CENTRI Internet of Things Advanced Security - IoTAS

Purpose-Built IoT Security from Chip to Cloud

CENTRI **Internet of Things Advanced Security – IoTAS**, is a complete, standards-based security solution designed to enable developers to quickly and easily implement device integrity, data encryption, data optimization and data insight into their products and services. IoTAS is a flexible, software-only platform embedded on endpoints, applications, gateways and the Cloud to secure and compress all data in motion and at rest to protect the privacy of you and your customers. IoTAS uses modern encryption, patented cache mapping technology and efficient algorithms resulting in superior security and device performance versus do-it-yourself projects.

Advantages of IoTAS

COMPLETE SOLUTION – IoTAS provides complete IoT security from devices to data. IoTAS establishes trusted device integrity, secures and optimizes IoT data in transit and at rest, and provides insights and intelligence to all activity with GUIs for user administration and forensics/analytics.

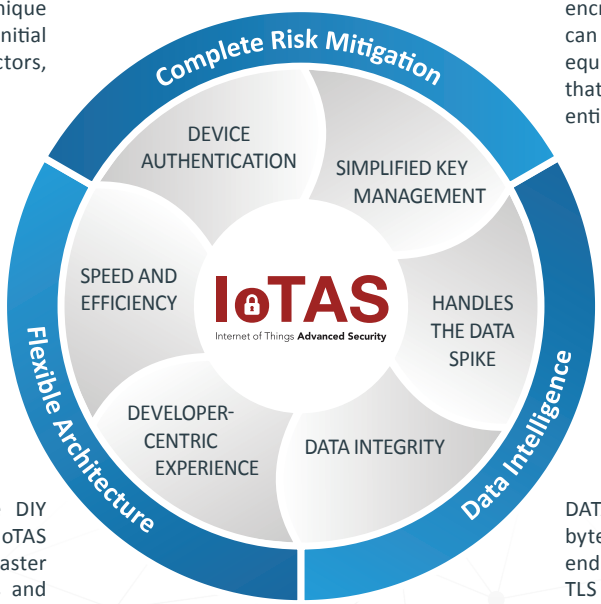
FLEXIBILITY – Many IoT endpoints from headless devices to large industrial equipment are severely limited with software space. With a 50kB footprint, IoTAS provides ultimate flexibility to fit on the smallest endpoints and platforms.

INTELLIGENCE AND INSIGHTS – Gain visibility of all data and device activity from forensics and anomalies with simple GUIs.

DEVICE AUTHENTICATION – IoTAS employs a trusted endpoint model for authentication without the need to exchange certificates. IoTAS uses existing machine-based ID to produce a unique CENTRI ID and establish root of trust upon initial connection that cannot be spoofed by bad actors, keeping your devices protected.

SPEED AND EFFICIENCY – IoTAS provides faster encryption and optimization, in a single pass of the data. Develop using 50% less calls resulting in twice the efficiency. IoTAS completes the connection handshake 50x faster than SSL/TLS. IoTAS preserves mission-critical uptme by using only 1% CPU power to provide up to 30% more uptime of battery-powered IoT equipment.

DEVELOPER-CENTRIC EXPERIENCE – Unlike DIY security tools such as SSL/TLS and SSH, IoTAS libraries and tools come pre-configured for faster integration to your endpoints, applications and Cloud. Reduce internal development time from months to days to implement expert IoT security into your products and services.



SIMPLIFIED KEY MANAGEMENT – IoTAS protects data at rest with patented "vault-less" technology to remove the risk and expense of managing your encryption keys. For comparison, other solutions can require Hardware Security Module (HSM) equipment that cannot scale or Cloud services that remove the control of your encryption keys entirely.

HANDLES THE DATA SPIKE – The increase in data traffic from IoT squeezes networks and Cloud storage. IoTAS compresses the data up to 80% to save bandwidth and Cloud storage costs. Other encryption solutions require additional compression tools that can negatively impact user experience.

DATA INTEGRITY – IoTAS never sends a single byte in the clear and works with a trusted endpoint-server model for data integrity. SSL/TLS was designed for the anonymous web – it does not protect against device attacks, leaves your application data open to Man-in-the-Middle attacks during the connection, and initiates a handshake partially in the clear exposing plaintext data hackers can intercept.

IoTAS Uses Widely Accepted Cryptographic Standards

Device Security	Key Exchange	Data Encryption	Message Authentication	Key Derivation Function
Hardware-based ID to guarantee IoT device authenticity	Elliptic Curve Diffie-Hellman Cryptography (ECDH) 25519 (Daniel Bernstein, 2005) used by Apple iOS	Salsa20 (Daniel Bernstein, 2005) symmetric key cipher certified by EU eStream in 2007	ChaCha20 (Daniel Bernstein, 2008) secret-key message authentication code used by Google Chrome	SHA-512 (FIPS 180-2 publication) cryptographic hash function designed by the National Security Agency

IoTAS Use Cases

Secure Things

Low power or battery-powered, mission-critical IoT devices connected to a Cloud or a mobile device via a gateway.

IoTAS provides complete encryption of data with endpoint authentication, no key vault and data compression.

Secure Central Command

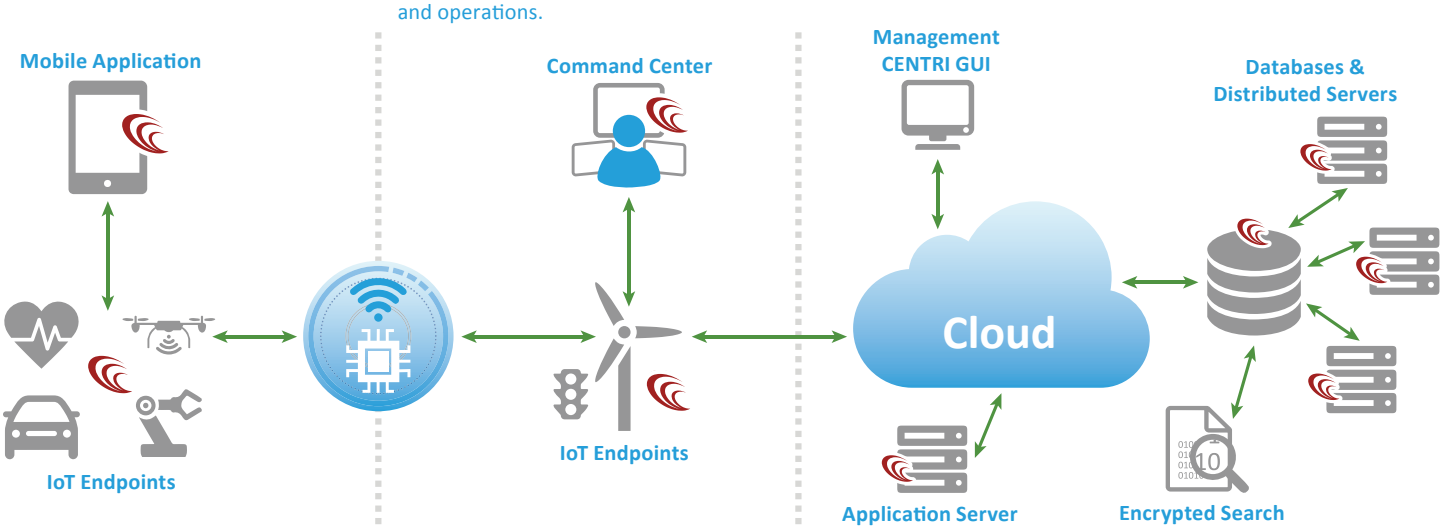
The control of unmanned edge devices and equipment from dams, power plants or military drones is highly sensitive and centralized.

IoTAS encrypts data in motion with endpoint authentication and low latency connections. Maintain control of device and operations.

Secure IoT Big Data

The combination of Big Data and the IoT to harness devices that collect data and the massive computing power to process and analyze all that data.

IoTAS secures data on and between devices and in the Cloud without disrupting the user experience, no key vault.



Technical Specifications

Specifications	IoT Endpoint	Cloud
Platforms Supported	Android, iOS, Linux, Windows	Linux, Windows and all major platforms, including AWS, Azure, Bluemix
Footprint	50kB based depending on platform and architecture	Less than 2MB depending on platform and architecture
Endpoint CPU Utilization	Between 0.05% – 0.3%	N/A

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.

IoTAS
Internet of Things **Advanced Security**

/centritech /centritechnology /company/centri-technology

www.centritechnology.com | +1 206.395.2793 | sales@centritechnology.com