security analyst, manufacturing and retail*

FLEXIBILITY

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

- **Having the ability to flexibly schedule subnets, remediation validations, etc.** Interviewees shared that it is very easy to schedule scans within Taegis VDR.
- **Having Taegis VDR asset-tag assignments as well as security team assignments.** Taegis VDR sets asset tags based on its self-learnings, but interviewees shared that their organizations' cybersecurity teams make asset-tag assignments based on their priorities.

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

Voice Of The Customer

"With Secureworks we are comfortable that we have done as much as we absolutely can to mitigate threats. We're in a nice place even knowing that the bad people continue to get better at being bad. I sleep better now."
– Global IT director, manufacturing

"Secureworks invested a lot of time and effort up front to prove that they are best in class. They showed that they are professional, knowledgeable, and well-connected. [Secureworks is] a real player in the security community."
– IT manager, construction services

"I don't see Secureworks as a vendor, but as a business partner. They are advisors. Their people genuinely care about our security level."
– Information security officer, pharmaceutical

"Early on, Taegis VDR wasn't fully trusted [by my organization's IT ops]. As time has gone by, they [have realized] that configuration issues are getting caught and critical pathways are better protected."
– Security analyst, manufacturing and retail

"We acquired a company and ran Secureworks before integrating [it] into our network. We then completed the necessary work to integrate [it] in safely."
– Information security officer, pharmaceutical

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 and licensing costs	$8,250	$42,900	$42,900	$42,900	$136,950	$114,936
	Total costs (risk-adjusted)	$8,250	$42,900	$42,900	$42,900	$136,950	$114,936

IMPLEMENTATION AND LICENSING COSTS

Evidence and data. Interviewees said implementation and training for Taegis VDR was fast, simple, and informative. Licensing was understood and generally less expensive than deprecated components.

Modeling and assumptions. To calculate the value of these costs for the composite organization, Forrester assumes the following:

- The composite agrees to a three-year term with standard pricing based on 2,500 endpoints.
- The composite's initial costs represent labor costs for planning, implementation, and training.

Risks. Risks that could impact the realization of these costs include:

- The organization's licensing costs, which may vary based on licensing terms including volume discounts.
- Implementation effort, which may vary based on the organization' readiness and the complexity of its technical and operational environments.

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 $115,000.

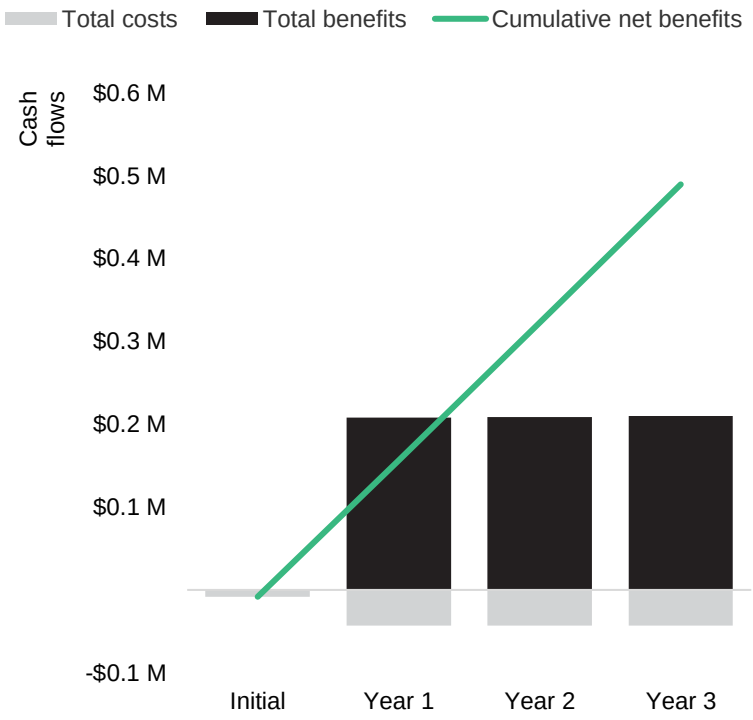
> **"A colleague described the actual implementation as hitting enter, then it is done. It is that easy."**
>
> *Information security officer, pharmaceutical*

Implementation And Licensing Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Implementation and licensing costs	Composite	$7,500	$39,000	$39,000	$39,000
Ft	Implementation and licensing costs	F1	$7,500	$39,000	$39,000	$39,000
	Risk adjustment	↑10%				
Ftr	Implementation and licensing costs (risk-adjusted)		$8,250	$42,900	$42,900	$42,900
	Three-year total: $136,950			**Three-year present value: $114,936**		

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	($8,250)	($42,900)	($42,900)	($42,900)	($136,950)	($114,936)
Total benefits	$0	$207,960	$208,760	$209,720	$626,439	$519,149
Net benefits	($8,250)	$165,060	$165,860	$166,820	$489,489	$404,213
ROI						352%
Payback						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Endnotes

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

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

[3] Ibid.


FORRESTER®