

---

# **DIGICERT® SECURE SITE PRO PARTNER SALES GUIDE**

Published: November 2020

# HOW TO USE THIS GUIDE

With this messaging and content guide, you'll be able to successfully position and sell DigiCert® Secure Site Pro TLS/SSL Certificates.

Inside you'll find:

- A deep dive on the various features available with Secure Site Pro
- Copy blocks, messaging and positioning statements
- The top reasons to buy Secure Site Pro

You're welcome to use this guide's information and phrasing as-is, or rework and reword the content to better fit your audience and voice. DigiCert doesn't require approval for repurposing information.

You may use this content on your website, in your own marketing materials, on email campaigns, or anywhere that helps you more efficiently position and sell products from the DigiCert family of brands.

# DIGICERT® SECURE SITE PRO PARTNER SALES GUIDE

Advanced, complete TLS/SSL solutions from the world leader in high assurance web security.

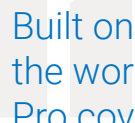
Your online presence is one of the most important places for your brand. When you protect your website, you protect your brand while building customer confidence. From small business to massive enterprises, DigiCert Secure Site Pro delivers the highest assurance of trust.

## When you need security, DigiCert Secure Site Pro is everything you need

Websites, and the businesses behind them, face constantly changing online threats. That's why Secure Site Pro offers a comprehensive solution that helps you to easily configure, monitor and respond to current and future threats— all from the leader in high assurance certificates.

Secure Site Pro includes advanced security features for a complete TLS solution, including:

- Certificate Transparency (CT) Log Monitoring
- Blocklist Checker and Malware Scanning
- Vulnerability Assessment
- Trust Seals
- Post-quantum Cryptography (PQC) Toolkit



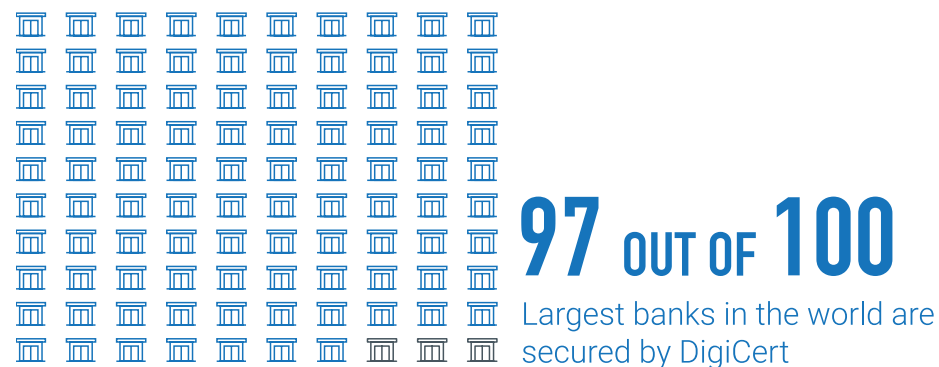
Built on a modern PKI infrastructure, and backed by the world's most trusted roots, DigiCert Secure Site Pro covers everything you need to provide assurance of your identity while ensuring customer trust.

# WHO IS DIGICERT?

DigiCert is the world's 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 and Internet of Things devices. DigiCert supports TLS and other digital certificates for PKI deployments at any scale through its certificate lifecycle management solution, CertCentral®. The company is recognized for its enterprise-grade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions.

## Priority Validation

Skip the line. Get your certificate faster with Priority Validation. All Secure Site Pro certificates benefit from a priority validation queue, meaning your certificate order is processed first, leading to faster issuance times. Avoid the wait and other delays with priority validation.



# CERTIFICATE TRANSPARENCY (CT) LOG MONITORING

The DigiCert CT Log Monitoring service allows you to monitor in real time the public CT logs for TLS/SSL certificates issued for the domains associated with Secure Site Pro certificates.

## What are CT logs?

Certificate Transparency is an open framework of logs, monitors and auditors created to help domain owners oversee digital certificates issued for their brands. CT logs help domain owners protect their brand by providing an easy process for discovering mis-issued or rogue certificates.

## CT Log Monitoring benefits:

- Gain visibility of the TLS/SSL certificates issued for domains you own with global monitoring and tracking against the public CT logs
- Reduce time and effort needed to monitor the logs by providing checks for DigiCert and non-DigiCert-issued certificates
- Ensure every certificate issued for your domains is trusted while gaining full oversight of which certificate authority issued each certificate

## Email notifications

After you've enabled CT Log Monitoring for a Secure Site Pro certificate order, you'll receive two types of email notifications—a daily CT log digest and, if needed, urgent notifications. Email notifications are sent to account admins.

## Daily CT log digest

Scheduled to occur once a day, this digest includes a daily rundown of new DigiCert-issued TLS/SSL certificates found in public CT logs. The daily digest is only sent if new DigiCert-issued certificates are discovered for a domain on the Secure Site Pro certificate order.

## Urgent CT log notification

The urgent notification is sent within minutes any time a non-DigiCert TLS/SSL certificate is issued for a domain on the Secure Site Pro certificate order.

# WHY USE CT LOG MONITORING?

Using CT Logs to monitor the TLS certificates attached to your domains is an industry best practice.

## How does CT Log Monitoring work with DigiCert Secure Site Pro?

CT Log Monitoring is a cloud service, so there is nothing to install or manage. After we've issued your Secure Site Pro certificate and enabled CT Log Monitoring for the order, you can immediately start using the feature to monitor any domain tied to the certificate.

### Top reasons to use DigiCert CT Log Monitoring:

- **Stay proactive** – Monitoring CT logs helps detect unauthorized certificates in just a few hours instead of days, weeks, or months. Domain owners can identify any certificates issued either without expressed approval or from outside their domain policy.
- **Speed up remediation** – Monitoring CT logs help identify any certificates that were issued outside of your organization's policy, thus allowing you to take quick revocation procedures as necessary.
- **Meet government compliance** – Due to a policy change\* in January 2019 by the United States Department of Homeland Security, all domains ending with .gov must be monitored by CT logs. Secure Site Pro is built to work with other TLD compliance requirements, too. Secure Site Pro's CT Log Monitoring feature is an easy way to review and report on all your domains.
- **Enforce internal policies** – Enforcing policy within your organization can be just as tricky as defending from outside threats. CT Log Monitoring can help you ensure all groups within your organization are adhering to your organization's policy and issuing only the company-approved certificates from approved Certificates Authorities.
- **Strengthen your security** – By providing transparency into the certificate issuance process and informing users about issued certificates, monitoring CT logs strengthens the chain of trust and makes online browsing safer for everyone.

\* <https://cyber.dhs.gov/ed/19-01/>

# BLOCKLIST CHECK

DigiCert Secure Site Pro includes a blocklist check tool. Quickly analyze your public domains with more than 70 antivirus scanners and URL/domain blocklist services. Use scan results to identify malware threats and take action to keep your own site from appearing on a blocklist.

DigiCert Secure Site Pro protects against costly damage



## Blocklist Checking features:

- Real-time on demand scans with notification if your domain is distributing malware or has been blocklisted
- Analysis using data from more than 70 third-party antivirus scanners and domain blocklisting services

DigiCert makes use of the world's leading source of information on malware, monitoring for:

- Malicious TLS/SSL certificates (SHA1 fingerprints)
- Malware TLS/SSL client fingerprints (JA3 fingerprints)
- Botnet C2 IP address:port combination associated with malicious TLS/SSL certificates

\* <https://www.herjavecgroup.com/wp-content/uploads/2018/07/2017-Cybercrime-Report.pdf>

# VULNERABILITY ASSESSMENT

Vulnerability assessments help you identify and take action against critical weaknesses in your website security.

Keep your business and your customers safe by identifying website vulnerabilities common in cyberattacks. A scan of your public-facing web pages, web-based applications, server software and network ports show weak points, organized by threat level, so you can quickly address the most urgent risk.

## Key benefits

- Simplify your processes with easy setup and use
- Avoid data breaches with proactive tools
- Identify website weaknesses before they become a liability
- View fixes to quickly identify vulnerability solutions

## Reasons to use Vulnerability Assessment

**Imperative** security protects your website and business

- View threats and mitigate risk
- Avoid becoming a target

**Automated**, seamless website scans reduce workload

- Scan automatically, at-will, or re-scan
- See vital reports

**Simplification** and customization make protection intuitive

- Little-to-no expertise required to start
- Clear and concise reports make it easy to swiftly respond

**Ongoing** checks address real-time threats

- View even the most recent threats without delay
- Stay current with continuous scanning

**Available** for DigiCert Secure Site Pro and DigiCert Secure Site Pro with EV

Scans	Sample Checks
Web Applications	All known web app vulnerabilities, such as SQL Injection, XSS (Cross Site Scripting), File Disclosure, Remote File Inclusion, PHP/ASP Code Injection, and Directory Traversal
Databases	Oracle® MySQL, PostgreSQL, Microsoft SQL Server®, Lotus Notes®, DB2®
Network Systems	All known web app vulnerabilities, such as SQL Injection, XSS (Cross Site Scripting), FiRouters, Firewalls, Switches/Hubs, Remote Access Servers, Wireless Access Points, Ipsec, PPTP, DHCP, DNS, LDAP, SNMP, VPNs, FTP, SSH, TELNET, Modems, Ant-Virus Systems
Operating Systems	Microsoft® - all versions, Solaris®, AIX®, HP-UX, SCO UnixWare®, BSD (OpenBSD, NetBSD), Linux - all distributions, AS/400®, VMS®, Mac OSX®, Novell NDS
Languages	SQL, ASP, PHP, Python, CGI, JavaScript, PERL, Ruby, .NET
OSI Layer 7 Apps	Web server, Database server, Mail server, FTP server, Proxy server



# TRUST SEALS

DigiCert Secure Site Pro includes use of one of two iconic seals—the DigiCert Secured site seal from the most trusted CA on the internet, or the Norton Powered by DigiCert seal, which is still the most recognized trust seal online.

## The advantage of using trust seals from DigiCert

DigiCert is the trusted Certificate Authority (CA) that powers the internet's most recognized and effective site seals—with nearly 90% of people recognizing it and 93% of customers continuing with an online purchase when they see it during checkout.

# WHAT IS THE POST-QUANTUM TEST KIT?

Most experts estimate that within the next five to fifteen years a sufficiently powerful quantum computer will be built with the required qubits and circuit depth to crack Rivest-Shamir-Adelman (RSA) and Elliptic-curve cryptographic (ECC) keys. DigiCert is working with several post-quantum industry players to create a PKI ecosystem that is quantum-safe and agile enough to face any future threats with our PQC Test Kit\*.

With hybrid TLS/SSL certificates, you can:

- Implement post-quantum encryption while preserving backwards compatibility
- Combine classical cryptographic algorithms with new post-quantum capabilities
- Protect your data from standard and quantum attacks with a single certificate

## How does the PQC Test Kit work?

With the PQC Test Kit, you can analyze your ecosystem for PQC vulnerabilities, and start preparing to deploy post-quantum certificates that will protect you in the future.

Because of the time it will take to develop, standardize, and deploy post-quantum cryptographic techniques, DigiCert is testing the viability of embedding post-quantum algorithms in hybrid certificates using this IETF draft. In the future, DigiCert will provide additional information about our post-quantum cryptography efforts and hybrid certificate development, along with information covering these topics:

- Immediate steps you can take to prepare for a post-quantum future
- Details about hybrid certificates and how they can protect current systems
- PQC toolkit resources and setup guide

For more information on post-quantum cryptography and threats, see these resources:

- [PQC Blog Series](#)
- [DigiCert's PQC webpage](#)

### The DigiCert PQC Test Kit includes:

- Hybrid RSA/PQC TLS/SSL certificates
- A modified Apache webserver/ISARA catalyst server
- Custom Firefox browser

\* <https://www.digicert.com/news/pr/digicert-gemalto-and-isara-partner-to-secure-the-internet-of-things-in-the-quantum-age/>

# DIGICERT CERTCENTRAL® SERVICENOW™ INTEGRATION

Manage the entire lifecycle of your TLS/SSL certificates where you work with DigiCert in ServiceNow.

In the past, managing a certificate workflow within ServiceNow required multiple tools and numerous manual tasks. DigiCert Secure Site Pro certificates integrate directly through an application in ServiceNow, so you can seamlessly manage certificates in one place, delivering faster issuance times, preventing certificate expirations and reducing manual tasks.

IT administrators can establish clear roles of administrators, approvers and requesters. With customized fields based on certificate purpose, location, owner, and expiration, it's quick and easy to organize, locate and monitor every certificate in your organization.



## Features

- Manage TLS/SSL certificates
- Track and find certificates
- Approve, reject or edit certificate requests
- Manage users and permissions

## Benefits

- Conveniently remain in ServiceNow
- Streamline deployment of new certificates
- Avoid security outages
- Speed up certificate delivery

# DIGICERT CERTCENTRAL® MULTI-YEAR PLAN

Avoid lapses by extending the life of your certificates.

## How does Multi-year Plan work?

The DigiCert Multi-year plan eliminates the need for annual per-certificate purchases by allowing you to select the duration of security coverage you want—up to six years, in total. Once you've selected a plan, you can easily renew that certificate when it reaches the end of its validity period at no additional cost. This helps reduce the possibility of an outage while simplifying your security management.

Multi-year Plan offers options for DigiCert Secure Site Pro certificates.

## DigiCert CertCentral Automation

With CertCentral Automation, Multi-year Plan allows you to take advantage of time-saving capabilities like:

- New order support for almost any ACME client running on the customer server
- Automation and Discovery across multiple servers for larger-scale networks
- The ability to utilize sensors for easy-to-manage, scalable ACME deployments
- Seamless integration with OEM solutions like F5, Citrix, NetScaler, A10 and popular server orchestration and management platforms
- Customizable automation through APIs that integrate your system with DigiCert tools
- Auto-renew configuration via CertCentral console

For more information, contact your partner account manager  
or send an email to [resellers@digicert.com](mailto:resellers@digicert.com)

© 2024 DigiCert, Inc. All rights reserved. DigiCert and CertCentral are registered trademarks of DigiCert, Inc.  
in the USA and elsewhere. Other names may be trademarks of their respective owners.