A Forrester Total Economic Impact^{TM} Study
Commissioned By Absolute
March 2018

FORRESTER®

Absolute Endpoint Visibility And Control Healthcare Edition

Forrester Consulting conducted a Total Economic Impact (TEI) study to provide readers with a framework to evaluate the potential financial impact of Absolute on their organizations. To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with experience using Absolute. The aggregated financial model of these organizations is presented here, along with the specific challenges faced by a healthcare organization and its results with Absolute. This healthcare-centric summary is based on a full TEI study, which can be downloaded here.

Through customer interviews and data aggregation, Forrester concluded that Absolute has the following three-year financial impact: $3.5 million in present value (PV) benefits versus PV costs of $1.4 million, resulting in a net present value (NPV) of $2.1 million and an ROI of 146%.

Quantified benefits. The following risk-adjusted quantified benefits are representative of those experienced by all of the companies interviewed:

- **Improved efficiency of security operations staff.** Triage and analytical work comprised a large portion of the approximately 1,000 monthly security-related incidents experienced by interviewed organizations. Absolute increased visibility of endpoints for security professionals, allowing them to conclude incidents 12 minutes faster, on average.
- **Increased efficiency at IT help desks.** With more up-to-date information on the endpoints being fed to the IT help desk, personnel could more quickly understand the situation surrounding a service request. This saved 10 minutes per request.
- **Reduced exposure to asset loss and data breaches.** Absolute Persistence™ provides a self-healing, two-way connection to any endpoint— even if they are off the network. Endpoints are able to to report or perform automated actions based on definable telemetry rules. Persistence reduced asset losses and the possibility of data exposure and breach.
- **Optimized asset life cycle planning and resource allocation.** With Absolute reporting, interviewed organizations had better visibility into endpoints and infrastructure. A healthcare information security manager that was interviewed noted that his organization justified a 10% reduction in endpoints after using Absolute to identify underutilized assets.

Unquantified benefits. The interviewed organizations experienced the following benefit:

- **Accelerated compliance audits.** Absolute's visibility and near-instant reporting on endpoint security posture enabled security professionals to more easily demonstrate compliance, assuring auditors that data was safely stored.

ROI
146%

Benefits PV
$3.5 million

Costs PV
$1.4 million

Payback
<6 months

SUMMARY

Based on a commissioned study, "The Total Economic Impact Of Absolute"

METHODOLOGY

The objective of the TEI 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 of Absolute, including interviews with Forrester analysts, Absolute stakeholders, and five current Absolute customers. Forrester constructed a financial model representative of the interviews using the TEI methodology.

COMPOSITE ORGANIZATION

This analysis uses a composite organization, based on the interviewees, to present the aggregate financial analysis.

RISK ADJUSTMENT

Forrester risk-adjusted the financial model based on issues and concerns of the interviewed organizations to account for uncertainties in benefit and cost estimates.

The Absolute Customer Journey

For this study, Forrester conducted five interviews with Absolute customers, representing the following industries: public infrastructure management, multinational consumer product goods, healthcare, engineering consulting, and corporate legal services. The challenges faced by the healthcare organization prior to use of Absolute, along with its achieved results post deployment, are presented below.

KEY FACTS

	Seven hospital campuses	2 million+ patients seen and 10 million+ procedures conducted annually	Compliant with HIPAA and PCI-DSS	16,000 endpoints and 15,000 mixed mobility FTEs

As a healthcare provider, this organization must meet regulatory standards set by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and the Payment Card Industry Data Security Standard (PCI DSS). The large amount of protected health information (PHI), personally identifiable information (PII), and payment data related to these regulations led to tremendous investments to keep data protected. Data encryption, the redaction of confidential data, and updating of process flows were the first steps to becoming compliant with these regulations, but the possibility of fines ranging from $100,000 to the millions, along with concerns of remediation activities that could further lower the bottom line, weighed heavily on the minds of leadership. Specifically, the healthcare organization called out additional soft costs in the form of credit monitoring programs and marketing efforts to reestablish patient confidence in the provider should a breach ever occur.

> "I think it's cheap insurance for compliance with data protection standards. I can sleep at night knowing that I won't necessarily need to report a breach, even if a device walks due to a theft scenario."
>
> *— InfoSec manager, healthcare organization*

The leaders of this organization questioned not only how to prove compliance with these regulations, but also how to improve the organization's posture to further reduce the possibility of data breaches and the likelihood of falling out of compliance. To operate in this regulation-heavy environment, these leaders needed an additive layer of protection that could defend against data breaches and IT asset loss, especially for those devices that traversed off the physical network. In essence, the organization wanted to go away from "fire-fighting mode" and become proactive in its approach to data security.

The healthcare organization deployed Absolute across its landscape, offering a new level of visibility, control, and remediation for endpoints. Automated reporting and remedial actions based upon telemetry and security-operations-(SecOps)-defined rules became available to the enterprise. This eliminated blind spots and created a near-foolproof method for locking data from threat actors.

The InfoSec manager of the organization stated:

"The combination of our Safe Harbor practices and Absolute lets me sleep a little better at night, knowing that I can meet our compliance requirements and produce documentation to validate it."

Key Investment Drivers And Results

The interviewed healthcare organization shared the following investment drivers:

- **The healthcare provider needed to become more proactive, rather than reactive, to security-related incidents.** Being responsive to incidents was no longer acceptable to the organization, given the context of regulatory measures and the morally proper action to take. To be proactive, the organization needed an endpoint solution that would give IT operators visibility along with predefined controls that would automate remedial actions, rather than wait for action from incident responders.

- **Compliancy to regulations like HIPAA and PCI-DSS was critical to ongoing business activities.** An embedded solution with self-healing properties would strengthen the Safe Harbor practices that the organization had already taken to ensure the additional peace of mind. The organization absolutely desired to avoid fines and post-breach remedial costs. Demonstrating compliance was another area of attention that the organization needed to address, especially for those devices that left the enterprise network.
- **Asset managers needed a deterrent to malicious and nonmalicious asset thefts.** Contractors and temporary employees caused the healthcare organization to revisit its policies and solutions set in place when thefts became a recurring theme. Though concerned with the cost of the physical assets, the organization was more focused on the value of the regulated data that may have been stored on the devices.
- **The organization needed to reach off-network devices with urgent patches and updates.** Existing endpoint solutions had a poor rate of patch completion and reporting. The healthcare provider needed a solution that sought out even dark endpoints with automated remediation actions: A single endpoint breach could lead to further information loss once it resurfaced on the enterprise network.

> "Absolute Persistence gives us assurance that theft is not a recurring scenario and that stolen devices don't become breach liabilities. Our other tools were not able to detect these devices and give us the sense of security that we now have."
>
> *— InfoSec manager, healthcare organization*

The interviewed healthcare organization achieved the following key investment results:

- **Improved coverage and compliance.** With Absolute, machines can go offline but become visible as soon as any network connectivity is available. SecOps is also empowered with better information to handle situations — it can see and control endpoints devices and freeze or wipe them when necessary. Staying compliant to regulatory measures became easier with automated telemetry-based rule sets.
- **Better physical asset management.** The healthcare organization gained insight into utilization rates of endpoints, allowing it to optimize infrastructure spending. In addition to process improvements, malicious and accidental thefts decreased significantly.
- **Increased visibility into endpoints.** Help desk efficiency increased as staff accessed fresher information about laptops and other devices. Noncompliant software that could lead to data breaches and fines was also detected and removed.

Composite Organization

To provide a deeper level of financial analysis, Forrester compiled and analyzed the results from the interviews with the healthcare organization and four other organizations. Forrester then constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected, covered in greater detail in the full study. The composite organization has the following characteristics:

Description of composite: This is a global, multibillion dollar organization. Its workforce is highly mobile, and most endpoints are PC laptops. Through its business operations, the composite collects large amounts of personally identifiable information, the treatment of which is subject to regulation around the globe.

Deployment characteristics: Much of the Absolute deployment was performed in the initial year, with the solution up and running in the cloud command center in week one. The deployment aimed to achieve three things: 1) optimize SecOps and help desk productivity, 2) enable data sharing within the security tool stack, and 3) centralize asset management.

Key assumptions
-16,000 business FTEs
-18,000 endpoint devices
-Mobile workforce largely using laptop PCs

Absolute Enables Greater Endpoint Visibility And Control

Before using Absolute, issues often arose at the interviewed organizations when devices left the enterprise network. Prior solutions were unable to provide endpoint visibility and control, which resulted in compliance failures. In some cases, these devices disappeared altogether, making endpoint security a difficult task. Evaluating security posture and proving compliance was a lengthy and difficult process, which led to missed business opportunities and corporate data exposure that prompted regulatory ramifications. By adopting Absolute, the interviewed organizations gained a centralized platform that more effectively assessed and secured a wide range of endpoints.

The benefit impact experienced by the composite organization is based on the past and current experiences of the five interviewees. Over three years, the composite organization experienced risk-adjusted benefits of $3.5 million.

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Security operations efficiency improvement	$151,200	$158,760	$166,698	$476,658	$393,904
Btr	IT help desk efficiency improvement	$54,000	$56,700	$59,535	$170,235	$140,680
Ctr	Asset loss reduction	$385,560	$364,354	$382,572	$1,132,486	$939,060
Dtr	Asset life cycle optimization	$1,231,200	$575,618	$604,399	$2,411,218	$2,049,085
	Total benefits (risk-adjusted)	$1,821,960	$1,155,433	$1,213,204	$4,190,597	$3,522,729

- **Security operations staff saw an efficiency improvement.** Following the implementation of Absolute, security operations staff saved an average of 12 minutes per incident response. With approximately 1,000 security incidents occurring each month, total savings over three years amounted to $393,904.
- **The IT help desk saved 10 minutes per request with more up-to-date information from Absolute.** The IT help desk handled 15,000 service-related requests every month. Absolute provided a 20% better resolution to endpoints than existing solutions, helping to reduce the help desk workload by a minimum of 1,200 hours per year and generating three-year savings of $140,680.
- **Absolute reduced asset loss and the possibility of data breaches.** Nonmalicious losses, such as an employee taking a computer home for his or her children to use, occurred roughly 2% of the time across the endpoint landscape. Malicious losses, such as asset theft by an employee or contractor, occurred 0.5% of the time. Recovery rates for nonmalicious losses were higher (80%) than malicious losses (20%). On both fronts, Absolute reduced losses and improved recovery, generating savings of $939,060 over three years.

> "We've got 16,000 PCs. If we can cut that down, we cut down subsequent licensing. Our goal is to justify a 10% reduction."
>
> *-- InfoSec manager, healthcare organization*

- **The organization optimized asset life cycle planning and resource allocation.** With the Absolute platform and greater visibility into endpoint assets, the composite organization determined that 10% of all endpoints were underutilized. Thus, the organization eliminated support costs for these assets, calculated at 20% of the value of hardware and software. In years 2 and 3, the composite avoided 2% of yearly endpoint, software, and infrastructure purchases. Three-year savings totaled $2,049,085.
- **The composite streamlined security operations and compliance audits.** Because scripts were delivered to endpoints that went dark upon coming online, security professionals needed to deploy only once. Additionally, both internal and regulatory compliance audits became simpler due to Absolute's faster reporting on endpoint security posture.

Implementation and integration took no more than one month.

Absolute Costs Include Licensing And Implementation

The composite organization experienced two categories of costs associated with the Absolute investment. Over three years, the composite organization experienced risk-adjusted costs of $1.4 million.

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	License-related costs	$539,100	$0	$509,450	$534,922	$1,583,471	$1,362,027
Ftr	Implementation and integration costs	$30,378	$21,507	$11,827	$11,827	$75,539	$68,590
	Total costs (risk-adjusted)	$569,478	$21,507	$521,277	$546,749	$1,659,011	$1,430,617

- **Annual licensing formed the majority of costs.** The composite organization managed 18,000 endpoints and purchased licenses on a yearly schedule. The organization's licensing costs considered user growth as well as retirement of underutilized endpoint assets, as reflected by lower Year 2 licensing costs.
- **Implementation costs made up less than 5% of total costs.** Beyond license and support costs, many interviewees encountered costs to integrate Absolute into security information and event management (SIEM) and IT service management (ITSM) solutions. Internal resources at the composite spent approximately 160 hours to do so.

An Absolute Investment Today Can Create Future Opportunities

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Absolute and later realize additional uses and business opportunities, such as the following:

- **Command and control capabilities are further enhanced with Absolute Reach.** Organizations can increase SecOps efficiency further with custom scripting commands that could be deployed in a single instance, including to those endpoints that are off of the enterprise network. The uses of such scripts are many, providing SecOps with improved querying and the capability to orchestrate and automate endpoint actions. Organizations can also find considerable benefit from the "deploy once" characteristic of Absolute, which eliminates the multiple deployment efforts necessary with alternative solutions.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

Absolute: Overview

The following information is provided by Absolute. Forrester has not validated any claims and does not endorse Absolute or its offerings.

Absolute Ensures Endpoint Visibility, Control, And Compliance — Beyond the Network

The Absolute platform enables IT security organizations to track every endpoint, find at-risk data, rapidly remediate vulnerabilities, and ensure compliance in the face of insider and external threats.

Absolute endpoint visibility and control saves organizations millions of dollars in security operations and IT asset management costs, while ensuring ongoing compliance. It cannot be disabled, protecting data, assets, and users — wherever they go.

Absolute delivers:

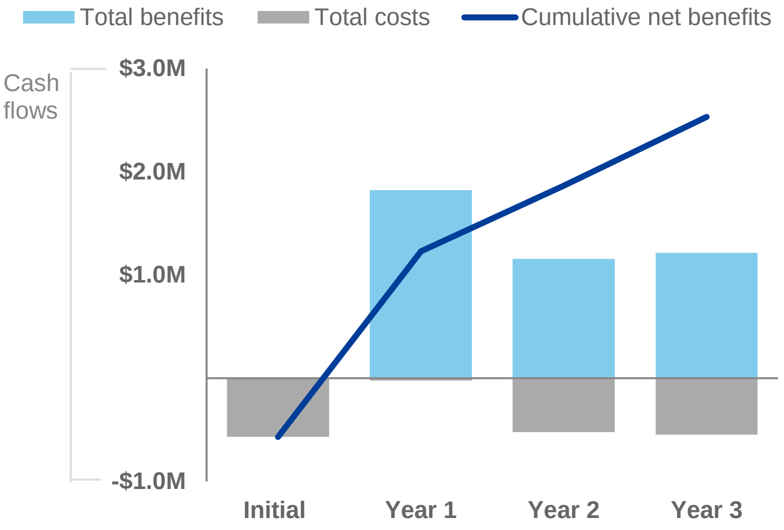
- Deep and persistent contextual awareness into hundreds of user and endpoint attributes to eliminate blind spots.
- Remote control over all endpoints devices to query, explore, and remediate — even when traditional options fail.
- Rapid response to stop and remediate incidents through automated triggers and custom workflow execution.
- Precision insights into any endpoint to mitigate risk and prove compliance.
- Unstructured data discovery and automated remediation to protect regulated data and ensure compliance with GDPR, HIPAA, HITECH, PCI, and other regulations.
- Rapid vulnerability assessment and remediation to stop ransomware attacks as they happen.
- Advanced IT asset management and security hygiene with the ability to seamlessly execute custom commands against targeted devices in just a few clicks.
- Instant activation across all endpoints without additional infrastructure needed.

Absolute's patented Persistence technology is already embedded in the firmware of more than one billion PC and mobile devices, integrated with hundreds of endpoint security controls, and trusted by over 15,000 customers worldwide.

To discover the benefits that Absolute's endpoint visibility and control platform can provide to your organization, visit www.absolute.com

Financial Summary

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 in Absolute. Forrester assumes a yearly discount rate of 10% for this analysis.



ROI
146%

NPV
$2.1 million

Payback
<6 months

For more information, you can download the full Absolute TEI analysis here.

Disclosures

The reader should be aware of the following:

- The study is commissioned by Absolute 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 Absolute.
- Absolute 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.
- Absolute provided the customer names for the interviews but did not participate in the interviews.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. https://go.forrester.com/consulting/

ABOUT TEI

Total Economic Impact™ (TEI) 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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility. https://go.forrester.com/consulting/content-marketing-consulting/