COALFIRE

DATA SHEET

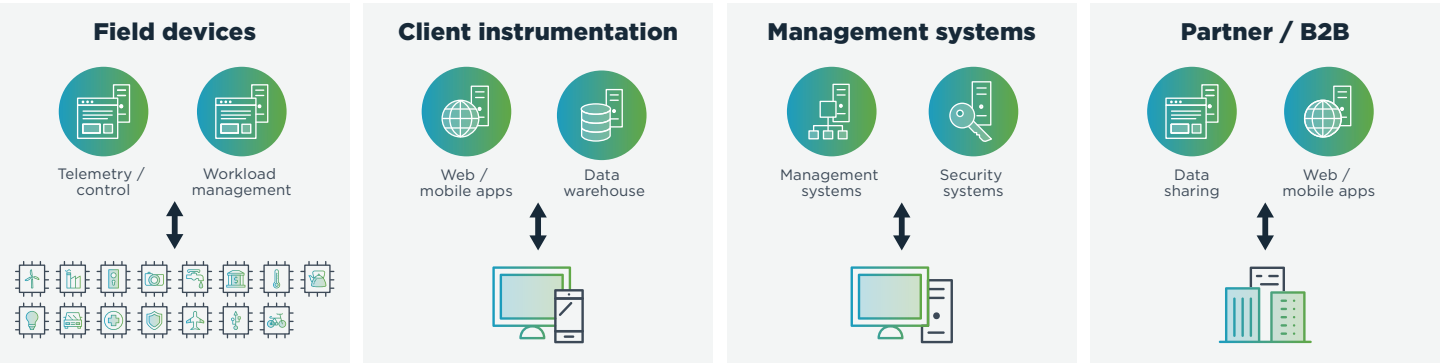
IoT application security assessment

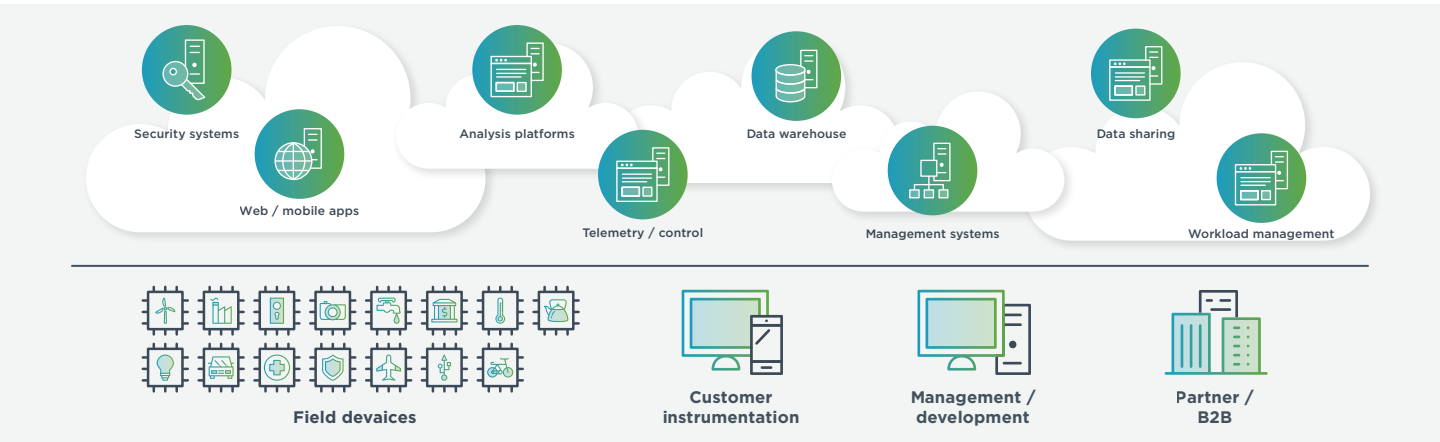
End-to-end security testing and scrutinization for the Internet of Things

As the Internet of Things (IoT) becomes more ubiquitous, attack surfaces multiply, and security must be approached with great care. Coalfire's IoT assessments help you navigate device- and ecosystem-related risks while balancing time-to-market demands. We map the entire IoT attack surface including architecture, communication protocols, hardware ports, firmware upgrade process, external media support, and platform details.

Be responsible for the entire attack surface you create and expose

IoT security is more than just securing the field device, whether that be a smart thermostat, vehicle, pacemaker, or a toaster. Getting a realistic grip on IoT security begins with an assessment scope that includes all relative hardware, communication technologies, data-sharing APIs, management of instrumentation-based web and mobile applications, and cloud-based data management platforms.





Hardware and embedded systems

- Physical hardware and communications
  - Wired review including Ethernet, USB, edge routers (Cradlepoint), Joint Test Action Group (JTAG) debugging and exploitation, logic sniffing and bus tampering, glitching and side-channel attacks, universal asynchronous receiver-transmitter (UART), Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I2C), and anti-tamper best practice checks
  - Wireless review including Wi-Fi (plus edge networks), Bluetooth, Bluetooth Low Energy (BLE), ZigBee, zWave, LoRa, near-field communication (NFC), radio frequency (RF), sniffing transmitted and received radio packets, modified and replayed packets for device takeover attacks, jamming-based attacks, and encryption key retrieval
- Embedded software and firmware
  - Identification and review of standard or customized services
  - Privilege escalation techniques
  - Firmware and service analysis and reverse engineering
  - Encryption and obfuscation analysis
  - Sensitive information leakage (hardcoded values in firmware, debugging binaries, etc.)
  - Analysis of third-party libraries and software development kits (SDKs)

Management applications and services

- Web applications
- Web services and APIs
- Mobile application review and testing including injection-based attacks, mobile app reverse engineering, insecure direct object reference (IDOR), insecure authorization and authentication, sensitive data leakage, cross-site request forgery (CSRF), business logic flaws, and outdated libraries and SDKs
- Management infrastructure
  - Cloud infrastructure health checks and testing
  - Internal and external network penetration testing
  - Red team operations including zero-configuration protocol exploitation; additional data-at-rest and data-in-transit assessment; and MQ Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), AWS, Digital Imaging and Communications in Medicine (DICOM), Signaling System 7 (SS7), and Global System for Mobile Communications (GSM) protocol attacks

Why Coalfire

- Our top-class testing capabilities include a dedicated hardware lab with state-of-the-art equipment that enables us to perform testing on a wide range of devices and use cases.
- We've conducted testing on numerous devices, including vehicles, medical devices, ATMs, and voting machines.
- Our AppSec consultants have experience in both software engineering and security consulting, which means we're able to deliver modern, actionable guidance on all aspects of application security.
- We conduct more than 1,000 complex projects each year for clients in the technology, healthcare, financial, manufacturing, energy, and retail industries.
- Our team comprises experienced testers of the world's largest cloud service providers, including Amazon, Google, IBM, Microsoft, Oracle, and Salesforce.
- For the past 10 years, we have trained and educated security professionals at Black Hat in the advanced tradecraft we developed.

Let Coalfire help you assess and secure any software or product you build.

Learn more about Coalfire's IoT application security assessments.

Coalfire.com | 877-224-8077

COALFIRE

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

DS_IoT_01212022