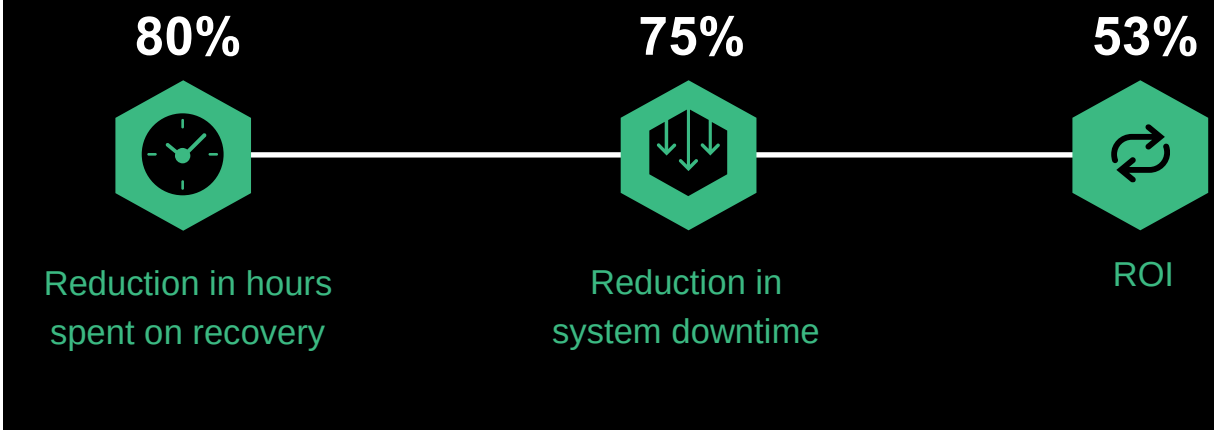
EXECUTIVE SUMMARY

FORRESTER®

The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery

KEY STATISTICS



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 cyberattack in the event that standard backups are impacted. CyberSense works within the vault to scan backups for signs of corruption due to ransomware, 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.[1] 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.

READ THE FULL STUDY

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.

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.
- **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.

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

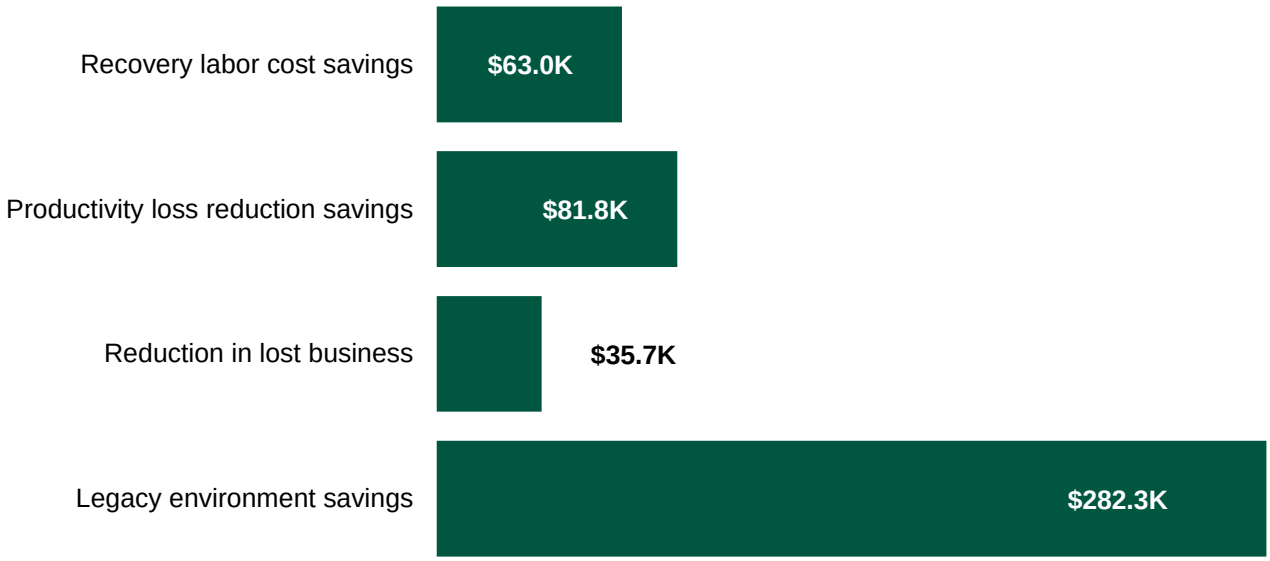
uses CyberSense to easily confirm that backups are safe and to find out where malicious activity comes from in order to mitigate damage before it becomes excessively costly.

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%.

Benefits (Three-Year)



DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Dell and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Dell PowerProtect Cyber Recovery.
- Dell reviewed and provided feedback to Forrester. Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning.
- Dell provided the customer name(s) for the interview(s) but did not participate in the interview(s).

ABOUT FORRESTER CONSULTING

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

Appendix: 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.