SOLUTION BRIEF

IoT
IoT Security

Securing Enterprise IoT from Vulnerabilities and Breaches

Intel and Sogeti High Tech/Capgemini deliver joint IoT security and management solutions from edge to cloud for manufacturing, energy, transport, and home applications

WITH IOT EXPECTED TO INCLUDE
26 BILLION CONNECTED "THINGS" BY 2020[1],
THE NUMBER OF POTENTIAL ATTACK POINTS
WILL SKYROCKET.

Executive Summary

The Internet of Things represents a massive business opportunity across just about every industry. But to realize that opportunity, enterprise IoT security must become a primary focus. With the number of connected devices set to reach 26 billion by 2020[1], the number of potential attack points is staggering—and hackers are ready to take advantage of it. As malicious players become more sophisticated and successful, enterprises need strong solutions to protect their IoT systems against known and emerging threats.

Intel and Sogeti High Tech/Capgemini have combined their security expertise to deliver an end-to-end IoT security solution. Their hardware and software components are pre-validated, assuring businesses of interoperability. They secure the entire IoT ecosystem, from edge to cloud. And they offer a path to IoT security accreditation, which an increasing number of businesses are finding valuable, whether they are building their own IoT infrastructure or offering connected devices and services to the markets they serve.

Solution Benefits

- **Pre-validation.** Off-the-shelf security components and capabilities pre-validated to work together.
- **Edge to cloud security coverage.** Hardware, middleware, and software to protect the whole IoT ecosystem.
- **Quick path to accreditation.** The right components and accreditation process for enterprises to apply for third-party certification or meet compliance objectives.
- **Security expertise.** Intel brings over 30 years designing sophisticated hardware, processing, and software technologies with an increasing focus on enabling security. Sogeti High Tech brings a dedicated team of security consultants with specialization in industrial cybersecurity.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

Authors

Peter Logan
IoT Solution Architect
Intel Internet of Things Group

Emmanuel Barsacq
Security Consultant
Sogeti High Tech

Solution Providers

- Intel. Silicon and device manufacturer and software and security developer, providing IoT solution ingredients to the industry.
- Sogeti High Tech. Wholly owned subsidiary of the Capgemini Group providing R&D, labs, consulting services, industry experience, and innovations focused on the energy and industrial sectors.

Business Challenge: Deploy Secure IoT Suitable for Accreditation

In 2016, the first truly high profile attacks involving connected devices occurred. The September Mirai attack on the Krebs on Security* site and the October attack on internet infrastructure company Dyn* did considerable damage, the latter having widespread effects for Twitter*, Reddit*, Netflix*, and others. These significant attacks come on the heels of mounting threats and breaches over the last several years, as shown in Figure 1.

There are now multiple discrete botnets for IoT devices. In today's rush-to-market environment, many of these devices are not as well thought out as they should be, leaving large security vulnerabilities. And malicious actors are not just targeting consumers. As more and more industries invest in IoT infrastructure, securing that infrastructure becomes a critical business objective, especially in light of these realities:

- Depending on the business model, unsecured IoT can pose risks both inside and outside the organization, so there's liability and reputational damage to consider.
- Hackers won't give up easily on the valuable resource IoT devices represent.
- DDoS attacks are severe from outside but even more so if they come from within.
- Ransomware has proven how valuable data is; connected assets are even more valuable. Holding IoT devices hostage gives attackers control of real-world, potentially mission critical, systems ranging from drug delivery to power grids to manufacturing lines—increasing ransomware value exponentially.

Enterprises adding IoT ecosystems are recognizing the need to secure hardware, OS, applications, and data storage—from connected devices at the edge through to the cloud. In fact, in a recent online survey on how developers are building IoT solutions, nearly half the respondents listed security and interoperability as their top two concerns.[2]

Companies need trusted partners to help design systems with hardware, software, networks, and storage that work together to provide the right level of security for their needs—and to help them validate their systems with accreditation, if appropriate for their markets.

Intel and Sogeti High Tech have developed a solution that delivers secure enterprise IoT, components pre-validated for interoperability, and an accreditation process—something being adopted by businesses needing to demonstrate that their systems are protected.

"The development of IoT projects in all sectors make cybersecurity a significant challenge. The two-year strategic partnership between Capgemini and Intel has produced a robust IoT platform that is customer-proven and security-certified. This is a major step forward for the Capgemini Group, enhancing the positioning for our XIoT platform among market leaders."

Philippe Ravix
Head of Innovation and XIoT Solution Owner

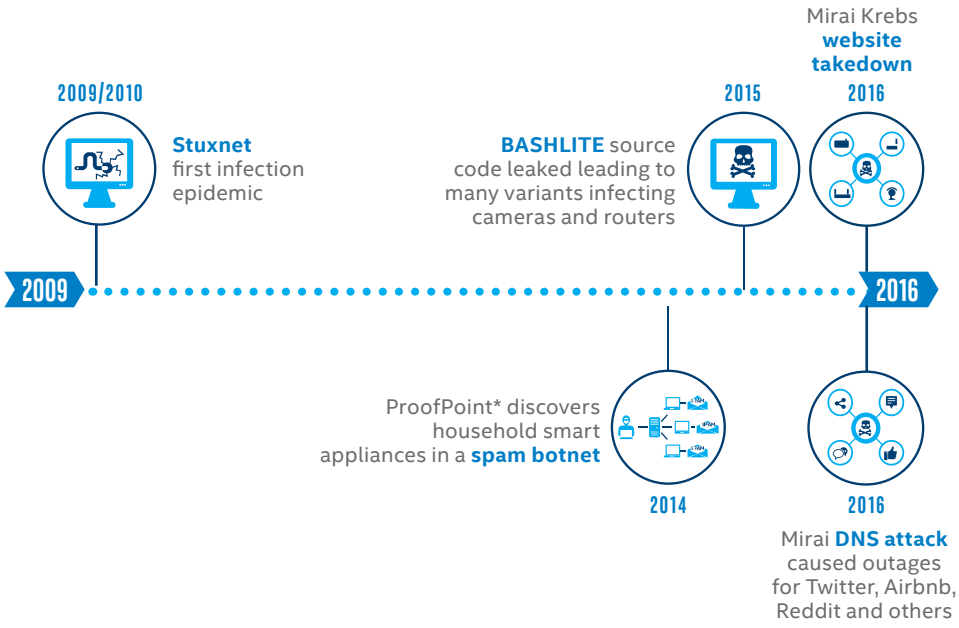

Figure 1. Malicious attacks on connected devices are growing more sophisticated and potent.

Secure IoT is Essential for a Range of Industries

Solutions accredited for security have traditionally been specified for particularly sensitive applications where critical infrastructure is at risk, like government contracts or power generation and distribution. But with increasing data volume, transmission, and exposure across the fast-growing Internet of Things, security has become critical for other verticals as well, for example healthcare, manufacturing, transport logistics, and consumer smart home services provided by utilities and telcos.

Solution Value: Pre-validation, Protection, and a Path to Accreditation

With pre-validated solution components, businesses can confidently deploy IoT security and protect their systems from emerging threats and attacks specifically targeting IoT. The solution provides a quick route to accreditation and guidance for success. And with the definition work completed as part of the accreditation process, businesses can reduce time to market. This time savings allows them to focus on their core business rather than building, securing, and pen testing their own solutions.

Solution Architecture: Intel® Edge Devices with Capgemini eObjects Platform

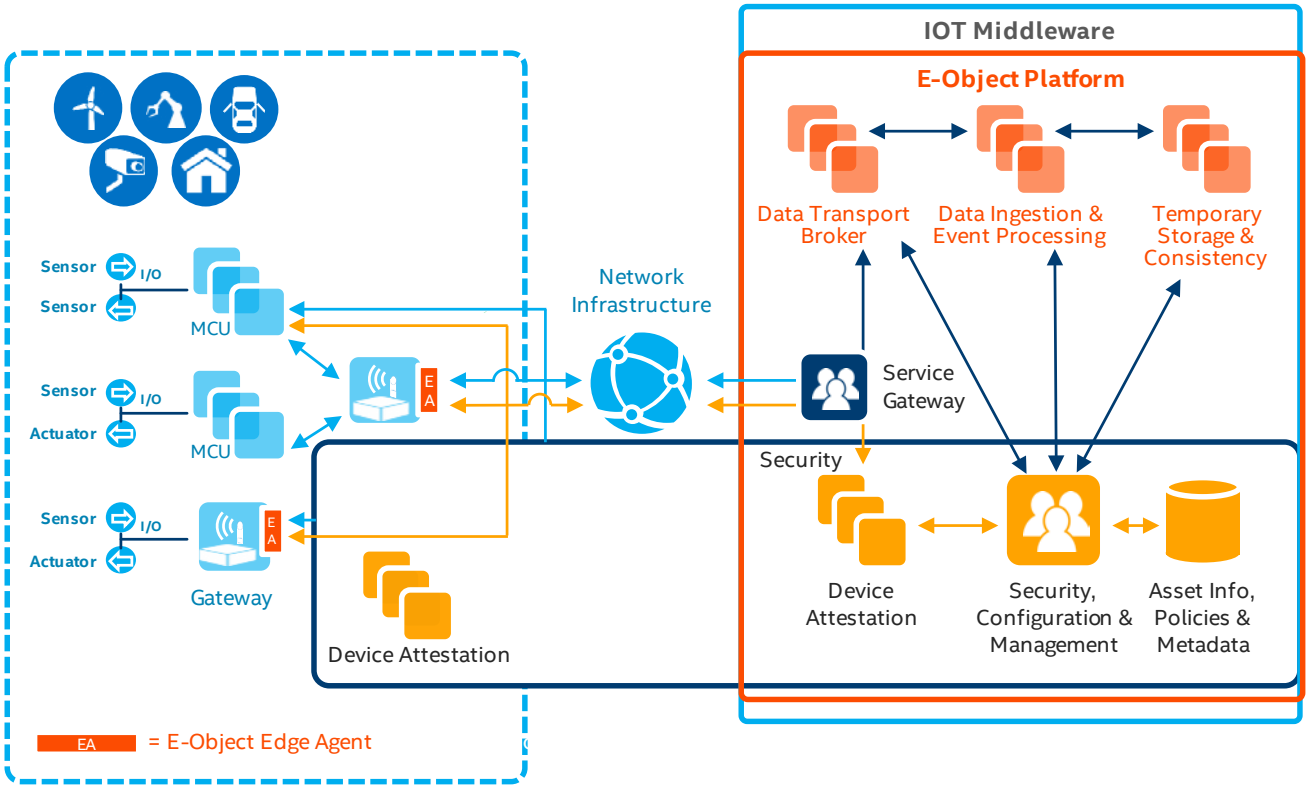

Figure 2. The joint architecture provides security and management for sensors and gateways, data transmission, and storage.

Solution Components

- Intel® technology-based sensors and gateways
- Intel reference design products and ODM/OEM products deployed at the edge
- Sogeti High Tech eObjects Platform:
  - Consists of multiple VMs, the Broker, LDAP, webserver, and the eObjects orchestration engine
  - Manages data flow from multiple gateways
  - Contains a connector library, which allows data synchronization between systems
- Intel® software package:
  - Installed on the gateway and in IoT middleware in the cloud
  - Manages end-to-end security between the gateway and the cloud, including updates and device lifecycle (Updates and management are handled by Wind River Helix* Device Cloud, a cloud-based service designed to manage and monitor IoT devices at large scale.)
- eObjects edge agent
  - Sogeti High Tech software package running on the gateway
  - Has built-in M2M protocols to identify and provision sensors, while data is aggregated and securely sent to eObjects

Accreditation Process

IoT security experts agree that security certification programs will truly improve IoT security only if the programs provide deep testing of the entire IoT ecosystem. According to Cesar Cerrudo, CTO of IOActive Labs and an IoT security researcher, testing would encompass the cloud infrastructure used by the product, any mobile or web apps, and any third-party products that integrate with the solution.[3]

In tandem with the joint architecture being developed by Intel and Sogeti High Tech, the Sogeti High Tech Cyber Security Unit followed procedures and practices of France's cyber defense and information security agency—the Agence nationale de la sécurité des systèmes d'information (ANSSI)—so that the solution would be certified to ANSSI standards. The Cyber Security Unit deals with risk analysis, civil security processes, and penetration testing.

Accreditation Steps and Deliverables

Deliverable 1: Preparation

This is an internal process companies can follow to self-audit and prepare for accreditation.

- Inventory the IoT architecture and platform components
- Define the scope and range of security coverage

Solutions Proven by Your Peers

Intel Solution Architects are technology experts who work with the world's largest and most successful companies to design business solutions that solve pressing business challenges. These solutions are based on real-world experience gathered from customers who have successfully tested, piloted, and/or deployed these solutions in specific business use cases. Solution architects and technology experts for this solution brief are listed on the front cover.

Deliverable 2: Accreditation

The Sogeti High Tech Cyber Security Unit creates a security accreditation dossier, adds their recommendations, and passes it to Sogeti High Tech authorities, who can deliver the IoT security accreditation.

Conclusion

The business potential of IoT is unprecedented—but so are security threats. New end-to-end platforms like the Intel-Sogeti High Tech joint solution allow enterprises to secure their IoT systems with ensured interoperability and pre-validated components. Sogeti High Tech helps companies implement an IoT solution and, through the accreditation process, helps guarantee that each solution is secure.

Find the solution that's right for your organization. Contact your Intel representative or visit **https://www.capgemini.com/utilities/energy-internet-of-things**

Learn More

- **Intel-Capgemini partnership:** https://www.uk.capgemini.com/resources/video/creating-new-business-models-for-utilities-with-capgemini-smart-home-solutions
- **Intel and Capgemini's commitment to innovation:** https://www.capgemini.com/global-technology-partners/intel

Related solution content:

- **Intel® IoT Security:** http://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html
- **Sogeti eObjects Platform:** https://www.capgemini.com/high-tech/e-objects-platform
- **ANSSI:** http://www.ssi.gouv.fr/en/
- **Intel® gateways:** http://www.intel.com/content/www/us/en/internet-of-things/gateway-solutions.html

[1] Gartner.com, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020" http://www.gartner.com/newsroom/id/2636073

[2] http://iot.ieee.org/images/files/pdf/iot-developer-survey-2016-report-final.pdf

[3] http://www.darkreading.com/iot/new-internet-of-things-security-certification-program-launched/d/d-id/1325676

0117/JB/MIM/PDF ♻ Please Recycle 335364-001US

Solution Provided By:

SOGETI intel Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING