digicert®

DIGICERT PARTNER SALES PLAYBOOK

Company Overview

DigiCert is the digital trust provider of choice for leading companies around the globe, enabling individuals, businesses, governments, and consortia to engage online with confidence, knowing their digital footprint is secure.

Key Facts

- Year Founded: 2003
- HQ Location: Lehi, UT
- Employees: >1300
- 200+ Partners

Customers

- 80%+ of F500
- 90% of top 100 global financial services companies
- Customers in over 180 countries

Solution Overview & Commercial Model

DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content, and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world.

DigiCert ONE managers include:

- DigiCert® TLS Manager
- DigiCert® Trust Lifecycle Manager
- DigiCert® Device Trust (IoT Trust Manager & Embedded Trust Manager)
- DigiCert® Software Trust Manager
- DigiCert® Document Trust Manager
- DigiCert® DNS Trust Manager

Pain Points

- Securing users, devices, documents, software, websites
- Business disruption caused by digital certificate outages, audit failures, or data breaches
- Expanding attack surfaces as the world becomes more hyperconnected
- Digital innovation that depends on identity, tamper-resistance, and data privacy

Elevator Pitch

With increasing cyberthreats, expanding attack surfaces, and adoption of zero trust architectures, digital trust investments are a strategic imperative for industry leaders and growth organizations seeking to distinguish themselves by operational efficiency, reduced business and cyberrisk, and digital innovation.

Key Customers Outcomes Achieved

- Reduce risk of business disruption caused by outages or audit failures
- Protect attack surfaces and improve cyberagility
- Enable digital innovation for connected products and digital processes

Partner Sales Motions

SELL-WITH: Most common for VADs, VARs, resellers, GSIs and hosting providers

- Reselling DigiCert Trust Solutions directly to end-customers
- Distributing DigiCert Trust Solutions to sub-resellers that resell to end-customers
- Register net-new oppprtunities at partners.digicert.com to receive the highest discounts on DigiCert ONE products and solutions

IMPLEMENTATION & DEPLOYMENT: Partners that have technical expertise in implementing and deploying cybersecurity solutions

- Implementations and set-up of Roots, ICAs, user and certificate profiles
- Deployment of DigICert ONE in private cloud, on-premise, and hybrid or multi-cloud environments

Partnership Value Proposition

Leverage our unified DigiCert ONE platform, significant demand for digital trust, and a robust partner program to reach more customers and drive business profitability.

- High growth market opportunity valued at $12B
- Comprehensive security portfolio with high margin solutions
- Scalability with expansive range of use cases
- Deep integrations and flexible, fast deployment options
- Easy onboarding and quick activation for short time to revenue
- Access to marketing and selling enablement resources
- DigiCert field sales support available for all customer interactions

DigiCert Contacts

Partner Sales: Contact your partner account manager.
Partner Operations: partnersupport@digicert.com
Partner Marketing: partnermarketing@digicert.com
Partner Enablement: enablement@digicert.com
DigiCert Partner Portal: partners.digicert.com
DigiCert Website: digicert.com

What is Digital Trust?

The world today is connected in a consequential way. Devices are everywhere. People are online constantly. Operational technology is now being rearchitected as connected infrastructure. And, the pace of digital transformation has accelerated, continuing to increase the surface area of how businesses, people and things are connected.

It is against this backdrop that digital trust is essen-tial. It is what enables us to build, participate in and grow this connected world that we now live in. It is the thing that enables us all to have confidence that the things we are doing online — whether these are interactions, transactions or business processes — are secure.

What are top indicators that an organization needs a PKI platform?

1. Unexpected expiration: Certs unknowingly expiring and certificate management complexity is becoming overwhelming.
2. No automation: Using a "homegrown" solution for managing certificates – no automation – and they have outgrown this solution.
3. Microsoft CA: They are using a free Microsoft tool to manage certs – no automation – and they have outgrown this solution. A very high percentage of customers were using Microsoft when they switched to DigiCert.
4. Knowledge & time to manage PKI: They are looking for a managed service – "Please take this off our plate, we aren't staffed appropriately to manage certificates."

What is the business driver for an organization to invest in a PKI platform?

PKI Administrators have faced increasing complexity and risk, with shrinking certificate validity periods, increasingly broad set of PKI use cases and more types of data that must be validated for certificates.

Identity & Access Managers are experiencing a demonstrable increase in the volume of authentications that must be handled due to zero trust policies, as well as an increase in the types of methods of access due to remote work policies and the need for stronger forms of authentication. Network Administrators, DevOps and Operational Technology Managers are facing an increase in the attack surface area they need to cover.

Target Market

Digital Trust: digital certificates, certificate management, key management, secure key storage, PKI-as-a-service, device lifecycle security, software supply chain security, digital signatures & identity proofing

Key Personas

- CIO / CISO / CPSO / IT Architects
- Buying Centers: Infrastructure & Operations, Identity and Access Management, DevSecOps, Product Security, Information Security, Network Security, Legal/ HR/Procurement

Key Industries

- Financial Services
- Government
- Healthcare
- Technology & Software
- Manufacturing
- Telecoms & Media
- Insurance
- Professional Services

Qualifying Questions

Certificate management and PKI services – Trust Lifecycle Manager

- How do you manage your certificates today? Is it centralized or managed in different departments?
- Do you have internal Certificate Authorities (CAs)? How do you manage these certificates?
- Do you have visibility into your certificate universe? Are you using any discovery or monitoring tools?

IoT Security and certificate management – IoT Trust Manager

- Do you have security challenges related to your IoT Devices?
- What is your workflow for provisioning IoT devices?, How do you provision certificates to IoT devices?
- How do you push secure code updates to your devices?

Secure software signing and key protection – Software Trust Manager

- How are you ensuring hat source code or builds are not tampered with? Do you sign commits?
- How do you protect your code signing private keys (see section on key protection)?
- How are you reducing risk in your software supply chain/ software development?

Securing documents with high-assurance digital certificates – Document Trust Manager

- How do your executives sign documents or outside agreements? And your legal team?
- Do you use e-seals to certify the origin, authenticity, and integrity of your documents and/or signed agreements?