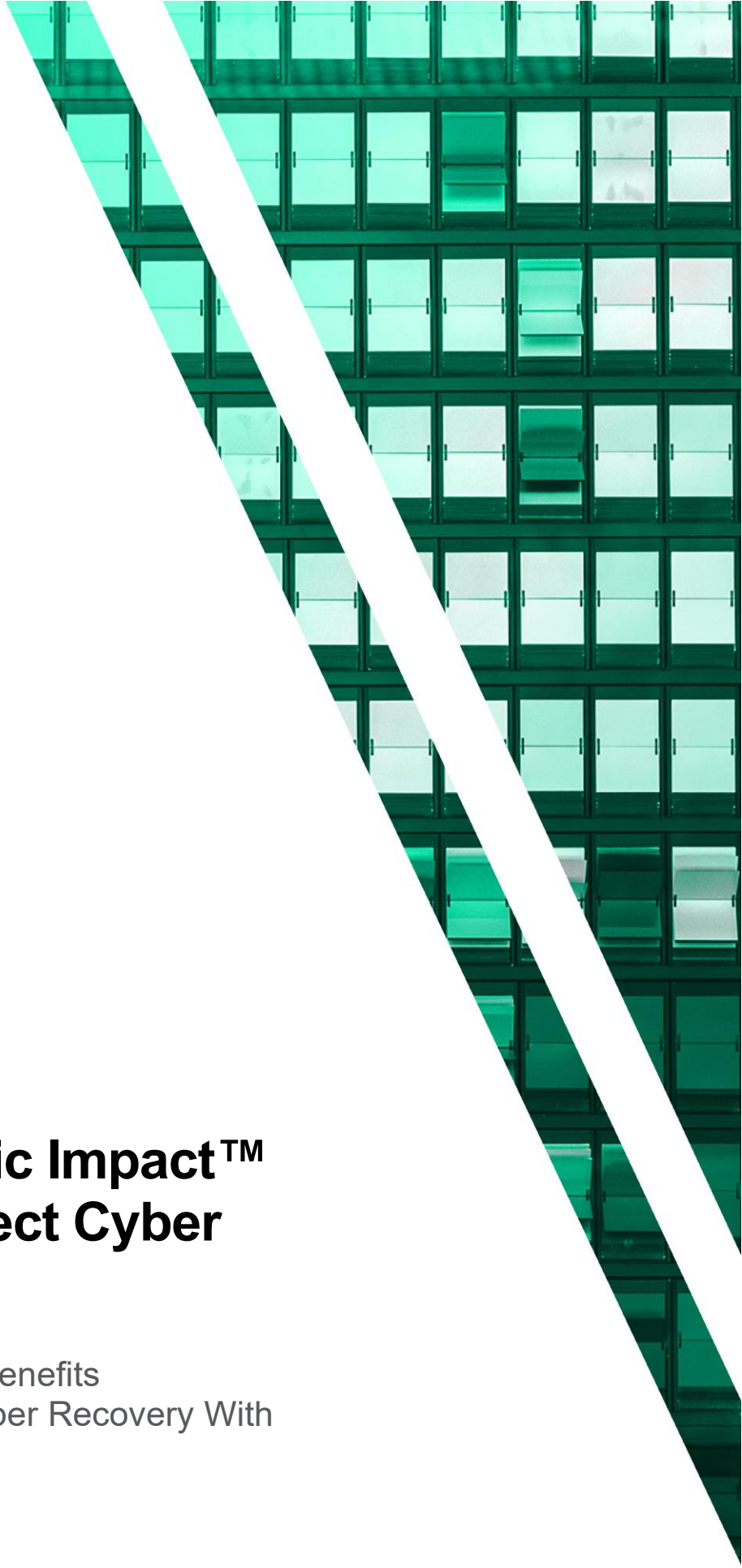
FORRESTER®



The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery

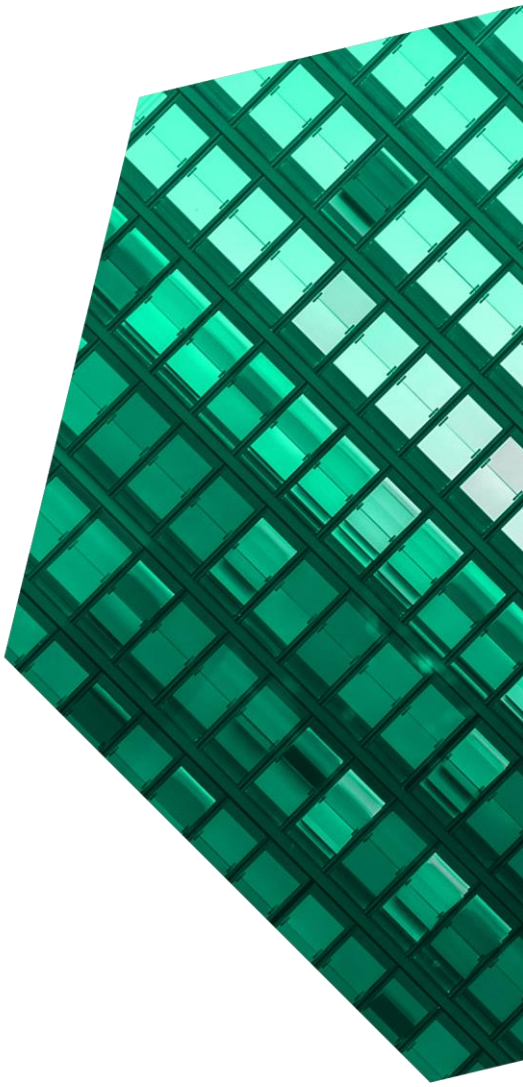
Cost Savings And Business Benefits Enabled By PowerProtect Cyber Recovery With CyberSense

AUGUST 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY DELL

Table Of Contents

Consulting Team: Elizabeth Preston
Jonny Cook



ABOUT FORRESTER CONSULTING

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

Executive Summary

Since 2020, the frequency of ransomware attacks has increased threefold, and the severity and sophistication of those attacks is also on the rise. When one hits, it can cripple an organization, and recovery can be time-consuming, costly, and even incomplete. The best insurance policy against an attack is a thorough cyber resilience strategy so you know your backups are valid and can be restored when needed.[1,2]

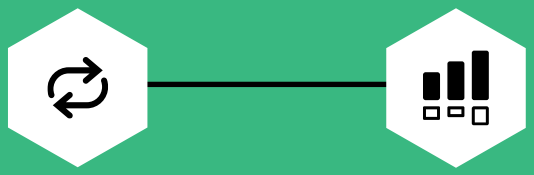
Dell's PowerProtect Cyber Recovery vault allows organizations to create immutable backups and store them in an isolated vault, enabling recovery of critical data and systems after a cyber attack in the event that standard backups are impacted. CyberSense works within the vault to scan backups for corruption or infiltration, providing an additional layer of support for faster, effective data recovery.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives with experience using PowerProtect Cyber Recovery. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a regional public sector organization with 1,500 employees, 200,000 constituents, and an annual budget of $500 million.

Prior to using PowerProtect Cyber Recovery, the interviewees' organizations had traditional recovery and backup systems in place. These systems were often costly, but they still did not inspire confidence they would mitigate the potential downtime and loss from situations such as ransomware attacks. While the organizations kept backups of their data in these systems, the systems were live and online. This made them vulnerable to backup-impacting events such as ransomware attacks that threatened significant losses.

KEY STATISTICS



Return on investment (ROI)
53%

Net present value (NPV)
$160K

To mitigate these concerns, interviewees looked for a solution that would help guarantee the resilience of their organizations in the face of a ransomware attack. They wanted to be able to access their backup data quickly and confidently, so they looked for a solution that could easily integrate with their existing backup systems and that they could trust. Ultimately, the interviewees chose to deploy PowerProtect Cyber Recovery on-premises. With PowerProtect Cyber Recovery, their organizations experienced faster data recovery and reduced downtime in the face of ransomware attacks. This contributed to a decrease in lost productivity and lost business as a result of attacks.

KEY FINDINGS

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

- **Reduction of time spent on data recovery by 80%.** With PowerProtect Cyber Recovery, the composite organization recovers its data with 80% less effort following a ransomware attack. Backup and recovery teams spend less time locating the data to restore and reimaging machining and data. Over three years, this reduction in recovery time is worth just less than $63,000 to the composite organization.
- **Reduction of system downtime by 75%, which reduces productivity loss.** When experiencing a ransomware attack, the composite restores its data and gets its systems back online 75% faster with PowerProtect Cyber Recovery than it could before. This dramatically reduces the disruption in employee productivity due to an attack, and it delivers almost $82,000 in regained employee productivity for the composite over three years.
- **A reduction in lost business due to downtime.** Because the composite organization recovers its data faster and reduces its downtime by 75% with PowerProtect Cyber Recovery, it experiences less business disruption, less impact to sales or service provision, and less negative publicity that might affect its brand reputation. Over three years, this reduction in lost business saves the composite organization $35,700.

Percent reduction in hours spent on recovery:

80%

- **Legacy environment savings of more than $282,000.** The composite organization retires previous backup storage when it invests in PowerProtect Cyber Recovery, and it saves the cost of the hardware and associated maintenance.

> **"Data is the value for any organization. If the organization loses its data, there's no value for the organization."**
>
> *Network administrator, local government*

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

- **Insurance savings.** Having the PowerProtect Cyber Recovery vault in place lowers the insurance risk for the composite and protects it from prohibitive insurance pricing aimed at organizations that don't have such systems.
- **Resiliency mindset and resiliency in other areas of the business.** Adopting the PowerProtect Cyber Recovery vault and CyberSense increases the organization's resilience maturity. Knowing this, the organization modernizes its thinking about future security and resilience decisions and investments.
- **Easier and faster audits.** With PowerProtect Cyber Recovery, the composite organization can prepare for audits more quickly and easily pass initial recovery checks during an audit.
- **Employee reassurance and confidence.** Employees knowing their data is secure in the

PowerProtect Cyber Recovery vault improves their peace of mind while working.

- **Dell partnership.** Interviewees who worked with Dell are confident in Dell's expertise and the quality of its solutions.
- **Early, proactive scanning with CyberSense.** CyberSense monitors backups to search for malicious activity and validates that the data is not compromised. The composite organization uses CyberSense to easily confirm that backups are safe and to find out where malicious activity comes from in order to mitigate damage before it becomes excessively costly.

"It's like having fire insurance. You carry it, and you don't realize how important and how valuable it is [or] what your return on investment is until you have to rebuild your home."

CISO, local government

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

- **Implementation, hardware, software, and three years of support totaling $184,000.** The composite organization pays $167,000 upfront for a three-year contract that includes hardware, software, and implementation support.
- **Internal implementation and ongoing management labor totaling $119,000 over three years.** The composite organization dedicates 30% of the efforts of four employees in infrastructure and systems engineering to its PowerProtect Cyber Recovery deployment for four months. After implementation, one dedicated resource spends 20% of their time on the ongoing management and testing of PowerProtect Cyber Recovery.

The representative interviews and financial analysis found that a composite organization experiences benefits of $463,000 over three years versus costs of $303,000, adding up to a net present value (NPV) of $160,000 and an ROI of 53%.

"The cost [of PowerProtect Cyber Recovery] is pennies compared to what we would be spending if we were down for even a week. The value is nothing compared to what we would be spending if we would get hit."

Network administrator, local government

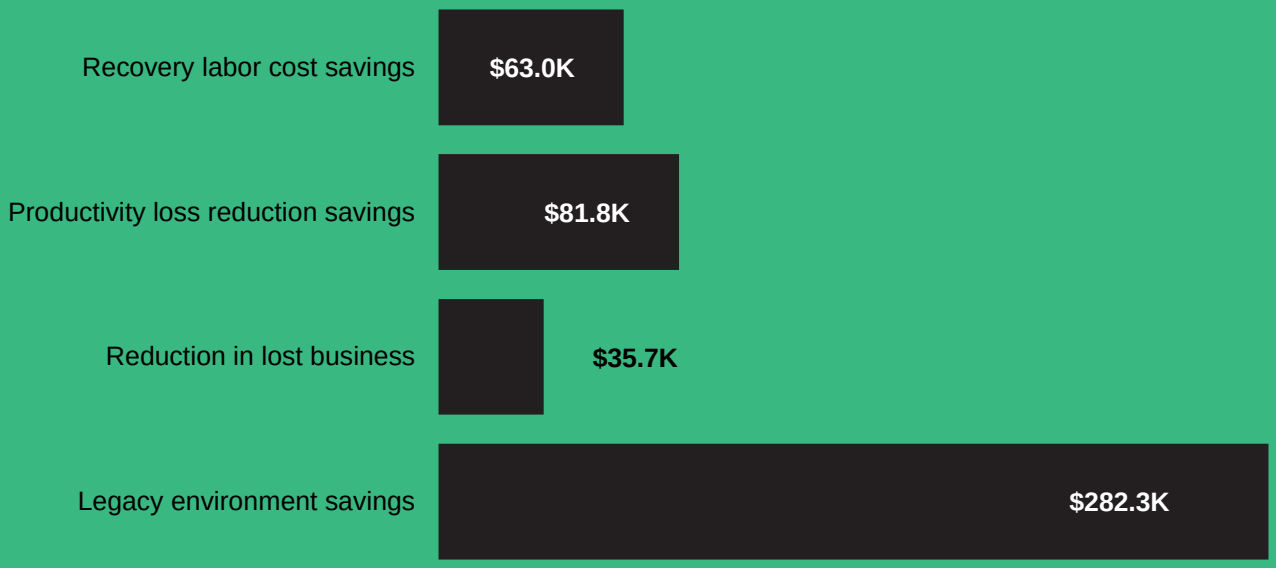
ROI
53%

BENEFITS PV
$463K

NPV
$160K

PAYBACK
18 months

Benefits (Three-Year)



“When you can go back to something like a vault that’s unaffected [and] immutable, those payloads are identified if you get CyberSense. You just save so much time and money. It’s unbelievable.”

— Solutions architect, public 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 Dell PowerProtect Cyber Recovery.

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 PowerProtect Cyber Recovery 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 Dell stakeholders and Forrester analysts to gather data relative to PowerProtect Cyber Recovery.

INTERVIEWS

Interviewed five representatives at organizations using PowerProtect Cyber Recovery 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 Dell PowerProtect Cyber Recovery Customer Journey

Drivers leading to the PowerProtect Cyber Recovery investment

Interviews				
Role	**Industry**	**Annual revenue/budget**	**Number of employees**	**Number of customers/constituents**
Network administrator	Local government	$150 million	1,000	88,000
Senior vice president (SVP) of IT	Financial services	$265 million	750	250,000
Chief information security officer (CISO)	Local government	$1 billion	1,800	281,000
Solutions architect	Public education	$115 million	1,500	10,000
IT infrastructure manager	Government agency	N/A	1,300	N/A

KEY CHALLENGES

Most of the interviewees' organizations had a traditional recovery system in place before investing in PowerProtect Cyber Recovery. While they backed up their data, the backup systems were often still on a network and therefore vulnerable. With their traditional backup recovery systems, they faced several challenges, including:

- **High overhead costs from disjointed backup and recovery solutions.** Some of the interviewees' organizations had multiple or duplicative backup systems implemented, which inflated software and hardware costs. A CISO in local government called their organization's security stack "exceptionally thick." They said: "[Our] biggest challenge was trying to winnow that security stack down and find the appropriate business partners that could take us to the next level, provide the bang for the buck that we were looking for, and fill the missing gaps that existed within the overall security framework."
- **Slow and costly recovery from ransomware attacks.** The solutions architect for a public education organization explained that their school district was hit by a ransomware attack that fully shut down its systems while implementing its existing backup systems. All its data was encrypted on a shared cluster, and it incurred significant time and monetary costs to get its internet and systems back up and running.

> **"We didn't want to be in the paper as an organization that was down [for] weeks or months because we had no data because we were wiped out."**
>
> *Network administrator, local government*

- **Vulnerability to backup-impacting events.** Without on-premises, air gapped, and isolated backups, backup-impacting events could limit the recovery of backup data and lead to total data loss for the organization. A network administrator at a local government noted that they felt a backup-impacting breach was an inevitability, and they said, "It's your fault if you didn't do

everything you could to prevent [the breach impacting backups]."

- **Outdated systems for a changing regulatory and insurance environment.** The CISO at a local government noted that while their organization had traditional backups, they wouldn't necessarily know at any given time whether a good backup was available. As ransomware attacks advance and insurance policies and regulations evolve with technological advances, the interviewees' organizations wanted to be in the best possible position to adhere to federal mandates and respond to threats.

"We started looking at products that would help us in that resiliency area, and the Dell PowerProtect system was best in class."

CISO, local government

INVESTMENT OBJECTIVES

The interviewees said their organizations often began to search for a new backup and recovery system when they watched other local businesses or municipalities suffer ransomware attacks. The interviewees knew their organizations could face a similar threat, and they wanted to implement best practices beforehand and take the actions they believed would have helped their counterpart organizations better handle attacks. Interviewees searched for a solution that would:

- **Provide a secure, isolated vault to guarantee resilience.** Interviewees wanted to ensure their ability to recover key information in the event of a major data loss event that could affect traditional backups, knowing that preventing every single attack was unlikely. The SVP of IT at a financial services organization told Forrester: "We wanted to make sure we had that information isolated, protected even further, because that's really your only saving grace, your backups and the integrity of those backups." The local government CISO said that Dell stood out because their air-gapped capability was somewhat unique among the vendors they evaluated.
- **Deliver backup data quickly.** The ability to recover backup data at all was critical for interviewees' organizations, but it was also important that they could recover backup data within a reasonable amount of time. IT employees didn't want to spend hours figuring out what they needed and how to access it before they could bring data back online.

"Our biggest concern is just making sure that our data is protected and can be recovered in the event of any type of incident, whether it be a disaster or cyber event, and having that assurance that the data is protected and available when needed."

SVP of IT, financial services

- **Easily integrate with existing backup systems.** Some interviewees' organizations used Avamar, Dell's in-production backup solution, or other Dell recovery systems. The ease of those systems' integration with PowerProtect Cyber Recovery and the options that a unified security solution provided made PowerProtect Cyber Recovery an attractive option.
- **Be supported by a partner their organization could trust.** The interviewees from organizations that already worked with Dell described a strong sense of trust and partnership with Dell. The CISO for a local government said Dell offers solutions with unique capabilities, and the IT infrastructure manager at a government agency said Dell's approach to cyber resilience compared to alternatives gave them additional confidence in Dell as a partner.

After evaluating multiple vendors, the interviewees' organizations chose PowerProtect Cyber Recovery and began deployment.

- Most of the interviewees' organizations opted for an on-premises instance of PowerProtect Cyber Recovery that was physically separate from most other security systems and operations, which reduced access and overall exposure to risk.

"If our backups get wiped out, we have an option to restore from something that attackers can't see."

Network administrator, local government

"If we got taken out overnight [and] the big one hit, how would we rebuild our services essentially in the next day and get those services stood back up quickly and efficiently and make sure that the data that we needed to get those solutions back into place was available to us with a level of immediacy? That was the approach that we were supposed to take in taking on the Cyber Recovery Vault."

CISO, local government

- Some interviewees' organizations backed up all of their data by replicating everything from traditional backups. Others chose only to use the PowerProtect Cyber Recovery vault for business-critical data to keep storage size minimal.
- The organizations could choose how often their data was backed up and how long it was retained after a backup, with most opting for a retention period between two and five weeks.
- Four out of the five interviewees' organizations used CyberSense, which integrates directly with PowerProtect Cyber Recovery. CyberSense works in the vault to monitor backups and detect corruption of data due to ransomware attacks without opening the backups themselves. CyberSense helps organizations understand when an attack occurs and speeds the recovery process by providing insights into where and how corruption takes place.

COMPOSITE ORGANIZATION

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

The composite organization has the following characteristics:

Description of composite. The composite organization has 1,500 employees and 200,000 constituents with an operating budget of $500 million. Before using PowerProtect Cyber Recovery, the organization had a disaster recovery backup system in place, but it did not have an isolated recovery vault. The composite organization is based on interviews with representatives of public sector organizations and one financial services organization, so benefits are modeled accordingly. However, benefit categories and frameworks are relevant for all industries.

Deployment characteristics. The composite organization deploys PowerProtect Cyber Recovery on-premises. It stores 50 terabytes (TB) of data in the vault, which includes its mission-critical data along with some additional high-value data backups. The organization backs up the data in regular intervals, which minimizes the solution's period of vulnerability.

"The fact that we had CyberSense that could run on top of [Cyber Recovery] to give us analytics that would tell us the health status of our data was something that nobody else could compare to."

CISO, local government

Key Assumptions

- **Public sector organization**
- **$500 million budget**
- **1,500 employees**
- **200,000 constituents**

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	Recovery labor cost savings	$25,323	$25,323	$25,323	$75,970	$62,975
Btr	Reduced productivity loss	$32,896	$32,896	$32,896	$98,688	$81,808
Ctr	Reduction in lost business	$14,364	$14,364	$14,364	$43,092	$35,721
Dtr	Legacy environment savings	$122,076	$108,576	$108,576	$339,228	$282,285
	Total benefits (risk-adjusted)	$194,659	$181,159	$181,159	$556,978	$462,789

RECOVERY LABOR COST SAVINGS

Evidence and data. Interviewees reported that with PowerProtect Cyber Recovery, their organizations recovered their data more quickly following ransomware attacks. Their organizations spent less time reimaging data and rebuilding surfaces and tools, and it was easier and faster for them to locate the data they wanted to restore and ensure that it was a recent and safe copy of the data.

- Without PowerProtect Cyber Recovery, interviewees' organizations that were hit by ransomware attacks hired lawyers, negotiators, and external recovery teams to try to get their data back from downed systems or malicious parties. Recovery timelines were weeks rather than days or hours. The local government CISO spoke of a school district in their city's greater metropolitan area that weathered a ransomware attack without a resiliency solution in place. They said: "When it came to recovering their mission-critical systems, they couldn't do it. … A recovery that should have taken them a couple of days took them the better part of a month."
- The solutions architect for the public education organization described an incident in which their district was hit by an attack before it used PowerProtect Cyber Recovery. Fifteen people from the school's IT team spent more than 1,000 hours of time for initial data recovery, including the reimaging of 7,000 devices. The district's insurance paid $250,000 for external employee costs. And although its email was back within a few days, the majority of systems took more than a week to return to normal business operations.

> **"[CyberSense] knocks a lot off of up-front research in determining what's a good backup and point of recovery."**
>
> *SVP of IT, financial services*

- The same interviewee said their public education organization experienced another attack after it started utilizing the Cyber Recovery vault. The organization experienced efficiencies in locating the data it wanted to restore to, ensuring the data was clean, and restoring the data to its physical system. Ultimately, it was able to restore the data

it needed within a couple of business hours, with a total of 20 to 22 hours of effort spent between its network system administrator, IT director, and a partner.

- The IT infrastructure manager at a government agency told Forrester that a small attack at their organization before using PowerProtect Cyber Recovery required three to four employees working to retrieve data for a few hours, plus another 3 to 4 hours to rebuild surfaces. After implementing the vault, the organization experienced another event in which it had to cut the connection between its servers and the production layer. It retrieved the surface immediately, and only one person spent a few hours to retrieve and verify the data and switch the business to a new server.
- CyberSense helped interviewees' organizations quickly determine which backup was the most recent unharmed version by regularly scanning backups for signs of malicious activity. The CISO at a local government noted that if their organization were to be hit by a ransomware attack without CyberSense and the vault, it wouldn't immediately know the steps towards data recovery. They said, "We would have to sift through all of our data to determine which mission-critical data needed to be recovered first."

  With CyberSense, interviewees' organizations spent less time trying to determine what data might have been compromised, and they could feel confident in immediately starting a reversion to a backup that CyberSense had determined to be safe. The SVP of IT at a financial services firm explained: "[CyberSense] shows you your last good backup or on your last scan that nothing was detected and this one looks good. And then you can do the instant recovery on the data domain just to make sure that the data that you're looking for is there. … CyberSense helps you make that determination a lot sooner."

Modeling and assumptions. Forrester modeled the impact for the composite organization based on the following assumptions:

- The composite organization experiences 0.38 material breaches per year from ransomware, or one breach every 2.63 years.
- In the event of a ransomware attack, the composite organization hires a third-party recovery team to aid with data recovery.
- On average, the third-party recovery team spends 200 hours recovering the data at a rate of $200 per hour.
- When the composite organization experiences a ransomware breach, its internal security and infrastructure employees each spend an average of 1,000 hours on data recovery.
- With PowerProtect Cyber Recovery, the amount of time both internal and external teams need to spend on data recovery when faced with a ransomware breach decreases by 80%.
- The fully burdened hourly salary of a security and infrastructure team member at the composite organization is $58.

Flexibility. Flexibility benefits may be viewed traditionally as future supplemental value enabled by longer-term added investments. But flexibility can also be applied to nearer-term benefits to identify relevant value and opportunities beyond what is financially measured in the benefit table to highlight different use cases, business models, industries, or IT maturities. For instance:

- Forrester's research reveals that of all types of material breaches, an average of about 20% are ransomware attacks.[4] But organizations in higher-risk industries, such as financial services, healthcare, life sciences, e-commerce, government, and others with high volumes of

personal data may see more than 0.38 ransomware attacks per year. Doubling the number to nearly 0.8 ransomware attacks per year could double the impact of this benefit.

- Organizations that rely more on third-party IT management and support services may expect higher costs related to recovery efforts. Forrester estimates that before the composite organization used Dell PowerProtect Cyber Recovery, it required 1,000 hours of internal resource time and 200 hours of more expensive third-party resource time to recover from a ransomware attack. But an organization leveraging more third-party services than internal resources could see even greater third-party management and support cost savings.
- The scale of an attack can greatly impact remediation efforts. An attack that impacts multiple geographic regions will require more time and resources to resolve. Estimated third-party and/or internal-resource hours could be much higher for global organizations.

Risks. The expected financial impact is subject to risks and variation based on factors including:

- The number of material breaches from ransomware the organization experiences per year.
- The organization's prior disaster recovery tools and data recovery processes.
- The scope and update frequency of the data protected with PowerProtect Cyber Recovery.
- Compensation amounts for employees and recapture rates of productivity on saved time.
- Whether or not the organization proactively utilizes CyberSense.

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 $63,000.

Recovery Labor Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Third-party time spent on data recovery processes (hours)	Composite	200	200	200
A2	Hourly rate for third-party recovery labor	Composite	$200	$200	$200
A3	Internal time spent on recovery by security and infrastructure teams (hours)	Composite	1,000	1,000	1,000
A4	Fully burdened hourly salary of a security professional	TEI standard	$58	$58	$58
A5	Material breaches from ransomware	Forrester research	0.38	0.38	0.38
A6	Reduction in time spent on recovery	Interviews	80%	80%	80%
At	Recovery labor cost savings	(A1*A2+A3*A4) *A5*A6	$29,792	$29,792	$29,792
	Risk adjustment	↓15%			
Atr	Recovery labor cost savings (risk-adjusted)		$25,323	$25,323	$25,323
	Three-year total: $75,970			**Three-year present value: $62,975**	

REDUCED PRODUCTIVITY LOSS

Evidence and data. When an organization experiences a ransomware attack, it often loses access to key systems and files, which disrupts business processes and impedes employees from doing their jobs. For the interviewees' organizations, restoring data and getting systems back online more quickly with PowerProtect Cyber Recovery reduced disruption to employee productivity associated with attacks.

- The network administrator in local government told Forrester: "When we got hit years ago, we were not with Dell backup at the time. So, we would have to restore from our latest backup point. Whatever was lost was lost, and that was that. If people had things saved in that 3-hour window [when] we didn't have a backup, they were out of luck. We couldn't do anything for them at all. … It could be hours' worth of productivity for a thousand people. It gets costly, and it gets to be a big-time waste."

Percentage reduction in downtime:

75%

- The solutions architect for the public education organization described extensive disruption for students and teachers for more than a week when their school experienced a ransomware attack without PowerProtect Cyber Recovery. They said: "There's wasted time with lack of productivity. … From the teacher's perspective, there's a lot of distractions during this time. … I think they dismissed school a couple of days early just from logistics. They had some logistical issues around communications they had to deal with. So, the first week was pretty crazy."

  With PowerProtect Cyber Recovery, the organization's systems were down for only a few hours, and they were back to business as usual by the end of the day.
- The IT infrastructure manager at a government agency also noted that a ransomware attack their organization experienced before using PowerProtect Cyber Recovery impacted almost every employee at the organization for a few hours. Employees lost their backup files, and rebuilding surfaces took another half a day. When the organization faced another suspicious event after implementing PowerProtect Cyber Recovery, its total recovery took 2 to 3 hours and did not affect employee productivity or business operations.
- The network administrator in local government noted that with an annual budget in the hundreds of millions, their organization operates on a budget of $600,000 to $800,000 per day. If its systems go down, it would be unable to deliver constituent services, but it would still face significant costs. The interviewee anticipated that data recovery would take one to two weeks with the PowerProtect Cyber Recovery vault, but months without it.

Modeling and assumptions. Forrester modeled the impact for the composite organization based on the following assumptions:

- The composite organization experiences 0.38 material breaches per year from ransomware, or one breach every 2.63 years.[5]
- In the event of a ransomware breach, all 1,500 employees at the composite organization lose out on 3 hours of productivity due to system downtime.[6]

- With PowerProtect Cyber Recovery, the amount of downtime the composite experiences due to a ransomware breach decreases by 75%.
- Each employee recaptures 50% of their saved time into productivity value.
- The fully burdened average hourly salary of an employee at the composite organization is $57.

Flexibility. Use cases and business models can again be considered for end-user productivity improvements as a result of reduced or avoided ransomware attacks. For example:

- Organizations with a larger percentage of highly skilled workers may consider using an increased average salary compared to what's modeled for the composite. Law firms, medical practices, financial organizations, and many tech companies likely have much higher hourly salaries than others such as government offices, brick-and-mortal retail, and others.
- As with the previous benefit, organizations that are at greater risk of ransomware attacks may estimate a greater number of ransomware attacks per year. This could significantly impact the amount of time employees spend dealing with delays, outages, and remediation.
- Organizations may also consider the additional costs of employee impact beyond resource time. A business that does not invest in proper planning and security will likely have more ad hoc issues — if not more major events — which can negatively impact employee engagement. Furthermore, public security failures can drive candidates away and increase hiring costs even more, which can further impact the business and quality by reducing overall employee skills and experience.

Risks. The expected financial impact is subject to risks and variation based on factors including:

- The number of material breaches from ransomware the experiences per year.
- The organization's prior disaster recovery tools and data recovery processes.
- The number of employees whose work is disrupted with downtime and how much that downtime affects each employee's productivity.
- The scope and update frequency of the data protected with PowerProtect Cyber Recovery.
- Compensation amounts for employees and recapture rates of productivity on saved time.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $81,800.

Reduced Productivity Loss					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Employees	Composite	1,500	1,500	1,500
B2	Business employee productivity time lost due to downtime (hours)	Forrester research	3	3	3
B3	Average fully burdened hourly salary of a business employee	TEI standard	$57	$57	$57
B4	Material breaches from ransomware	Forrester research	0.38	0.38	0.38
B5	Reduction in downtime with Dell PowerProtect Cyber Recovery	Interviews	75%	75%	75%
B6	Productivity recapture	TEI standard	50%	50%	50%
Bt	Reduced productivity loss	B1*B2*B3*B4*B5*B6	$36,551	$36,551	$36,551
	Risk adjustment	↓10%			
Btr	Reduced productivity loss (risk-adjusted)		$32,896	$32,896	$32,896
	Three-year total: $98,688		**Three-year present value: $81,808**		

REDUCTION IN LOST BUSINESS

Evidence and data. In addition to the time and labor costs organizations incur when responding to an event and lost productivity for employees when systems are down, firms that experience a breach often suffer a loss in revenue due to an inability to provide services or reputational damage that translates to increased customer churn and a need to rebuild brand equity. Organizations that can recover data faster and minimize their downtime experience less business disruption, a smaller impact to sales or service provision, and decreased chances of negative publicity or customer risk that affect their brands' reputations.

- The solutions architect for the public education organization said that before investing in the PowerProtect Cyber Recovery vault, their school district would completely lose basic functionality when its systems went down after an attack. They said: "[The district] couldn't access the internet [and couldn't] connect SIS [student information systems]. They couldn't process payroll. They couldn't do any of the normal functions that you would expect on a day-to-day [basis]."

> **"Every day that we're not open, we are losing revenue. If we're not providing services to the public, we could lose millions of dollars."**
>
> *CISO, local government*

- The local government CISO told Forrester, "The fact that we have the ability to do this recovery that much quicker [with PowerProtect Cyber Recovery] means that the potential to lose the confidence that the public … has in us is unlikely to happen the way it would [if we were] out of service for the better part of a month." They also noted that if their organization was unable to

provide services to constituents as expected, it would likely face fines in addition to loss of public trust.

Modeling and assumptions. Forrester modeled the impact for the composite organization based on the following assumptions:

- The composite organization experiences 0.38 material breaches per year from ransomware, or one breach every 2.63 years.[7]
- In the event of a ransomware breach, the composite organization loses $56,000 in revenue from direct business disruption and reputational damage.
- With PowerProtect Cyber Recovery, the amount of downtime the composite experiences due to a ransomware breach decreases by 75%.

Flexibility. The business impact of a ransomware attack can vary greatly across industries and even among similar businesses. Although Forrester modeled results for the composite organization, readers should consider the following:

- Organizations may also consider other cost savings. For example, government agencies and financial and healthcare organizations may see significant fines or penalties from an attack.
- Organizations in industries with high volumes of data, greater reliance on technology, a focus on online delivery, and/or a high usage of personally identifiable information may expect significantly higher losses. For example, if a pharmaceutical company was hit with a successful ransomware attack, it could find the whole business at risk of folding. Similarly, a retail firm could see years of significant losses in profit and eroded customer trust, a healthcare organization could put lives at risk, and a manufacturer that leverages IoT devices for actionable insight may lose its competitive advantage.

For example, a $10 billion business has an unweighted average of about $1.1 million per hour every day of the year, but most businesses will have much higher averages during peak hours and even greater ones during key events and seasons, such as Black Friday and the holiday season. Being the victim of a ransomware attack during these periods — which is not an unlikely assumption considering bad actors try to target organizations during critical times — could mean lost profits of hundreds of thousands or millions of dollars per hour.

> **“If we got hit and our hosts [went] down and all of our servers were deleted, we would have a very hard time running [emergency dispatch services]. … We have a jail. We have a health facility that has Alzheimer’s patients, elderly patients, and brain injury patients. … If we got hit, it would affect constituents absolutely.”**
>
> *Network administrator, local government*

Risks. The expected financial impact is subject to risks and variation based on factors including:

- The number of material breaches from ransomware the organization experiences per year.
- The organization’s prior disaster recovery tools and data recovery processes.
- The organization’s total revenue and business model, including the percentage of customer-

generated revenue, customer retention rates, and brand equity.

- Susceptibility to lost business from downtime and reputational damage from a material breach.
- The scope and update frequency of data protected with PowerProtect Cyber Recovery.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $35,700.

Reduction In Lost Business

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Lost business from downtime	Composite	$56,000	$56,000	$56,000
C2	Material breaches from ransomware	Forrester research	0.38	0.38	0.38
C3	Reduction in downtime with Dell PowerProtect Cyber Recovery	Interviews	75%	75%	75%
Ct	Reduction in lost business	C1*C2*C3	$15,960	$15,960	$15,960
	Risk adjustment	↓10%			
Ctr	Reduction in lost business (risk-adjusted)		$14,364	$14,364	$14,364
	Three-year total: $43,092		**Three-year present value: $35,721**		

LEGACY ENVIRONMENT SAVINGS

Evidence and data. Alongside labor savings during recovery, interviewees said their organizations were able to reduce capital expenditures related to hardware, maintenance, and off-site storage.

- The IT infrastructure manager at a government agency estimated that their organization reduced its hardware costs and overhead by between one and two full-time equivalent (FTE) employees by retiring backup storage solutions.
- The CISO at a local government said their organization also experienced hardware and software savings when it retired two different backup solutions. They estimated direct savings in the tens of thousands to hundreds of thousands of dollars. In addition, they noted that the labor required to manage their organization's backup solutions went from two to three engineers to just 20% of one person's time. The CISO said, "It has definitely made life much easier on the engineers who were responsible for administering the backups and validating that our data is recoverable. … We put into place solutions that look after themselves for the most part."

Modeling and assumptions. Forrester modeled the impact for the composite organization based on the following assumptions:

- The composite organization previously utilized another on-premises backup solution that cost $15,000.
- One IT FTE is dedicated to maintenance of this legacy system at a fully burdened annual cost of $120,640 (or an hourly cost of $58).
- When the composite organization switches to PowerProtect Cyber Recovery, it retires its previous solution and the associated hardware and maintenance labor at the start of Year 1.

Flexibility. Legacy cost savings are straightforward, but some organizations including those that fit into Forrester's "modern" or "future-fit" IT maturity categories may want to consider the value of reinvesting cost savings back into operations.[8] For example, a government organization may consider how cost savings can enable more services and/or increase public good. Private businesses could look to the value enabled by that reinvestment.

Forrester modeled that the composite organization saves more than $280,000 PV in legacy cost savings. In this study, the business case shows more than $460,000 in total benefits enabled by just over $300,000 in costs (PV over three years). If legacy software and hardware contracts can be ended quickly, the business case could also include a plan to reinvest that $280,000 in legacy cost savings (plus an additional $20,000) for the same total return, while requiring less saved cash for investment. Other organizations may not see legacy cost savings until later, but they can still open new opportunities for investment.

Risks. The expected financial impact is subject to risks and variation based on:

- The organization's previous expenditure on backup hardware or software and the level of associated maintenance.
- The organization's ability and willingness to immediately retire or reduce its reliance on legacy solutions.
- The burdened cost of IT employees.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $282,300.

Legacy Environment Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Retired hardware savings	Interviews	$15,000	$0	$0
D2	Time that IT professionals save on backup management and maintenance (hours)	Interviews	2,080	2,080	2,080
D3	Fully burdened hourly salary of an infrastructure professional	Composite	$58	$58	$58
Dt	Legacy environment savings	D1+D2*D3	$135,640	$120,640	$120,640
	Risk adjustment	↓10%			
Dtr	Legacy environment savings (risk-adjusted)		$122,076	$108,576	$108,576
	Three-year total: $339,228		**Three-year present value: $282,285**		

UNQUANTIFIED BENEFITS

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

- **Insurance savings.** The solutions architect for the public education organization told Forrester their school district avoided a 25% increase in insurance premiums by implementing the backups and vault, even though its insurance company had to pay out for a previous ransomware attack the organization experienced. They said, "We have seen other districts actually be denied insurance because they don't have secure backups or proper security in place."
- **Resiliency mindset and resiliency in other areas of the business.** The local government CISO told Forrester: "Now, because we have gone down that road [with Cyber Recovery for resilience], it has become front and center to almost everything we do now with solution selection. When we look at a product we're going to bring in, we make sure that there is some type of resiliency benefit involved with it now. Just making that one change made us take a strategic tact in how we were doing things and made sure we focused in on this new way of securing our systems and data in the long-term." The SVP of IT at the financial services organization said, "[Cyber Recovery] definitely took us past the baseline [maturity level in a third-party assessment] into a more mature and intermediate maturity level for cybersecurity."
- **Easier and faster audits**. The network administrator at a local government said that with PowerProtect Cyber Recovery, their organization saved 80 hours preparing for a one-time voluntary IRS audit. They also noted that during the audits, having the vault helped the organization quickly pass initial recovery checks. They said: "We've been through a number of audits this past year, and they asked about our backups and our retention. And we can tell them, 'Yeah, we have this retention. But we also have our vault.' That usually shuts down our conversation pretty quick like, 'Oh, okay. We're good.' It has helped in audits."
- **Employee reassurance and confidence**. Interviewees said having their organizations' data backed up with PowerProtect Cyber Recovery helped improve their peace of mind at work. The solutions architect for the public education organization mentioned: "To me, the vault is

sleep insurance. It makes me sleep like a baby at night because I don't have to worry about my data. So, the vault is an easy sell for me."

- **Dell partnership.** Interviewees who worked with Dell said they are confident in Dell's expertise and the quality of its solutions. The CISO in local government said, "[Having Dell as a] business partner [for security] … could take [my organization] to the next level."
- **Early, proactive scanning with CyberSense.** CyberSense monitors backups to search for malicious activity and validates that the data is not compromised. The solutions architect for the public education organization described: "The thing I like about CyberSense is the intelligence behind [it] and the crawling of the data, [and] going through the data set and looking for bad payloads, because they're there. A lot of times they'll sit there for months. And when you can identify them, and when they show up, you can be more proactive in your security measures." The interviewee noted their organization recently had malicious content show up in a scan, and it used CyberSense to find out where it came from so it could mitigate damage before it became excessively costly.

"The AI that drives CyberSense has definitely paid off for us. It's helped us identify things that don't need to be in there, helped us identify things that may be suspect, and to go back and get a different version of the data."

CISO, local government

FLEXIBILITY

Flexibility represents additional capability that could be turned into future business benefit, providing an organization with the right or the ability to engage in future initiatives but not the obligation to do so. The value of flexibility is unique to each customer. Scenarios in which a customer might implement PowerProtect Cyber Recovery and later realize additional uses and business opportunities include:

- **Preparation in the face of regulatory and insurance changes**. The SVP of IT at a financial services organization expressed that using a solution like PowerProtect Cyber Recovery could greatly benefit their organization in interactions with insurance companies and regulators. They said that cybersecurity insurance is starting to look for backup types like PowerProtect Cyber Recovery, and they speculated that insurance prices would become prohibitive or unavailable for organizations that don't have such systems. They said: "We don't have any requirements to actually have an air gap solution in place, but that has been added to [the] audit scope [of regulators] within the last couple of years. … It is something that they're looking for. They're making recommendations, and I see that coming in the near future."
- **Avoided organization and brand dissatisfaction**. By reducing the impact or completely avoiding malware and ransomware attacks and avoiding public regulatory and compliance issues, organizations can avoid hurting their companies' and brands' reputations. Negative brand events directly impact sales and require additional internal or external teams to work on PR and marketing recovery efforts.
- **Faster recovery and reduced downtime during breaches beyond the early years of deployment.** Whether their organization had already faced a ransomware breach with PowerProtect Cyber Recovery or not, nearly all

interviewees agreed that their firm would face malware and ransomware threats after the three-year analysis period regardless of whatever initial lines of security they set up. For them, having the PowerProtect Cyber Recovery vault in place is insurance against future attacks that could upend their businesses for weeks, and they are confident that it will greatly serve their organizations when they put it to use for active recovery. The CISO at a local government said: “I figure that we can reconstitute things with hardware availability within a day [or] maybe two without. If we went old school, it could take us several weeks.”

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**
Etr	Implementation fee, hardware, software, and three-year support cost	$183,700	$0	$0	$0	$183,700	$183,700
Ftr	Internal implementation and ongoing management costs	$53,080	$26,540	$26,540	$26,540	$132,700	$119,081
	Total costs (risk-adjusted)	$236,780	$26,540	$26,540	$26,540	$316,400	$302,781

IMPLEMENTATION FEE, HARDWARE, SOFTWARE, AND THREE-YEAR SUPPORT COST

Evidence and data. Interviewees' organizations signed three- to five-year contracts with Dell that included hardware, software, installation, and implementation support and services from Dell and/or a third-party partner.

- The CISO of a local government said their organization paid for hardware with a one-time upfront cost, but that it pays ongoing costs for CyberSense, Retention Lock, and recovery software.
- Vaults for the interviewees' organizations generally contained 35 to 65 TB of data.

Modeling and assumptions. Forrester modeled this cost based on the following:

- The composite organization pays $167,000 upfront for a three-year contract that includes hardware, software, and implementation support.
- Pricing may vary. Contact Dell for additional details.

Risks. The expected financial impact is subject to risks and variation based on factors including:

- The organization's amount of storage space.
- The organization's amount and type of data.
- The service contract selected.

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 $184,000.

"If [decision-makers] haven't felt the pain of what ransomware recovery looks like, they're a little hesitant to spend that money, but anybody who has been bitten by the ransomware bug, they don't blink an eye, they're like, 'Give it to me, I'm ready.'"

Solutions architect, public education

Implementation Fee, Hardware, Software, And Three-Year Support Cost						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Implementation fee, hardware, software, and three-year support cost	Interviews	$167,000			
Et	Implementation fee, hardware, software, and three-year support cost	E1	$167,000	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Implementation fee, hardware, software, and three-year support cost (risk-adjusted)		$183,700	$0	$0	$0
	Three-year total: $183,700		**Three-year present value: $183,700**			

INTERNAL IMPLEMENTATION AND ONGOING MANAGEMENT COSTS

Evidence and data. The interviewees' organizations incurred the following internal costs related to their investment in PowerProtect Cyber Recovery:

- **Internal implementation labor.** Interviewees described implementation processes of approximately four months, including planning, deployment, and testing.
    - This process involved two to three employees from IT and infrastructure teams as well as employees from network or compliance as needed. Employees started with planning sessions to determine backup content and retention periods and to implement policy development and security controls.
    - Most of the employees worked with Dell's vault deployment and professional services teams to help with both implementation decisions and actual hardware and software deployment, though some interviewees' organizations also brought in third-party consulting firms or partners. Representatives from Dell conducted some handover sessions to ensure employees understood the solutions and how to monitor the system and retrieve data.
    - After setup, the organizations worked internally and with Dell to conduct initial recovery testing and to adjust and revise backup parameters based on storage amounts and data intake windows.
- **Ongoing management and testing.** Most interviewees' organizations tapped just one or two employees from infrastructure and system engineering teams to run and validate

> **"Bringing in Dell to help us do the implementation and integration was key. … They can help you do it much quicker, much more efficiently, [and] get it done right. They train your people as the implementation and integration [are] going because they work hand-in-hand with those particular people."**
>
> *CISO, local government*

PowerProtect Cyber Recovery on an ongoing basis. The number of employees with access to the vault was deliberately limited to use as few access points as possible. Ongoing management includes daily health checks to ensure data replication is working plus monthly and quarterly recovery testing. Quarterly testing time ranges from one day up to two weeks to test everything with an application-by-application or surface-by-surface approach.

Modeling and assumptions. Forrester modeled this cost based on the following information:

- The composite dedicates 30% of the time of four infrastructure and system engineering employees to PowerProtect Cyber Recovery deployment for four months.
- One dedicated resource spends 20% of their time on the ongoing management and testing of PowerProtect Cyber Recovery.
- The average fully burdened monthly salary of an internal resource who supports implementation and ongoing management is $10,053.

Risks. The expected financial impact is subject to risks and variation based on factors that may increase costs or extend deployment, including:

- The organization's scope of deployment, legacy technology landscape, maturity of existing processes, and level of change management needed to deploy PowerProtect Cyber Recovery.
- The organization's unique organizational requirements, processes, or technology complexities that can limit or lengthen implementation (e.g., regional regulatory demands, specific integrations, high data access and protection requirements).
- The number, expertise, and skill sets of the organization's existing employees and internal deployment teams.
- The burdened cost for each employee who participates in PowerProtect Cyber Recovery implementation and ongoing management.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $119,100.

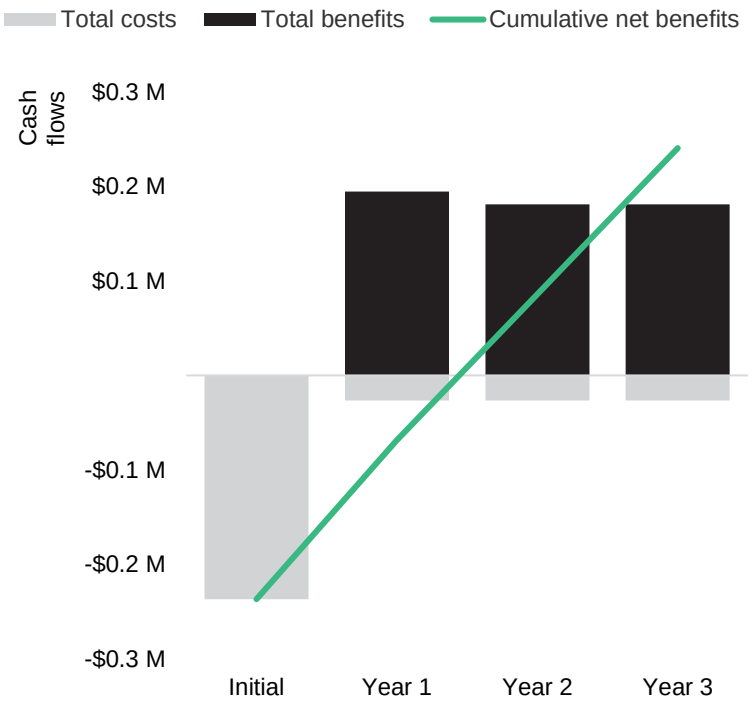
Internal Implementation And Ongoing Management Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Time for implementation (months)	Interviews	4			
F2	Internal resources who support implementation	Composite	4			
F3	Percent of time dedicated	Interviews	30%			
F4	Resources who support ongoing management	Composite		1	1	1
F5	Percent of time dedicated	Interviews		20%	20%	20%
F6	Average fully burdened monthly salary of an internal resource who supports implementation and ongoing management	TEI standard	$10,053	$10,053	$10,053	$10,053
Ft	Internal implementation and ongoing management costs	(F1*F2*F3*F6)+ (F4*F5*F6*12)	$48,254	$24,127	$24,127	$24,127
	Risk adjustment	↑10%				
Ftr	Internal implementation and ongoing management costs (risk-adjusted)		$53,080	$26,540	$26,540	$26,540
	Three-year total: $132,700			**Three-year present value: $119,081**		

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	($236,780)	($26,540)	($26,540)	($26,540)	($316,400)	($302,781)
Total benefits	$0	$194,659	$181,159	$181,159	$556,978	$462,789
Net benefits	($236,780)	$168,119	$154,619	$154,619	$240,578	$160,008
ROI						53%
Payback						18.0 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Supplemental Material

Related Forrester Research

"Assess Your Technology Resilience Maturity," Forrester Research, Inc., April 17, 2023

"The Best Tech Organizations Are Future Fit," Forrester Research, Inc., September 28, 2022

Appendix C: Endnotes

[1] Source: "The State Of Ransomware Attacks And Defenses," Forrester Research, Inc., February 2, 2022.

[2] Source: "The Forrester Wave: Data Resilience Solution Suites, Q4 2022," Forrester Research, Inc., December 8, 2022.

[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 Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] Source: "Future Fit Technology Strategies Require A New Approach To Making Investment Decisions," Forrester Research, Inc., March 28, 2023.


FORRESTER®