DigiCert Secure Site SSL

Always evolving to provide the best in SSL/TLS solutions

digicert®

DigiCert Secure Site SSL is the new standard for businesses who take securing their data and identity seriously. With prioritized validation and support, the most recognized trust mark on the web, and the industry-leading management platform, DigiCert is always evolving to provide our customers the best in SSL/TLS solutions.

Building customer trust and maintaining a secure digital infrastructure requires continuous diligence and can be undone in seconds. For most organizations, keeping up with the proliferation of online threats simply isn't feasible. Instead of going it on your own, feel confident relying on DigiCert as your partner in online security.

DigiCert's new Secure Site certificates include everything an organization needs to enhance their ecommerce operations and online presence, while also simplifying management and mitigating threats across your network.

DigiCert Secure Site is a three-part solution:

1. Secure Site SSL Certificate

The only certificate with the Norton Seal, proven to be the leading trust mark that can reduce bounce rates and increase customer confidence.

A $1.75 million replying-party warranty protects you in the event of a certificate-related compromise, and exclusive concierge service and validation ensure you never waste time waiting when you need help.

2. CertCentral Management Console

Our award-winning platform allows you to manage your certificates from issuance to renewal.

With discovery and vulnerability scanning tools you can easily find every certificate on your network – both internal and external (and even those not issued by DigiCert) – and receive easy-to-read reports highlighting any security risks such as weak signatures or misconfigured certificates.

Control issuance with multi-user accounts with customized roles, and automate certificate renewal to avoid costly network downtime.

3. DigiCert's Unmatched Infrastructure

No CA values investment more than DigiCert. We have built a developer-friendly REST API for native integration into your processes and systems, and a scalable backend to support high-issuance volumes. You may not be a Fortune 500 company yet, but DigiCert is the CA that can grow there with you.

The Value of Identity

Everyone is worried about the proliferation of phishing, online scams, and fake information.

No matter what size your organization is, you and your customers are vulnerable to social engineering attacks ranging from fake login pages to CEO spear-phishing.

Take control of your online presence with Secure Site certificates and DigiCert's unique brand protection features. Our validation procedures – which exceed industry standards – ensure that no one will ever be able to impersonate your organization or receive a certificate in your name.

Use EV (Extended Validation) certificates to clearly communicate to your users – both customers and employees – that they are on your legitimate website and not an imposter's with unique browser UI that displays your registered company or brand name.

DigiCert's strict validation process allow you to enforce your organization's certificate policies, insuring only authorized employees can request and receive certificates without slowing them down or requiring time-consuming management from your IT department.

DigiCert Secure Site brings greater security, simplified management, and enhanced performance to your organization. Talk to a sales representative today.

For more information, please contact a DigiCert sales representative at 1.855.800.3444 or email sales@digicert.com.

The operational cost of website insecurity

Manually managing certificates is expensive. On average, it costs $288 plus 4 hours of management per certificate.[1]

The Global 5,000 have spent up to $15 million to recover from certificate outages and up to $25 million in compliance costs.[2]

There were at least 255,065 unique phishing attacks worldwide – a 10% increase from the previous year. An attack is defined as a phishing site that targets a specific brand or entity.[3]

Consumer are more concerned than ever with doing business on the web with 1 in 13 URLs in 2017 found to be malicious. A ~3% increase year over year.[4]

1 Reference: 1Case Study: Scalable Key and Certificate Lifecycle Management with Cisco Systems," Session ID: SPO1-303, RSA Conference 2011, Cisco Systems Inc.

2 Reference: https://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/

3 Reference: http://docs.apwg.org/reports/APWG_Global_Phishing_Report_2015-2016.pdf

4 Reference: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf