digicert® | wattwatchers DIGITAL ENERGY

Streamlining IoT Security: Wattwatchers & DigiCert® ONE

CASE STUDY

Energy Innovator Wattwatchers Streamlines IoT Security, Becomes Enterprise-Ready with DigiCert® ONE

Executive Summary

Company name: Wattwatchers
Industry: Energy
Headquarters: Sydney, Australia

Key business requirements:

- Meet enterprise-grade security standards to support growth
- Uplevel software and device security that integrates current and future best practices
- Automate certificate provisioning and renewal across IoT devices
- Sign firmware automatically to ensure only trusted code runs on devices
- Integrate PKI and firmware signing into CI/CD pipeline via API

Solution:

- DigiCert Device Trust Manager
- DigiCert Software Trust Manager

Key benefits:

- Certificate management of IoT devices is now automated, ending the need for manual tracking or intervention
- Automated firmware signing set up within several days, saving weeks of work compared to DIY
- Small team delivers enterprise-grade security without having to scale up resources
- Fortified security posture significantly expands enterprise sales opportunities
- Company saved approximately AU$40,000 in deployment costs

Requirement

Achieve Enterprise-Level Security with API-Driven Efficiency

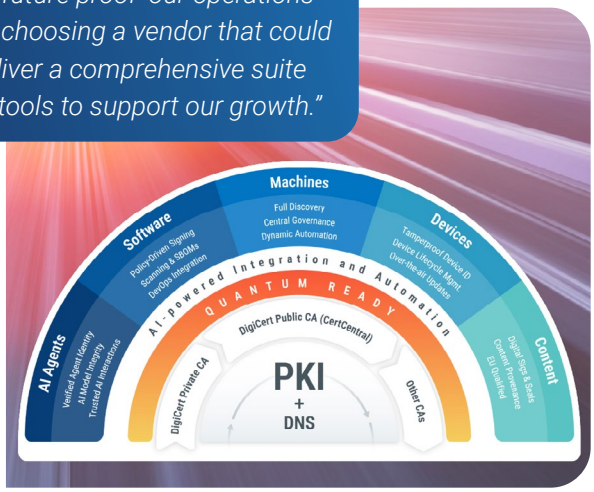
Over the last few years, Wattwatchers evolved from their consumer-centric startup roots to focus on large enterprises such as public utilities, energy retailers, and commercial property managers. This strategic shift toward a more sustainable business model promised to accelerate growth in both their smart device technology and their "energy data as a service" offerings.

However, this pivot also brought about new challenges, most obviously increased scrutiny of the company's security practices. Enterprise prospects had rigorous demands around data protection, device identity, and certificate management, driven by the move toward stricter standards and regulations within the corporate and energy sectors.

As Wattwatchers prepared to launch their next-generation 6MW IoT devices, Chief Innovation Officer Grace Young recognized a critical challenge. The company would require a trustworthy, robust, and scalable solution to avoid significantly increasing resources for security troubleshooting while meeting their new customers' rigorous expectations. Wattwatchers' API-driven architecture also demanded a security solution that could seamlessly integrate with existing systems. This solution needed to automate key tasks such as firmware signing and device identity validation using PKI.

"Our APIs and the ingress of data through the system into our database and then out to our customers is our primary 'product'—it's not just the hardware, but access to the data our devices generate," Young explained. "Because we have a strong ethos of running lean, we needed a solution with very strong API integration. Our production processes needed to be able to link into it, and we needed it to be baked into our continuous integration environment."

"When we were deciding which PKI solution to use, we sought to 'future proof' our operations by choosing a vendor that could deliver a comprehensive suite of tools to support our growth."



Solution

DigiCert® ONE Automates Secure Device Identity and Firmware Signing

Wattwatchers wanted a comprehensive digital trust solution that could meet all their security and operational needs while providing the necessary functionality as the company scaled. They found it within the DigiCert® ONE platform. Device Trust Manager could efficiently secure Wattwatchers' device identities and communications, so that each device in the field could be uniquely authenticated and securely managed without requiring additional resources. And DigiCert Software Trust Manager automated firmware signing, embedding security into Wattwatchers' continuous integration environment and guaranteeing that only authorized firmware would run on their devices.

"When we were deciding which PKI solution to use, we sought to 'future proof' our operations by choosing a vendor that could deliver a comprehensive suite of tools to support our growth," Young said. "We didn't want to deal with multiple vendors for different parts of our operations like certificate management and software signing, which just adds complexity, costs, and potential points of failure. DigiCert's digital trust platform enabled us to automate it all, allowing our small team to deliver an efficient, resilient, and secure digital infrastructure for our enterprise customers. This allows us to prioritize customer value without being slowed down by complex configuration on the back end."

Leveraging APIs to support security and operational goals

DigiCert® ONE's API was a key differentiator from competing solutions. "Our biggest use product is ultimately our API. We spend a lot of time on the user experience, but the APIs we saw in competing solutions seemed like they were designed based on what the back end looked like, rather than thinking about how teams like ours would actually use them," Young pointed out. "When we looked at DigiCert's API documentation, we felt that 'it thinks like we do.' The user experience for our developers was very well done."

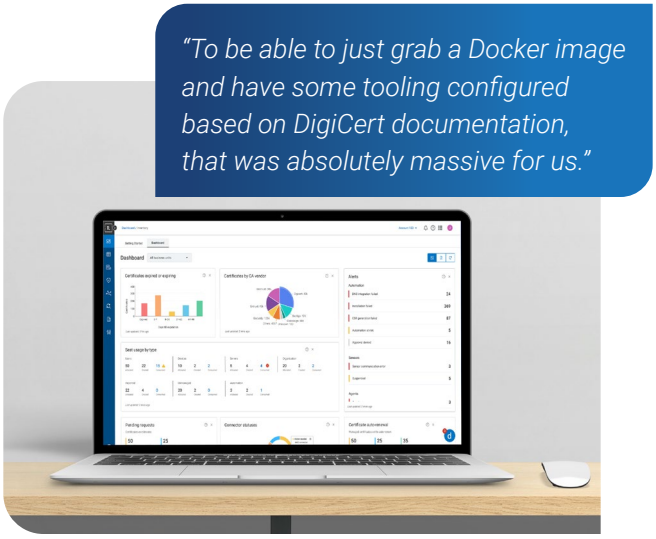
As a result, DigiCert® ONE's OpenAPI spec allowed Wattwatchers to quickly map out how it would fit within the company's own processes. "We were able to quickly work out which API calls we needed to make and when," said Young, adding that DigiCert experts talked them through even the most nitty-gritty details to get them where they needed to be. "They solved problems the way we would solve problems because they were thinking about it from the customer's perspective. That was a really big plus for us," Young added.

Streamlining certificate management using APIs

Managing certificates across thousands of IoT devices already posed a significant challenge for Wattwatchers, and the company knew this issue would only intensify with their growing customer base. Device Trust Manager allowed them to automate all aspects of certificate lifecycle management by integrating DigiCert's API directly into their provisioning and operational workflows. Devices could now independently request, receive, and renew certificates, reducing the burden on the team and minimizing the risk of mismanaged certificates.

"The hardest part for us in terms of organizational maturity was understanding how the certificate lifecycle itself worked, not in getting our heads around how to use Digicert's solutions. We'd read a paper by Amazon about best practices, but we didn't have the internal experience or expertise to know how we could effectively and efficiently operationalize them. A simple example is that we weren't sure what the lifespan of our birth certificates should be—three years, one year, six months?" said Young. "We had a number of conversations with the DigiCert team working through these issues—even before we had actually selected DigiCert® ONE as our final solution. The DigiCert team were immensely helpful for us in terms of building our maturity and understanding of PKI. That was really important for us."

This API-driven approach minimized operational overhead and made it possible to efficiently scale certificate management. "With the 6MW, we've automated all of that so that every device has a certificate and a private key. We're solid on that front moving forward, and that's important, particularly when you're dealing with devices like ours that have a long life-expectancy in the field," Young said.



"To be able to just grab a Docker image and have some tooling configured based on DigiCert documentation, that was absolutely massive for us."

Automating firmware signing at scale

In addition to certificate management, Wattwatchers needed a means to ensure the integrity of device firmware, no matter how many devices the company produced. Just as DigiCert Device Trust Manager automated the certificate lifecycles for devices, Software Trust Manager automated firmware signing, embedding secure practices directly into their continuous integration environment. Now, each new firmware release is automatically signed and verified, eliminating the risk of unauthorized code running on their devices.

"To be able to just grab a Docker image and have some tooling configured based on DigiCert documentation, that was absolutely massive for us," said Young. "Now every single time we do a release build—whether it's a pre-release or production build—it automatically goes through Software Trust Manager. Software Trust Manager then signs them, places them wherever they need to be deployed, and secures them."

The CI integration took Wattwatchers about seven days to implement and deploy. "We saved weeks of work. If we put an opportunity cost of $250 an hour for a developer within, say, four weeks, we've probably saved that much money," Young said. "Now we keep hearing feedback from people in the industry, who are working with other IoT and energy device providers, saying, 'You folks are ahead of the game.'"

Leveraging DigiCert's expertise to fast-track organizational and security maturity

Wattwatchers has made great strides in increasing the security of their offerings—and more broadly, their organizational maturity around security and PKI—as a result of working with DigiCert. Now they were running a secure framework for their devices and firmware that met the needs of interested enterprise customers.

As Wattwatchers was not moving from a pre-existing system and the 6MW was in limited release at the time of writing, Young wasn't yet able to provide hard, quantifiable benefits in using DigiCert® ONE. However, she noted that having the comprehensive benefits supplied by DigiCert Software Trust Manager and Device Trust Manager enabled them to tick the important boxes about security that enterprise customers require.

Young estimates that around 50% of the sales team's current lead pipeline requires the level of security they now support—a market they would not otherwise be able to serve. Said Young: "Partnering with DigiCert has allowed us to build a resilient, secure infrastructure that meets the expectations of our largest customers while keeping our operations lean and efficient."

Learn more about how DigiCert® ONE can help you meet your enterprise security challenges and reach out to a DigiCert expert here.