CertCentral® Discovery

Comprehensive oversight of your cryptographic assets

Overview

CertCentral® Discovery is a scanning service that enables organizations to inventory and manage cloud- and network-based certificates, keys, and cryptographic assets.

CertCentral® Discovery's rich feature set gives TLS and security administrators the insight and tools needed to detect and remediate vulnerabilities before they impact the business, through a self-governing infrastructure that minimizes maintenance and ensures integrity of operations.

Key benefits

- Gain visibility over your landscape of cetificate and cyptographic assets

- Reduce risk by identifying and remediating issues before they occur

- Reduce rogue activity with enforcement of corporate security policy

Comprehensive oversight of your TLS certificates, SSH keys, and server-based cryptographic assets
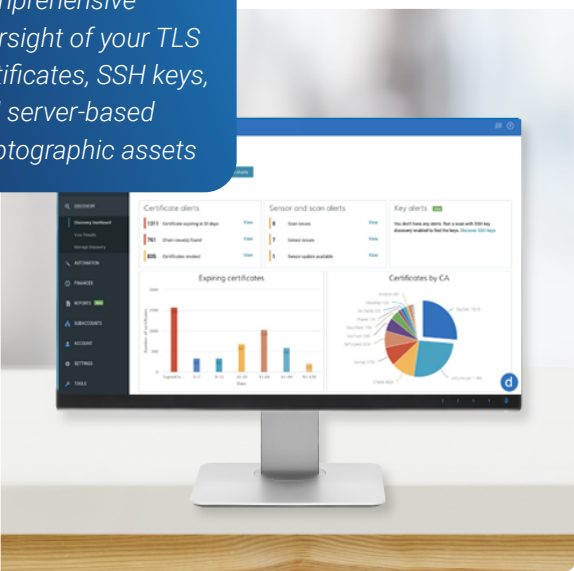
Cloud-, network-, and file-scanning for comprehensive discovery

TLS & SSH Discovery inventories your cloud- and network-based TLS/SSL certificates and SSH keys, along with their attributes. In addition, private roots can be imported for analysis and management of discovered certificates issued from those roots.

Certificates located in protected areas, such as air-gapped environments, can be imported for management to provide centralized alerts and notifications.

TLS/SSH Discovery scans large networks quickly, can perform multiple scans simultaneously, and can blocklist specified domains to further enhance scan efficiency.

Object Discovery inventories public and private TLS certificates, SSH keys, and user, S/MIME and code signing certificates on the filesystem and system registries, and examines archives (keystores, .zip and .jar) and binary files (.exe, .dll, .so) for algorithms, providing IT professionals with a complete picture of the cryptographic assets resident on a server.

Detect & remediate risk

Assess security risk: Review SSL security ratings for all discovered and imported certificates, with prompts for improving security or correcting configurations.

Manage vulnerabilities: Evaluate servers for recent known TLS/SSL security vulnerabilities. Review and remediate weak protocols and ciphers and misconfigured intermediates or other chain-of-trust issues.

Alert and notify: Configure in-console and email alerts for certificate expiration thresholds, escalate notifications to additional recipients, and import certificates in protected zones for expirations alert handling.

A self-governing infrastructure

CertCentral® Discovery is delivered through a self-governing infrastructure, reducing IT maintenance and providing continuous system status and oversight. Sensors and agents continuously ping the discovery service, automatically update, and deliver notification alerts on disruption in function.

Supported platforms

Web servers: Apache HTTP, Apache Tomcat, NGINX, IBM HTTP, Microsoft ISS

Load balancers: CertCentral® Discovery is platform agnostic and can find certificates on any device in the network.
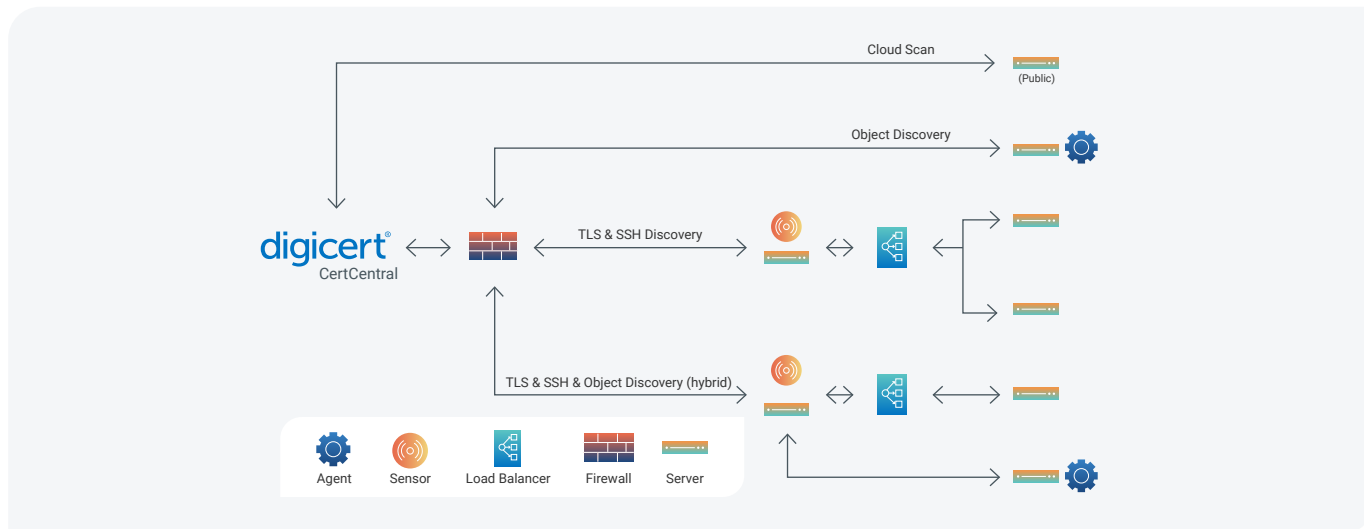
About DigiCert, Inc.

DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. 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. For more information, visit digicert.com or follow @digicert.

Get started today

To get started with CertCentral® Discovery, please contact your account manager or email sales@digicert.com.