

The Global TLS Certificate Authority Market

Key Insights for Enterprise End Users

A Frost & Sullivan White Paper

www.frost.com

by **Swetha Krishnamoorthi**, Senior Industry Analyst, Cybersecurity and
Jarad Carleton, Principal Analyst, Cybersecurity

| | |
|---|----|
| Introduction | 3 |
| The Importance of Transport Layer Security (TLS) Certificates | 4 |
| <i>The Major Functions of TLS Certificates</i> | 5 |
| The State of the Market | 5 |
| <i>Market Share Analysis</i> | 6 |
| <i>The Future of the Market</i> | 9 |
| The Final Word. | 10 |

INTRODUCTION

Two-thirds of the UK population, about 44 million consumers, used digital payment methods in 2017¹. In the US market, consumers have also embraced digital payments, spending \$453.46 billion on the Web for retail purchases². While this is great news for the e-commerce sector, approximately 6.17 million data records are stolen every day³. Line of business (LoB) and information security executives need to remember, a Web site is the first touchpoint for B2B and B2C interactions in the digital world and it is the first indicator of the security posture of an enterprise. The growing volume of online fraud resulting from phishing and online brand impersonation is a serious challenge for enterprises around the world that is directly impacting brand reputation. Additionally, reputational damage is a rising concern among enterprises as more consumers are increasingly wary of digital transactions because of security concerns.

Two methods frequently used by cyber criminals to steal user data, such as banking information and personally identifiable information (PII), are:

1. Email or SMS-based phishing attacks that trick users into clicking on links leading to impersonated Web sites to capture log in credentials
2. Man-in-the-Middle (MitM) attacks

Because of these factors, today's highly mobile and Wi-Fi connected environment makes it critical to encrypt data transmission from laptops, tablets, and smartphones to Web sites for data protection.

Frost & Sullivan research shows that as online fraud continues to grow, consumer digital trust in organizations is negatively impacted. This erodes enterprise brand equity and revenues for those businesses perceived as less secure. In fact, the 2018 Global State of Online Digital Trust survey and index conducted by Frost & Sullivan directly links falling digital trust to lower revenues. This is illustrated by the fact that 48% of consumers state that they stop using a service if they believe their data was compromised as a result of using that service⁴.

Whether the data compromise is the result of a data breach, phishing, Web site impersonation, or a MitM attack, digital trust and enterprise revenue is the collateral damage. Furthermore, the Global State of Online Digital Trust study shows that consumer digital trust is in jeopardy. Globally, only 38% of consumers reported higher levels of digital trust, while 40% of consumers trust levels remained the same, and 22% reported a decrease in digital trust. For the US, France, Italy, and Japan, the data provides a warning for online business because digital trust levels are so low that 1-2 major cyber incidents could push digital trust into negative territory. In 2018, consumers in the UK, Germany, and Australia, reported they have less digital trust online than they did 24 months ago (Figure 1).

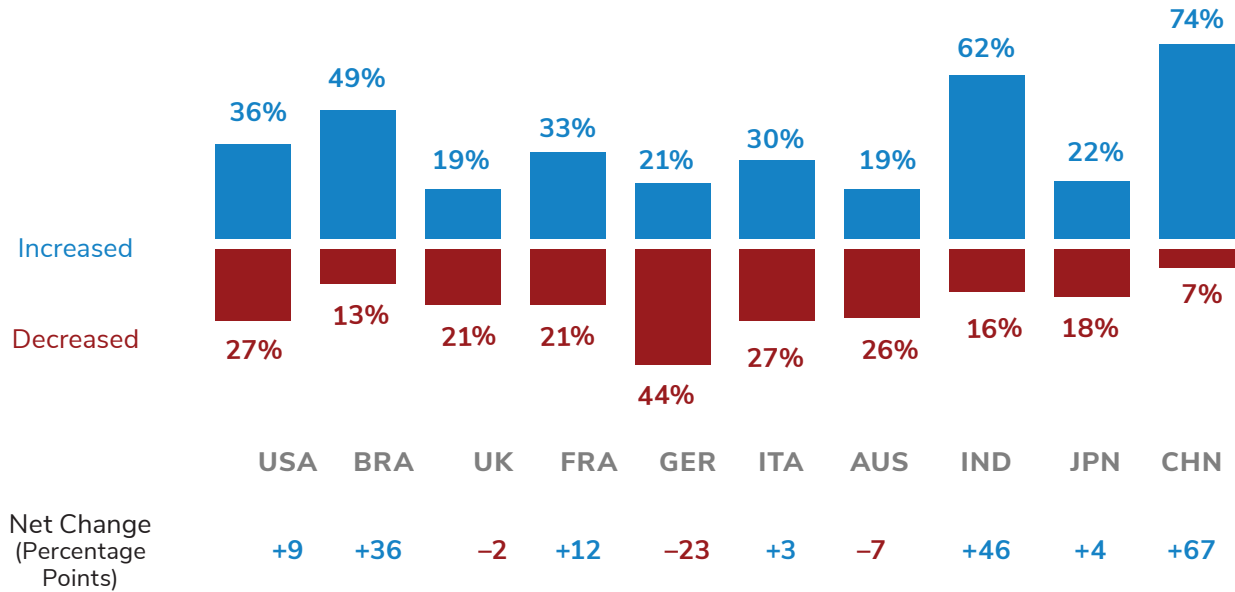
1 <https://www.statista.com/statistics/491938/digital-market-outlook-digital-payment-users-by-segment-uk/>

2 <https://www.digitalcommerce360.com/article/us-ecommerce-sales/>

3 <https://breachlevelindex.com/> as of 19 December 2018.

4 CA Technologies 2018 State of Online Digital Trust Survey conducted by Frost & Sullivan—<https://www.ca.com/us/collateral/white-papers/the-global-state-of-online-digital-trust.html>

FIGURE 1: End-User Change in Online Digital Trust in Organizations Over the Last 2 years, Global, 2018⁵



N = 900.

Source: CA Technologies 2018 State of Online Digital Trust Survey conducted by Frost & Sullivan

In light of the crisis of falling digital trust of Internet users, it is essential for enterprises to boost trust by providing a safer, high assurance, encrypted digital environment. Likewise, enterprises can protect their own processes and put in place stronger security controls by requiring high assurance identity verification processes for the tools they use for encryption, such as digital certificates. The default use of HTTPS (hypertext transfer protocol secure) to encrypt data traffic to and from a Web site will enhance digital trust, particularly now that the major browsers notify users that sites using unencrypted HTTP are unsecure.

THE IMPORTANCE OF TRANSPORT LAYER SECURITY (TLS) CERTIFICATES

TLS⁶ certificates are issued by a certificate authority (CA) and are bound by strict industry standards that govern certificate issuance. These enable inbound and outbound data encryption between the Web servers they are installed on and the browsers on endpoints⁷ accessing Web sites. When properly implemented, TLS

⁵ Ibid.

⁶ TLS or Transport Layer Security is the updated and more secure version of SSL (Secure Socket Layer) and the two terms are used interchangeably

⁷ Desktops, laptops, tablets, and smart phones are collectively referred to as endpoints.

certificates protect data in transit from being read by cyber criminals and nation-state cyber adversaries, provided that one of the endpoints is not compromised by malware.

On Web sites using a TLS certificate and depending on the type of certificate used, in the URL bar of their browser visitors will see:

1. A padlock displayed in the URL bar of the browser (domain validation, or DV)
2. A padlock in the URL bar of the browser and the ability to view company information in the certificate details (organization validated, or OV), or
3. The name of the company or another visual indicator such as the color green (extended validation, or EV)

There are several reasons to use TLS certificates, but the primary business purpose is to protect data in transit from unauthorized access by a cyber adversary. TLS certificates help enterprise protect their brands as well as demonstrate to customers that internal security controls have been implemented. TLS certificates help establish, rather than erode, digital trust. This is important since Google Chrome and other major browsers began notifying users in 2018 that Web sites using clear text data transfer are not secure. Today, when a user goes to an unencrypted site, a warning is displayed and the user must confirm they want to visit the site despite the stated security risk.

Since Google's Chrome browser is used by about 61.5% of users globally⁸, the warnings have shaped Internet user behavior. Additionally, because Google search results give higher preference to sites using TLS certificates and since Google controls approximately 64.4% of the search engine market⁹, business owners cannot afford to ignore the importance of data encryption for inbound and outbound Web site data traffic.

The Major Functions of TLS Certificates

- **Authentication**—The certificate authorities verify different types of information about an organization before issuing an SSL certificate, such as control of a domain, if the domain owner is a business or an individual, the physical mailing address, or the legal existence of an organization.
- **Encryption**—The TLS certificate encrypts any data exchanged between the user and Web site, which is otherwise transmitted as plain text accessible to hackers.
- **Data Integrity**—TLS certificates prevent data loss or alteration during data transmission by using a message authentication code (MAC) algorithm.

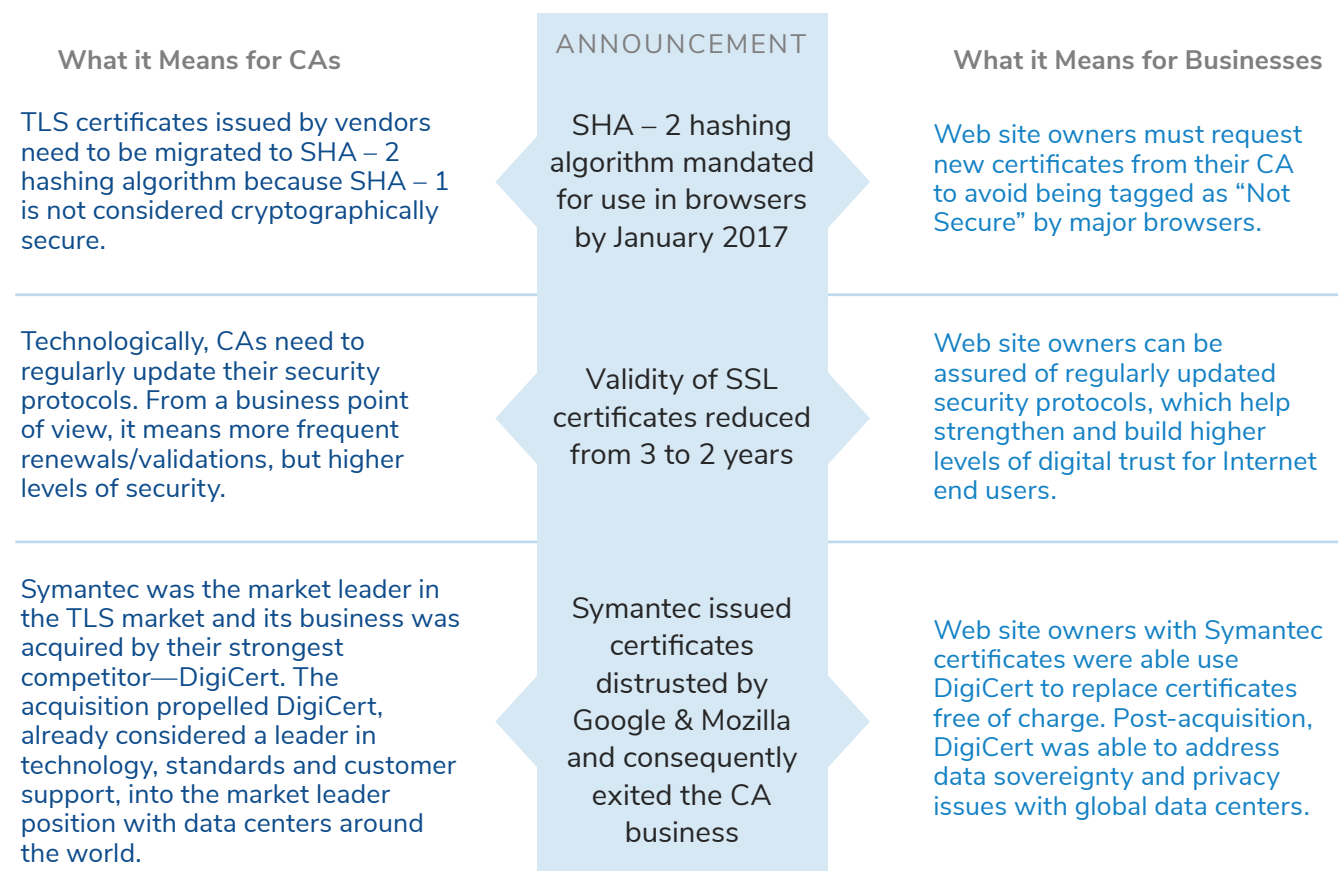
THE STATE OF THE MARKET

The last two years have been eventful in the global high assurance (HA) certificate market. Highlights of a few major announcements that had a significant impact on HA Certificates market are described in Figure 2.

⁸ October 2018, <http://gs.statcounter.com/>

⁹ October 2018, <http://gs.statcounter.com/search-engine-host-market-share>

Figure 2: HA Certificates Market Announcements & Implications, Global, 2016–2018



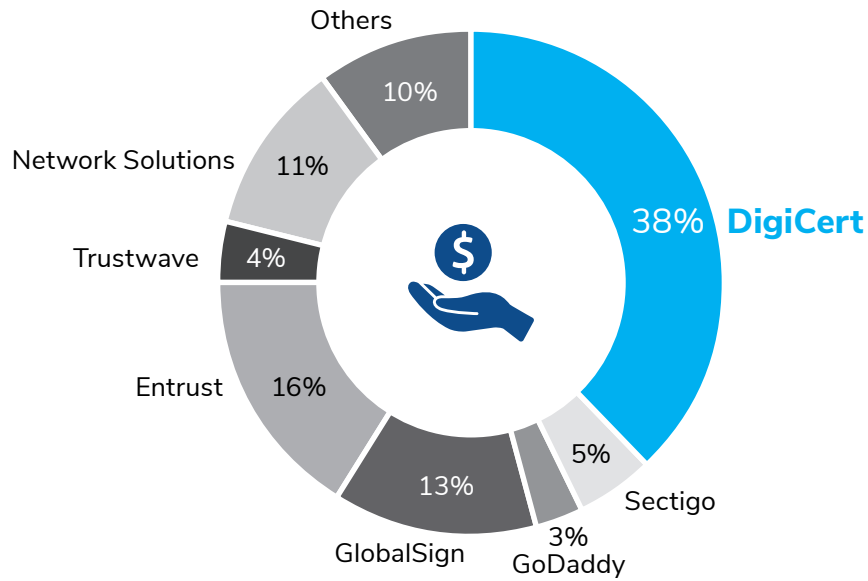
Distrust of Symantec issued certificates shook the competitive dynamics of the SSL market when millions of Web sites were facing the prospect of being tagged “Not Secure.” Some of the Web sites included the world’s biggest financial institutions, which handle highly sensitive consumer data and monetary transactions. The fallout led Symantec to exit the CA market and the business was acquired by DigiCert, a respected and trusted CA. The acquisition consolidated part of the market and propelled DigiCert into the global market leading position for HA certificates.

Market Share Analysis

With market consolidation, the high assurance certificates market share has undergone a major change since Frost & Sullivan last examined the market. An analysis of market positions for CA vendors in 2018 reflects that DigiCert gained significant market share and is the leader for high assurance certificates targeting the enterprise market.

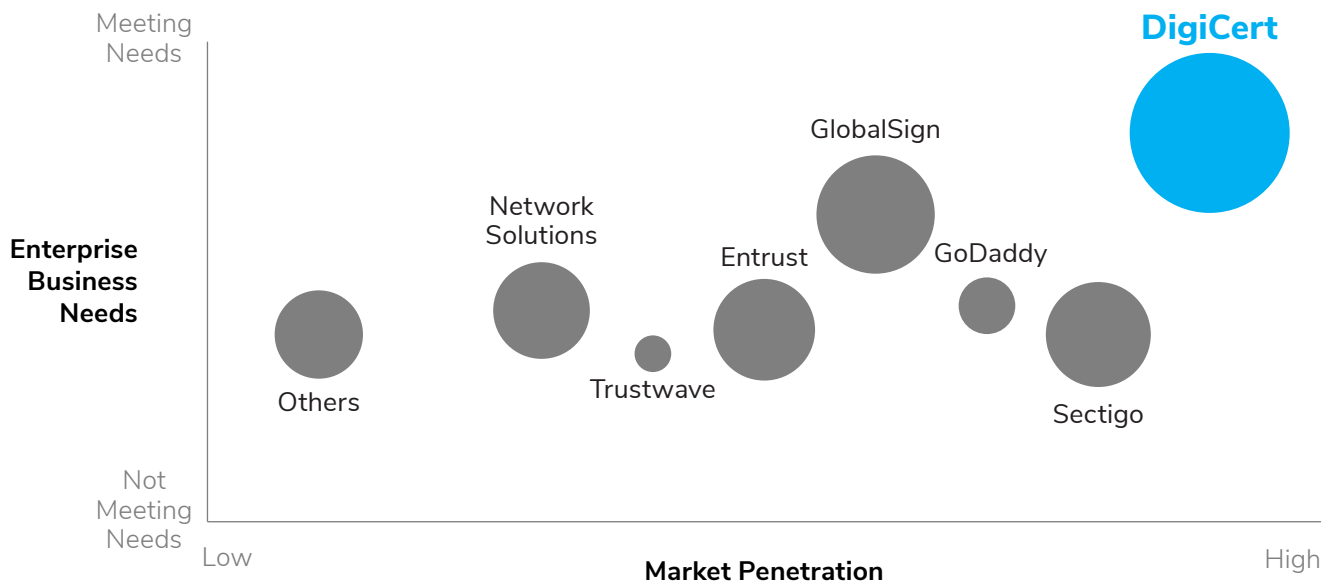
However, the CA vendors with a higher focus on DV certificates, including Sectigo and GoDaddy, lost market share because businesses focus the majority of certificate budgets on HA certificates. Because HA certificates hold more significance for medium and large enterprises, especially in the financial, healthcare, and retail verticals, DigiCert is expected to retain its market leading position because of its HA focus (Figure 3).

FIGURE 3: Total HA Certificates Market: Percent of Revenue, Global, 2018



The competitive landscape (Figure 4) illustrates the market positioning of CA vendors participating in the HA certificate market across several parameters, including seal recognition, trust, price, customer loyalty, install base, and vertical representation. The size of each bubble corresponds with the percent of revenue each vendor has achieved.

FIGURE 4: Competitive Landscape, HA Certificates Market, Global, 2018



Most vendors in the SSL certificate market compete in the DV space, which has become price sensitive as a result of LetsEncrypt's free offerings. In contrast, the HA certificate market strikes a balance between value and price. Because the certificates themselves have little scope for differentiation, vendors differentiate between them based on value-added features and services for the price offered. Trustwave, GoDaddy, Sectigo, and Network Solutions offer certificates at a lower cost compared to vendors such as DigiCert, Entrust, and GlobalSign. However, CAs competing merely on price don't tend to invest as much in research and development and have a more difficult time meeting the business needs of enterprise customers. An exception in the market is DigiCert, which has invested heavily in R&D to ensure that customers never have to worry about the validity of its certificates as standards evolve. In addition, having access to a CA with modern infrastructure, global data centers, and scalability is as important as dashboards that reduce the time and effort involved with certificate management.

Price should never be the sole deciding factor for an enterprise when choosing a CA. It is important to also consider five additional areas:

1. **Management consoles**—A well-developed management console can save time and help ensure compliance. Both time and compliance can have a quantifiable impact on an enterprise IT budget.
2. **Technical support**—The availability of a top-rated technical support department that can quickly resolve issues impacting a business can save significant time and revenue for an enterprise.
3. **Automation**—The automation of tedious, time-consuming processes involved with certificate requisition will free up skilled IT personnel to work on higher value tasks for the enterprise.
4. **Security seal brand recognition**—Internet savvy and less technically inclined end users are more confident using Web sites with security seal brands they recognize, such as Norton.
5. **Scale and global reach**—in a global digital economy, a CA with data centers around the globe with the capability to scale solutions to meet the needs of growing enterprise is important.

Industry trust in the CA, as well as brand recognition among Internet end users, should also be deciding factors for enterprises in need of HA certificates. That is because Internet-savvy end users are influenced by:

1. Indicators that a Web site is using HA certificates, and
2. Security seal brand recognition

Those two factors have an impact on the willingness of Internet-savvy end users to conduct commercial transactions on known as well as new/previously unknown Web sites. For that reason, the importance of consumer awareness of CA security seals is a fact that enterprises cannot ignore as the struggle to increase online digital trust continues.

Following a security seal awareness and trust survey in 7 nations¹⁰ targeting 1,000 consumers who shop online, Norton seals powered by DigiCert and DigiCert-branded seals are recognized by 86% of online consumers based in important economies around the world. In addition, DigiCert was ranked by survey respondents as being amongst the top 3 most trusted CA brands globally, which ultimately can have a

¹⁰ USA, UK, France, Germany, China, Japan, and Australia

positive bottom line impact for DigiCert enterprise customers that culminates in higher completed purchases and fewer abandoned shopping carts.

Figure 5 provides a high-level comparison of features and functionalities offered by competing CA vendors in the high assurance certificate market.

FIGURE 5: Key HA Certificate Features by Major CA Vendors, Global, 2018

| | Company | | | | | | | | |
|----------------------------------|----------|---------|---------|------------|---------|-----------|-------------------|--------|-----------|
| | DigiCert | Sectigo | GoDaddy | GlobalSign | Entrust | Trustwave | Network Solutions | Certum | SwissSign |
| Integrated cert. mgmt. & console | ✓ | ✓ | | | ✓ | ✓ | | | ✓ |
| Rapid HA cert. issuance | ✓ | | | | | | | | |
| Web scanning | ✓ | | ✓ | | ✓ | | ✓ | | |
| IoT Solutions | ✓ | ✓ | | | ✓ | | | | |
| Digital certs. | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| Digital signature services | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ |
| 24/7 customer support | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Easy cert. automation | ✓ | ✓ | | | | | ✓ | | ✓ |
| PKI mgmt. | ✓ | ✓ | | ✓ | ✓ | | | | ✓ |

The Future of the Market

Frost & Sullivan projections indicate that the global HA certificate market will continue to expand through 2020 to achieve a compound annual growth rate (CAGR) of 15% as a result of increasing demand for HA security certificates. The projected growth is based in part on the increasing security awareness of Internet end users, most of which do not understand how encryption works but understand the importance of

encryption to protect their data. This in turn boosts their digital trust in conducting business online. Other growth factors include improving the security of IoT devices and ensuring proper security for code signing.

With the market at the cusp of transformation and additional growth—particularly in respect to its role in helping to secure IoT—a solid growth strategy based on responsive service, a flexible and broad portfolio, and consistent investment in R&D is required to get ahead of and lead the market.

Enterprise demands are changing as increasing numbers of consumers go online to conduct a wide variety of commercial transactions. Today, TLS certificates are a baseline requirement for conducting online business and cannot be ignored by any organization regardless of geo-political boundaries. In addition, following the mandate to restrict the validity of certificates to 2 years, the frequency that enterprises need to renew security certificates has increased by approximately one third. In a clear example of DigiCert's commitment to investing in tools that help over-burdened IT professionals simplify certificate management, it developed its PKI Certificate Management Platform for Enterprise. Inside the platform, enterprises can customize workflows for their organization, automate certificate issuance, and alleviate the burden of human error involved with manually tracking certificates in cumbersome spreadsheets, thereby ensuring certificate renewals and business continuity.

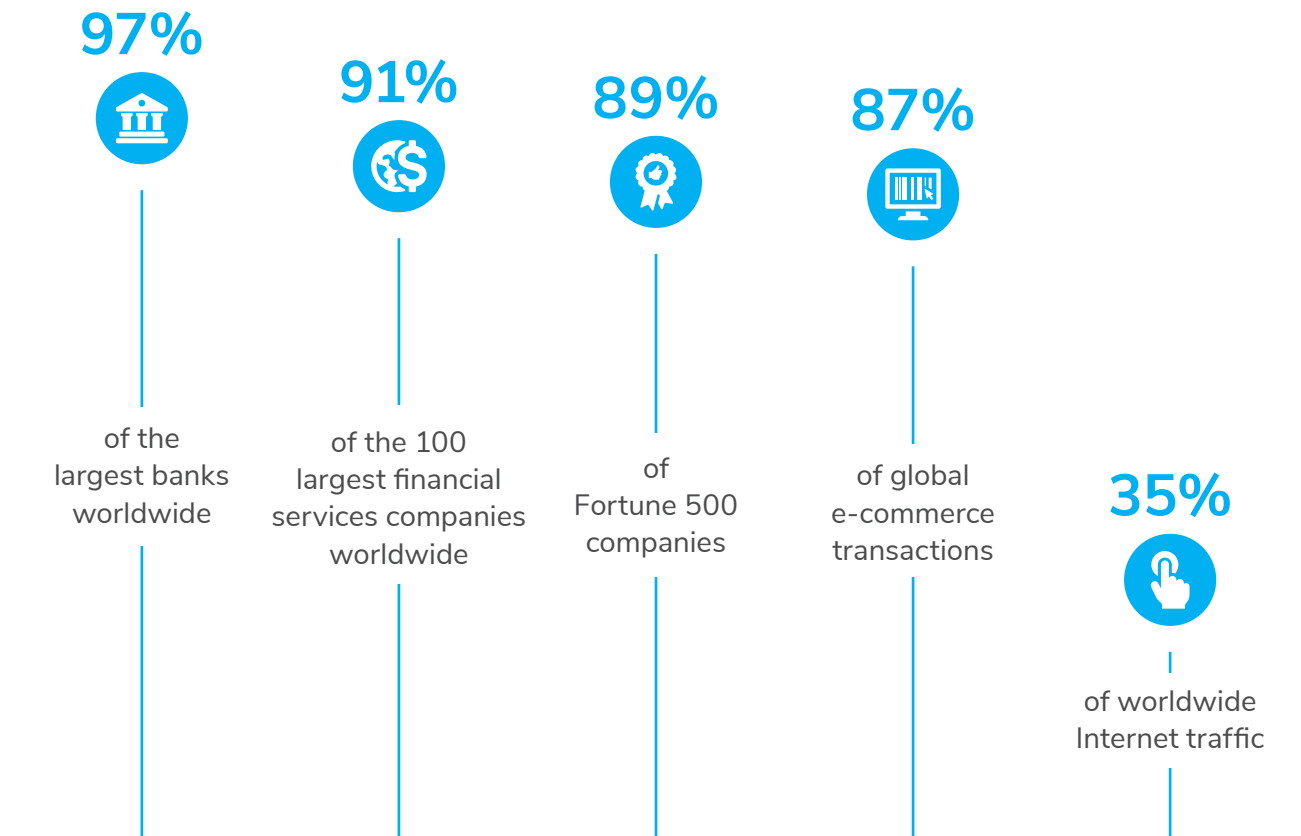
Another area that demonstrates DigiCert's commitment to investing in the future of its business is its early support for IoT security with client, device, and HA certificates. As more enterprises implement IoT solutions at part of the digital transformation of their businesses, ensuring that each IoT device has been secured is crucial. Depending on the size of an organization, the number of IoT devices the business relies upon can number in the hundreds, thousands, or even hundreds of thousands. To ensure business continues without unexpected interruption, data going to these devices must be authenticated as coming from an authorized source, the data must be kept private, and it be protected from falsification. DigiCert is well positioned to provide this level of security for enterprise-class IoT, and it further strengthened its ability to serve this important market by acquiring global infrastructure from Symantec upon its exit from the CA vendor industry.

THE FINAL WORD

The high level of infrastructure investment and R&D has enabled DigiCert to become a truly global full-service CA provider while leaping ahead of competition. In the process, DigiCert has become a market leader and a CA known for high levels of service, trusted security, desirable management tools, and a flexible portfolio. DigiCert offers severely time constrained IT and information security professionals the help, tools, and processes to successfully secure parts of the business that enhance digital trust, while reducing the management hours required to get the job done.

In a world where digital trust has been eroding as the non-technical online population becomes more security conscious, an enterprise has one chance to make a positive first impression with its security practices. Working with a trusted market leader that invests R&D dollars each year into future proofing its product portfolio and management tools helps to ensure enterprise customers will not have to scramble to implement new certificates from a different CA as market conditions change.

FIGURE 6: Secured by DigiCert—Global HA Security Certificate Market Leader



In the market for HA security certificates, organizations that are committed to security need to consider the choice of a CA carefully and keep in mind that focusing exclusively on price points for certificates is the fastest potential path to hidden and unexpected additional internal costs. Savvy organizations need to look beyond the momentary allure of a supposed lower price point to better understand the cost savings, and ultimately the positive ROI, that can be attained by working with a full service provider like DigiCert.

SILICON VALLEY

3211 Scott Blvd
Santa Clara, CA 95054
Tel +1 650.475.4500
Fax +1 650.475.1571

SAN ANTONIO


7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel +1 210.348.1000
Fax +1 210.348.1003


LONDON

566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost • myfrost@frost.com
<http://www.frost.com>

NEXT STEPS 

 **Schedule a meeting with our global team** to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

 Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

 Visit our **Digital Transformation** web page.

 Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

IN
PARTNERSHIP
WITH

digicert[®]

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:

Frost & Sullivan
3211 Scott Blvd
Santa Clara CA, 95054