## Summary

It's not surprising that large-scale industrial IoT deployments are an increasingly appealing target for cybercrime. They have hundreds, even thousands, of possible points of entry (the attack surface), from wireless-enabled sensors at the edge through the industrial IoT gateway and outward to the cloud. Only by scrupulous attention to every one of these points can security be reasonably assured, and this requires more than the minimal password maintenance, firewalls, and other fundamental tools.

The process is hampered by many factors, most notably by the fact that IoT itself is new and there is no single standard or overarching set of standards that define it. In addition, many of the industrial IoT's constituent parts were not designed to be inherently secure and sometimes don't have the memory or other resources to implement security, there are numerous (often incompatible) wired and protocols in use, and a long list of other concerns. That said, of all the elements in an industrial IoT deployment, security will prove to be the most important in the long term, and the time and money required to implement and maintain it will be well spent.

This content was developed together with Siemens Digital Industries Software.