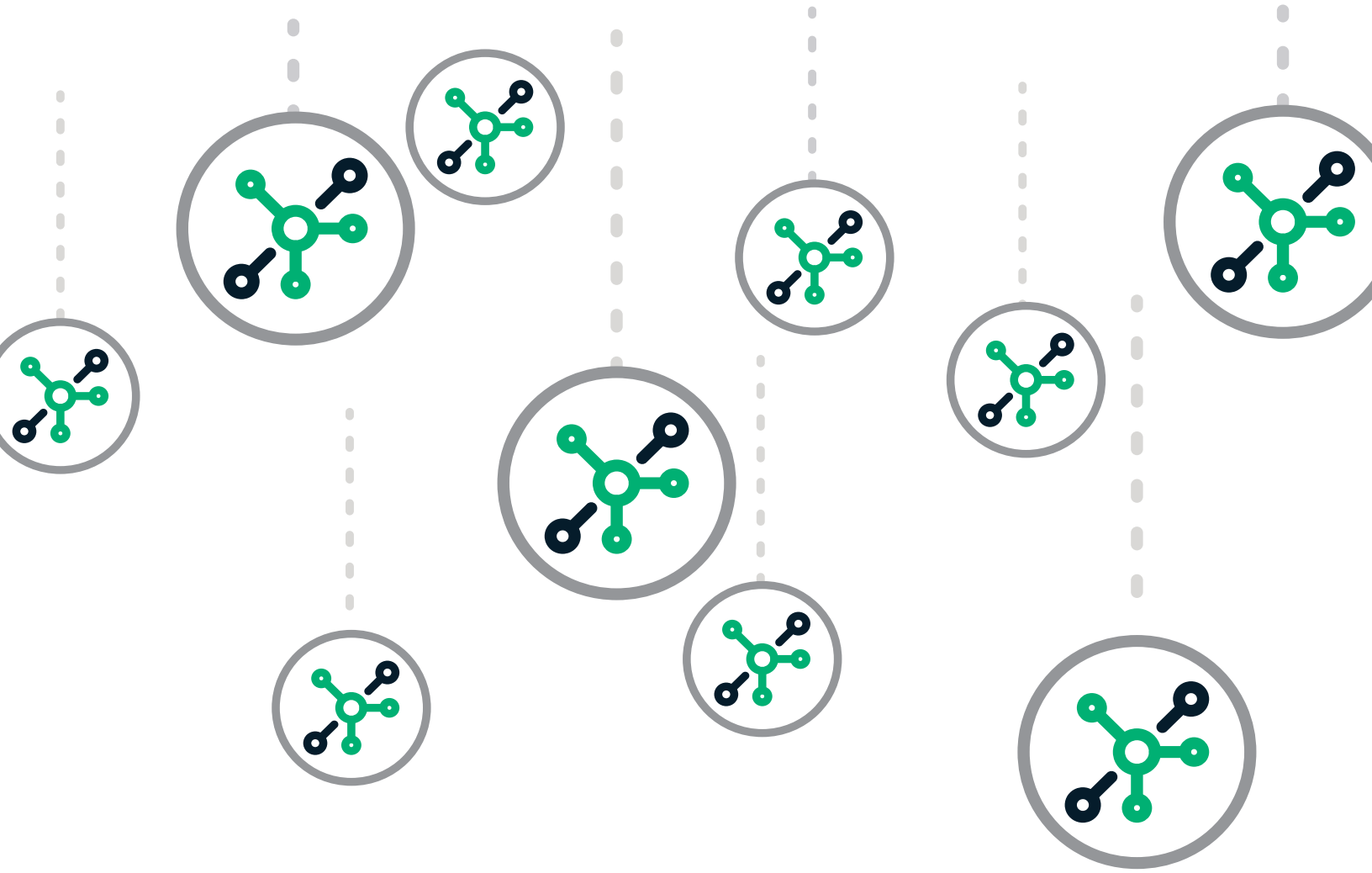
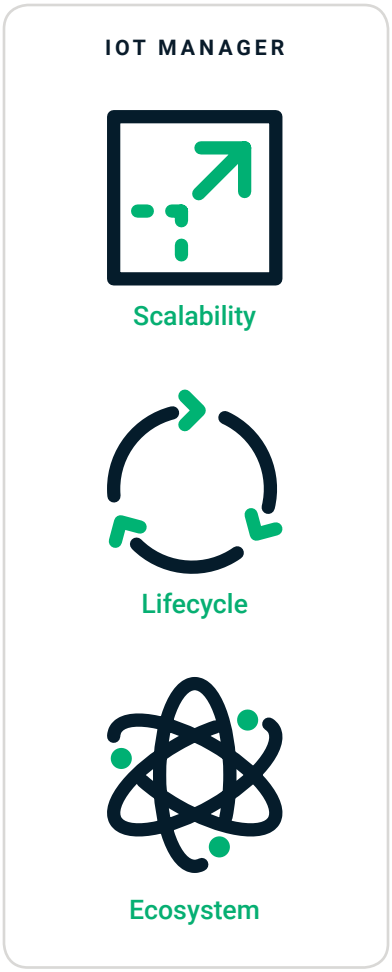
SECTIGO



IoT Manager

Overview

With more than one billion devices deployed today, Internet of Things (IoT) is among the most important growth areas for technology in the coming years. With research predicting as many as 50 billion active IoT devices by 2020, companies of all sizes and industries are planning and implementing IoT strategies to improve productivity, responsiveness, and their ability to delight customers.



Unfortunately, after several years of highly damaging attacks exploiting vulnerabilities in IoT networks, it has become clear that security has not kept up with the growth of this new platform. Too often, IoT device networks are susceptible to rogue, infected, and malicious software, which can inflict harm on companies' operations, their customers, and the online community at large. One result of this trend is recent legislation requiring companies creating and operating IoT networks to provide protection against exploits.

Sectigo's IoT Manager provides trusted, mutual-authentication solutions for all IoT devices and networks, enabling companies to securely build out and scale their ecosystems and manage the full device lifecycle.

Challenges

Recent history has proven that for an IoT implementation to be secure, it must include unique, fool-proof identifiers for all devices on the network. Weak identity options, like providing access control strictly through passwords, do not rise to this level of protection. Even one-and-done certificates are not effective. From manufacturers to network service providers to consumers, maintaining IoT ecosystems in-house has become too daunting a task — especially for those managing hundreds to millions of devices.

From device creation through customer use, every stage presents possible dangers for the ecosystem. Manufactures worry about device integrity and ecosystem standards as well as what could happen to their brand reputation should issues occur. Network service providers face issues of DDOS and botnet attacks, customer outages caused by these assaults, and compromised data and consumer privacy. Finally, the enterprises operating IoT networks must be comfortable that their devices follow best practices in device integrity and ecosystem standards.

While the ideal solution is a PKI management system, most products on the market are seen as too expensive and time consuming for many companies to implement.

- Built to scale
- Quick to implement
- Easy to manage
- Cost effective

Solution: Sectigo IoT Manager

To protect an IoT ecosystem against outside threats, Sectigo IoT Manager utilizes a secure, cloud-based portal that issues trusted third party PKI certificates for authentication and lifecycle management of the IoT network to protect it throughout its lifespan. All in a solution that's effective, efficient, and easy to manage.

Through the use of a third-party PKI solution, device registration certificates are installed by the PKI provider at the first point of network connection, thus helping to protect devices from interception or malicious software installation. Once connected to the private network ecosystem, devices can link only to those authorized on the network. Any device without the proper authentication credentials will not be allowed to connect.

By building an ecosystem of trusted devices for customers and partners, Sectigo's IoT Manager helps organizations bring secure devices to the market quickly and contributes to the company's security throughout the product lifecycle.

SECTIGO

Working with our partners to deliver a platform that's built to scale, quick to implement, easy to manage, and cost effective, Sectigo has created a solution that's available across a wide range of industries — from industrial automation and medical devices to telecommunications and smart cities.

Using x.509 PKI certificates and custom hybrid TLS/SSL certificates, the IoT Manager's high-availability, batch-issuance system allows administrators to easily enroll, download, and decrypt certificate batches quickly and efficiently. Plus, it meets requirements for many industry standards, including WiMAX Forum, GSMA, Zigbee, OCF, and Joint Venture-Silicon Valley.

Sectigo's IoT Manager offers:

- CA signing and hosting services
- Batch PKI certificate issuance
- Identity and registration certificates
- Device authority partnership for KeyScaler
- Automated certificate installation and provisioning
- Certificate lifecycle management
- HSM provisioning and management

With support centers spanning the globe — from the U.S. and Canada to India and the UK — Sectigo IoT Manager can help organizations worldwide protect their IoT ecosystems. Plus, Sectigo offers support in English, Spanish, Simplified Chinese, Korean, Arabic, German, Russian, and Hebrew. And with datacenters in Manhattan, NY and Manchester, UK, Sectigo has an issuance capability of 250 million certificates per day.

Whatever your industry and wherever your company, Sectigo IoT Manager can help to secure your IoT ecosystem — protecting your data, your customers, and your brand reputation.

About Sectigo
Trusted by enterprises globally for more than 20 years, Sectigo (formerly Comodo CA) provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority, with more than 100 million SSL certificates issued across 150 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape.