Internet of Things for Home Automation

Consumers are fascinated by the prospect of the connected home for the cost savings, convenience and safety but particularly because of the highly valuable savings in time. Autonomous vacuum cleaners, timed lights, smart thermostats, weather sensing sprinklers, and video doorbells are just some of the devices expected to drive $350 billion in economic value in 2025. Device OEMs will gather customer data to help improve their products, create valuable new services, and even predict home owner needs. Consumer adoption will increase as prices fall, but won’t face mass market adoption until privacy and data concerns are addressed. A smart home device provider that can prove they can protect the consumer will have a significant advantage over their competition.

IoT Demands Different Security

The technologies we have used to protect computers and networks for the past 20 years are not the right fit for the Internet of Things revolution. Connected IoT devices to the Cloud require a holistic security solution that is purpose-built to answer these unique needs. Traditional security solutions available today still use Internet technology that was designed for anonymous browser to server communications. Browsers exchange (in the clear) the minimum acceptable security protocols necessary to establish a connection. However, IoT devices today are specially designed and connected for specific intentions. Unknown devices can be rejected and security protocols can be agreed upon ahead of time. This type of IoT solution is fundamentally more secure and easier to control because the devices and the hosts are all known entities with closed methods of communicating. However, new innovations in IoT devices have created other challenges.

IoT Challenges for Home Automation Providers

- Weak authentication of smart home devices connected to the Cloud
- Consumer data exposure via devices, gateways, apps and the Cloud
- Low power devices run hot with less uptime using heavy load security
- Footprint limitations for security solution on “headless” devices

CENTRI IoTAS - Internet of Things Advanced Security

Unlike security solutions for the broad Internet, those designed for the Internet of Things can define exactly which devices can connect and how they will secure their data, before they begin communicating. By encrypting and compressing the data as it’s created, as it’s delivered, and even as it’s stored on servers, IoTAS provides the simplest yet the most comprehensive and secure solution for IoT projects.

IoTAS was designed to protect resource constrained IIoT devices and their data while in use on the device, in motion across the network or at rest in storage. IoTAS employs a trusted device model without vulnerable certificate exchanges so only known endpoints are connected. Usable data is protected from internal rogue employees and external hackers. Man-in-the-middle attacks cannot eavesdrop or transmit bad data. Denial of Service (DDoS) attacks launched from devices can never begin when the device only accepts verified commands protected by IoTAS.

Fast Facts

- By 2025 a 10% reduction of estimated property value damage is expected due to IoT devices
- 17% expected time savings due to home automation
- Analyzing IoT data will generate $5 billion in device upgrade opportunity per year
- Home appliance suppliers are expected to increase their margin by 7% with data driven upgrades
- Consumer energy management applications could have an economic impact of $50-$110 billion globally in 2025
- Energy-control application adoption could reach 25-50% in advanced economies by 2025
IoTAS for Home Automation: Secure home solution for providers and end customers

IoT Endpoint & Data Integrity:
- Device Authentication
- Secure Data at Rest
- Secure Data in Motion
- Data Optimization

IoT Cloud Protection:
- Secure Data at Rest
- Data Optimization

IoT Data Visibility:
- Analytics
- Forensics
- User Management
- Encrypted Search

IoTAS Deployment:
- Home automation device
- Mobile application
- Gateway appliance
- Cloud
- Databases and distributed servers

IoTAS Secures:
- Control of home automation devices
- Confidential customer data (PII)

Cloud: The approach of securing the data before it is transmitted, between trusted devices, eliminates the Cloud/network issues like man-in-the-middle attacks and mitigates DDoS attacks. Unlike traditional SSH, no information is passed in the clear – so no agent can sit in-between and pretend to speak the same language. In addition, DDoS attacks are reduced by a factor of 4 since the usual anonymous introduction between devices is eliminated. When the device and the data are secured with IoTAS, any potential network breach is made irrelevant.

Data: Bad actors can come from inside or outside an organization and your solution needs to take data security into account on the device, in transit, and once it gets to the servers in the Cloud. IoTAS uses advanced encryption to protect all data in transit between any endpoints and at rest. A disgruntled employee can take proprietary process information or hackers can use social engineering to login and download company data, but the data is unusable on any device that is not authorized. Applications on trusted devices (phones, servers, work stations) transparently access the information; any data downloaded to thumb drives or unauthorized devices cannot be decrypted and is worthless.

Device: The security of devices is critical not just for protecting consumer data but because hacked devices can cause physical security problems. The more that we automate the more vulnerable we become to hackers without the right security solution. IoTAS provides device integrity so that any connection from an untrusted device is immediately dropped. Malware delivered from untrusted connections is eliminated and only your trusted commands are allowed.

CENTRI IoTAS vs. Alternatives

Security solutions should be evaluated by the level of security they provide vs the impact to the overall project. The following two axes provide the best practices you should follow when evaluating any IoT security solution.

Axis 1: Security Quality

Cloud: The approach of securing the data before it is transmitted, between trusted devices, eliminates the Cloud/network issues like man-in-the-middle attacks and mitigates DDoS attacks. Unlike traditional SSH, no information is passed in the clear – so no agent can sit in-between and pretend to speak the same language. In addition, DDoS attacks are reduced by a factor of 4 since the usual anonymous introduction between devices is eliminated. When the device and the data are secured with IoTAS, any potential network breach is made irrelevant.

Data: Bad actors can come from inside or outside an organization and your solution needs to take data security into account on the device, in transit, and once it gets to the servers in the Cloud. IoTAS uses advanced encryption to protect all data in transit between any endpoints and at rest. A disgruntled employee can take proprietary process information or hackers can use social engineering to login and download company data, but the data is unusable on any device that is not authorized. Applications on trusted devices (phones, servers, work stations) transparently access the information; any data downloaded to thumb drives or unauthorized devices cannot be decrypted and is worthless.

Device: The security of devices is critical not just for protecting consumer data but because hacked devices can cause physical security problems. The more that we automate the more vulnerable we become to hackers without the right security solution. IoTAS provides device integrity so that any connection from an untrusted device is immediately dropped. Malware delivered from untrusted connections is eliminated and only your trusted commands are allowed.

+1 206.395.2793 | sales@centritechnology.com
**Peer to Peer:** Unlike most IoT security solutions, IoTAS does not require an Internet server to secure the communication. For example, a gateway at a home can monitor gardening sprinklers delivering water and if it detects an abnormality it can shutoff that device, all without an Internet connection.

**Axis 2: IoT Solution Impact**

- **Solution Footprint:** CENTRI has the smallest device footprint to accommodate a wide range of home automation equipment. Depending on the device and network requirements the CENTRI solution can be as little as 50kB.

- **Power Efficiency:** A small form-factor device is always limited by the power it consumes. A battery-operated handheld device that requires large amounts of processing power can run hot and limit battery life. IoTAS uses cache mapping technology and efficient algorithms for 20% less CPU utilization and up to 30% more uptime of IoT equipment.

- **Bandwidth and Cloud Storage:** Reducing bandwidth is important with cellular or satellite connected devices where IoT data transmission can be costly. IoTAS compresses the data up to 80% depending on the type of data, (e.g., text, audio, video) thereby speeding delivery and reducing the overall costs of adding bandwidth or Cloud storage.

- **Delivery Speed:** Many IoT environments feature thousands of devices sending large data sets. IoTAS is 100-150x more efficient establishing a handshake (i.e., device identification) required for communication than the standard SSH protocol (2-3 milliseconds vs 250-300 milliseconds).

- **Cost:** IoTAS offers less Total Cost of Ownership (TCO) for several reasons including 4-8x server efficiency, “vault-less” key management technology, and a developer-centric complete solution launching in days vs. months for DIY solutions.

**Summary**

CENTRI IoTAS – Internet of Things Advanced Security, offers home automation providers looking to secure their devices, gateways, data, and Cloud a complete solution that meets the unique requirements of low-power equipment and chipsets. IoTAS also solves the security challenge for consumers and companies as it protects IoT data in the Cloud in multi-tenant and shared environments. The solution uses cache mapping technology and efficient algorithms for lower CPU utilization, heat reduction and increased uptime of devices. When you make the security decision for your IoT project make certain your solution takes into account your needs today and into the future. Unlike DIY or repackaged enterprise solutions, CENTRI IoTAS delivers a security platform that is purpose-built for the trusted, known endpoints of IoT for the connected home.


**About CENTRI**

CENTRI provides a complete, advanced security solution for the Internet of Things. Our flexible, software-only platform enables thing makers and developers to quickly get to market with purpose-built IoT security to protect their data from chip to Cloud. CENTRI eliminates the risk of data theft and delivers device integrity with modern, standards-based technologies for the connected world. For more information visit centritechnology.com or email us at sales@centritechnology.com.

CENTRI and IoTAS are trademarks of CENTRI Technology Inc. in the U.S. All other product and company names herein may be trademarks of their respective owners.

[centritechnology.com](http://centritechnology.com)  /centritech  /centritechnology  /company/centri-technology

+1 206.395.2793  |  sales@centritechnology.com