

# IoT Security Services

## Securing your vehicles, medical devices, and every last connected thing

Smart cars. Smart security cameras. Smart medical implants. Even the smart egg tray in your smart fridge. Everything around you is always connected and communicating, swapping data with other devices and uploading it to the global internet to help your automobile, home, factory, business, and body perform better. It's no wonder that, according to Gartner, by 2020, over 20 billion connected things will be in use across a range of industries.\*

And as these devices become more integral to our lives, the need to secure them grows at pace. Many IoT technologies suffer vulnerabilities. Attackers favor them as they're off radar for IT security groups. Botnets can control them on a global scale, enabling massive DDoS attacks. Even safety critical systems such as medical devices and transportation systems are at risk, thanks to gaps in security created by lengthy development cycles. Despite this, many security teams have neither the time nor expertise to secure connected devices on their own. But you don't have to go it alone. You've got Rapid7.

Whether you're creating a new IoT product or deploying an IoT solution, our experienced and skilled consultants will help you identify risk and vulnerabilities, and apply solutions to mitigate security issues across your IoT ecosystem. With years of experience across sectors including Consumer, Medical, Enterprise, Industrial, and Transportation, our experts are industry leaders who conduct cutting edge IoT research, publish books, release white papers, present at conferences, and conduct thousands of assessments, advisory engagements, and penetration tests every year.

### Our IoT Security Services

With a wide range of IoT services, Rapid7 is ready to meet the needs of your organization. Can't find what you're looking for? Get in touch—we offer custom solutions, too.

#### Threat Modeling

Rapid7 understands the complexity of IoT and connected systems and will assess the highest risk systems and communications, so you can focus on the entry points that matter. Working closely with your team, we'll develop comprehensive threat models of your entire system that can evolve and live with your complete product lifecycle and help you identify and mitigate the most critical issues, as well as provide a document of your product's security posture.

#### Device Design Consulting

Designing hardware is often the first step of a major project and can determine your limitations and weaknesses. This service provides your engineers with one-on-one time with our security consultants during design time. We offer consulting from the ground up so that hardware issues don't become the Achilles heel of your software security architecture.

\*"Internet of Things Primer for 2016." Gartner Inc., 31 March 2016.

## Testing and Vulnerability Assessment

### IoT Penetration Testing

Our penetration and system analysis testing goes beyond basic analysis to consider the whole ecosystem of the IoT technology, covering every segment and how each impacts the security of the whole. Our testing includes the IoT mobile application, cloud APIs, communication and protocols, and embedded hardware and firmware.

### Hardware Testing

Rapid7 will examine the physical security and internal architecture of the device – including internal components – to determine the breadth and depth of its physical attack surface. This service may include component indication, firmware extraction, identification of test points, and reconfiguring the device’s hardware to bypass authentication, intercept traffic, and/or inject commands that may pose a significant risk to your organization and clients.

Key areas of testing:

- Exposed network services
- Device communication protocols
- Physical access to the device’s UART, JTAG, SWD, etc.
- The ability to extract memory and firmware
- Firmware update process security
- Storage and encryption of data

### Protocol Testing

Rapid7 will test communications to and from the device. This includes testing the cryptographic security of encrypted transmissions, the ability to capture and modify transmissions of data, and fuzzing of the communication protocols. We will assess the security of communication protocols and determine the risk to your organization and clients.

This includes capture and detailed analysis of network communications protocols including:

- Bluetooth/BLE
- Ethernet
- FlexRay
- Wifi 802.11
- LIN
- MOST
- Zigbee
- CAN
- SPI
- ZWave
- KWP
- I2C

### Firmware Analysis

Rapid7 will extract and examine the content of the firmware in an attempt to discover backdoor accounts, injection flaws, buffer overflows, format strings, and other vulnerabilities. We will also assess the device’s firmware upgrade process for vulnerabilities and perform a secure boot review process to ensure that public key encryption and upgrade functionality is secure.

---

### Incident Response

After an attack, getting information from anything more than device logs can be a non-trivial task. Rapid7’s hardware teams can assist in pulling information directly from a product. This service is focused mainly on criminal cases and law enforcement; often, IoT devices have tracking and recording capabilities not publicly exposed. Our incident response team can determine what information is available for use in an investigation.

### Transportation Security

Planes, trains, and automobiles – or anything that moves, really – often have a complex set of requirements. And no one understands them better than us. Speed and cost are key areas of the complex systems that make up automotive, locomotive, and avionic security. Many security companies simply try to add encryption or an IDS solution, but these actions only increase overhead and costs and never address the real problem. Rapid7 goes beyond understanding CAN, LIN, FlexRay, and other network protocols to provide assessments and recommendations that won’t affect the product’s performance, but will solve your specific needs and concerns. To make the process as easy as possible, we work with OEs and Tier suppliers to fit into their development workflows.

---

### Secure your connected devices

**Call:** 866.7.RAPID7

**Email:** sales@rapid7.com