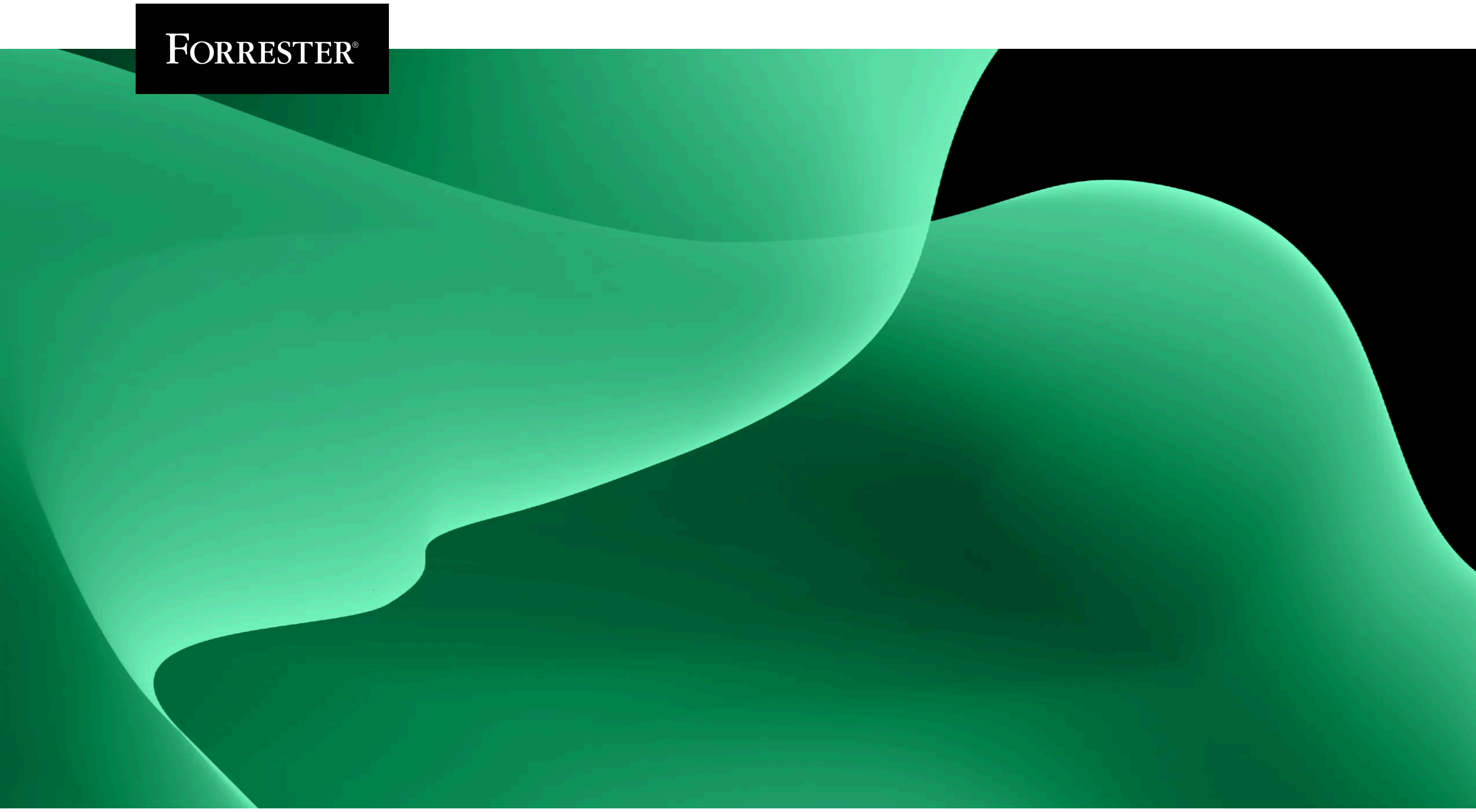
Total Economic Impact

The Total Economic Impact™ Of DigiCert ONE

Cost Savings And Business Benefits Enabled By DigiCert ONE

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY DIGICERT, JULY 2025



Executive Summary

Managing certificates is time-consuming and carries risks of security issues and outages — especially as the demand for more certificates and faster renewals continues to grow.[1] Often, different departments handle certificates independently, leading to inconsistent policies and limited visibility across the organization. Legacy tools and manual processes make it difficult to automate tasks, stay compliant, detect misconfigurations, and monitor certificates effectively. At the same time, the use of certificates is expanding rapidly to support products, IoT devices, and software — while certificate lifespans are shrinking due to new regulations and industry mandates from companies like Google and Apple.[2]

DigiCert ONE is a public key infrastructure (PKI) and domain name system (DNS) platform that helps organizations reduce costs, avoid PKI-related outages, improve security, and streamline operations by combining certificate lifecycle management and full public/private certificate services with specific support for core use cases, including infrastructure, software, device, and content trust solutions.

DigiCert commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying DigiCert ONE.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of DigiCert ONE on their organizations.[4]

312%

Return on investment (ROI) ⓘ

$10.1M

Net present value (NPV) ⓘ

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers from five enterprise organizations with experience using DigiCert ONE. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is an enterprise with over 200,000 certificates.

Interviewees said that prior to implementing DigiCert ONE, their organizations struggled with fragmented certificate management. This meant there was a lack of central visibility and control, which led to inconsistent practices, ownership confusion, monitoring shortfalls, and substantial operational risk. Further risks and inefficiencies existed due to the manual handling of many certificates and the use of legacy certificate management tools, with the lack of certificate renewal automation leading to significant avoidable labor.

After the investment in DigiCert ONE, the interviewees' organizations centralized certificate management and introduced key improvements to reduce administrative time, minimize security risks, and support business growth. These changes have enhanced their ability to respond to an ever-changing certificate landscape. Key results from the investment included standardized policies, the elimination of manual processes, automated renewals, stronger security, and increased agility to support market expansion.

Key Findings

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

- **A reduction in the cost of incidents by $2.8 million.** The composite organization finds that the frequency of incidents is reduced dramatically, as is the average cost per incident.
- **A reduction in labor costs for renewing certificates that are in place when DigiCert is implemented by $7.9 million.** Switching from legacy tools and manually managed certificates to DigiCert ONE significantly reduces the time and effort the composite organization spends on certificate provisioning and renewals, cutting labor costs as a result of this significant shift to automation.

- **Increased revenue growth from meeting partners' or customers' strict security standards of $1.3 million.**
- **Deprecated legacy tools savings of $993,000.** The composite organization is able to retire a blend of vendor and homegrown tools, saving costs for licensing, hosting, and maintenance.
- **Labor cost savings from removing the manual provisioning and renewing of new certificates of $396,000.** The composite organization transitions all manually managed certificates to DigiCert ONE, significantly reducing the average time to provision and renew certificates.
- **Labor cost savings from removing the provisioning and renewing of new certificates with legacy tools of $30,000.** The composite organization reduces the cost of both provisioning and renewals with DigiCert ONE.

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

- **Consolidated cloud-based certificate management.** DigiCert ONE provides the composite organization with a single cloud-based platform. This provides full visibility into its certificate landscape and enables standardized policies and processes. This leads to significant time and labor savings, stronger security, fewer incidents, and greater agility to manage change.
- **Product development improvements.** The composite organization is able to reduce certificate-related development labor significantly. Issuing certificates is no longer a bottleneck, misconfigured certificates are avoided, and time to market is shortened.
- **Thorough integration.** Integration with existing platforms like Intune, Amazon, and Google Cloud is secure, robust, and straightforward, enabling the composite organization to consistently enforce policies and reduce administrative overhead.
- **Responsive support.** DigiCert provides the composite organization with responsive and effective support, addressing issues quickly and efficiently.
- **Employee satisfaction.** Central teams, developers, and internal auditors at the composite organization report higher satisfaction due to automation, fewer incidents, time savings, and the ability to focus on more strategic, value-driven work.
- **Customer satisfaction.** Fewer incidents and clear adherence to certificate management best practices help build customer trust and support stronger retention.
- **Audit and compliance.** The composite organization is better equipped to meet regulatory requirements with DigiCert ONE. Centralized visibility, standardized policies, and built-in reporting reduce audit workloads and the effort needed for follow-up tasks.
- **Postquantum cryptography preparedness.** DigiCert's involvement in postquantum computing research and in setting interoperability standards makes the composite organization's leaders more confident that the organization's future security needs will be met.

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

- **DigiCert licensing, premium support, and implementation costs of $2.1 million.** The composite organization incurs implementation costs, including planning and DigiCert professional services assistance, as well as ongoing costs for licensing and premium support services.
- **The cost of migrating existing certificate workflows to DigiCert ONE, totaling $1.1 million.** The composite organization needs to transition its 200,000 in-place certificates to DigiCert ONE, which requires discovery, inventory, review, and provisioning activities. Transitioning manually managed certificates typically requires more effort.
- **Labor costs for setting up policies of $46,000.** The composite organization undertakes a one-time project to set up PKI policies and certificate templates during implementation.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $13.3 million over three years versus costs of $3.2 million, adding up to a net present value (NPV) of $10.1 million and an ROI of 312%.

0%

Share of certificates manually managed after implementing DigiCert ONE

Key Statistics

312%

Return on investment (ROI)

$13.3M

Benefits PV

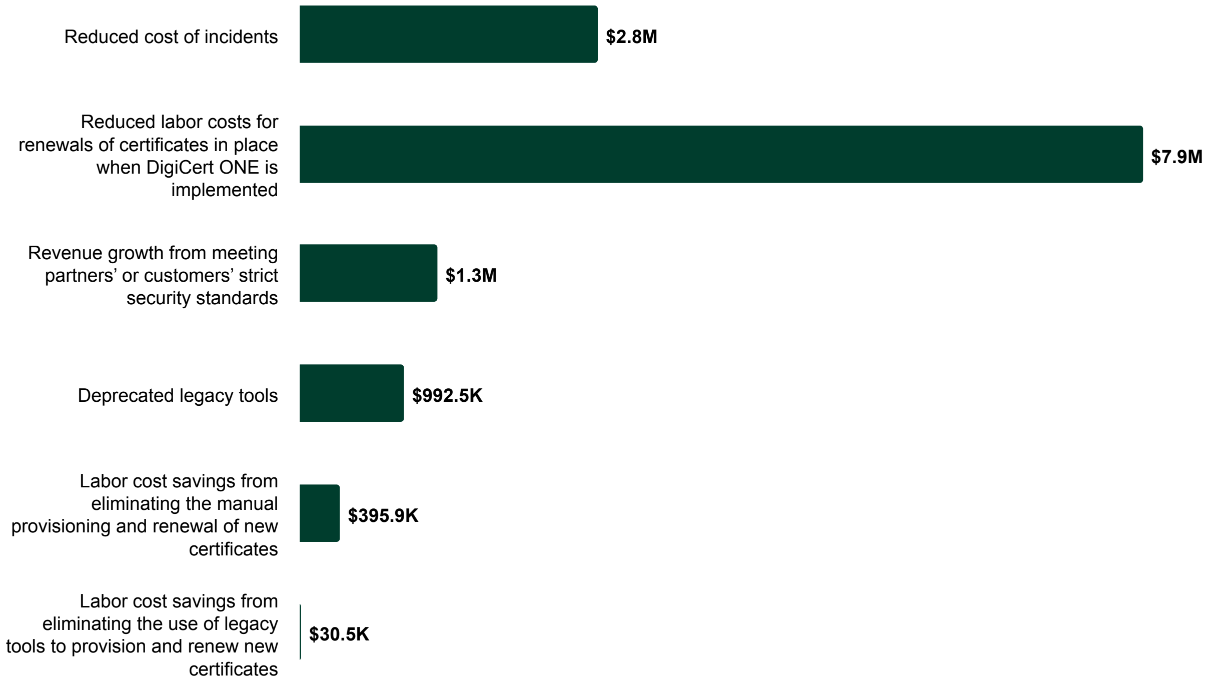
$10.1M

Net present value (NPV)

<6 months

Payback

Benefits (Three-Year)



The DigiCert ONE Customer Journey

Drivers leading to the DigiCert ONE investment

Interviews

Role	Industry	Region	Annual revenue
Global product security officer	Medical device manufacturing	Global (Europe HQ)	$10 billion
Chief reliability officer	Cloud security	Global (North America HQ)	$2 billion
Intellectual property protection manager	Software solutions	Global (Europe HQ)	$5 billion
Chief innovation officer	Energy equipment and solutions	Australia	Not available
Software engineer	Government department	Australia	Not available

Key Challenges

Interviewees' organization relied on a mix of legacy tools and manual processes for managing digital certificates. Multiple teams — and in some cases, individual developers — were responsible for certificate management, with about 20% of certificates handled manually. Due to the lack of centralized control, interviewees said it wasn't possible to enforce consistent policies or standardized processes across the organization.

Interviewees noted how their organizations struggled with common challenges, including:

- **Incidents.** The interviewees described incidents and close calls related to expiring certificates that weren't effectively monitored and renewed. Some certificates lapsed or came close to lapsing, triggering production emergencies. Other certificates expired without warning, leading to outages that affected customers, damaged trust, and required extensive post-incident reviews.
- **Operational challenges.** Interviewees shared that managing and tracking certificates was difficult, especially with multiple departments and owners involved in renewals. In some cases, developers handled certificate signing requests and key management manually — an approach that introduced inefficiencies and didn't follow best practices.
- **Security concerns.** Interviewees said their organizations faced risks due to their reliance on a less secure, network-level security model that wasn't centrally managed. They also faced risks from manual key handling, inconsistent certificate controls, and a lack of centralized visibility — making it hard to track usage or spot expiring certificates. Discovery gaps left unknown certificates unmanaged. Missing certificate profiles, weakened authentication, and limited revocation capabilities delayed threat response. Legacy systems also failed to support modern security standards.
- **Interoperability and partnerships.** Interviewees at organizations with customer-facing products said poor certificate management made it hard to enter new markets and form partnerships. Nonstandard certificates complicated integration with other vendors. As they expanded into new geographic markets, stricter security reviews revealed gaps that caused slowdowns in growing their business. Rapid product development — driven by components' end of life or market demands — added pressure to fix these issues and avoid becoming a bottleneck.
- **Audit and compliance.** According to interviewees, meeting regulatory requirements across industries and regions — especially in sectors like healthcare — required a shift to centralized, standardized certificate management. Audits were costly and time-intensive, as fragmented systems made it difficult to validate environments and prove compliance.
- **A lack of best practices.** Interviewees shared that centralized certificate management is an industry best practice. Their legacy tools lacked modern integration, making it difficult to support secure authentication and identity

management — especially for cloud-connected products. Manual certificate handling was not only inefficient but also introduced a significant risk of outages.

Solution Requirements/Investment Objectives

The interviewees searched for a solution that could:

- **Deliver centralized certificate management.** Interviewees shared that their organizations needed a single, centralized solution to manage certificates across the entire organization — including machines, software, infrastructure, and IoT environments. Key requirements included full visibility with discovery capabilities, standardized policies and processes, and strong monitoring, alerting, and reporting features. The software engineer at a government department shared, "We wanted to bring everything into one ecosystem."
- **Offer simplification and automation.** The interviewees wanted to implement best practices for renewals at their organization, which included eliminating time-consuming and error-prone manual renewals. They also wanted to take advantage of simplification opportunities, such as using standard protocols, more robust and thorough integrations, and better support of monitoring, compliance, and tracking.
- **Provide better security.** Interviewees wanted the solution to be cloud-based, provide highly secure machine-to-machine communications, and provide APIs that were easy to use while meeting robust security requirements. The chief innovation officer at the energy equipment and solutions company shared: "We did a quick market review and picked about four different providers. DigiCert's API was the best in our appraisal for our purpose, with ease of use while providing standard protocols and thorough integration."
- **Improve compliance and auditing.** Interviewees needed the solution to provide standardization, flexibility, as well as policy setting and reporting capabilities in order to transform compliance and regulatory auditing from time-consuming and expensive tasks to controlled, effective, and optimized tasks.
- **Be ready for the future.** Interviewees said they were looking for a solution that could adapt to changing regulations, support global expansion, and strengthen device security protocols. Some also wanted assurance that the solution would be prepared to address future risks from quantum computing.

> *"We required robust authentication mechanisms, effective identity management, and integrity protection. Our goal was to find a single tool to manage all these aspects. DigiCert ONE achieved this without necessitating additional resources for development, testing, or risk management."*
>
> **Global product security officer, medical device manufacturing**

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 interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite organization.** The composite organization is an enterprise that manages 200,000 certificates. It has a central team responsible for certificate management. However, a large percentage of certificates are managed by other departments without adherence to standard policies or processes, and the central team lacks visibility of these. Multiple vendor and in-house tools are utilized, and 20% of certificates are manually managed. The use of certificates rises 20% per year due to expanding needs within products, IoT devices, and software.
- **Deployment characteristics.** The composite organization follows a multi-tiered implementation. It prioritizes the transition to DigiCert ONE of certificates managed with legacy tools and certificates that require near-term renewals; this process is completed within two months. New certificates are provisioned in DigiCert ONE. The remaining certificates — both manually managed and those managed with in-house tools — are transitioned according to near-term renewal dates and other organizational priorities.

KEY ASSUMPTIONS

- An enterprise
- 200,000 certificates in place
- 5,000 new certificates in Year 1
- 20% growth in new certificates

Analysis Of Benefits

Quantified benefit data as applied to the composite organization

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Reduced cost of incidents	$1,035,000	$1,125,000	$1,215,000	$3,375,000	$2,783,509
Btr	Reduced labor costs for renewals of certificates in place when DigiCert ONE is implemented	$2,639,569	$3,167,483	$3,800,979	$9,608,030	7,873,094
Ctr	Revenue growth from meeting partners' or customers' strict security standards	$425,000	$510,000	$612,000	$1,547,000	$1,267,656
Dtr	Deprecated legacy tools	$364,000	$400,400	$440,160	$1,204,560	$992,517
Etr	Labor cost savings from eliminating the manual provisioning and renewal of new certificates	$128,510	$159,667	$195,798	$483,975	$395,889
Ftr	Labor cost savings from eliminating the use of legacy tools to provision and renew new certificates	$9,675	$12,150	$15,492	$37,317	$30,476
	Total benefits (risk-adjusted)	$4,601,754	$5,374,700	$6,279,428	$16,255,882	$13,343,141

Reduced Cost Of Incidents

Evidence and data. Interviewees shared that moving to DigiCert ONE significantly reduced the number of outages and security incidents, lowered the average cost per incident, and helped minimize reputational damage with customers and partners. The reasons they gave for the improvement were consistent:

- Moving all certificate management to DigiCert ONE provided a full-function, centralized certificate management solution, which enabled central policies, broad discovery capabilities, and visibility across the entire organization. The intellectual property protection manager at a software solutions company said: "We had some weak and mismanaged policies. Without a strong policy, there will be security holes that could be altered to include malware. That's a big deal."
- The interviewees appreciated DigiCert ONE's strong monitoring, alerting, and automated renewal capabilities. Incidents or near incidents previously led to outages for employees or customers; they also involved significant labor to prevent or resolve incidents and perform post-incident reviews. The intellectual property protection manager at the software solutions company shared, "We had a certificate revoked, blocking a production line and costing over $50,000."
- The interviewees shared that DigiCert ONE's APIs provided highly reliable integrations. The software engineer at the government department shared: "We use Intune for our device management, so one prerequisite was that we wanted a PKI service that could integrate easily with Intune. DigiCert was one of those, and it integrates seamlessly."
- The interviewees also said that DigiCert ONE ensured secure identification/authentication, encrypted communications, and the use of best-practice security protocols.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Before implementing DigiCert ONE, the composite organization experiences 24 certificate-related incidents in Year 1, 26 certificate-related incidents in Year 2, and 28 certificate-related incidents in Year 3.
- After implementing DigiCert ONE, the certificate-related incident count is reduced to one per year.

- The average cost reduction per incident is $50,000.

Risks. This benefit may vary across organizations for the following reasons:

- The frequency and significance of certificate-related incidents.
- The average cost per incident and the opportunity for cost reduction.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.8 million.

> *"I have not been on a call with a customer related to certificates in the two years that we have had DigiCert."*
>
> **Chief reliability officer, cloud security**

Reduced Cost Of Incidents

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Incidents prior to implementing DigiCert ONE	Composite organization	24	26	28
A2	Incidents after implementing DigiCert ONE	Interviews	1	1	1
A3	Average cost reduction per incident	Interviews	$50,000	$50,000	$50,000
At	Reduced cost of incidents	(A1-A2)*A3	$1,150,000	$1,250,000	$1,350,000
	Risk adjustment	↓10%			
Atr	Reduced cost of incidents (risk-adjusted)		$1,035,000	$1,125,000	$1,215,000

Three-year total: $3,375,000 **Three-year present value: $2,783,509**

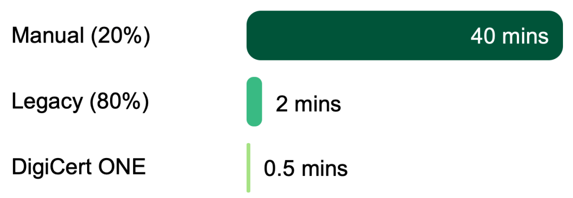
Reduced Labor Costs For Renewals Of Certificates In Place When DigiCert ONE Is Implemented

Evidence and data. The interviewees shared that transitioning existing certificates to DigiCert ONE led to savings on labor costs for both renewals via legacy tools and manual renewals.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The number of certificates in place before DigiCert ONE is implemented and that need renewing is 273,000 in Year 1, 327,600 in Year 2, and 393,100 in Year 3. The composite organization enters Year 1 with 200,000 certificates at various stages of the certificate renewal period and with an average renewal period of less than a year, accounting for the additional certificate renewals.
- 80% of in-place certificates are managed with legacy tools.
- The average renewal time per certificate is 2.0 minutes with legacy tools and 40.0 minutes manually. Implementing DigiCert ONE reduces the average renewal time per certificate to 0.5 minutes.
- The average fully burdened hourly rate for a certificate provisioning FTE is $75.

Certificate Renewals (Averages Per Certificate)



Note: Converting manual certificate renewals to DigiCert ONE reduces average renewals time by 98.75%. Converting legacy tool certificate renewals to DigiCert ONE reduces average renewals time by 75%.

Risks. This benefit may vary across organizations for the following reasons:

- The number of certificates in place when DigiCert ONE is implemented and the average renewal frequency.
- The average time required to renew certificates manually and with legacy tools.
- Labor rates.

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 $7.9 million.

Reduced Labor Costs For Renewals Of Certificates In Place When DigiCert ONE Is Implemented

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Previously provisioned certificates that need renewals	Composite organization	273,000	327,600	393,100
B2	Percentage of certificates previously provisioned with legacy tools	Composite organization	80%	80%	80%
B3	Certificates that need renewal and were previously provisioned with legacy tools	B1*B2	218,400	262,080	314,496
B4	Renewal time per certificate with legacy tools (minutes)	Interviews	2.0	2.0	2.0
B5	Renewal time per certificate with DigiCert ONE (minutes)	Interviews	0.5	0.5	0.5
B6	Certificates that need renewal and were previously provisioned manually	B1*(100%-B2)	54,600	65,520	78,624
B7	Renewal time per certificate manually (minutes)	Interviews	40.0	40.0	40.0
B8	Fully burdened hourly rate for a certificate provisioning FTE	Composite organization	$75	$75	$75
Bt	Reduced labor cost for renewals of certificates in place when DigiCert ONE is implemented	(B3*(B4-B5)+ B6*(B7-B5))*B8/60	$3,105,375	$3,726,450	$4,471.740
	Risk adjustment	↓10%			
Btr	Reduced labor cost for renewals of certificates in place when DigiCert ONE is implemented (risk-adjusted)		$2,794,838	$3,167,483	$3,800,979

Three-year total: $9,608,030 **Three-year present value: $7,873,094**

Revenue Growth From Meeting Partners’ Or Customers’ Strict Security Standards

Evidence and data. Interviewees noted that implementing DigiCert ONE led to revenue growth as a result of expanded market reach and improved customer retention. The interviewees at the medical device manufacturer, software solutions company, and energy equipment and solutions company reported that they gained new business opportunities by strengthening the security of their products and services with DigiCert ONE — helping them build trust with customers and partners.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization is able to grow revenue as a result of meeting partners' or customers' strict security standards by $10 million in Year 1, $12 million in Year 2, and $14.4 million in Year 3.
- The revenue growth impacted by DigiCert ONE's capabilities is 50%. The remaining 50% is due to recognizing opportunities and effective planning, product implementation, and communications to partners and customers.
- The composite organization's net margin is 10%.

Risks. This benefit may vary across organizations for the following reasons:

- Product opportunities due to security improvements.
- Market size.

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 $1.3 million.

50%

Revenue increase from business growth due to product security improvements for one interviewee's organization

> *"Customers were asking, 'What do you do to ensure that unauthorized code doesn't run on your devices?' We realized that DigiCert's software signing process was completely compatible with what we were trying to achieve."*
>
> **Chief innovation officer, energy equipment and solutions**

> *"By providing trusted certificates, we can securely manage our devices and their identities remotely. This approach helps us build trust within the hospital environment and gain a competitive advantage."*
>
> **Global product security officer, medical device manufacturing**

> *"Prior to DigiCert, customer confidence in our certificate management was questionable, we frequently had to get vendor assistance, and we had renewal risks. Now things are going so well that we don't even know who our DigiCert support person is."*
>
> **Chief reliability officer, cloud security**

Revenue Growth From Meeting Partners' Or Customers' Strict Security Standards

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Revenue growth from meeting partners' or customers' strict security standards	Composite organization	$10,000,000	$12,000,000	$14,400,000
C2	Percentage of revenue impacted by DigiCert ONE's capabilities	Interviews	50%	50%	50%
C3	Net margin	Composite organization	10%	10%	10%
Ct	Revenue growth from meeting partners' or customers' strict security standards attributed to DigiCert One	C1*C2*C3	$500,000	$600,000	$720,000
	Risk adjustment	↓15%			
Ctr	Revenue growth from meeting partners' or customers' strict security standards (risk-adjusted)		$425,000	$510,000	$612,000

Three-year total: $1,547,000 **Three-year present value: $1,267,656**

Deprecated Legacy Tools

Evidence and data. Interviewees shared that their organizations had a mix of homegrown and legacy tools that they were able to eliminate when they implemented DigiCert ONE. Areas of savings included licensing for vendor tools, IT development for homegrown tools, IT maintenance, and hosting.

Modeling and assumptions. Based on the interviews, Forrester assumes the composite organization experiences deprecated legacy tool cost savings of $455,000 in Year 1, $500,500 in Year 2, and $550,200 in Year 3.

Risks. This benefit may vary across organizations for the following reasons:

- The costs to license, host, and maintain vendor tools.
- The costs to enhance, host, and maintain homegrown tools.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $993,000.

> *"We no longer maintain an on-premises infrastructure supporting certificates. This is much better in many ways. For one thing, there's a cost savings."*
>
> **Software engineer, government department**

Deprecated Legacy Tools

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Deprecated legacy tools (homegrown or vendor solutions)	Interviews	$455,000	$500,500	$550,200
Dt	Deprecated legacy tools	D1	$455,000	$500,500	$550,200
	Risk adjustment	↓20%			
Dtr	Deprecated legacy tools (risk-adjusted)		$364,000	$400,400	$440,160

Three-year total: $1,204,560 **Three-year present value: $992,517**

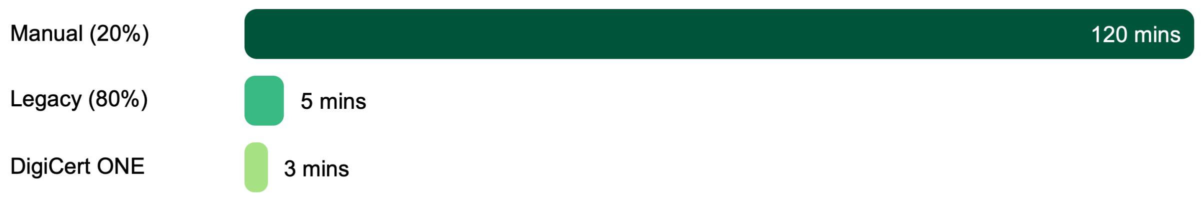
Labor Cost Savings From Eliminating The Manual Provisioning And Renewal Of New Certificates

Evidence and data. The interviewees said that they essentially eliminated manual provisioning and maintenance at their organizations. On average, they experienced significant time savings for provisioning and renewal per new certificate due to DigiCert ONE's streamlined provisioning and renewal capabilities, including automated renewals for a large percentage of certificates.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The number of new certificates it provisions is 5,000 in Year 1, 6,000 in Year 2, and 7,200 in Year 3.
- Prior to implementing DigiCert ONE, it would provision 20% of new certificates manually: 1,000 in Year 1, 1,200 in Year 2, and 1,440 in Year 3.
- The average time to manually provision a new certificate is 120 minutes; the average time to provision a new certificate with DigiCert ONE is 3.0 minutes.
- The composite organization would renew 100 new certificates manually in Year 1, 250 in Year 2, and 400 in Year 3.
- The average time to manually renew a certificate is 40.0 minutes; the average time to renew a certificate with DigiCert ONE is 0.5 minutes.
- The fully burdened hourly rate for a certificate provisioning FTE is $75.

Certificate Provisioning (Averages Per Certificate)



Note: Converting manual certificate provisioning to DigiCert ONE reduces average provisioning time by 97.5%. Converting legacy tool certificate provisioning to DigiCert ONE reduces average provisioning time by 40%.

Risks. This benefit may vary across organizations for the following reasons:

- The number of new certificates manually provisioned per year.
- The average time required to provision and renew certificates manually.
- Labor rates.

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 $395,000.

Labor Cost Savings From Eliminating The Manual Provisioning And Renewal Of New Certificates					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	New certificates that need provisioning	Composite organization	5,000	6,000	7,200
E2	Percentage of new certificates provisioned manually	Composite organization	20%	20%	20%
E3	New certificates provisioned manually	E1*E2	1,000	1,200	1,440
E4	Manual provisioning time per certificate (minutes)	Interviews	120.0	120.0	120.0
E5	Provisioning time per certificate with DigiCert ONE (minutes)	Interviews	3.0	3.0	3.0
E6	New certificates renewed manually	Composite organization	100	250	400
E7	Manual renewal time per certificate (minutes)	B7	40.0	40.0	40.0
E8	Renewal time per certificate with DigiCert ONE (minutes)	B5	0.5	0.5	0.5
E9	Fully burdened hourly rate for a certificate provisioning FTE	B8	$75	$75	$75
Et	Labor cost savings from eliminating the manual provisioning and renewal of new certificates	(E3*(E4-E5)+ E6*(E7-E8))* E9/60	$151,188	$187,844	$230,350
	Risk adjustment	↓15%			
Etr	Labor cost savings from eliminating the manual provisioning and renewal of new certificates (risk-adjusted)		$128,510	$159,667	$195,798
	Three-year total: $483,975		**Three-year present value: $395,889**		

Labor Cost Savings From Eliminating The Use Of Legacy Tools To Provision And Renew New Certificates

Evidence and data. Interviewees said their organizations fully transitioned certificate provisioning and maintenance to DigiCert ONE. By centralizing processes and using DigiCert ONE's streamlined tools, they saved time on provisioning. Even greater time savings came from automating most certificate renewals through DigiCert ONE.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization provisions 5,000 new certificates in Year 1, 6,000 in Year 2, and 7,200 in Year 3.
- Prior to implementing DigiCert ONE, it provisions 80% of new certificates with legacy tools: 4,000 in Year 1, 4,800 in Year 2, and 5,760 in Year 3.
- The average time to provision a new certificate with legacy tools is 5.0 minutes; the average time to provision a new certificate with DigiCert ONE is 3.0 minutes.
- Using legacy tools, the composite organization would renew 400 new certificates in Year 1, 800 in Year 2, and 1,500 in Year 3.
- The average renewal time per certificate with the legacy tools is 2.0 minutes; the average renewal time per certificate with DigiCert ONE is 0.5 minutes.
- The fully burdened hourly rate for a certificate provisioning FTE is $75.

Risks. This benefit may vary across organizations for the following reasons:

- The number of new certificates provisioned with the legacy tools per year.
- The average time required to provision and renew certificates with the legacy tools.
- Labor rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $30,000.

> *"DigiCert's API was intuitive, well documented, and aligned with our developer's mental model."*
>
> **Chief innovation officer, energy equipment and solutions**

Labor Cost Savings From Eliminating The Use Of Legacy Tools To Provision And Renew New Certificates

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	New certificates that need provisioning	E1	5,000	6,000	7,200
F2	Percentage of new certificates provisioned with legacy tools	Composite organization	80%	80%	80%
F3	New certificates provisioned with legacy tools	F1*F2	4,000	4,800	5,760
F4	Provisioning time per certificate with legacy tools (minutes)	Interviews	5.0	5.0	5.0
F5	Provisioning time per certificate with DigiCert ONE (minutes)	E5	3.0	3.0	3.0
F6	New certificates that need renewals	Composite organization	400	800	1,500
F7	Renewal time per certificate with legacy tools (minutes)	Interviews	2.0	2.0	2.0
F8	Renewal time per certificate with DigiCert ONE (minutes)	B5	0.5	0.5	0.5
F9	Fully burdened hourly rate for a certificate provisioning FTE	B8	$75	$75	$75
Ft	Labor cost savings from eliminating the use of legacy tools to provision and renew new certificates	(F3*(F4-F5)+ F6*(F7-F8))*F9/60	$10,750	$13,500	$17,213
	Risk adjustment	↓10%			
Ftr	Labor cost savings from eliminating the use of legacy tools to provision and renew new certificates (risk-adjusted)		$9,675	$12,150	$15,492

Three-year total: $37,317 **Three-year present value: $30,476**

Unquantified Benefits

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

- **Consolidated, cloud-based certificate management.** A centrally managed solution provides the composite organization with a number of benefits. Interviewees specifically noted the ability to create standard policies and processes, optimize labor-saving practices, have organizationwide certificate visibility, clearly identify certificate ownership and accountability, and ensure that security measures, monitoring, and renewal automation are in place to minimize security and outage risks.

> *"We can centrally manage this, and we easily know what we use, where we use this, and also that we can ensure standards."*
>
> **Global product security officer, medical device manufacturing**

- **Product development improvements.** Interviewees shared that they reduced certificate-related development labor by over 50% due to the ease of use of DigiCert's APIs. Interviewees also said they reduced the time for product quality assurance in terms of validation and verification by over 50%. The time savings helped them bring products to market faster.

- **Thorough integration.** DigiCert ONE's robust, seamless integration with existing systems like Intune, Amazon Web Services, and Google Cloud makes the overall certificate process more user-friendly and consistent.
- **Responsive support.** DigiCert provides responsive and effective support to the composite organization, addressing issues quickly and efficiently. The software engineer at the government department shared: "Their responsiveness was great. No issues getting to them, and whenever we had any queries or anything, if we saw any issues they got onto it very quickly."
- **Employee satisfaction.** Employee satisfaction improved across IT teams for several reasons. Interviewees noted that central teams gained full control and visibility, eliminating the manual work and risk tied to certificate provisioning and renewals. Developers no longer had to manage certificates themselves, reducing stress and security concerns. Internal auditors benefited from having centralized policies and processes in a more structured environment.
- **Customer satisfaction.** By following best-practice security standards, organizations can give customers of the composite organization confidence that their certificate management system is secure and reliable. Interviewees noted higher customer satisfaction and retention due to fewer issues with certificate expirations and fewer management errors.
- **Audit and compliance.** DigiCert ONE helps the composite organization reduce regulatory compliance costs by introducing standardized protocols, certificates, and reporting. Interviewees noted that its centralized, automated system eased audit workloads and made it simpler to meet regulatory requirements. This was especially important for industries with strict data protection rules like HIPAA and GDPR. The interviewees also noted that implementing DigiCert ONE improved their organizations' ability to respond to evolving security threats.

> *"Now we are sure that we have all of the [certificate usage] information. ... Before we said, 'As far as we know.' We now are confident going into audits."*
>
> **Intellectual property protection manager, software solutions**

> *"The centralized and automated approach reduced the audit load and made compliance easier, significantly lowering the costs associated with audits. We are in a highly regulated industry. Our audits went from costing over a million dollars a year to a couple of hundred thousand."*
>
> **Chief reliability officer, cloud security**

- **Postquantum cryptography preparedness.** Interviewees shared that DigiCert's role in postquantum cryptography research and standards development gives their leadership greater confidence that future security needs will be anticipated and addressed.

> *"We are going to see quantum computing hit its stride within the next few years. I'm really enamored with the fact that DigiCert seems to be at the cutting edge of that."*
>
> **Chief innovation officer, energy equipment and solutions**

Flexibility

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

- **Meeting internal requirements.** DigiCert ONE provides the ability to make changes to policies and procedures globally, by use case, by department, or by geographic region. With central control, these changes can be done easily and quickly.
- **Improving the response to change.** Interviewees said DigiCert ONE helped their organizations adapt to regulations, expand into new regions, and strengthen machine security. It also enabled them to respond quickly and cost-effectively to changes in certificate management requirements.
- **Adapting to product development and manufacturing changes.** Interviewees shared that DigiCert ONE's APIs enabled them to rapidly adapt to new use cases and certificate types, saving effort and improving their time to market. The chief innovation officer at the energy equipment and solutions company shared, "We can quickly build a custom tool to match a workflow, which has simplified our manufacturing and provisioning processes."

> *"We deliver to over 140 countries worldwide, each with unique market and regulatory requirements. The flexibility to centrally manage our products throughout their lifecycle was a key requirement for us. Therefore, we sought a holistic solution that could be seamlessly integrated into our existing processes to support these diverse needs."*
>
> **Global product security officer, medical device manufacturing**

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

Analysis Of Costs

Quantified cost data as applied to the composite organization

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Gtr	DigiCert ONE licensing, premium support, and implementation costs	$42,000	$750,750	$825,300	$907,200	$2,525,250	$2,088,159
Htr	Cost of migrating existing certificates to DigiCert ONE	$1,100,000	$0	$0	$0	$1,100,000	$1,100,000
Itr	Labor costs for DigiCert ONE policy set-up	$49,500	$0	$0	$0	$49,500	$49,500
	Total costs (risk-adjusted)	$1,191,500	$750,750	$825,300	$907,200	$3,674,750	$3,237,659

DigiCert ONE Licensing, Premium Support, And Implementation Costs

Evidence and data. Interviewees said their organization incurred implementation costs, including those for planning and DigiCert professional services assistance. They also paid ongoing costs for licensing and premium support services.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Licensing is $650,000 in Year 1, $715,000 in Year 2, and $786,000 in Year 3.
- Premium support services cost $65,000 in Year 1, $71,000 in Year 2, and $78,000 in Year 3.
- Internal and professional implementation and training costs are $40,000.

Risks. These costs may vary across organizations for the following reasons:

- The variability and complexity of the existing infrastructure.
- The use of premium support services.
- The maturity and size of the central team.
- The cooperation of any departments affected.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.1 million.

> *"We told DigiCert that we had very limited time for deployment. I was surprised how quickly it was done."*
>
> **Software engineer, government department**

DigiCert Licensing, Premium Support, And Implementation Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Licensing	Interviews		$650,000	$715,000	$786,000
G2	Premium support	Interviews		$65,000	$71,000	$78,000
G3	Implementation and training costs (internal and professional services)	Interviews	$40,000			
Gt	DigiCert licensing, premium support, and implementation costs	G1+G2+G3	$40,000	$715,000	$786,000	$864,000
	Risk adjustment	↑5%				
Gtr	DigiCert licensing, premium support, and implementation costs (risk-adjusted)		$42,000	$750,750	$825,300	$907,200

Three-year total: $2,525,250 **Three-year present value: $2,088,159**

Cost Of Migrating Existing Certificates To DigiCert ONE

Evidence and data. The interviewees said that transitioning their in-place certificates to DigiCert ONE required discovery, inventory, review, and provisioning activities. They also shared that transitioning manually managed certificates typically required more effort.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- It has 200,000 certificates in place when DigiCert ONE is implemented, with 80% provisioned before the renewal process.
- Discovery, inventory, review, and provisioning activities take 5 minutes per certificate.
- The fully burdened hourly rate of a certificate provisioning FTE is $75.

Risks. These costs may vary across organizations for the following reasons:

- The cooperation of any departments affected.
- The ratio of manual to legacy managed certificates.
- The percentage of certificates transitioned at the time of renewal.
- Labor rates.

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 $1.1 million.

Cost Of Migrating Existing Certificates To DigiCert ONE

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Previously provisioned certificates	Composite organization	200,000			
H2	Percentage of certificates provisioned before renewal	Interviews	80%			
H3	Time to discover, inventory, review, and provision per certificate (minutes)	Interviews	5			
H4	Fully burdened hourly rate for a certificate provisioning FTE	B8	$75			
Ht	Cost of migrating existing certificates to DigiCert ONE	H1*H2*H3*H4/60	$1,000,000	$0	$0	$0
	Risk adjustment	↑10%				
Htr	Cost of migrating existing certificates to DigiCert ONE (risk-adjusted)		$1,100,000	$0	$0	$0
	Three-year total: $1,100,000		**Three-year present value: $1,100,000**			

Labor Costs For Policy Set-Up

Evidence and data. The interviewees highlighted that setting up PKI policies and certificate templates was a one-time project during implementation; they held periodic reviews per their organizational requirements.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization has 150 initial policies and templates to add to DigiCert ONE. These include Certificate Policies, Certificate Practice Statements, plus certificate configuration templates for automation.
- Reviewing, adjusting, and implementing policies takes 4 hours per policy.
- The fully burdened hourly rate for a certificate provisioning FTE is $75.

Risks. These costs may vary across organizations for the following reasons:

- Different policy-to-certificate ratios.
- Different labor requirements to define and create policies.

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 $50,000.

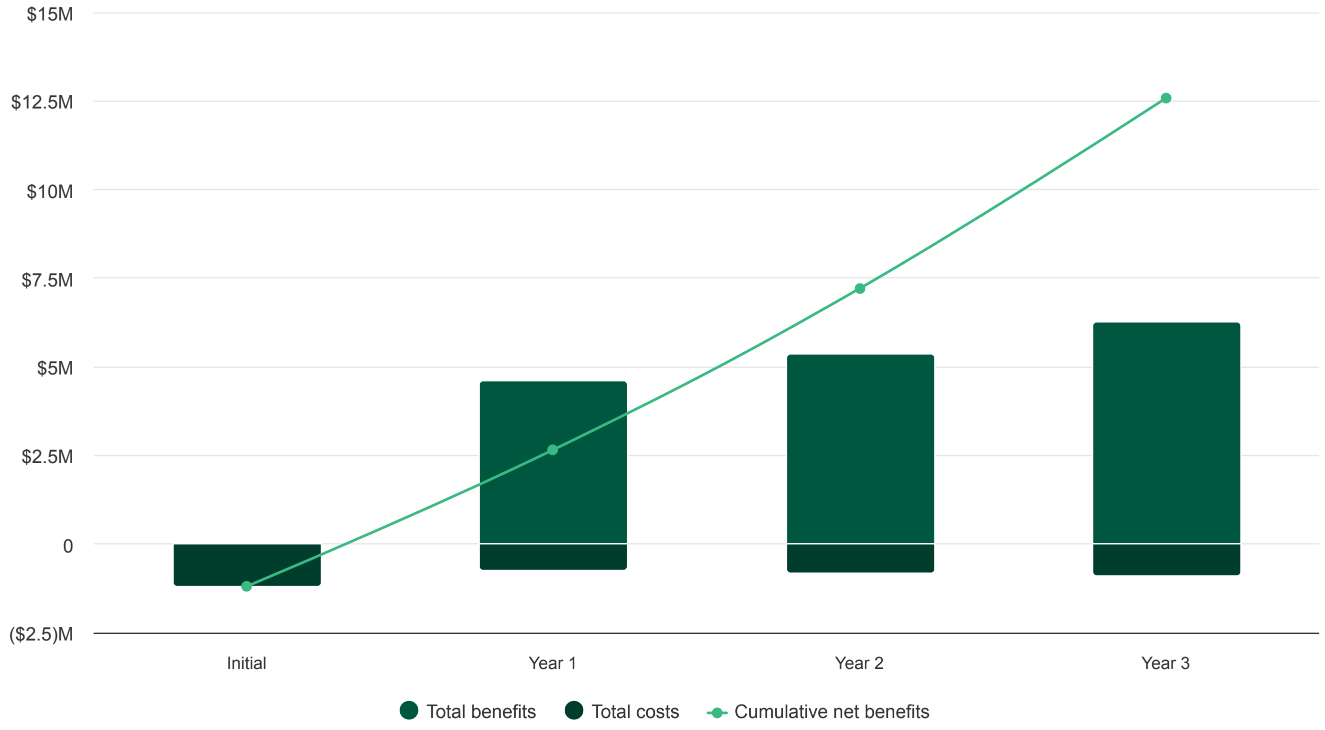
Labor Cost For Policy Set-Up

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	Number of policies	Composite	150			
I2	Time to review, adjust, and implement each policy (hours)	Interviews	4			
I3	Fully burdened hourly labor rate for a certificate provisioning FTE	B8	$75			
It	Labor cost for policy set-up	I1*I2*I3	$45,000	$0	$0	$0
	Risk adjustment	↑10%				
Itr	Labor cost for policy set-up (risk-adjusted)		$49,500	$0	$0	$0
	Three-year total: $49,500		**Three-year present value: $49,500**			

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($1,191,500)	($750,750)	($825,300)	($907,200)	($3,674,750)	($3,237,659)
Total benefits	$0	$4,601,754	$5,374,700	$6,279,428	$16,255,882	$13,343,141
Net benefits	($1,191,500)	$3,851,004	$4,549,400	$5,372,228	$12,581,132	$10,105,482
ROI						312%
Payback						<6 months

ⓘ Please Note

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.

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.

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 DigiCert ONE.

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 DigiCert ONE can have on an organization.

Due Diligence

Interviewed DigiCert stakeholders and Forrester analysts to gather data relative to DigiCert ONE.

Interviews

Interviewed five decision-makers at organizations using DigiCert ONE to obtain data about 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.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

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

Risks

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."

Financial Terminology

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

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

Appendixes

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Supplemental Material

Related Forrester Research

The Top Trends Shaping Identity And Access Management In 2025, Forrester Research, Inc., March 6, 2025

The Future Of Quantum Security, Forrester Research, Inc., February 13, 2025

APPENDIX C

Endnotes

[1] Source: Clint Wilson, Voting Period Begins: SC-081v3: Introduce Schedule of Reducing Validity and Data Reuse Periods, Certification Authority Browser Forum.

[2] Source: The Top Trends Shaping Identity And Access Management In 2025, Forrester Research, Inc., March 6, 2025.

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

[4] Please note that DigiCert commissioned this report prior to the close of its acquisition of Ultra DNS, hence the absence of metrics related to DNS.

Disclosures

Readers should be aware of the following:

This study is commissioned by DigiCert and delivered by Forrester Consulting. It is not meant to be used as 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 study to determine the appropriateness of an investment in DigiCert ONE. For any interactive functionality, the intent is for the questions to solicit inputs specific to a prospect's business. Forrester believes that this analysis is representative of what companies may achieve with DigiCert ONE based on the inputs provided and any assumptions made. Forrester does not endorse DigiCert or its offerings. Although great care has been taken to ensure the accuracy and completeness of this model, DigiCert and Forrester Research are unable to accept any legal responsibility for any actions taken on the basis of the information contained herein.

DigiCert reviewed and provided feedback to Forrester, but 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 of the study.

DigiCert provided the customer names for the interviews but did not participate in the interviews.

Consulting Team:

Eric Hall

PUBLISHED

July 2025