

IoT SECURITY DEPLOYMENT PLATFORM



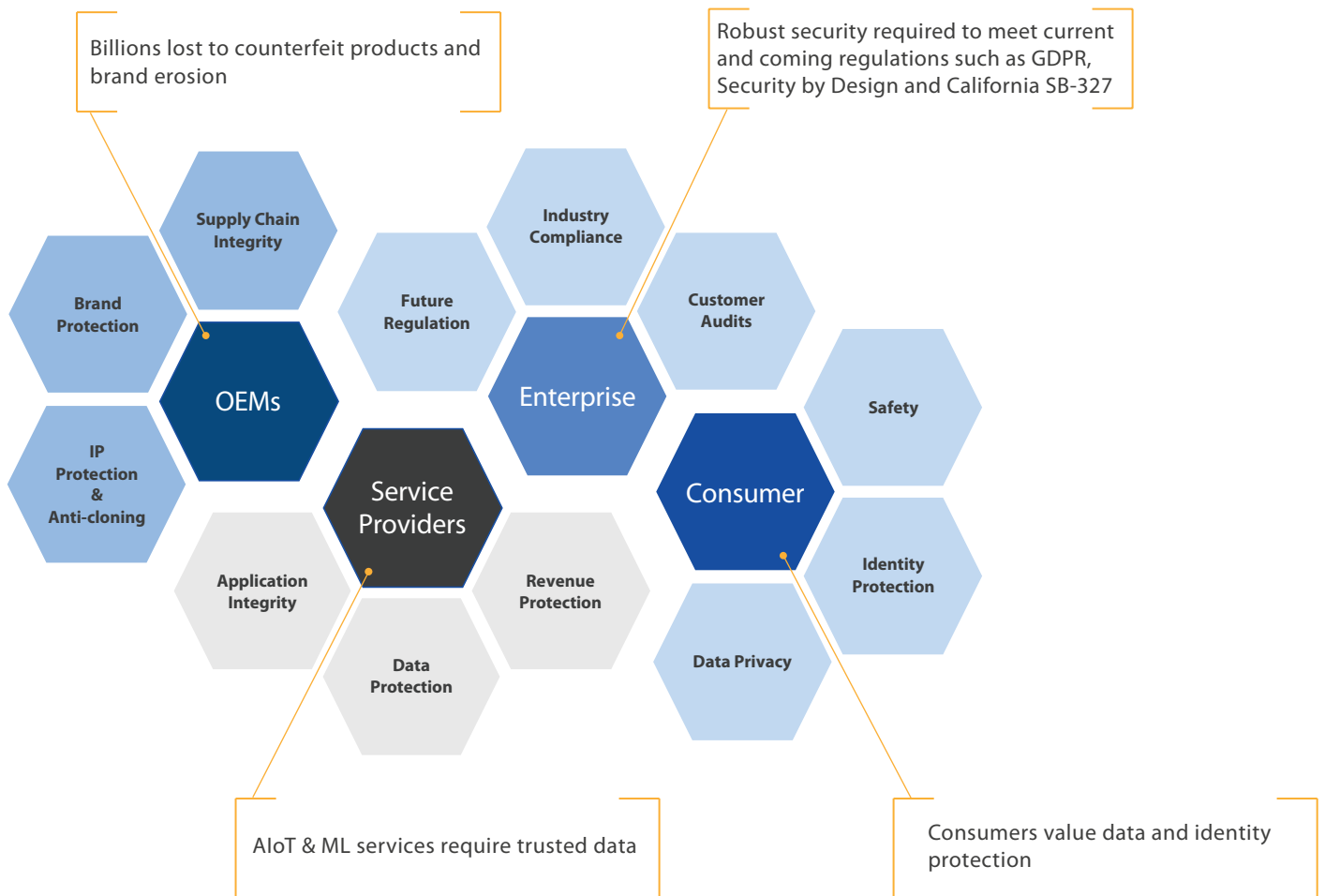
▶ SIMPLIFYING IoT SECURITY

Define, provision and deploy robust IoT device security using an efficient device programming system, easy-to-use tools and a flexible commercial model.

Your OEMs care about strong device security for IoT applications



Original Equipment Manufacturers (OEMs) require robust hardware and software security for IoT devices to protect their brand and meet regulatory, data privacy and safety requirements. The best design approach is to build hardware-based security into their products.



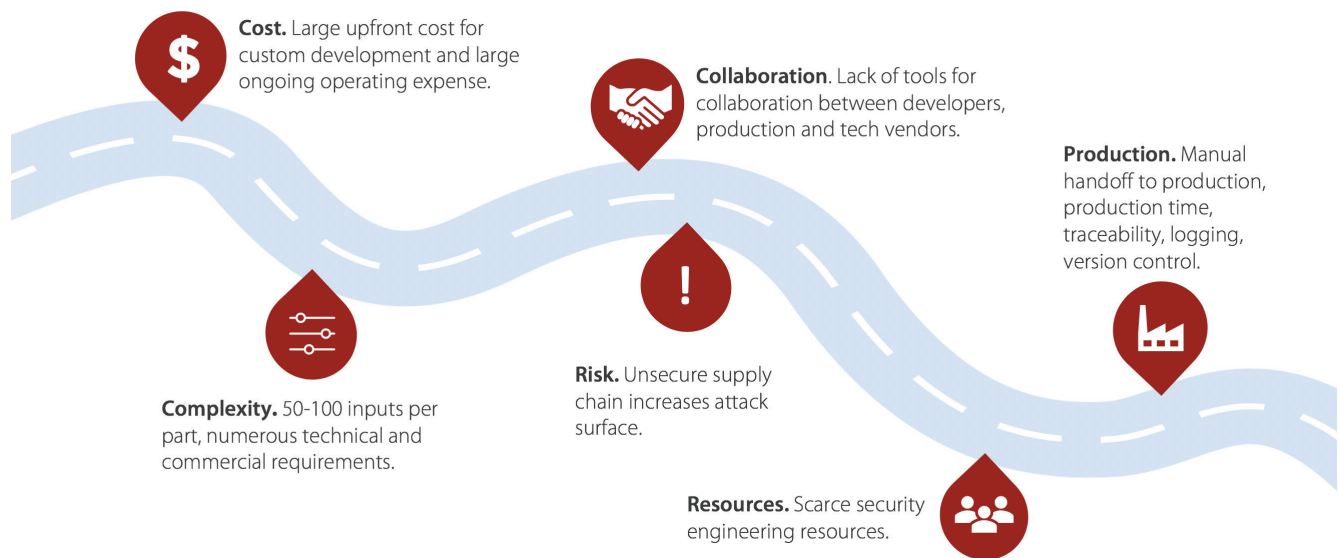


IoT Security Landscape

Address OEM security use cases with a flexible and automated security deployment system

Roadblocks OEMs and contract manufacturers (CMs) Face Deploying Hardware-based Security

Traditional hardware based security deployment options challenge OEMs and CMs to manage:





SentriX Security Deployment Platform Benefits

The SentriX® security deployment service offers a cost-effective and flexible security provisioning process resulting in additional revenue generating services that can be offered to OEMs.



Ease of Use

- Intuitive software tools for design to production collaboration
- Software tools are white label and can be branded
- Pre-configured security use cases



Commercial Flexibility

- Available as a turnkey security deployment system
- Available as an upgrade to a Data I/O PSV7000 or PSV5000 programming system



Scalability

- Use for low-volume prototyping or high-volume production
- Integrated with Data I/O automated high-volume programmers



Ecosystem

- Largest ecosystem of silicon partners for security deployment
- Leverage large and growing catalog of supported devices



Device Security Expertise

- SentriX software abstracts the complexities of modern silicon security programming models, saving your specialized development teams valuable time
- Data I/O customer engineers are leading experts in the usage and deployment of silicon device security and are available to assist your security product definition

Remove the Roadblocks to Success: Simplifying IoT Security

SentriX Technical Highlights

The SentriX security deployment process eliminates roadblocks to building secure products for your OEMs.



High-security Deployment

- Integrated FIPS 140-2 compliant hardware security module (HSM)
- Uses public key infrastructure (PKI) and offers certificate authority (CA) choice
- Secure provisioning up to 1,000 parts per hour
- Pre-manufacturing assembly security deployment
- Authenticates parts as original silicon
- Cryptographic protection of secrets and firmware
- Supports silicon hardware Roots of Trust
- Supports internal or external signing key generation
- Works with encrypted firmware
- Programs firmware and data in addition to security deployment
- Air gapped and works offline





Integrated security definition and programming job management software tools bridges the gap between design and production. Securely provision devices in manufacturing during a pre-board placement process with SentiX. Post-production reports and certificates provide complete traceability.

- Security and programming job management software
- Import keys, certificates and data needed for OEM use cases
- Securely wrap OEM secrets and keys to production equipment hardware security module (HSM)
- Intuitive tools for OEMs and production facilities
- Complete traceability solution
- High capacity and small parts handling

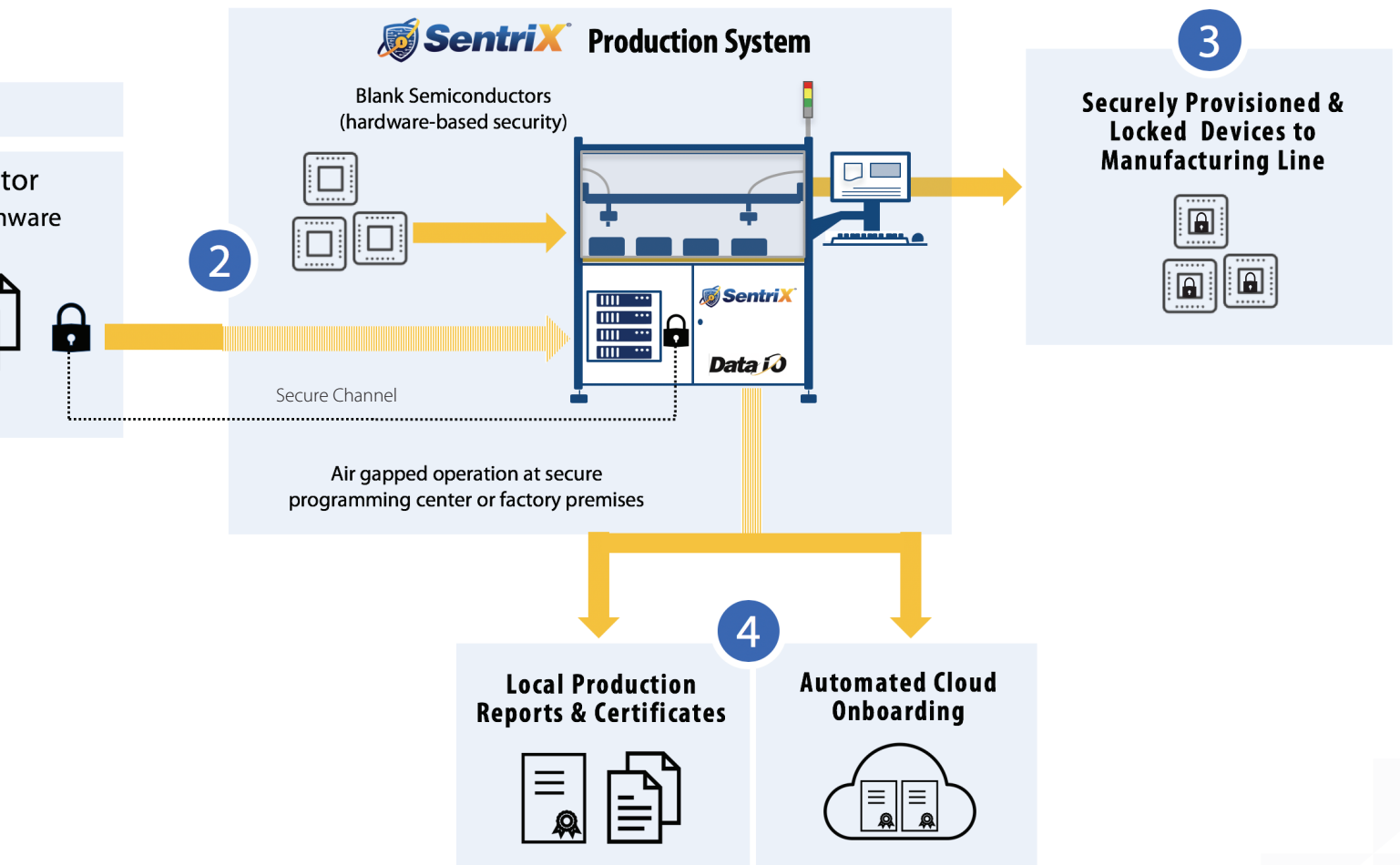
OEM Development

SentiX Product Creation
Protected credentials & firm

1

 10110
01010 

Simplifying IoT Security: How It Works





In collaboration with the leading global semiconductor vendors, Data I/O supports two security deployment models: 1) pre-configured use cases and 2) custom. Pre-configured use cases support the most common security definitions out-of-the-box and is the easiest to use. Custom enables complete flexibility for OEM use cases. In both approaches, the security job configuration is designed to require minimal input and silicon security expertise from the OEM.



SentiX Go™

- Easy-to-use
- Supports most common use cases
- Moderate flexibility
- Suitable for high or low volume

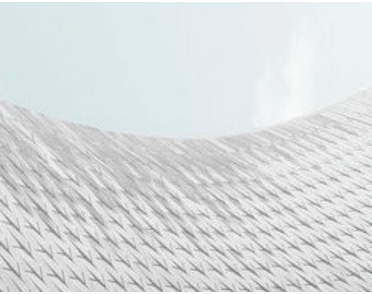
1. Silicon ID (read)
2. Chip Authenticity
3. OEM Device Identity
4. Cloud Onboarding
5. OEM Device Authentication
6. IP Protection
7. Secure Boot
8. Access Control
9. Secure Communications
10. Firmware Update



Custom

- Powerful collaboration tool
- Supports complex provisioning
- High flexibility
- Suitable for high volume

A custom security flow supports complex security requirements enabling you to take full advantage of the security features in a security IC or microcontroller.



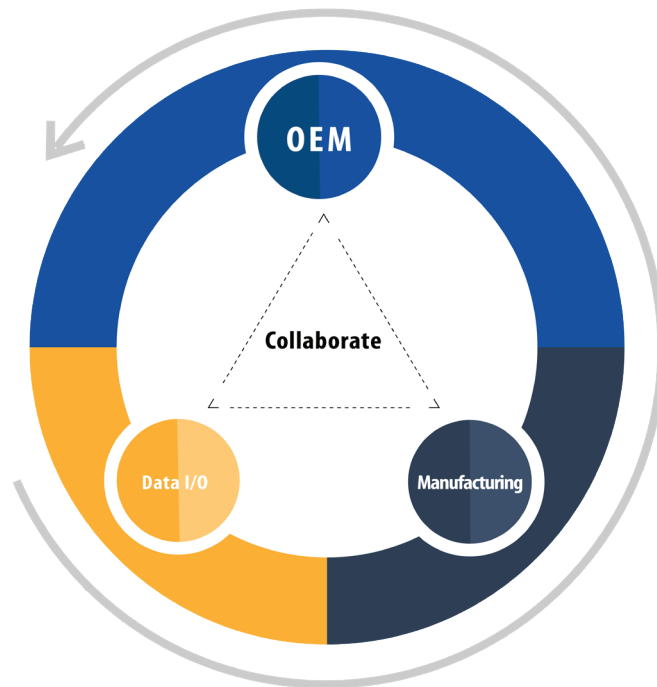
Flexible Security Deployment Models

SentriX Product Creator™ – A Powerful Collaboration Tool

Streamline your security development and collaborate with your manufacturing teams and Data I/O partners.

- Imports keys and certificates needed for selected use cases
- Enables OEM security profile definition for production
- Protects OEM secrets by wrapping them to the production equipment HSM

Collaborate directly with your manufacturing teams and/or with Data I/O on pre-configured use cases or a custom security flow with the SentriX Product Creator software application.





Industry Partners

Data I/O collaborates with leading companies throughout the electronics design and manufacturing supply chain to enable the SentriX Security Deployment Platform.

Sentrix Deployment



Silicon Partners



Technology Partners



What We Do

Our security deployment platform and silicon device programming equipment deliver the most secure and efficient system to deploy firmware, data and secrets into IoT and automotive devices in high volume electronics manufacturing.



Founded
in 1972

Over 50 years
of experience



NASDAQ:
DAIO

Public company
with audited &
published financials



ISO9001:2015
Certifications

Redmond, WA &
Shanghai, China



Global Service
& Support

Over 60 service
& support engineers
worldwide



Automated Programming
Systems Globally

>400 automated
programming systems
deployed globally

About Data I/O

Applications Secured with SentiX Security Deployment Platform



Automotive & Transportation

Automotive and logistics technology OEM uses a secure root of trust and identity to protect user data and maintain privacy.



Consumer & Home Automation

Smart locks, connected white goods and other consumer devices protect OEM IP and meet customer usage requirements by using low power hardware security-based microcontrollers.



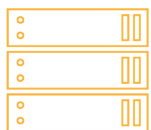
Industrial & Smart City

Smart meter and connected industrial controls OEMs are mandated by government regulations to support strong security to protect data and systems.



Medical

Medical device OEMs require strong IC authentication at the hardware level to support highest product quality and prevent counterfeit components.



Data Center

Data center servers and backplane controllers use security ICs and secure microcontrollers to ensure only signed code is executed, ensure supply chain integrity and to protect data from unauthorized access.



▶ **SIMPLIFYING IOT SECURITY**



Data I/O Corporation
6645 185th Avenue NE
Suite 100
Redmond, WA 98052 USA

Telephone: +1 425-881-6444
Toll Free in USA: 800-426-1045
FAX: +1 425-867-6972

Europe
Data I/O GmbH
Gräfelng, Germany
Website: www.dataio.de
Email: salesgmbh@data-io.de

Asia
Data I/O Electronics (Shanghai) Co. Ltd
Shanghai, China, PRC
Website: www.dataio.cn
Email: ChinaSales@dataio.cn