



IoT Security Solutions are in Big Demand

On track to reach nearly \$300 billion in market value by 2033, the national IoT security market helps companies tackle existing and new threats against their interconnected devices.

As the burgeoning network of interconnected devices embedded with sensors, software and other technologies, the Internet of Things (IoT) is impacting everything from everyday household items to industrial machinery to medical devices. This interconnected world also presents unique security challenges, including the potential for data breaches, cyberattacks and physical security threats.

As IoT expands, the list of existing and potential threats against it is also growing. “Fortunately, the market for advanced IoT security is expanding, too, with numerous companies specializing in or at least providing tools to help keep businesses and individuals safe from increasingly sophisticated cybercrime,” online business startup community *Built In* explains.

“IoT security involves outfitting IoT devices with the latest tools in order to secure the transfer of data, prevent hacking and ensure that privacy standards are maintained,” it adds. “Ensuring IoT security both protects user personal information and saves costs associated with a breach, making the practice an important initiative.”

The Spotlight is on IoT Security

Customer privacy and data security are major focuses for organizations and governments right now. This increased focus on security is driving growth in the U.S. IoT security market, which is currently valued at around \$35 billion and on track to reach nearly \$300 billion by 2033, according to a [recent IMARC Group report](#).

Collectively, the IoT security market is posting a compound annual growth rate (CAGR) of 23.7%. “Increasing regulatory obligations are pushing the market to emphasize customer privacy and data security,” IMARC Group notes in its report. “Companies are investing in advanced security solutions and compliance methods to comply with severe rules, ensure strong protection for connected devices, and create confidence in IoT technology across sectors.”

The IoT security market is also benefitting from a host of new laws and security standards focused on enhancing safety and cyber resilience across a wide range of business sectors, including healthcare, manufacturing and transportation. In

response, organizations in those sectors are investing in more advanced security solutions and compliance measures.

According to *IoT Business News*, some of the new technologies being used to enhance IoT security include advanced encryption, biometric integration (e.g., fingerprints and retinal scanners) and zero trust architecture, whereby the devices themselves enforce end-to-end encryption for all transmitted data.

“Zero trust architecture will do this by requiring authentication at the point where it is sending data,” the publication explains, “and by not being allowed to talk to other IoT devices on the network unless explicitly required.”

Uncle Sam is Playing Catch-up

When the IoT Cybersecurity Improvement Act of 2020 went into effect, it included new guidance for securely procuring IoT. The law also required 23 civilian federal agencies to implement IoT cybersecurity requirements. It’s been five years since the act was signed into law, and several agencies have yet to complete their IoT inventories, according to *FedScoop*.

The publication says six agencies didn’t share their time frames for inventory completion, and the Small Business Administration doesn’t use any IoT technologies, which federal agencies are using for purposes like controlling access to devices/facilities and monitoring systems and equipment.

FedScoop says three of the 23 civilian agencies have completed their IoT inventories: the State and Treasury departments and the Nuclear Regulatory Commission. Ten agencies said they were on track to finish their inventory work by the end of fiscal year 2024, while another three plan to meet their inventory requirements by fiscal year 2025.