An IDC White Paper, sponsored by DigiCert

IDC | ANALYZE THE FUTURE

DigiCert PKI Platform Optimizes Security Operations Leading to Improved Business Results

RESEARCH BY:

Frank Dickson
Program Vice President,
Cybersecurity Products, IDC

Harsh Singh
Senior Research Analyst,
Business Value Strategy Practice,
IDC

January 2021 | IDC Doc. #US45385819

Navigating this White Paper

Click on titles or page numbers to navigate to each section.

Executive Summary

Organizations can save nearly $1 million annually by adopting a cloud-based, fully managed PKI service to address the growing complexity of network and endpoint security and authentication requirements, according to an IDC analysis of the costs associated with managing PKI.

The IDC study commissioned by DigiCert found IT security and infrastructure staff frequently burdened by implementing and managing PKI due to a variety of factors, including rising pressures of providing secure and reliable connectivity across hybrid and multicloud environments, the skyrocketing number of connected devices requesting network access, and the soaring pace of data growth in the organization. Organizations found that cloud-based, managed security services improve efficiency and free up the IT security and infrastructure teams to improve reliability and the security posture. In some cases, the automation provided by the managed PKI service can eliminate costly vulnerabilities and configuration issues that result in costly disruption and identify errors that can lead to the loss or exposure of sensitive data.

The DigiCert PKI Platform is a cloud-based (with an on-premises option) security service platform designed to enable organizations to quickly issue digital certificates for authentication, encryption, and digital signing. The PKI platform helps companies manage confidential information, authenticate the identity of users and devices, verify the integrity of documents and protect data in transit. IDC conducted research that explored the value and benefits of using DigiCert PKI Platform to optimize the tasks and processes that support these goals and activities. This research was based on interviews with multiple DigiCert customers that used the service platform. IDC found that they realized significant benefits by leveraging its capabilities to help IT and security teams be more productive and better contribute to business needs.

DIGICERT PKI PLATFORM BUSINESS VALUE HIGHLIGHTS

Click on highlights below to navigate to related content within this white paper.

326%
five-year ROI

13 months
to breakeven

72% faster
deployment of certificates

60% more
productive PKI management staff

60% more
efficient IT security teams

42% more
efficient IT infrastructure staff

76% reduction
in unplanned downtime

$156,000
reduced operating expense

Based on IDC's calculations, these organizations realized discounted benefits worth $951,000 per organization per year by:

- Increasing the productivity of IT, PKI, and security management teams in the performance of routine operations
- Supporting faster issuance and renewal of certificates leading to improved business operations
- Reducing IT operating expenses for security and security-related operations
- Improving end-user productivity by reducing the effects of unplanned downtime on business users

DigiCert PKI Platform Product Overview

DigiCert's managed PKI service is an automated, cloud-based PKI platform that can support a wide variety of security use cases from secure email, Wi-Fi device authentication, and secure remote access to mobile device management, document signing, and strong web authentication. The DigiCert PKI Platform service can support high-volume, fast certificate issuance and provides automatic certificate deployment and custom certificate request approval rules on a publicly trusted root compatible with all major operating systems and secure applications including email, document signing, mobile device management, and remote access. In addition to certificate issuance and management for user and device certificates, the service reduces costly configuration errors by eliminating the need for self-signed certificates and providing manual tracking. The service also provides the flexibility to use various provisioning processes and supports leading mobile device management vendors.

For managing user and device certificates, the service can be customized to your organization's unique certificate workflows and Active Directory to support rule-based automatic provisioning and issuance within minutes. The tool supports a variety of protocols including REST, Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST), and Windows Autoenrollment.

Following the completion of this study, DigiCert released DigiCert ONE, a container-based platform. DigiCert ONE centralizes user and device certificate management for a variety of deployment models and PKI use cases. DigiCert Enterprise PKI Manager, an application on top of the DigiCert ONE platform, manages device identity, authentication, encryption, and integrity for enterprises, similarly covering use cases like the ones mentioned in this document. Enterprise PKI Manager, can be combined with other Managers including DigiCert Secure Software Manager, DigiCert IoT Device Manager, DigiCert Document Signing Manager and DigiCert CertCentral TLS Manager, to centralize user and device certificate management and trust across

IT architectures. As this study was done before this product's release, we do not have feedback from DigiCert customers on this new update, but the fundamentals of savings on staffing, cost, and productivity may apply for the new deployment models. IDC has not validated the assertion as part of this research study.

The Business Value of DigiCert PKI Platform

Study Demographics

IDC conducted research that explored the value and benefits of using DigiCert PKI Platform to optimize IT infrastructure. The project included nine interviews with organizations using the service platform that had experience with or knowledge about its benefits and costs. During the interviews, companies were asked a variety of quantitative and qualitative questions about the impact of the solution on their IT and security operations, businesses, and costs.

Table 1 presents study demographics and profiles. Organizations interviewed had a base of 42,389 employees of which 35,833 of those employees were using IT services. These IT users are supported by an IT staff of 9,766. IT teams were responsible for the operation of 508 business applications serving 28.89 million external customers. From a vertical industries standpoint, organizations come from the manufacturing, government, marketing, telecommunications, nonprofit, financial services, education, and retail sectors. (Note: All numbers cited represent averages.)

TABLE 1

Firmographics of Interviewed Organizations

	Average	Median
Number of employees	42,389	6,000
Number of IT staff	9,766	300
Number of IT users	35,833	5,000
Number of external customers	28.89 million	3,200
Number of business applications	508	125
Number of devices used by employees	59,167	25,000
Revenue per year	$29.0 billion	$800 million
Industries	Manufacturing (2), government, marketing, telecommunications, nonprofit, financial services, education, and retail	

Source: IDC, 2019

Choice and Use of DigiCert PKI Platform

The companies surveyed described usage patterns for DigiCert PKI Platform as well as provided a snapshot of their overall IT and business environments. They also discussed the rationale behind their choice of the DigiCert platform. Customers cited a number of factors for choosing DigiCert including improved management made possible by a cloud-based solution, fully automated issuance and renewal capability, and the ability to standardize key security functions. The company's reputation with Fortune 500 companies was cited as well as the benefit of the expertise available from DigiCert staff that helped with implementation. Study participants elaborated on these benefits:

- **Easier certificate issuance:** *"The biggest challenge that DigiCert solved was integrating our internal portal for the issuance of certificates. This is significant because a user who needs to acquire a certificate can go in and put into our system what they need, and that information is seamlessly handed off into DigiCert and returned. It's fully automated for issuance support and renewal. This level of integration into our existing infrastructure was highly attractive for our business."*
- **Improved standardization:** *"We needed a common security certification platform that everybody was on the same page with instead of having one group doing self-signed certificates and another group doing a different type of certificate. The objective was to get a standard in place for all departments to use."*
- **Easier management:** *"Our organization is growing but unfortunately our IT staff has not. We wanted to eliminate our internal certificate authority which was an internal piece of hardware that my staff and I had to manage. It was a 'spinning plate' we had to keep moving. If it fell and broke, then it was my problem. The ability for DigiCert to provide PKI services in the cloud was really attractive. Since we were already working with them, there was no need for me to look elsewhere."*
- **Ability to protect key data:** *"We found that DigiCert was the gold standard and used by a large percentage of Fortune 500 companies. We were also impressed with their expertise. Since our information is highly classified, we looked at other industries that also need to protect sensitive information such as banks. The DigiCert platform itself was all encompassing. They also did some consulting with us to help us with implementation and understanding our overall IT infrastructure. They definitely were the best fit, so the cost was worth it."*

Table 2 describes the organizational usage of DigiCert PKI Platform. As shown in Table 2, the number of internal users supported was 31,306 that are utilizing 75,356 devices. In addition, the number of external-facing websites supported was 165, and the number of business applications was 435. Additional usage patterns are presented in Table 2. (Note: All numbers cited represent averages.)

TABLE 2

Organizational Usage of DigiCert PKI Platform

	Average	Median
Number of branches/sites	47	16
Number of internal users supported	31,306	4,200
Number of external users supported	2.89 million	2,000
Number of external-facing websites	165	55
Number of business applications	435	20
Number of network endpoint devices	75,356	3,350
Total revenue	36%	34%

Source: IDC, 2019

Table 3 provides more data on DigiCert certificate usage. The greatest usage was noted in two areas: multidomain and SSL inspection, both at 89% of organizations surveyed. The code signing and client application were calculated at 67%, and Wi-Fi device authentication and VPN were calculated at 56%. Additional usage patterns are also presented in Table 3.

TABLE 3

DigiCert Certificate Usage

	Percentage of Interviewed Organizations
Multidomain	89
SSL inspection	89
Code signing	67
Client	67
Wi-Fi device authentication	56
VPN	56
Document signing	44
S/MIME	11

Source: IDC, 2019

Business Value and Quantified Benefits

IDC's Business Value model expresses the benefits for organizations using the DigiCert PKI service platform to support their security infrastructure and ongoing operations. Survey data from DigiCert customers was applied to this model to arrive at an array of quantified post-deployment benefits. Using this methodology, IDC found that these customers realized significant value for their IT, security, and business operations.

These benefits were tied to a number of value-added service characteristics. The use of DigiCert fostered more efficient IT operations by increasing the productivity of IT and security teams and optimizing the tasks and processes they undertook daily. These efficiencies increased their ability to support lines of business (LOBs) by issuing and renewing certificates more quickly and performing other security-related tasks. Additional benefits centered on reducing IT infrastructure costs and the effects of unplanned downtime on business users contributing to greater productivity and helping LOB units operate more effectively in pursuit of business goals. Study participants discussed the most significant benefits of using the DigiCert PKI Platform service:

- **Ease of management:** *"DigiCert had the best overall expertise and pricing. We wanted all of our certificates on one single platform, and its management platform allows us to track everything. It simplifies complex processes and makes them easy to implement and manage."*
- **Improved performance:** *"We liked the flexibility and features that it gave us. We can issue certificates that go in the applications themselves. We are trying to tie up and encrypt the entire stack all the way from the end user down to the database. We have requirements for any PKI information to be encrypted."*
- **Simpler management and lower costs:** *"It's a comprehensive tool that is easy to use, so it makes tasks and operations easier to manage. We also did a cost comparison and found its prices were about 10% less than everyone else we looked at."*
- **Good fit for the organization:** *"We felt that DigiCert was the best at handling root certificate security and certificate issuance. We wanted to use a trusted and well-known third party in our verification process. Another big factor in our decision was that we had a consultant come over with significant managed PKI expertise. He helped with our entire initiative and did a really good job of due diligence. He said DigiCert fit our organization the best, and everybody agreed."*
- **Builds trust:** *"DigiCert ensures that our system is stable and can be trusted internally and externally. One of the biggest challenges internally is that we've got so many different applications. Some of them are so old that they are just not going to work. And in some cases, they might work, but not securely. Externally, it shows we are serious about security and that your information is trusted … so they complete the deal. Finally, DigiCert plays a big role in integrating with our internal service portal. That is huge because it saves both time and money."*

IDC quantified the total value that study participants are achieving through their use of DigiCert PKI Platform. Based on IDC's calculations, these organization realized discounted benefits worth $951,000 per organization per year.

Improvements in IT and Security Efficiencies

DigiCert PKI Platform was designed to optimize processes that manage access to confidential information, authenticate the identity of users and devices, and verify the integrity of documents and communications. The platform is cloud based and offers over 30 out-of-the-box certificate profiles, integrates with applications such as Active Directory, and automates the often complex management tasks associated with security operations. DigiCert PKI targets core security functions such as identity management for IoT and network access, directory services, and business applications and addresses a variety of functional areas including:

- Secure remote access
- VPN
- Wi-Fi access points
- Mobile device management
- Secure network access
- Smart card log in
- Secure email
- Secure code signing and key protection
- Secure documents and signing

Study participants described how DigiCert PKI Platform freed them up to focus on larger issues of IT security, a benefit made possible by the platform's ability to proactively identify vulnerabilities and work on permanent fixes. They also described its ability to speed up certificate issuance from weeks to days and provide a smoother process with less glitches and unexpected events. Admins spent less time on security, and time was freed up for IT and security teams to focus on more strategic projects. Study participants elaborated on these and other benefits:

- **Time freed up to focus on strategic projects:** *"DigiCert PKI Platform freed up time to concentrate on the bigger picture. Some employees have been repurposed to focus on our overall larger strategy, which is migrating the majority of our on-premises to the cloud. We were able to dedicate them to the implementation of the cloud structure."*
- **Simpler certification management:** *"Our IT operations became much faster. We love the portal. It literally takes a couple of minutes to provision a certificate. And it's self-serve. I have 14 admins that use it, and it causes minimal disruption to their work. You submit the request then you get a certificate installed on the server."*
- **More efficient certificate management:** *"We're more efficient. DigiCert helps us spend our time where we think it's more effective. We don't have to worry about frantic phone calls because a presenter or a vendor showed up the last minute. We can issue certificates and grant access from anywhere."*
- **Better security focus:** *"We are able to focus on our larger issues of IT security, proactively uncovering vulnerabilities, and working on permanent fixes or temporary patches."*

IDC quantified these and other benefits. Table 4 shows PKI environment management impacts. These are the benefits associated with security teams specifically dedicated to working with the DigiCert platform compared with their previous certificate environment. These teams saw a 60% improvement in time freed up, which is worth about 4.2 FTEs. This translated into a staff time cost savings per year of $422,000.

TABLE 4

PKI Environment Management Impact

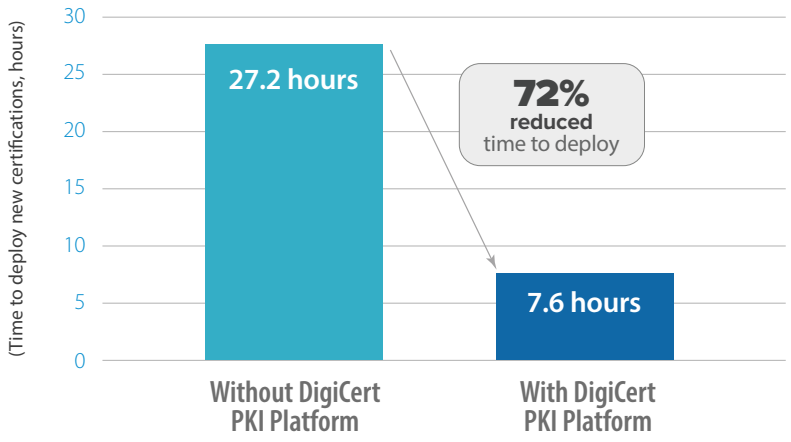
	Before DigiCert PKI Platform	With DigiCert PKI Platform	Difference	Benefit (%)
PKI environment management (FTE equivalent per organization per year)	7	2.8	4.2	60
Staff time cost per year	$697,000	$276,000	$422,000	60

Source: IDC, 2019

As described previously, DigiCert PKI offered companies the benefit of speeding up certificate issuance significantly and creating a smoother process for security teams. IDC looked more closely at how these efficiencies affected issuance, as shown in Figure 1. The time required to deploy certificates was significantly reduced from 27.2 hours on average to 7.6 hours, representing a 72% improvement.

FIGURE 1

IT Certificate Security Staff Impact



Source: IDC, 2019

Table 5 shows quantified gains in certificate security staff efficiency associated with routine tasks. FTE equivalence values (per organization per year) showed that about 3.5 FTEs were freed up, a 60% improvement. These gains were reflected in staff time cost savings per year, which were calculated at $352,000.

TABLE 5

IT Certificate Security Staff Impact

	Before DigiCert PKI Platform	With DigiCert PKI Platform	Difference	Benefit (%)
IT certificate security (FTE equivalent per organization per year)	5.9	2.4	3.5	60
Staff time cost per year	$589,000	$237,000	$352,000	60

Source: IDC, 2019

As mentioned previously, study participants discussed how DigiCert PKI allowed admins to do their jobs with a minimal amount of interruption and overhead. Table 6 looks at the impacts of the platform on IT teams and IT infrastructure management. Average equivalent FTEs (per year per organization) needed to manage any PKI-related IT infrastructure were reduced from 5.5 to 3.2, representing a 42% improvement. Translated into financial terms, this amounted to an annual cost savings of $233,000.

TABLE 6

IT Infrastructure Management Impact

	Before DigiCert PKI Platform	With DigiCert PKI Platform	Difference	Benefit (%)
Management of IT infrastructure productivity impact (equivalent FTEs)	5.5	3.2	2.3	42
Salary cost per year per organization	$552,000	$319,000	$233,000	42

Source: IDC, 2019

These benefits extended to auditing teams as well. Some organizations described to IDC a newfound ability to implement audit policies as a result of utilizing the DigiCert PKI Platform. Other organizations that had previous policies in place told IDC about the time savings they were achieving as a result. Table 7 shows the overall impacts of the platform on audit and compliance teams. After deployment of DigiCert PKI Platform, these organizations saw about 1.2 FTEs freed up, representing a 25% improvement. Translated into financial terms, this amounted to annual cost savings of $115,000.

TABLE 7

Audit Policy Staff Impact

	Before DigiCert PKI Platform	With DigiCert PKI Platform	Difference	Benefit (%)
Audit policy staff (FTE equivalent per organization per year)	4.5	3.4	1.2	25
Staff time cost per year	$454,000	$339,000	$115,000	25

Source: IDC, 2019

The security team efficiencies described previously also meant less disruption for LOB users. One practical outcome was that help desk operations related to security and certificate issuance not only received less calls but, when calls were made, they were more quickly resolved. As one study participant commented: *"We are also able to respond faster to our internal trouble tickets with our different hardware and software — we have been able to reduce that queue dramatically."* As shown in Table 8, IDC calculated that post-deployment calls and tickets per week were reduced from 13.4 to 4.6 on average, representing a 66% improvement. In addition, time to resolve was reduced from 15.4 hours to 2.9 hours, a substantial improvement of 81%. From a productivity standpoint, help desk teams saw a 90% improvement in the amount of time they needed to spend on certificate-related tickets.

TABLE 8

Help Desk Impact

	Before DigiCert PKI Platform	With DigiCert PKI Platform	Difference	Benefit (%)
Calls/tickets per week	13.4	4.6	8.9	66
Time to resolve (hours)	15.4	2.9	12.6	81
Total FTE Impact	3.7	0.4	3.4	90
Total staff time value per year	$372,000	$36,200	$336,000	90

Source: IDC, 2019

Unplanned Downtime

Interviewed companies spoke to IDC about the impacts of the DigiCert PKI Platform on unplanned downtime and business productivity. Companies described how they were able to reduce the incidence of unexpected outages and discussed how this benefit extended to LOB operations.

IDC quantified these benefits as shown in Table 9. The average frequency of outages per year was reduced substantially from 11.3 to 2.3, a 79% improvement. In addition, average time to resolve was reduced from 8.7 hours to 1.6 hours, representing an 81% improvement. Overall, these organizations are observing a 76% improvement in end-user productivity, as represented by the value of the time they gained back.

TABLE 9

Unplanned Downtime Impact

	Before DigiCert PKI Platform	With DigiCert PKI Platform	Difference	Benefit (%)
Frequency per year	11.3	2.3	8.9	79
Time to resolve (hours)	8.7	1.6	7.1	81
Lost productivity due to unplanned outages (FTE impact	16.4	4	12.4	76
Value of lost productivity per year	$1.14 million	$277,000	$870,000	76

Source: IDC, 2019

Less downtime for business end users translates into positive revenue impacts. As shown in Table 10, across all companies surveyed, total additional revenue per year amounted on average to $3,010,366. In addition, total recognized revenue per year under the IDC model was $451,555 after taking into account a 15% operating margin.

TABLE 10

Unplanned Downtime Revenue Impact

	Per Organization
Total additional revenue per year	$3,010,366
Assumed operating margin	15%
Total recognized revenue per year — IDC model	$451,555

Source: IDC, 2019

Business Impacts of DigiCert PKI Platform

As described previously, interviewed companies discussed how using the DigiCert PKI Platform service led to optimized performance for the core security operations supporting their businesses. They described how this resulted in better business results and lower operational cost. Study participants underscored the value of having quick turnaround times for certificate issuance and more confidence in data security across their organizations. Also cited were the benefits of full encryption that gave employees more freedom to work in their locations of choice. In the case of one company, this approach was supportive of new initiatives in corporate security policy. As a result of these benefits and other efficiencies described, companies were able to generate more business opportunities leading to improved business results. Study participants elaborated on these benefits:

- **More predictable business operations:** *"We are seeing more predictable costs and timing. We can easily tell somebody how much it's going to cost them to do X, Y, and Z. And then we can give them a reliable time frame for when it will be installed and be up and running."*
- **Can pursue new business opportunities:** *"We created a custom application for our dealers to target potential buyers with a special discount tied to a particular vehicle based on their personal profile. Because of the amount of personal and financial data associated with this application, we had to find a way to encrypt everything down to the data at rest. This is now what's driving a lot of our strategic policy to encrypt everything."*
- **Increased business confidence:** *"We have more confidence in our data security, more consistency across our locations, and more peace of mind."*
- **More flexibility for end users:** *"Before DigiCert, people would get a nastygram on their laptops from the security team because they didn't lock it down at their desk properly. Now we've got everything encrypted so employees can take their laptops and their work anywhere."*
- **Freed up staff time:** *"Because we no longer have to wait a week for a certificate, the process is now much faster. Every time you have to wait, it costs money because there are people you are paying who are waiting. To manage more efficiently is an ongoing goal throughout the company."*

Table 11 presents quantified benefits for business end users after companies adopted DigiCert PKI Platform. On average, there were gross productivity gains of 26%. Translated monetarily, this resulted in a value of end user time of $147,000. Additional metrics are also presented in Table 11.

TABLE 11

Enhanced User Productivity

	Per Organization
Number of users impacted	8
Gross productivity gains	26%
Productive hours gained	$4,000
End-user impact (FTE equivalent per organization per year)	210%
Value of end-user time	$147,000

Source: IDC, 2019

DigiCert PKI Platform has been designed to be a cost-effective solution, and this feature was borne out in discussions with study participants. Table 12 presents impacts for operating expense reduction after companies deployed DigiCert PKI Platform. The average total operating expense reduction on an annual basis was $156,500. Additional metrics are presented in Table 12.

TABLE 12

Operating Expense Impact

	Per Organization
Total operating expense reduction per year	$156,500
Assumed operating margin	15%
Total recognized operating expense reduction per year — IDC model	$23,475

Source: IDC, 2019

Table 13 presents total additional revenue per year accrued to DigiCert customers based on new business opportunities. After deployment of the PKI Platform, this amounted to $50,000 on average across all companies.

TABLE 13

Business Opportunity Revenue

	Per Organization
Total additional revenue per year	$50,000
Assumed operating margin	15%
Total recognized revenue per year — IDC model	$7,500

Source: IDC, 2019

ROI Summary

IDC's analysis of the financial and investment benefits related to study participants' use of DigiCert PKI Platform is presented in Table 14. IDC calculates that, on a per organization basis, interviewed organizations will achieve total discounted five-year benefits of $8.56 million based on IT and security staff efficiencies, increased user productivity, improved cost of operation, and other factors as described.

These benefits compare with projected total discounted investment costs over three years of $2.01 million on a per organization basis. At these levels of benefits and investment costs, IDC calculates that these organizations will achieve a five-year ROI of 326% and break even on their investment in 13 months.

TABLE 14

Five-Year ROI Analysis

	Per Organization	Per 1,000 Users
Benefits (discounted)	$8.56 million	$273,300
Investment (discounted)	$2.01 million	$64,200
Net present value (NPV)	$6.55 million	$209,100
ROI (NPV/investment)	326%	326%
Payback period (months)	13	13
Discount rate	12%	12%

Source: IDC, 2019

Challenges/Opportunities

IT teams, especially at large organizations, are frequently managing siloed or fragmented PKI implementations, which may include a mixture of customized infrastructure to support internal-certificate authority operations and on-premises infrastructure to support email security, document signing, or other use cases. While the compounding management overhead and ability to scale to support business growth is often the catalyst for a managed PKI service, it can complicate the implementation and extend the time to replace legacy infrastructure without disrupting existing workflows.

In such situations, organizations can consider a phased approach such as transitioning to a hybrid model before deploying to a private or public cloud. Modern PKI solutions can ease the transition by providing deployment flexibility across on-premises, private and public cloud, and hybrid.

Conclusion

PKI has withstood the test of time. Researchers have not come up with a better framework for authentication, encryption, and digital signing applications. This study has documented how cloud-delivered and a fully managed PKI service has proven its ability to support

the scalable application of confidentiality, authentication integrity, access control, and nonrepudiation of transactions. Organizations have integrated the service with their existing security infrastructure, including secure Wi-Fi, web authentication, mobile device management, secure remote access, and solutions for digitally signed/encrypted mail and document signing.

Driving the need for a cloud-delivered and fully managed PKI service is the desire of security and operations teams to reduce complexity at a time when hybrid and multicloud environments are multiplying, making the job of managing sensitive resources much more difficult. The corporate network is becoming increasingly distributed and while these changes, ushered in by digital transformation, foster efficiency and productivity improvements, managing risk, security, cost, control, visibility, and oversight has become a significant challenge. Attackers seize on the resulting complexity, and this is placing pressure on security teams to prevent cybercriminals from successfully targeting high-risk employees and exploiting technology gaps and disjointed processes to steal sensitive information. It only takes one misstep — an inadequately configured or mismanaged security solution, poorly communicated policies, or a gap in enforcement mechanisms — to generate a fissure that cybercriminals can squeeze through to reap valuable data. This is one of the many factors that have prompted organizations to adopt a cloud-delivered and fully managed PKI service.

The recent pandemic reminds us of the value of a cloud-delivered and managed PKI service in managing a crisis. Enterprises may need to dramatically scale up or down their PKI services in a very short period of time. Without prior planning, a self-managed PKI may be challenged to meet a huge surge of demand to maintain employees' productivity, or it may incur high cost overrun from unanticipated major drops in demand for services.

In addition, as the IoT landscape evolves, organizations are expected to be collecting and analyzing more sensor data than ever before. These devices require a mechanism to authenticate to other systems and often an encrypted tunnel for transmitting sensor data.

As this study has shown, DigiCert's customers had shown an increased ability to deploy the appropriate certificate correctly and quickly, thus building trust among their end users and freeing up IT security and infrastructure staff to work on other critical projects. Furthermore, these customers showed increased business benefits from stronger performing certificates. What that results in is that these DigiCert customers are achieving overall economic value of more than 4 to 1 on their investment.

Appendix

Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of DigiCert PKI Platform as the foundation for the model. Based on interviews with organizations using the service platform, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of DigiCert PKI Platform.** In this study, the benefits included staff time savings, productivity benefits, and operational cost reductions.
2. **Created a complete investment (five-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using DigiCert PKI Platform and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of DigiCert PKI Platform over a five-year period. ROI is the ratio of the net present value (NPV) 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 a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the five-year savings is calculated by subtracting the amount that would have been 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 IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

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

MESSAGE FROM THE SPONSOR

DigiCert is a leading provider of scalable TLS/SSL, IoT and PKI solutions for identity and encryption. The most innovative companies, including 89% of the Fortune 500 and 97 of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers, enterprise and Internet of Things devices. The company is recognized for its enterprise-grade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions. For the latest DigiCert news and updates, **visit www.digicert.com or follow @digicert.**

About the Analysts

Frank Dickson
Program Vice President, Cybersecurity Products, ID

Frank Dickson is a Program Vice President within IDC's Cybersecurity Products research practice. In this role, he leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response and Orchestration (AIRO); Identity & Digital Trust; Legal, Risk & Compliance; Data Security; IoT Security; and Cloud Security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank Dickson

Harsh Singh
Senior Research Analyst, Business Value Strategy Practice, IDC

Harsh is responsible for developing return-on-investment (ROI) and cost-savings analysis on enterprise technological products. Harsh's work covers various solutions that include datacenter hardware, enterprise software, and cloud-based products and services. Harsh's research focuses on the financial and operational impact these products have on organizations that deploy and adopt them.

More about Harsh Singh

About 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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701
USA
508.872.8200

idc.com @idc

IDC Doc. #US45385819