COALFIRE

DATASHEET

Internet of Things (IoT) product security

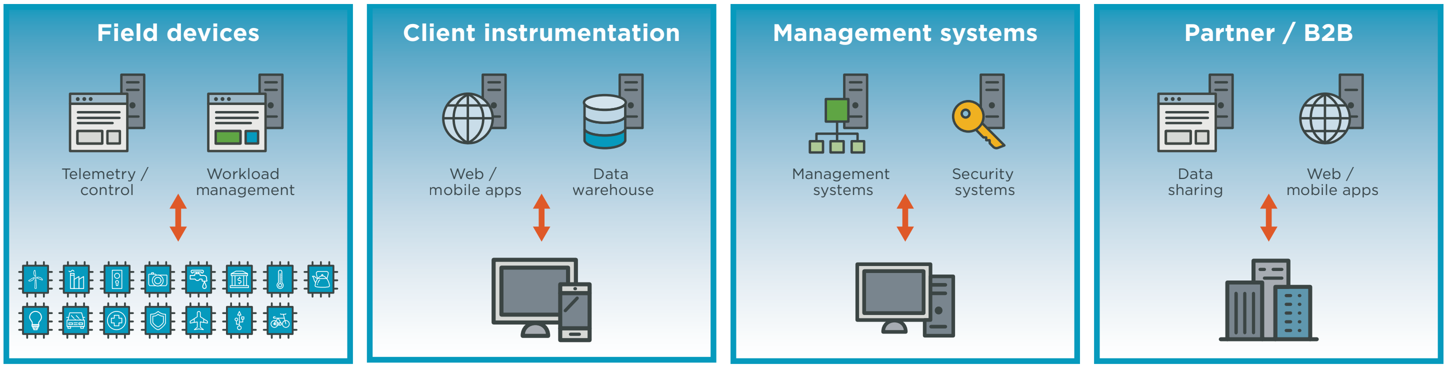
Be confident that your IoT devices are protected

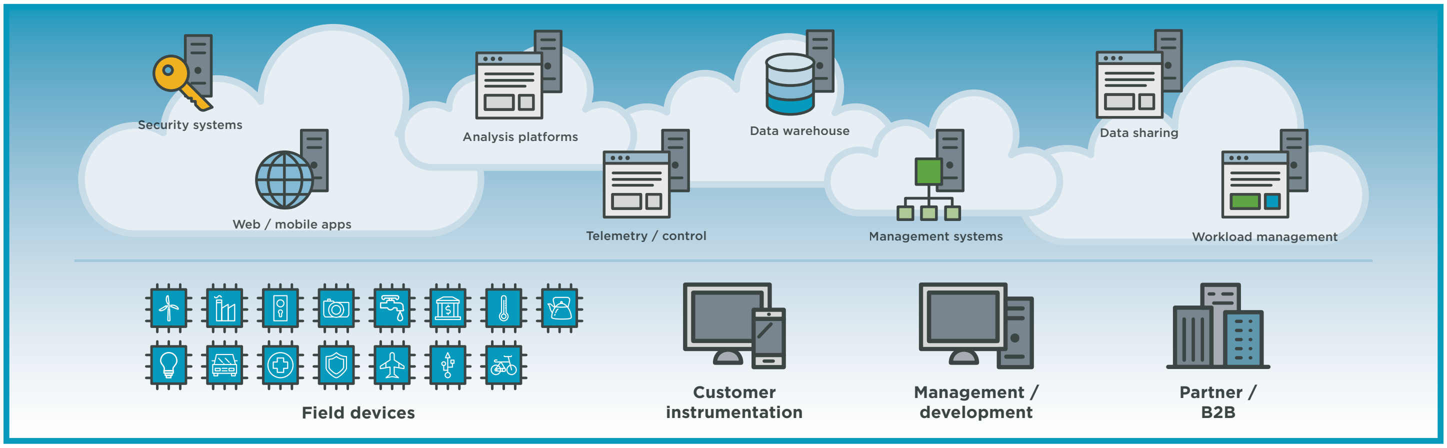
The number of connected devices has skyrocketed in the past few years, and exponential future growth is on the horizon. Because of IoT's rapid evolution, innovative disruptions are occurring at a staggering pace, especially in the industrial IoT (IIoT) and smart infrastructure, consumer IoT, and medical IoT (IoMT) spaces.

Coalfire's unique approach to IoT security is an end-to-end testing strategy that helps you successfully navigate risks, while balancing time-to-market demands.

Our solutions cover various areas including:

- Smart utility and grid management
- Smart building and city management
- Connected appliances, home automation systems, and vehicle automation
- Connected healthcare technologies





Our comprehensive IoT security solutions involve detailed analysis of the entire IoT product ecosystem. Key attack surfaces include:

IoT hardware and embedded systems

- Physical hardware and communications
  - Wired review including Ethernet, USB, Joint Test Action Group (JTAG), universal asynchronous receiver-transmitter (UART), serial peripheral interface (SPI), and inter-integrated circuit (I2C)
  - Wireless review including Wi-Fi, Bluetooth, near-field communication (NFC), and radio frequency (RF)
  - Advanced hardware attacks
- Embedded software and firmware
  - Identification and review of standard or customized services
  - Privilege escalation techniques
  - Firmware and service analysis/reverse engineering

IoT management applications and services

- Web application testing
- Mobile application testing, e.g., Android, iOS
- API penetration testing, e.g., representational state transfer (REST), simple object access protocol (SOAP)

IoT management infrastructure

- Cloud infrastructure testing, e.g., AWS, Azure, Google Cloud, VMware
- Enterprise penetration testing, e.g., internal, on-premise, wireless
- Red team operations

WHY COALFIRE?

- Our dedicated team of more than 90 penetration testers has experience with many different types of engagements, including work on the largest cloud service providers' IoT service platforms. Intimate knowledge and a deep understanding of these platforms enable every testing engagement to be thorough and comprehensive.
- Coalfire Labs has conducted testing in the automotive industry, for medical device manufacturing companies, and on ATMs and voting machines.
- We bring expert knowledge of the risks associated with legacy and cutting-edge technologies and how they impact commercial and government organizations.
- We continuously monitor the evolving threat landscape and help further the industry through speaking engagements, tool discovery, process development, and publications.
- Coalfire Labs has top-class testing capabilities, including a dedicated hardware lab that contains state-of-the-art equipment that enables us to perform testing on a wide range of devices.

DS_IoT_110520

PROTECT EVERY ASPECT OF YOUR IOT SOLUTION WITH A COMPREHENSIVE TESTING APPROACH.

Learn more about Coalfire's IoT product security services.

Coalfire.com | 877.224.8077

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com**