SECTIGO®

Effective certificate management relies on enhanced discovery

Digital certificates are everywhere

These small pieces of technology, powered by public key infrastructure (PKI), are the gold standard to secure and authenticate human and machine identities, and establish and maintain digital trust.

Certificates provide the strongest level of user and device authentication, underpin the security of the digital world, and are relied on by all technologies from the oldest to the newest, like blockchain and Web3.

Their ubiquity within a single organizational IT ecosystem can be staggering, being utilized to provide digital trust for everything from websites, applications, email messages, IoT devices, document signatures, mobile devices, and users.

The average IT ecosystem is more complex than ever and is often a mix of hybrid and multicloud infrastructures. As a result, organizations rely on increasing numbers of digital certificates to maintain digital trust. The number of digital certificates deployed in the average enterprise ecosystem can number thousands or tens of thousands. Each of these secures and authenticates critical internal and external processes.

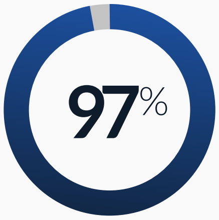
For enterprise IT teams, the management of increasing numbers of digital certificates is a challenge. Those tasked with this important job know the importance of certificate discovery as the first step to proper management – after all, they cannot protect what they cannot see. As reliance on digital certificates increases, IT teams must have a seamless way to fully discover every single digital certificate deployed across an enterprise ecosystem or risk the ramifications of poor certificate management.

O2, Ericsson, Cisco, Spotify, LinkedIn, Slack, Microsoft, SpaceX Starlink, NASA. What does each of these companies have in common, apart from being well-recognized and trusted by millions?

Every single one of them, and many more besides, have suffered costly outages as a direct result of an unexpected digital certificate expiry - in some cases affecting millions of customers, causing cascading sets of failures across the technology ecosystem and sometimes resulting in data breaches.

For modern IT teams, discovery must be the foundation of every certificate management solution, to avoid falling foul of unexpected expiry and the consequences that result.

The problem is that digital certificates don't live in just one place; they're distributed in significant numbers across web servers, load balancers, firewalls, containers, and multi-cloud environments causing management and visibility complications. The challenge for IT teams is to discover them. All of them.



97% of organizations claim that lack of visibility is a risk[1]

Comprehensive visibility is critical

Market-leading Certificate Lifecycle Management (CLM) platforms enable an automated and continuous discovery process to search for and discover all certificates deployed across an enterprise IT ecosystem, as well as proactively ensuring that certificates are provisioned to align with company policies.

This is where organizations that rely on manual discovery and monitoring of increasing numbers of certificates, of different types, and from multiple origins, begin to struggle.

When someone changes their name or leaves the company, when a machine is disposed of, or when a cryptographic algorithm is compromised, IT teams must quickly find and revoke those certificates in a sea of other certificates.

Today's IT ecosystems are vast and interconnected. For those managing the lifecycle of digital certificates in an ecosystem, getting it wrong, or failing to discover all digital certificates deployed in an ecosystem can have far reaching consequences.

Risks of poor certificate management

Costly outages

Outages to critical business systems can have a devastating impact on an organization's bottom line. Unfortunately, outages due to expired, forgotten, or simply improperly installed certificates are all too common.
In fact, Sectigo research revealed 31% of enterprises have experienced outages due to expired, stolen, or revoked certificates[2].

Insufficient inventory

To maintain a secure and compliant environment, certificate audits must be performed effectively for each and every device, user, and application process. According to Sectigo research, 77% of enterprises reported that they struggle to successfully renew digital certificates[3].

Manual management

Nearly half (47%) of organizations say they use spreadsheets, scripts, or basic tools to manage digital identities[4]. This manual approach to identity management hampers visibility into all digital identities and potentially creates an opportunity for bad actors to exploit.
Monitoring the constant additions, removals, and modifications to certificates is impossible in a spreadsheet and is difficult at best with basic tools.
Just 26% of respondents in the latest Sectigo research rate their organization's visibility into all managed digital identities as "excellent"[5].

[1,2,3,4,5] Managing Digital Identities: Tools & Tactics, Priorities & Threats, Sectigo Research, Conducted by Enterprise Management Associates (EMA), 2021

Certificate discovery is going to get more challenging

For many organizations, full certificate discovery is already a challenge. In large organizations, use cases for digital certificates are broad in number, and in many cases the deployment of digital certificates is siloed across many departments within an organization. This makes it hard for CISOs and their teams to easily discover all digital certificates issued across the enterprise network.

Compounding this issue is the fact that digital certificates can be procured from a variety of Certificate Authorities (CAs), and enterprise IT teams actively choose to deploy digital certificates originating from different CAs for redundancy reasons. This, coupled with siloed certificate issuance outside of the view of IT teams, subjects the organization to significantly increased risk.

90-day TLS

But, for all organizations, certificate discovery is about to become even more challenging. On March 3, 2023, Google announced in its "Moving Forward, Together" roadmap the intention to reduce the maximum possible validity for public TLS certificates from 398 days to 90 days.

This reduction to a 90-day maximum validity for SSL/TLS marks a major shift for IT teams. With the number of certificates used by organizations expected to increase at least fivefold as a direct result of 90-day maximum term, it is vital that organizations have a robust solution in place to fully discover all certificates currently deployed and be prepared for that at least fivefold increase when 90-day TLS comes into effect.

The time to enable enhanced certificate discovery is now.

Sectigo Certificate Manager's enhanced discovery tool

Sectigo Certificate Manager (SCM) is designed to deliver full certificate discovery within the most complex of IT environments. With SCM, IT teams can automatically identify, import, and audit all digital certificates, regardless of the issuing Certificate Authority.

SCM's enhanced discovery feature obtains actionable certificate data that assists IT teams in reducing maintenance time, and enables IT teams to have complete control over digital certificate inventory, reducing risk and enabling agility.

Key features of Sectigo Certificate Manager

Network discovery

Discover all certificates, regardless of where a certificate is installed, whether it's behind a firewall, on premise, or in the cloud, Sectigo Certificate Manager can locate every certificate across an enterprise network, regardless of its origin.

Microsoft Active Directory discovery

Centralize discovery tasks and access one active directory (i.e., Microsoft Active Directory) rather than many, thereby facilitating the acquisition of all relevant and necessary metadata.

Certificate discovery buckets

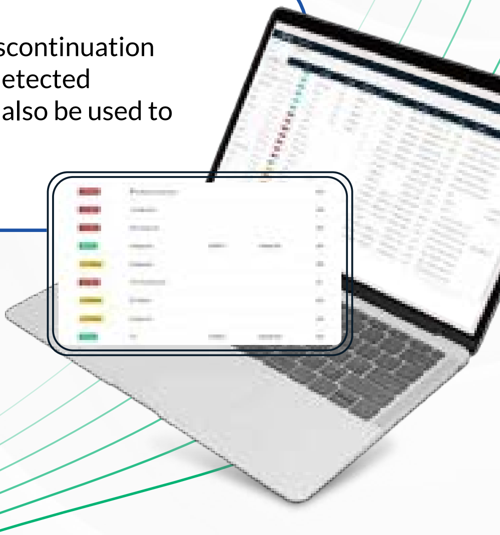
Source certificates automatically depending on your own set of criteria (such as name convention, standards, etc). Discovered certificates can be auto-assigned to the proper organization/department.

Certificate notifications

Get notifications where you need them. Email notifications can get lost in your inbox. With SCM, stakeholders and team members receive automatic alerts of expiring certificates across multiple communication channels such as Slack and Teams, ensuring rapid renewal, reducing the risk of outages and breaches.

Certificate discovery reporting

Plan out renewal, migration, and discontinuation actions by examining and filtering detected certificate data in reports that may also be used to assess security compliance.



Sectigo Certificate Manager Enhanced Discovery

Reduce risk

All imported and identified certificates are automatically categorized, filtered, and examined. Certificates will be sorted appropriately, enabling the completion of the appropriate lifecycle duties. Alerts and notifications can be sent to assist your team in resolving issues before they arise.

Be in control

Prevent risk, preserve uptime, and obtain actionable knowledge into your organization's certificate status. Save cost by avoiding significant losses caused by security flaws, system downtime, and even brand damage. SCM’s enhanced discovery provides the critical certificate metadata required to remediate vulnerabilities, including certificate type, expiration date, location, and more.

Simple housekeeping

Automate the inventory process, enable robust audit events, and reduce the labor of manual management across many platforms. Sort certificates and customize filters that suit your needs through SCM’s simplified interface, look for overlaps, and prevent outages.

Stay agile

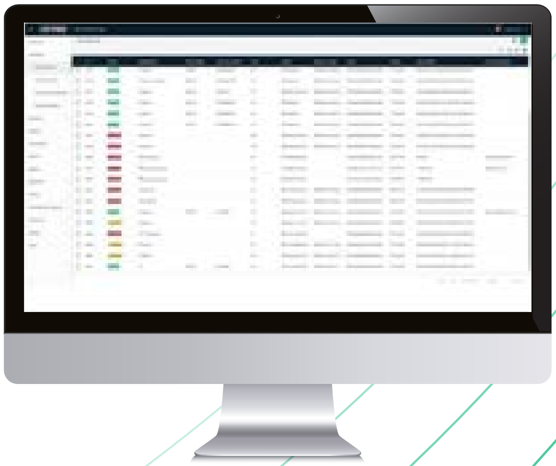
With the flexibility to automate scan times or just run on-demand scans and view findings on your schedule, you won't need to "babysit" scan times and results. Real-time notifications can be received through your preferred communication channels (i.e. Teams, Slack) so you and your team don’t miss any important messages.

It’s time to discover everything

Poor certificate discovery can lead to costly errors, service outages, even security breaches. Failure to identify and manage all certificates deployed across an IT ecosystem can leave organizations exposed to vulnerabilities, as expired or compromised certificates can serve as entry points for malicious actors.

In the wake of the 90-day TLS era, where certificates require much more regular renewal, certificate discovery is the crucial first step towards fully-automated certificate lifecycle management.

With SCM’s advanced discovery, organizations can identify and track all certificates, regardless of origin, enabling them to streamline the management process, reduce manual efforts, and minimize the potential for human errors. Ultimately, this retains a strong foundation of digital trust, enhancing the organization’s overall security posture.



Digital trust and security have never been more important. A comprehensive and automated approach to certificate discovery is no longer optional but a critical necessity for organizations striving to protect their data, systems, and customers.

To find out more about how Sectigo Certificate Manager can enable your organization with advanced, continuous certificate discovery:

Contact us