SOLUTION BRIEF

Intel® IoT Technology
Security Automation

Developing and Deploying Strong IoT Security

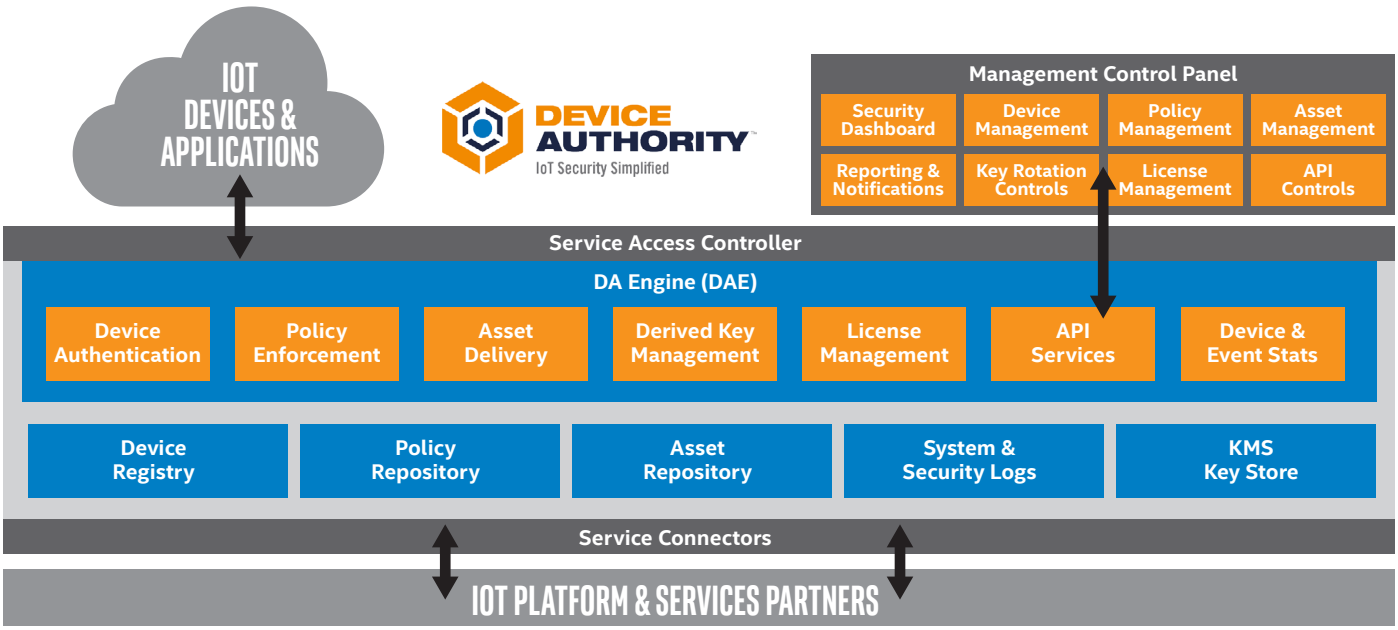
Executive Summary

Intelligent Intel® IoT Gateway technologies perform critical functions within many IoT environments, providing a natural bridge between operational technology (OT) and information technology (IT) systems. IoT promises countless efficiencies, increased competitiveness, improved customer service, and even brand-new market opportunities—and Intel® IoT technology-based solutions play a key role in turning the potential of IoT into reality.

However, deploying strong security is hard and always has been. Deploying strong IoT security is even harder. According to Gartner, by 2020, around 25 percent of all identified security breaches will involve IoT. New security challenges have been introduced in IoT applications due to the scale and pace of adoption, as well as the physical consequences of compromised IoT security. These challenges cannot be effectively addressed by traditional IT security solutions.

To address this, Device Authority has introduced a new paradigm of IoT security automation that accelerates and simplifies the deployment of strong IoT security. They help their partners and customers simplify the process of establishing a robust, end-to-end security architecture within the IoT and deliver efficiencies at scale through security automation that integrates and interoperates with Intel IoT Gateways.

Device Authority solutions provide a critical foundation for establishing and maintaining trust and IoT security for Intel IoT Gateways and the devices, applications, and data relying on them to securely enable data collection, analytics, decision-making, process automation, and control systems.



Device Authority's KeyScaler™ IoT Security Automation Platform provides active device authentication and policy enforcement to deliver four mission-critical IoT security solutions: device provisioning, credential management, secure updates, and end-to-end data protection.

Secure Device Provisioning

The process of introducing and onboarding devices into an IoT application must be securely controlled, while meeting the specific requirements of each IoT environment. Device Authority's patented device key generation and registration controls provide a highly secure, policy-driven trust anchor for onboarding and provisioning devices. Device Authority is also involved in Intel's zero touch onboarding proof of concept, which delivers an automated "headless" device registration, enabling secure, "phone home" provisioning of remote devices at scale—without manual intervention, physical control, or system access to target devices.

Device Authority's patented dynamic device key generation process provides definitive hardware-level device identification while producing unique, one-time-use authentication and encryption keys for each communication session. This device-based trust anchor forms a security foundation for the critical functions operating across the IoT environment.

Secure Credential Management

Managed PKI services from companies like Symantec and DigiCert have revolutionized the cost and complexity of digital certificate infrastructure. Many of these services now include support for smaller, lightweight, IoT-style certificates to help deliver stronger security to a wider range of devices. In order to take full advantage of these services while addressing the challenges of deploying and managing PKI at IoT scale, Device Authority's Secure Credential Management solution directly integrates with Symantec and DigiCert to securely automate certificate provisioning, revocation, and renewal processes. Most importantly, the solution creates a direct, authenticated, policy-enforced binding between devices and the credentials that are assigned to them. This prevents the use of certificates and keys from unauthorized devices.

Secure Updates

Unauthorized software and firmware updates are a major threat vector for IoT devices. Unlike other cyber attacks, IoT breaches can have physical consequences that result in loss of life or property. They can also introduce substantial legal liability and destroy brand reputation. There are three critical security requirements for delivering updates securely to IoT devices: securing access to the updates, verifying the source of the updates, and verifying the integrity of the updates.

Device Authority's Secure Updates solution delivers each of these critical requirements for IoT environments. Through the application of the dynamic key generation technology, access to secure updates is restricted to authorized devices. Updates are also specifically encrypted for target devices and are not exposed as unprotected software or firmware downloads. Lastly, secure updates ensure that both the update source and the integrity of the updates themselves are verified, delivering end-to-end protection for device updates.

Device Authority's Secure Updates solution does not rely on network transport security for update protection and is transport agnostic to support both over-the-air (OTA) and over-the-network (OTN) updates, utilizing various transport protocols.

Policy-Driven Encryption

Data is the currency of IoT applications for both its rightful owners and hackers working to exfiltrate valuable information assets for financial gain, infrastructure disruption, or industrial espionage. While IoT data brings unparalleled potential for understanding, adapting, and controlling the world around us, it also dramatically expands cyber vulnerabilities that can result in the loss of intellectual property and privacy while exposing insight into critical infrastructure and industrial control processes.

Data transfer mechanisms utilizing transport-based security protocols have been substantially compromised and do not guarantee end-to-end data security. IoT data requires advanced, policy-driven, end-to-end security to protect data—in motion and at rest—as it moves between devices and applications.

Device Authority's policy-driven encryption solution utilizes their patented dynamic key generation, device-derived key technology, and crypto-policy agents to provide "drop-in," application-level crypto that is configurable for specific data payloads and transmissions. Dynamic keys ensure that each data payload can be encrypted with one-time-use keys that are not shared or stored. Individual data elements can also be encrypted for specific recipients, independently from data transport protocol security. Using Device Authority's "set and deploy" policies to determine precisely which data needs to be encrypted, their smart agent technology takes care of processing and encrypting the vast quantities of data generated at the device or network edge. This ensures regulatory compliance and the mitigation of risk and data loss.

A Reliable Trust Anchor

With device provisioning, a reliable, policy-enforced trust anchor is required for establishing a trusted security baseline and end-to-end protection for IoT applications.

Utilizing Intel IoT Gateway technology, Device Authority delivers this critical trust anchor to:

- Enable organizations to focus on delivering core business value without the distractions, learning curves, and technical expertise required for in-house security development and maintenance
- Provide automation and scalability that is unattainable with manually intensive security deployments
- Effectively manage IoT application risk and compliance while increasing brand protection

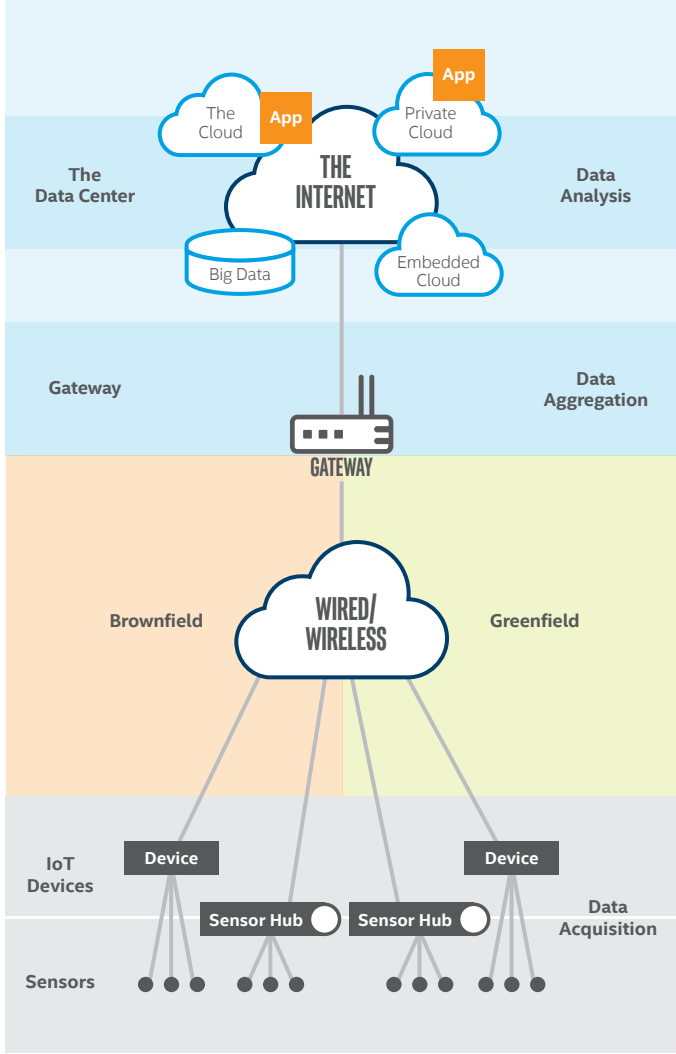
Industry Verticals

Key industry verticals require advanced security solutions to mitigate risk and reduce the threat-surface exposure of mission-critical IoT applications. These verticals can be broadly identified as:

1. Those regulated by privacy legislation, such as healthcare, financial services, or even automotive (consider pay-as-you-drive insurance, for example)
2. Those driven by competitive pressure to protect intellectual property or control processes such as industrial, manufacturing, or engineering design
3. Critical infrastructure projects where a cyberbreach would have significant socioeconomic impact on entire cities or countries, such as smart utility grids, smart cities, and connected transportation
4. IoT platform providers and PaaS and IaaS providers who must be trusted to provide access and data security for their enterprise customers

The IoT Security Imperative

The competitive benefits of IoT will go to the organizations that can most rapidly achieve and support IoT enablement, while ensuring that what they have enabled is secure and protected. Intel IoT Gateway technology, together with Device Authority, provide a critical foundation for competitive IoT enablement.



Device provisioning requires end-to-end protection, from the edge to the cloud.

Learn More

For more information about the Device Authority KeyScaler™ IoT Security Automation Platform, visit **deviceauthority.com**.

To learn more about Intel® IoT Technology, visit **intel.com/iot**.

1016/DW/CMD/PDF ♻ Please Recycle 334934-001US