Today's connected businesses demand better IoT security.

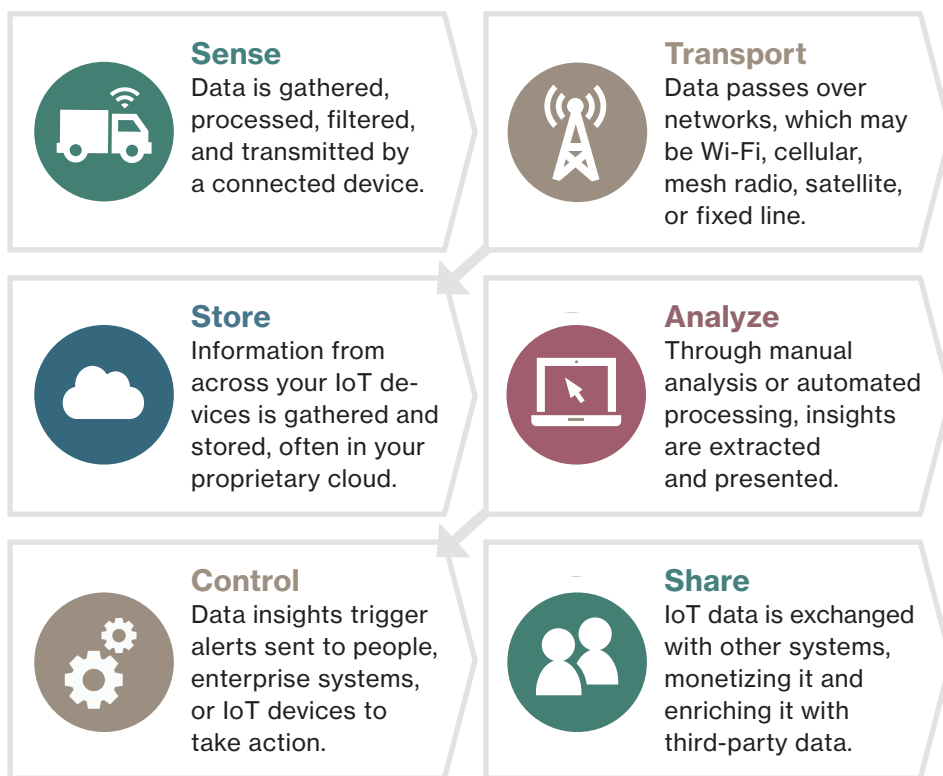**Verizon IoT Security Credentialing**

verizon✓

The Internet of Things (IoT) is filled with countless online connections. Connected IoT devices such as smart home appliances, wearables and industrial control sensors represent a new entry point for cyber-attackers to compromise business systems. In order to protect the IoT, an additional layer of security is needed to address:

- IoT devices deployed in diverse and remote locations, many times outside an organization's network

- Commercial devices lacking in security features and prone to remote hijacking

- Devices that support critical infrastructure including systems in the energy, transportation and financial services sectors

- Routine updates and patches on all connected devices

The answer to these challenges? Verizon IoT Security Credentialing.

The Verizon IoT Security Credentialing Solution

Verizon IoT Security Credentialing (IoT SC) provides digital certificate-based device credentials that establish trust in your IoT ecosystem. It also ensures that company data is delivered without compromise through the IoT life cycle below.

Sense
Data is gathered, processed, filtered, and transmitted by a connected device.

Transport
Data passes over networks, which may be Wi-Fi, cellular, mesh radio, satellite, or fixed line.

Store
Information from across your IoT devices is gathered and stored, often in your proprietary cloud.

Analyze
Through manual analysis or automated processing, insights are extracted and presented.

Control
Data insights trigger alerts sent to people, enterprise systems, or IoT devices to take action.

Share
IoT data is exchanged with other systems, monetizing it and enriching it with third-party data.

IoT SC credentials are a critical component of an organization's IoT trust. The solution's framework enables strong authentication between a device and server, and between one device and another. And just as identity credentials allow employees to access device vendor networks and systems, IoT SC credentials issued to connected devices will ensure only trusted devices can communicate with your organization's infrastructure. Security Credentialing will also protect data exchanged between a wide range of devices from smart phones to tablets — devices from all major companies as well as any device that leverages standard digital certificate protocols.

IoT Security Credentialing Case Study: FiOS Quantum Gateway

Verizon FiOS Quantum Gateway (FQG) routers provide FiOS customers with access to the Internet using wireless-enabled devices such as computers, laptops, tablets and gaming consoles. By issuing IoT SC credentials to the millions of FQG routers in the field, Verizon was able to identify each customer's router as authentic, and secure the communication to and from the router in order to perform management operations such as firmware updates and software patches. By uniquely identifying each router, Verizon ensured that the right content and services were delivered to the correct customer. And because all network communication is encrypted, IoT SC ensured FiOS customers had the ability to attest that its ecosystem uses secure communication to reduce traffic interception.

Verizon's unique provisioning process securely deploys credentials to routers in the field, after manufacturing and shipment to the end-customer. Should a customer's credential expire or otherwise need to be updated, the same provisioning process removes the previous credential and replaces it with one that has been newly-issued. And if a router drops out of service, its credential can be revoked, indicating that this router is no longer in use.

IoT devices in the field

Verizon IoT Secure
Credentialing Solution

FiOS Quantum
Gateway router
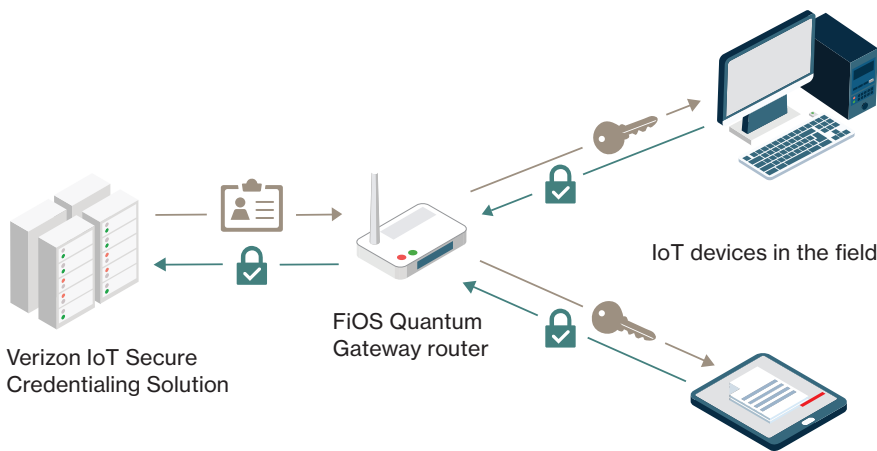
So, if you're looking to add security to your IoT devices operating in the field, all you need is Verizon IoT Security Credentialing. Verizon works with the customer to create a credential issuance profile that meets the usage requirements. Once defined, Verizon manages the entire credential provisioning and validation service for the customer. IoT SC uses standard digital certificate protocols and is applicable to a broad set of IoT devices.

Because better does matter.

The Verizon IoT Security Credentialing solution protects networks in three ways:

- **Application Protection**
  Adds an over-the-top (OTT) layer of security to protect devices and applications, regardless of provider.

- **Trusted Authentication**
  Designed so that only specified devices/users are granted access to applications or devices.

- **Data Privacy**
  Protects the confidentiality of data by encrypting traffic to and from the device.

The IoT allows organizations to create truly transformative solutions, driving business decisions based on data captured and analyzed in near real-time. Coupled with our top-rated network, the Verizon IoT Security Credentialing solution offers customers the most robust, secure ecosystem to unlock the value of their connected devices.

98%

Ninety-eight percent of the Fortune 500 rely on Verizon's services and technologies. Verizon 4G LTE is America's largest and fastest network.[1]

[1]Internet of Things: Science Fiction or Business Fact?, Harvard Business School, September 2014.