End-to-end Security for the Internet of Things

The internet of things (IoT) is revolutionizing industries from agriculture to shipping to robotics, with connected devices creating a complex web of captured data, and command and control information traveling around networks at the speed of light. These connected devices can streamline processes and allow companies to create innovative operational architectures, but it is not without risk.

As systems begin to operate autonomously with more and more automated decisions, it is necessary that IoT devices are trusted and their data is secured. If an automated system is fed incorrect data, whether innocently through simply misidentifying a device, or with bad intentions through falsification, the whole integrity of the system is compromised. Incorrect smoke detector data can trigger building sprinklers, inaccurate temperature readings can cause control systems to make potentially harmful adjustments, and so on.

Trust begins with identity. In order to ensure the integrity of the entire system, it is crucial to securely establish and maintain the full lifecycle of IoT devices themselves, and the data they generate. These identities and their associated credentials must be trusted and useable across numerous connected ecosystems, between different devices, from devices to humans, and from devices to all varieties of cloud services. The data from these devices must be kept confidential and secure, and the system needs to be able to verify where it came from and control what systems can access it.

Existing solutions in the new “connected everything” world have tried to employ cryptographic security methods that were barely sufficient in the old, mostly disconnected and siloed landscape. They involve hard coded usernames and passwords that are an easy target for bad actors, or managing individual X.509 certificates on thousands of devices, which isn’t scalable and creates a huge management burden.

What’s needed instead is a system for establishing the trust and to manage the full lifecycle of IoT devices and their data. Enter ForgeRock, the leading platform provider of digital identity management solutions. By applying our vast knowledge of using digital identity to map the relationships between people, devices, and things to machine-to-machine (M2M) IoT environments, we are able to provide a security solution purpose-built for the internet of things.

ForgeRock® Edge Security offers complete end-to-end security for IoT deployments. It ensures the integrity of IoT devices and their communication using secure, standards-based tokens instead of insecure hard coded usernames and passwords, or managing thousands of individual PKI certificates. It adds a rock solid security layer to IoT hardware used at the edge, including leveraging highly secure on-chip Trusted Execution Environments (TEE) if available, and comprehensive, policy based controls for publishing and subscribing to data streams from edge devices, making it as easy to protect data coming from IoT devices as it is to protect a web page.

This technology preview contains descriptions of planned features and functionality. Please refer to the product documentation for full details of included features.
ForgeRock Edge Security is part of the ForgeRock Identity Platform™, and is comprised of two components designed specifically for IoT:

- **ForgeRock Identity Edge Controller** installs on popular edge hardware such as IoT gateways or unconstrained IoT devices. It provides zero-configuration device onboarding, issues and manages secure tokens for each device, and can even provide Hardware Root of Trust for the device itself, providing superior protection from man-in-the-middle and other types of attacks. This gives a broad range of deployment options depending on how strenuous security needs to be for a particular deployment. The ForgeRock Identity Edge Controller can also function autonomously when there is no active connection to the ForgeRock Identity Platform, ideal for edge installations where network access is not always guaranteed.

- **ForgeRock Identity Message Broker** installs on-prem, in cloud, or on the edge, and can receive data streams from thousands of IoT devices. It authenticates the source and secures the data, and authorizes the data flow with the proven policy-based mechanism of ForgeRock Access Management. The broker can also translate from popular IoT protocols such as MQTT and CoAP, and standard HTTPS and websockets. It can even be configured to install on the same hardware as the ForgeRock Identity Edge Controller, providing an all-in-one IoT edge security solution.

The two components together form a strong and secure foundation to ensure the trust of the device identity, in combination with using the same device credential as the trusted source of data being authenticated and authorized for sending data to the cloud.

![Diagram of ForgeRock Edge Security and Unified Platform](image_url)

ForgeRock Edge Security brings Hardware Root of Trust and useful identity capabilities such as standards-based tokens, authentication, and authorization to devices on the edge.

These components work together with the complete ForgeRock Identity Platform to provide a new level of security for IoT deployments. The ForgeRock Identity Platform brings carrier grade scalability, contextual security, and trusted relationships to IoT, supporting on-prem, dynamic cloud architectures, and hybrid cloud deployments.

Don’t let security be a limiting factor in the design of your IoT hardware, software, and solutions. Close the IoT security gap with innovative security, proven open standards, high scale, and advanced management tools with ForgeRock Edge Security, part of the ForgeRock Identity Platform.

### About ForgeRock

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

Get free downloads at www.forgerock.com and follow us @ForgeRock