

# IoT Security: Striking a balance between opportunity and risk

The world is connected by devices—devices that collect and share information through the Internet of Things (IoT). IoT offers consumers and businesses powerful benefits, and to realize those benefits, it's important to secure IoT solutions for their integrity and for the protection of your corporation and brand reputation.




## Consider this:

**Billions of connected devices** are potential access points to cyber attacks.


**IoT security is—and should be**—a major concern for individuals and enterprises of all sizes and industries.

**Security needs** for a consumer IoT system are far different from the needs of a complex, mission-critical, enterprise system.




**46%** said **security concerns** were an impediment to IoT adoption.<sup>1</sup>

IoT risk and security management is an issue that demands attention now—security was identified as a primary inhibitor to IoT adoption in a recent report by 451 Research.



**Security attacks, including DDoS** have been caused, in part, by IoT devices<sup>2</sup>

The attacks underline the need for vigilance with IoT security and the importance of being able to view, manage and update IoT devices and firmware after the point of manufacture.



**IT Security versus IoT Security**

IoT security must be robust and vigilant because IoT devices are connected to the physical world.



**Striking balance**

Businesses need to strike the balance between protecting their infrastructure and capitalizing on the IoT's potential.

## IoT security is a continuous lifecycle

IoT solutions are broad and complex, requiring a robust set of security measures to ensure integrity and safety.

A cognitive lifecycle approach to IoT Security continuously evolves as new threats emerge; these new threats are fed into the environment for which protection and intelligence must be provided.



IBM Watson IoT Platform has security by design engineered into the platform and the infrastructure on which the platform is based.

- 1. Device and data protection**
  - Secure device-to-cloud interaction
  - Protection of payload data and encryption
  - Continuous validation of device identity to protect platform integrity and control information access
  - Authentication and access controls for users, applications and gateways
- 2. Proactive threat intelligence**
  - Expert, comprehensive risk analysis
  - Visualizing threats for prioritized response
  - Alerts from real-time analysis of device behavior and interaction patterns

- 3. Cognitive risk management**
  - Develops risk hypotheses by correlating security events with conditions across IoT landscape
  - Self-adapts to changing risk profiles
  - Initiates incident response based on confidence parameters
  - Optimizes threat forensics capture to contend future threats
  - Continually improves with experience

## Manage the integrity of your IoT solutions with IBM

Embark on your IoT Security strategy today. Learn more about IBM's simplified approach to IoT Security.



### Insights: Gain a deeper understanding of IoT security

- Learn from IBM IoT security experts and get the latest resources, news and insights to keep your IoT applications and services secure.

[Learn more about IBM IoT security](#)



### Watson IoT Platform Security Blog

- Secure your IoT solutions with IBM Watson IoT Platform
- Enhanced Security Controls for IBM Watson IoT Platform

[See the blog](#)



### The IBM point of view: IoT Security

- The connectivity of “things” presents an exciting environment for innovation and opportunity, but also a broad set of security challenges and threats.

[Read the paper](#)