The Business Value of Entrust

Jennifer Glenn
Research Director,
Security and Trust Group, IDC

Megan Szurley
Business Value Manager,
Business Value Strategy Practice, IDC

THIS PDF USES HYPERLINKS

Table of Contents

Business Value Highlights . . . 3

Executive Summary . . . 3

Situation Overview . . . 4

Entrust Overview . . . 5

The Business Value of Entrust . . . 5

Study Firmographics . . . 5

Choice and Use of Entrust . . . 6

Business Value and Quantified Benefits . . . 8

Staff Productivity Benefits from Entrust . . . 10

Business Enablement Benefits from Entrust . . . 14

ROI Summary . . . 16

Challenges/Opportunities . . . 17

Conclusion . . . 17

Appendix 1: Methodology . . . 18

Appendix 2: Supplemental Data . . . 19

About the IDC Analysts . . . 20

Message from the Sponsor . . . 21

BUSINESS VALUE HIGHLIGHTS

Click any link and look for the ➤ symbol on the corresponding page. Use the Return to Highlights button to return this page.

$272,000
average annual benefit per 10,000 active certificates managed

310%
three-year return on investment

58%
more productive user identity tool/certificate management teams

64%
more productive authentication control implementation and management teams

8-month
payback on investment

56%
more productive data security teams

41%
more digital certificates issued per month

46%
less certificate expirations per month

$612,500
in three-year annualized cost savings from tool retirement/consolidation

Executive Summary

Entrust has been providing identity-centric security solutions to customers for more than 50 years. The company continues to invest in enhancing its security offerings around authentication and access to include AI-enabled solutions and growing its technologies in data security, machine identities, and all communications in between. These technology areas are the foundation of a zero trust security approach and provide Entrust with an opportunity to demonstrate how these technologies work together to provide compounding value. The company combines critical functions across data security, identity, and threat protection to help organizations protect sensitive information from compromise.

IDC conducted research that explored the value and benefits for organizations using Entrust to decrease the complexity of trust management as they evolve digitally.

Based on interviews with Entrust customers, IDC calculated that these customers will achieve average annual benefits worth $3.5 million per organization ($272,000 per 10,000 active certificates managed) and a three-year ROI of 310% through:

- Automating workflows, increasing visibility, and decreasing complexity for staff managing authentication, identity, certificates, and data security
- Decreasing operational costs by unifying and consolidating the trust management environment
- Improving business results by increasing customer retention, trust, and satisfaction

Situation Overview

Data is the heart of modern business. It powers business operations and customer-facing products that generate revenue and informs decision-makers on advancements in both areas. The digital transformation has facilitated the storage, usage, and sharing of all this data. IDC research shows that the majority of enterprises derive most of their value from digital technologies.

The risks to digital businesses are vast. External forces, including malicious actors, aim to disrupt business and exfiltrate valuable information for extortion or resale. Trusted users also present several risks, such as inappropriately accessing information or having a threat actor take their credentials. Regulatory and compliance requirements create risk in the form of expensive fines and reputational damage if organizations do not comply with standards. Finally, the massive amount of data in storage, processing, and transmission across multiple cloud and on-premises environments creates risk by overburdening the teams responsible for managing and securing it. Layoffs, budget cuts, and flexible working environments only exacerbate these risks.

Ensuring the integrity and security of corporate data in the face of these risks requires a coordinated effort across IT; identity and access; and data and information security teams. This includes sharing information and technology resources between teams but also finding efficiencies where possible.

This Business Value study demonstrates the financial benefits organizations achieve by using multiple technologies from the Entrust portfolio. The quantitative results from this survey show how consolidating critical zero trust technologies can reduce costs, simplify operations, and improve overall security.

Entrust Overview

Entrust secures data, devices, and users across all environments, from on-premises datacenters to cloud and hybrid infrastructures. Its solutions integrate critical functions across data security, identity, and risk mitigation, helping organizations safeguard sensitive information. A zero trust approach to security requires a strong focus on identity (both human and machine) and data security. The combination of these technologies hardens the internal operations of the enterprise by making it more difficult for any user or device — malicious or trusted — to access sensitive data.

A zero trust approach to security starts with a foundation of strong identity management and protection. This provides organization and control over any identities accessing corporate resources, including employees, customers, and partners. Identity extends beyond human users. Machine identities — the devices that store, process, and share data — also require authentication and authorization to use data and should be part of a zero trust approach.

Data security technologies are also a critical building block in a zero trust approach. Data is the lifeblood of the organization but the biggest vector for risk. Data security solutions such as key management, encryption, and digital certificates ensure the integrity of data as it moves between different connections.

Entrust's suite of identity and data security solutions supports zero trust implementations by helping organizations innovate quickly while safeguarding information from unauthorized access or breaches. Its platform-based approach offers consistency and automation, allowing enterprises to do more with less.

The Business Value of Entrust

Study Firmographics

IDC conducted research that explored the value and benefits for organizations using Entrust to gain control over authentication and certification efforts to ensure the security of their environment. The research included six interviews with organizations that used Entrust and had knowledge about its benefits and costs. IDC asked the interviewed companies various quantitative and qualitative questions to assess Entrust's impact on security staff and their overall business.

Table 1 shows the firmographics of the interviewed organizations, which were large and had an average of 37,600 total employees and $12 billion in annual revenue. They had 2,702 IT staff members supporting 789 business applications. The study had global representation, with interviewed organizations in the United States (2), Chile, India, Singapore, and the United Kingdom, and included organizations from the financial services (3), healthcare (2), and manufacturing sectors.

TABLE 1

Firmographics of Interviewed Organizations

Firmographics	Average	Median	Minimum	Maximum
Number of employees	37,600	14,000	2,000	100,000
Number of total IT Staff	2,702	2,250	210	6,000
Total number of business applications	789	376	7	3,000
Annual revenue	$12B	$975M	$500M	$45B
Countries	United States (2), Chile, India, Singapore, United Kingdom			
Industries	Financial Services (3), Healthcare (2), Manufacturing			

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Choice and Use of Entrust

In their detailed conversations with IDC, study participants discussed the decision criteria that ultimately led to their selection of Entrust. During their evaluation period, they found Entrust to be a comprehensive security solution that addressed the gaps in their previous systems and seamlessly integrated with the existing tools and technologies within their organization. They felt that it was a cost-effective solution that offered robust support and focused on next-generation digital security, including zero trust principles. Entrust was especially appealing because it simplified digital identity and certificate management globally.

Study participants elaborated on their selection of Entrust:

Holistic security solution (Manufacturing):

"My organization selected Entrust because we had some use cases that our previous solutions did not cover. We had a combination of legacy solutions that were not updated appropriately. That triggered a search for a holistic tool around security solutions. We evaluated several vendors, and, looking at the end-to-end offerings, along with how well it integrated with our current ecosystem, we selected Entrust."

Tight environment integration (Healthcare):

"My organization looked at several solutions when we were in our due diligence process. We compared what we were looking for versus what these technologies were providing. We selected Entrust because it integrated with our existing tools [and] technologies and supported mobile applications. The implementation cost and support model were also appealing."

Zero trust solution (Healthcare):

"My organization had a public data breach of medical data back in 2018. That breach resulted in new security investment and a lot of implementation of security technologies. At the time, we did not have a zero trust solution, so we went to the market and ended up choosing Entrust. A couple of factors led to this decision. First, the reputation — they have been doing identity security for some time. Secondly, the business organization is focused on the zero trust product as the primary offering, not doing something else and branching out to zero trust."

Next-generation digital security support (Financial Services):

"My organization selected Entrust because it is a price-effective solution that focuses on the next generation of digital security. They have robust support, security trust, and certificate management — all in a single solution."

Certificate and encryption simplification (Financial Services):

"My company started using Entrust a couple of years back because we were having some challenges managing the digital identity certificates and encryptions across a distributed global network."

Table 2 (next page) provides an aggregate view of the study participants' Entrust environment. At the time of the interviews, Entrust supported many endpoints accessing internal networks (59,550), employees using internal applications (31,482), and identities (321,413). Entrust's management of 130,324 active certificates further highlights its large footprint within interviewed organizations. The table below shows additional usage metrics.

TABLE 2

Organizational Usage of Entrust

Entrust Environment	Average	Median
Number of endpoints accessing internal network	59,550	7,500
Number of employees using internal business applications	31,482	7,990
Number of protected workforce and customer identities	321,413	145,000
Number of managed active certificates	130,324	100,000
Number of supported business applications	620	376
Percent of supported revenue	61%	75%

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Business Value and Quantified Benefits

The interviews that IDC conducted indicated that study participants significantly benefited from Entrust deployment. The comprehensive trust management solution provided process automation, robust identity management systems, and data protection and increased overall system reliability. The solution's ability to fully integrate within the overall operating environment and existing infrastructure was crucial to safeguarding sensitive information and maintaining trust. Additionally, customers found that Entrust enhanced overall visibility across their entire environment, enabling accurate incident reporting and simplified certification processes.

Study participants stated the following about Entrust's most significant benefits:

Ability to safeguard sensitive information (Financial Services):

"Entrust has provided my organization with encryption technologies, secure communication channels, and protection for data both at rest and in transit. These three things are very crucial for safeguarding sensitive information and ensuring that there are no unauthorized access and data breaches. They are a really significant benefit for my organization."

Trust and credibility (Manufacturing):
"Entrust has enabled my organization to develop trust and credibility when getting compliance certifications. This is because, with better organization visibility, we have more accurate information about how many incidents globally happened. Entrust has significantly minimized risk."

Complete application protection (Healthcare):
"The largest benefit of Entrust is that my organization could integrate all [its] applications, regardless of their environment, and still enable SSO and MFA. It is pretty easy to manage, and, as a result, we have no application that isn't protected by Entrust."

Strong identity management system (Healthcare):
"Entrust is quite fast, especially when deploying new encryptions. It enables my company to have a strong identity management system in place that we can leverage when we innovate. It helps us quickly add new users or give certain users stronger protections to these innovative projects."

Automated certificate validation (Financial Services):
"A big benefit of Entrust is that it automatically validates and manages certificates and their expirations. This has led to system reliability and reduced efforts across various teams."

Authentication centralization (Financial Services):
"Having a single robust solution that has been consistent over time and can be implemented across the bank's different digital channels is where my organization sees the main benefit of Entrust. This allows us to centralize all final customer authentication management."

Figure 1 (next page) illustrates IDC's calculations of the average annual benefits interviewed organizations achieved from deploying Entrust. As the figure shows, IDC quantified average annual benefits at $3.5 million per organization **($272,000 per 10,000 active certificates managed).**

The study categorized these benefits as follows:

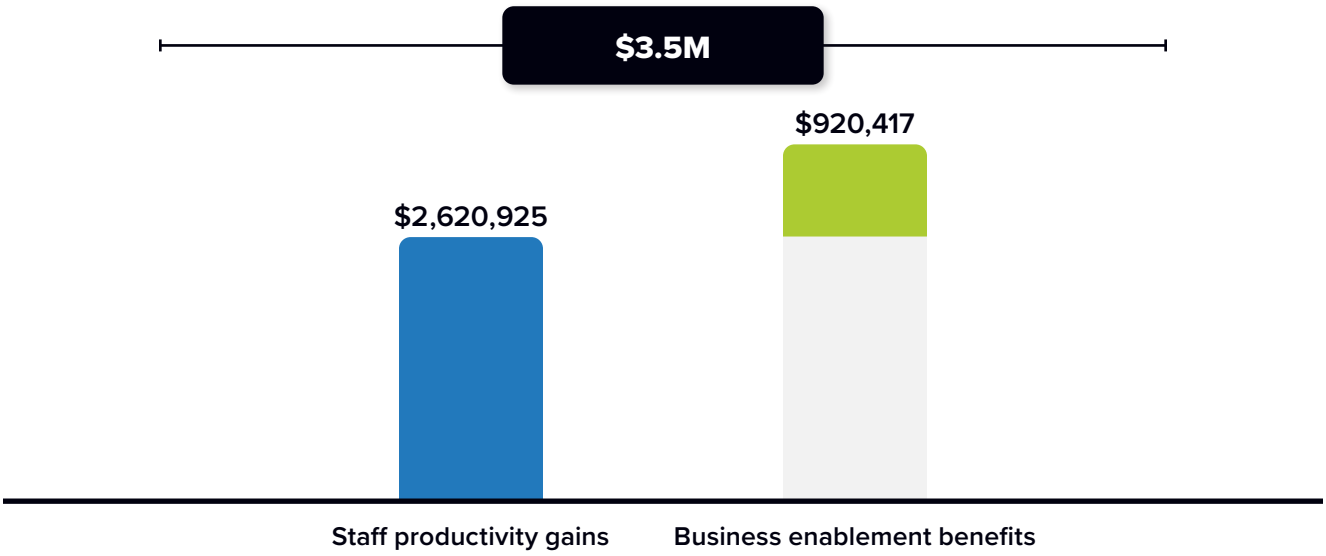
- **Staff productivity gains:** Entrust automated workflows and increased visibility, enabling staff members managing authentication, identity, certificates, and data security to work with greater productivity.
- **Business enablement benefits:** Interviewed organizations were able to consolidate trust tools and recognize higher annual revenue from deploying Entrust.

FIGURE 1

Average Annual Benefits per Organization

($ per interviewed organization)

For an accessible version of the data in this figure, see Figure 1 Supplemental Data in Appendix 2.



n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Staff Productivity Benefits from Entrust

Interviewed organizations made it clear to IDC that Entrust enabled their staff to work with significantly greater productivity. Those managing authentication, identity, certificates, and data security benefited from the solution's automation to reduce the manual effort of tasks such as provisioning, certifications, and security protocol deployment. Entrust also improved visibility across the entire organization, helping staff discover certificates, mitigate risks, and monitor their environment with far greater ease.

Study participants discussed the productivity benefits in greater detail:

Reduction of manual processes (Healthcare):

"Entrust has saved staff time by automating workflows, providing seamless user provisioning and de-provisioning, security enhancements, and reduced manual processes. A lot of frustration and unnecessary escalation has been eliminated!"

Greater authentication efficiency (Healthcare):

"Entrust gives our authentication managers much greater efficiency with automation and has drastically reduced errors."

Quicker certification (Financial Services):
"Issuing FIDO-based certifications and SSO is streamlined with Entrust. We can do it in two business days with Entrust; it used to take seven days before because it was such a manual process."

Improved ability to discover and manage certificates (Financial Services):
"Entrust helps my company improve [its] ability to discover and manage digital certificates. The platform has a central repository, which allows us to easily locate and manage our digital certificates to monitor the expiry dates, manage the revocation, and maintain compliance with regulations. It has streamlined processes."

Reduced phishing attack risk (Financial Services):
"My company has reduced the risk of phishing attacks with Entrust because we have the ability to actively monitor and detect threats daily, which we could not do before. We also have scheduled meetings with the security teams to get feedback on the security protocols and the mechanisms we have implemented."

Advanced threat detection (Financial Services):
"With Entrust, my organization has gained advanced threat detection. We use responsive machine learning and AI tools to help identify unusual behaviors and any kind of potential threats quicker. With the help of identity verification and MFA, we were able to secure and prevent any kind of unauthorized access."

To measure Entrust's productivity impact, IDC first examined staff that worked on authentication control implementation and management within interviewed organizations. The solution provided teams with centralization and streamlined workflows. Ultimately, this simplification enabled tighter access control while enabling quicker accommodation to end users requiring access to sensitive applications, devices, and services.

The following authentication control-based KPIs demonstrate the risk reduction and access benefits that organizations achieved with Entrust:

- Passwordless multi-factor authentication covering 94% of employees at organizations using the function
- 70% quicker issuing of FIDO-based certificates and SSO to provide employees with access to the necessary applications

As **Table 3** (next page) shows, the centralization and simplification Entrust provided enabled teams to be notably more productive (64%), meaning the authentication team could work with the equivalent productivity level of having 11.3 additional FTEs on staff. IDC valued this productivity improvement at $1,130,938 annually.

TABLE 3

Authentication Control Implementation and Management Team Productivity Gain

Productivity Gain	Before Entrust	With Entrust	Difference	Benefit
Equivalent productivity level, FTEs	17.6	**28.9**	11.3	64%
Value of staff time per year	$1,762,500	**$2,893,438**	$1,130,938	64%

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Next, IDC evaluated the impact of Entrust on the team managing user identity at the interviewed organizations. This team significantly benefited from the unification of their identity management environment, which simplified the management of users across the entire company, especially when implementing and managing MFA and SSO.

This environmental unification enabled identity management teams to achieve a 58% productivity boost (see **Table 4**) — the equivalent of having 7.3 additional team members on staff. The annual value of this productivity was $727,222.

TABLE 4

User Identity Tool/Certificate Management Team Productivity Gain

Productivity Gain	Before Entrust	With Entrust	Difference	Benefit
Equivalent productivity level, FTEs	12.5	**19.8**	7.3	58%
Value of staff time per year	$1,250,000	**$1,977,222**	$727,222	58%

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Interviewed organizations also found that those managing public or private PKI certificates enhanced their productivity with Entrust. The solution automated tedious workflows and centralized the overall trust environment, helping teams manage certificate expiration, ownership, and volume with greater effectiveness. Importantly, these improvements helped teams issue more certificates per year and face fewer expirations. A financial services

participant noted, *"The automation provided by Entrust has enabled my organization to pinpoint the certificates much faster. Previously, we used to take up to a couple of hours, but now, within minutes, we can track it down."*

To establish Entrust's impact on certification management efforts, IDC calculated that interviewed organizations achieved the following efficiencies or KPIs:

- 41% more digital certificates issued per month
- 65% less staff time required to issue digital certificates to users/devices
- 46% fewer certificate expirations per month

In terms of productivity improvements, teams were able to work with the equivalent productivity level of having 7 additional FTEs on staff — amounting to a significant productivity boost of 64%. The value of this gain was $696,533 annually (see **Table 5**).

TABLE 5

Public/Private PKI Management Team Productivity Gain

Public/Private PKI Management Team Productivity Gain	Before Entrust	With Entrust	Difference	Benefit
Equivalent productivity level, FTEs	10.9	**17.8**	7.0	64%
Value of staff time per year	$1,088,333	**$1,784,867**	$696,533	64%

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Finally, IDC assessed the data security team in this engagement. Interviewed organizations found that Entrust provided a unified environment to support their zero trust implementations, which reduced the risk of breaches by automating routine tasks such as key or secret management and session controls. They also benefited from greater visibility, which enabled quicker vulnerability identification and tighter integrations.

Table 6 (next page) depicts that, as a result, the zero trust solution enabled teams of highly skilled individuals to work with significantly greater productivity (56%), freeing up their time to focus on higher-value tasks. The value of this enhancement was $509,555 per year.

TABLE 6

Data Security Team Productivity Impact

Productivity Impact	Before Entrust	With Entrust	Difference	Benefit
Equivalent productivity level, FTEs	9.1	**14.2**	5.1	56%
Value of staff time per year	$914,000	**$1,423,555**	$509,555	56%

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Business Enablement Benefits from Entrust

Through a series of comprehensive questions about Entrust's overall operational benefits, IDC found that the solution significantly enhanced business success for the interviewed organizations, particularly in terms of cost optimization and revenue generation. Entrust offered the necessary functionality and tools to act as a single trust management solution. This allowed study participants to consolidate or retire existing security tools, thereby reducing operational costs. Additionally, the automation that Entrust provided improved business agility and system reliability for both end users and customers. This enhancement helped businesses better serve their customers, gain their trust, and secure their loyalty.

Customers discussed the business-related benefits of using Entrust in detail:

Tool consolidation cost reduction (Financial Services):
"My organization has benefited from Entrust serving as a single solution that consolidates all security policies for clients, which simplifies processes and reduces costs."

Greater user trust (Financial Services):
"Entrust has helped to establish trust with the users by guaranteeing the authenticity of the digital identities by issuing digital certificates. We are ensuring secure transactions, communications, and adherence to the industry standards that regulators mandate."

Increased business agility (Manufacturing):
"Since deploying Entrust, customer authentication is happening on time without them having to contact us, and the customer retention rate has gone up as a result. We have also had fewer problems in audit. Having a singular trust solution has improved business continuity and disaster management. All of this improves overall business agility."

Reduced fraud-based losses (Financial Services):

"Entrust has moved the lever when it comes to reducing our risk appetite regarding the amount of fraud we're willing to tolerate annually. By reducing losses related to risk, we undoubtedly increase our profitability as a company."

Higher system reliability (Financial Services):

"Entrust has impacted our ability to support business agility because we are proactively monitoring thousands of certificates without risk of accidental actions or any kind of manual error. Like I said, we have reduced all the outages due to the expired certificates by 90%. As a result, the system reliability is high, which helps us achieve business growth."

As the study noted above, Entrust's robust functionality enabled study participants to reduce IT costs. Importantly, the tool served as a single, unified solution for the life-cycle management of certificate-based user and machine identity. This enabled interviewed organizations to consolidate or retire legacy security solutions and reduce annual IT spend by $612,500 (see **Table 7**).

TABLE 7

Business Enablement — IT Cost Savings

IT Cost Savings	Annualized
Tool retirement/consolidation savings	$612,500

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

The final area that interviewed organizations indicated Entrust impacted was their revenue. IDC found that study participants recognized higher net revenue because the solution increased customer trust, satisfaction, and retention.

Table 8 (next page) illustrates the overall revenue impact. IDC calculated that business enablement amounted to $2,400,000 in total additional gross annual revenue per organization. IDC's financial model then applied a 15% operating margin assumption, revealing a net annual revenue gain of $360,000 per organization.

TABLE 8

Business Enablement — Higher Revenue

Business Enablement — Higher Revenue IDC Model	Per Organization	Per 1,000 Active Certificates Managed
Total additional gross revenue per year	$2,400,000	$18,416
Assumed operating margin	15%	15%
Total additional net revenue, IDC model	$360,000	$2,762

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

ROI Summary

To summarize this engagement, IDC calculated an average three-year ROI that factored in the benefits study participants achieved from deploying Entrust. **Table 9** shows that these companies will achieve three-year discounted benefits worth an average of $8,368,600 per organization through staff productivity enhancements and improved business results. These benefits compare with total three-year discounted costs of $2,043,500 per organization, resulting in an average three-year ROI of 310%, with a payback period of eight months.

TABLE 9

Three-Year ROI Analysis

ROI Analysis	Per Organization	Per 1,000 Active Certificates Managed
Discounted benefits	$8,368,600	$64,214
Discounted investment	$2,043,500	$15,680
NPV	$6,325,100	$48,534
ROI	**310%**	**310%**
Payback	**8-month**	**8-month**
Discount factor	12%	12%

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Challenges/Opportunities

The identity and data security solutions that Entrust offers show a measurable impact for enterprise buyers. These impacts don't exist in a vacuum. Identity and data security solutions are part of a larger cybersecurity ecosystem. The current environment for security purchases leans heavily on consolidation. Many of the enterprises IDC speaks to are trying to reduce the number of vendors they work with.

This presents both a challenge and an opportunity for Entrust. Existing customers will be looking for new ways to add value to their current investments and infrastructure, whether by unifying their data security requirements with a machine identity strategy or layering additional authenticators on top of their user identity deployments. However, this move toward consolidation may make it harder for Entrust to unseat incumbents with similar portfolios.

Conclusion

The research IDC conducted highlights the demonstrable value of Entrust's security solutions for organizations. By integrating critical functions across data security, identity, and risk mitigation, Entrust helps enterprises safeguard sensitive information and maintain trust.

The study demonstrates that Entrust's solutions enhance security, streamline operations, reduce complexity, and improve overall system reliability. Organizations benefit from automation, increased visibility, and the ability to manage digital identities and certificates more effectively. This improves productivity and reduces operational costs.

Entrust's focus on zero trust principles and next-generation digital security positions it as a vital partner for organizations navigating the complexities of digital transformation. The positive feedback from interviewed organizations underscores Entrust's ability to deliver robust, integrated security solutions that support business agility and growth. By consolidating security tools and providing a unified approach to trust management, Entrust enables organizations to achieve higher levels of security, efficiency, and customer satisfaction.

Appendix 1: Methodology

IDC used its standard ROI methodology for this project, gathering data from current Entrust users as the foundation for the model.

Based on interviews with organizations using Entrust, IDC performed a three-step process to calculate the ROI and payback period:

1. **IDC gathered quantitative benefit information during the interviews using a before-and-after assessment of Entrust's impact.** In this study, the benefits included IT cost reductions and avoidances; staff time savings and productivity benefits; and revenue gains.
2. **IDC created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Entrust and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **IDC calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for organizations' use of Entrust over a three-year period. ROI is the ratio of the net present value and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on several assumptions:

- IDC multiplied time values by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For this analysis, IDC used assumptions of an average fully loaded $100,000 salary per year for IT staff members and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumed that employees work 1,880 hours per year (47 weeks x 40 hours).
- IDC calculated the net present value of the three-year savings by subtracting the amount that organizations would have realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because Entrust requires a deployment period, the full benefits of the solution are not available during this time. To capture this reality, IDC prorated the benefits on a monthly basis and then subtracted the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

Appendix 2: Supplemental Data

This appendix provides an accessible version of the data for the complex figure in this document. Click “Return to original figure” below the table to get back to the original data figure.

FIGURE 1 SUPPLEMENTAL DATA

Average Annual Benefits per Organization

Average Annual Benefits	Per Organization
Staff productivity gains	$2,620,925
Business enablement benefits	$920,417
Total	**$3.5M**

n = 6; Source: IDC Business Value In-Depth Interviews, November 2024

Return to original figure

About the IDC Analysts

Jennifer Glenn

Research Director, Security and Trust Group, IDC

Jennifer Glenn is research director for the IDC Security and Trust Group and is responsible for the information and data security practice. Jennifer's core coverage includes a broad range of technologies including messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates. As part of this research, Jennifer will demonstrate the critical role of data security in top enterprise initiatives such as generating customer trust and digital transformation.

More about Jennifer Glenn

Megan Szurley

Business Value Manager, Business Value Strategy Practice, IDC

Megan Szurley is manager for the Business Value Strategy Practice, responsible for creating custom business value research that determines the ROI and cost savings for enterprise technology products. Megan's research focuses on the financial and operational impact of these products for organizations once deployed and in production. Prior to joining the Business Value Strategy Practice, Megan was a consulting manager within IDC's Custom Solutions division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Megan partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

More about Megan Szurley

Message from the Sponsor

In today's interconnected world, a breach can start anywhere in the organization: through employees, customers, or connected devices and applications.

To mitigate risk, we rely heavily on cryptographic hardware, software and credentials (such as keys, certificates and secrets), but not without challenges as we are securing more things than ever, from increasingly sophisticated attacks, all while trying to keep up with compliance and regulatory change and requirement.

Entrust helps organizations gain control over their cryptographic assets by providing centralized visibility, lifecycle management, and automation capabilities. Whether on-premises, cloud, or hybrid, Entrust's solutions reduce operational costs and build customer trust to conduct business securely and seamlessly. When connections between people, data, and systems are secure, your business will be protected and can operate with confidence.

Learn how our comprehensive identity-centric security solutions can benefit your organization.

Visit entrust.com

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com @idc @idc

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.