ENABLING HARDWARE SECURITY FOR THE INTERNET OF THINGS

SAFE HARBOR

NASDAQ: DAIO

The matters that we discuss today will include forward-looking statements that involve risks factors that could cause Data I/O Corporation's results to differ materially from management's current expectations. We encourage you to review the Safe Harbor statement contained in the earnings release as well as our most recent SEC filings for a complete description. Additionally, those forward-looking statements are made as of today, and we take no obligation to update them.

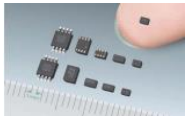
WHO WE ARE

"Data I/O enables the secure digital world by designing, manufacturing, and selling programming systems to global electronic device manufacturers."

Supporting the Secure Digital World

Data I/O's programming systems are used by the world's leading manufacturers, programming centers, and contract manufacturers, to securely program integrated circuits and bring their devices to life.

Circuits Need To Be Programmed



Options for Programming (DAIO customers)

OEMs

Contract Manufacturers

Programming Centers

Data I/O On-Line or Off-Line Programming

Final Assembly

End User

ATTACKS INCREASING

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

Stuxnet-style attack on US smart grid could cost government $1

A new report into the insurance implications of a wide-scale cyber-attack on the US energy sector reveals just how costly the breach would be for government and insurers.

The Lloyds 'Business Blackout' report was co-authored by the insurer and the University of Cambridge Centre for Risk Studies, whilst also seeking the advice of the Cabinet Office, the Department of Homeland Security and security firms including IOActive and Context, among many others.

Stuxnet-style attack on US smart grid could cost government $1 trillion

The report sets out a scenario where a group of hackers, using the Erebos Trojan, seek to infect and take offline electricity generation control rooms to introduce an electricity black-out across 15 states including New York and Washington.

Researchers said that the attack, 'improbable' but 'technologically possible', would likely result in huge government and insurance pay-outs, as well as a rise in mortality rates, a decline in trade (as ports shut down), a disruption to water supplies (as electric pumps fail), and general chaos on transport networks.

German Steel Mill Meltdown: Rising Stakes in the Internet of Things

'Smart' home devices used as weapons in website attack

3 hours ago | Technology

Share

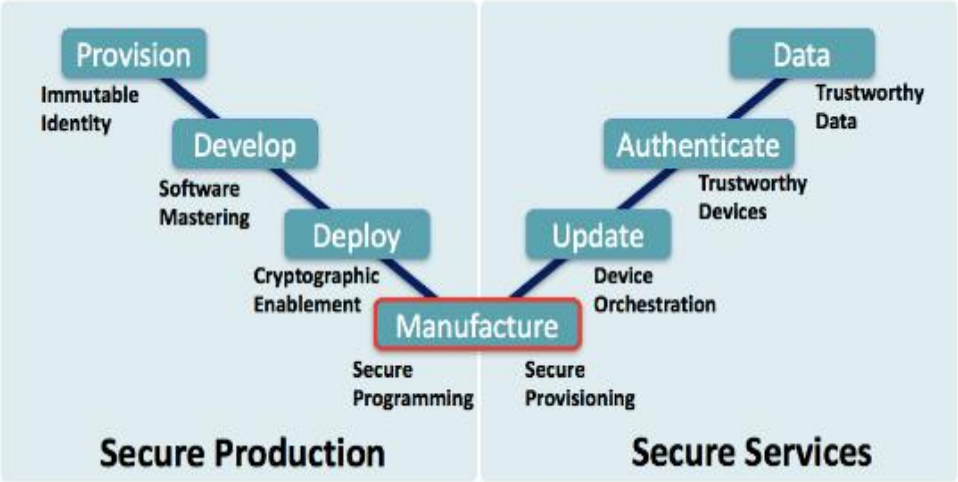
Challenges and Opportunities

- **Secure Manufacturing:** Delivering a Secure Supply Chain
  - IP Protection
  - Anti Cloning
  - Overbuilding Protection
- **Security Provisioning:** Maintaining Device Identity and Firmware Integrity throughout the lifecycle of the product
  - Secure Identities
  - Secure Boot
  - FW Encryption
  - Secure Provisioning
  - Secure Updates

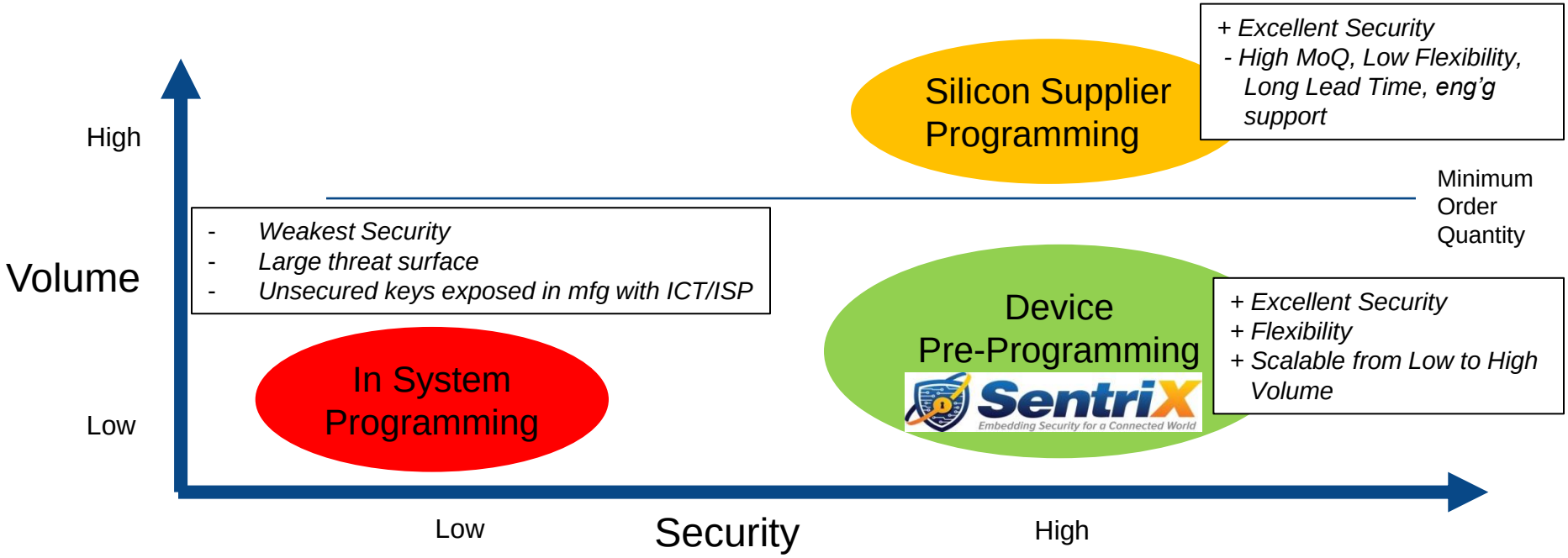
Both Secure Manufacturing and Firmware Integrity are Delivered Through Managed and Secure Programming at Device Manufacture

Secure Production at the Center of the Secure IoT

- **Secure Production** is the foundation for IoT value-added services by establishing “Root of Trust” at device creation
- **Data I/O’s *leading position* as the global device programming leader** makes us uniquely qualified to deliver security at device ‘birth’



Security Provisioning Approaches



Device pre-programming offers a cost-effective, trusted and integrated method for secure provisioning at any volume

A cost-effective security provisioning and data programming system to:

- *Embed security for trusted devices during pre-programming process*
- *Enable a secure supply chain for OEM's of any size and volume*
- *Deliver secure framework to maintain firmware integrity throughout product lifecycle*

SECURE PROVISIONING

Secure OEM Premise or
Secure Programming Center Premise

OEM

Data I/O OEM Tool

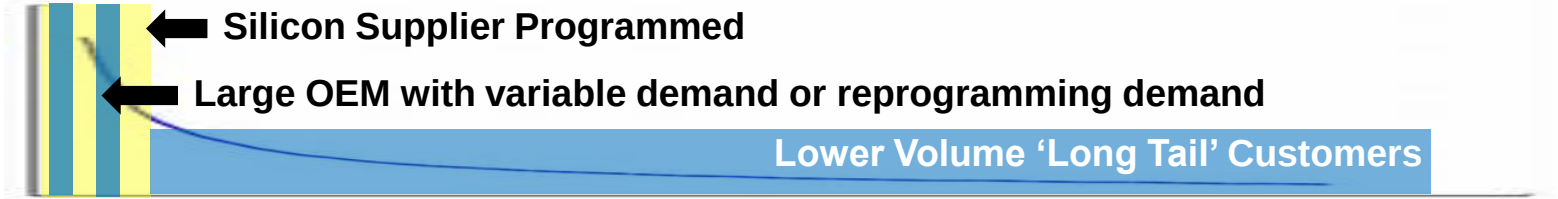
Blank Inventory from Semi Supplier or Distributor

Physical security and controlled access

Provisioned Devices

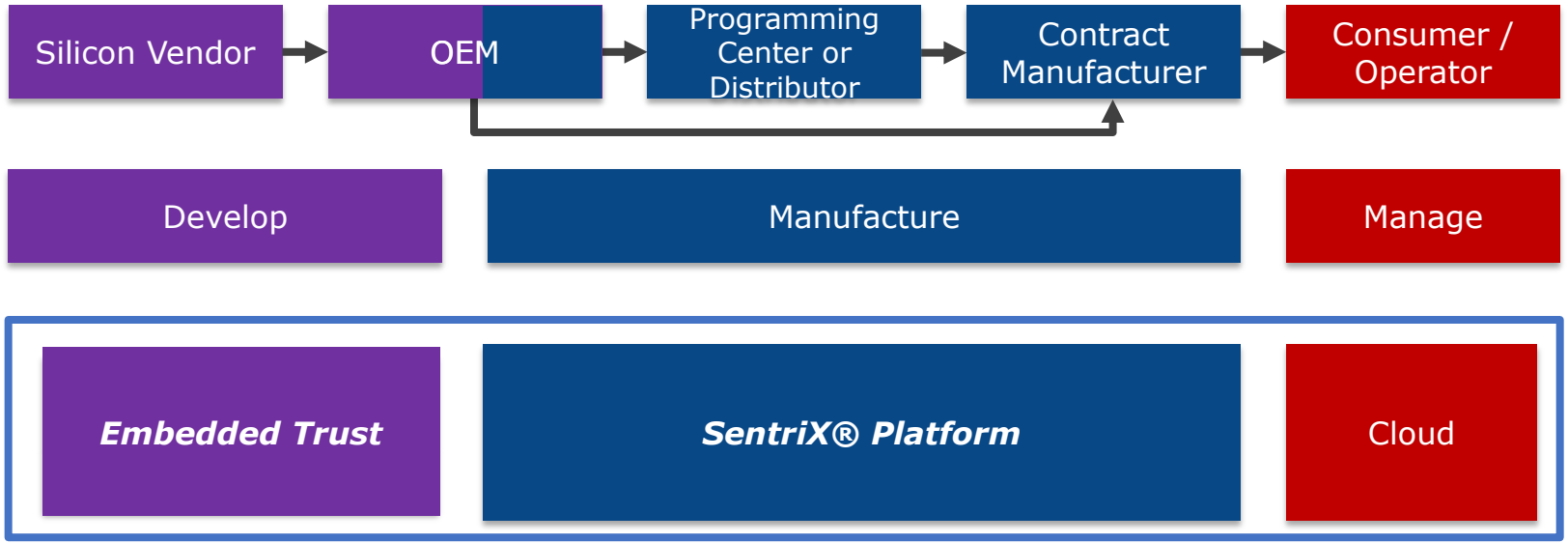
Business Potential

- Long Tail distribution of customers is typical for Silicon Vendors in IoT
- Very high volume customers can be mostly provisioned by the Silicon supplier directly if their demand is predictable



- Smaller customers and rapid requests often do not fit well within the direct Silicon supplier programming flow. Logistics partners and their associated programming centers support this market.
- Some Large OEMS will also be 'reprogramming' devices
- Data I/O and our Programming Center Partners provide a secure, cost effective solution for:
  - Orders below factory MoQ
  - Rapid orders
  - Secondary programming and reprogramming, including large OEMs and their ecosystems

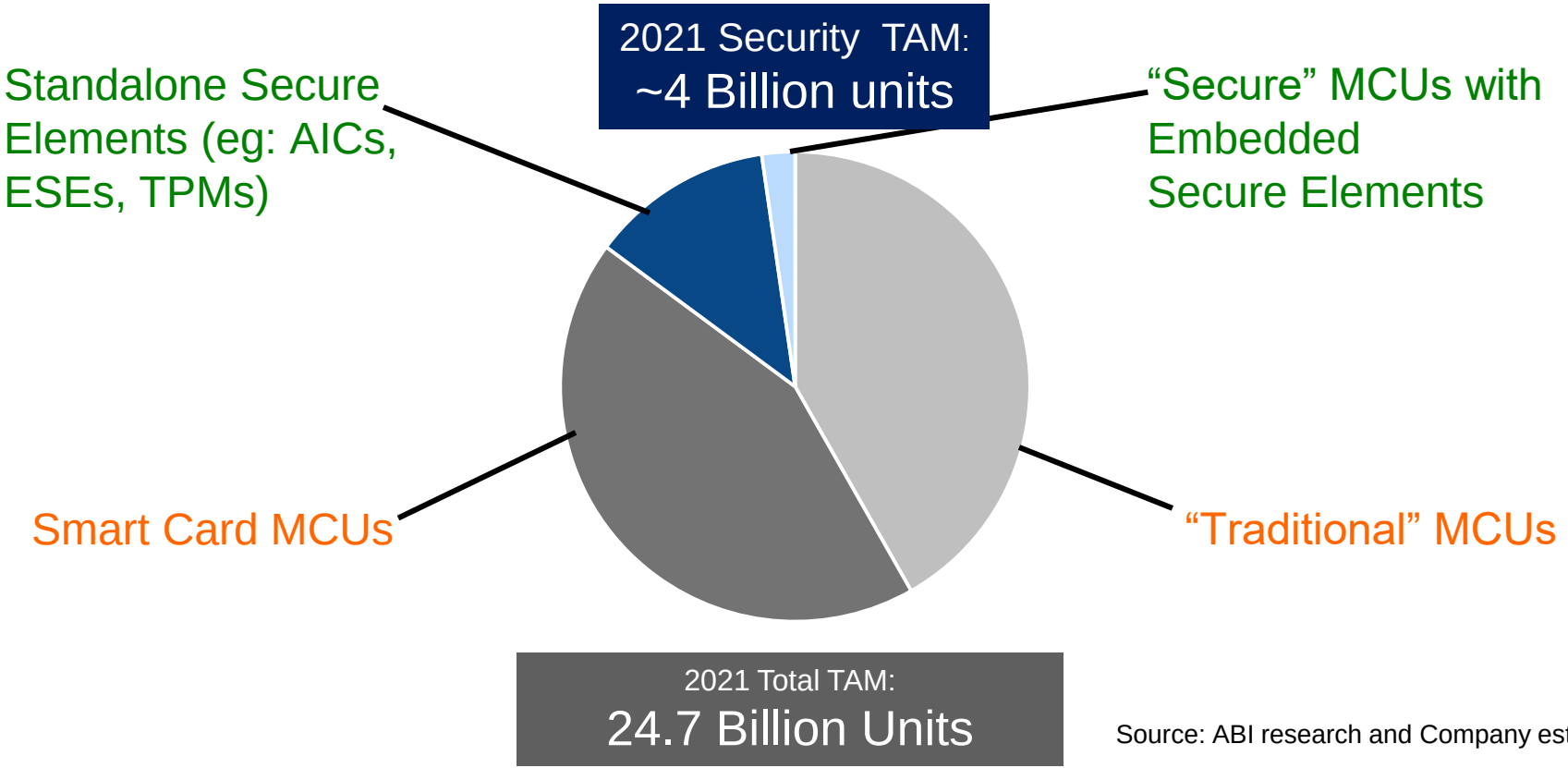
Solutions to Secure IoT Supply Chain



Security Partnerships

SECURE CONNECTIONS FOR A SMARTER WORLD

Our Opportunity – 4 Billion Secure Units in 2021



Source: ABI research and Company estimates

SUMMARY

- **IoT Device security** is being driven by escalating attacks on the Internet of Things devices
- **Secure Elements or Secure MicroControllers** are the best solutions for IoT device security
- **The best way to provision** these devices in moderate volume is at the chip level in a secure programming environment
- **Data I/O SentriX® platform is an ideal solution** for this upcoming wave of security provisioning demand
- **The SentriX platform delivers very high ROIC** to Programming Centers, OEM customers, and Silicon Suppliers
- **Data I/O is actively recruiting** ecosystem partners to help make this solution readily available

DISCUSSION

SentriX™ Platform Go To Market

- **The security programming market** is in its early phase.
- **Data I/O is developing a standard platform** and partnering with leading programming centers and global Silicon Suppliers to evangelize the market and create demand with early adopter customers
- **Data I/O and our partners enable all customers**, not just the highest volume customers.
- **Solutions are available now**, with expanding device support over time.

Device Support Roadmap

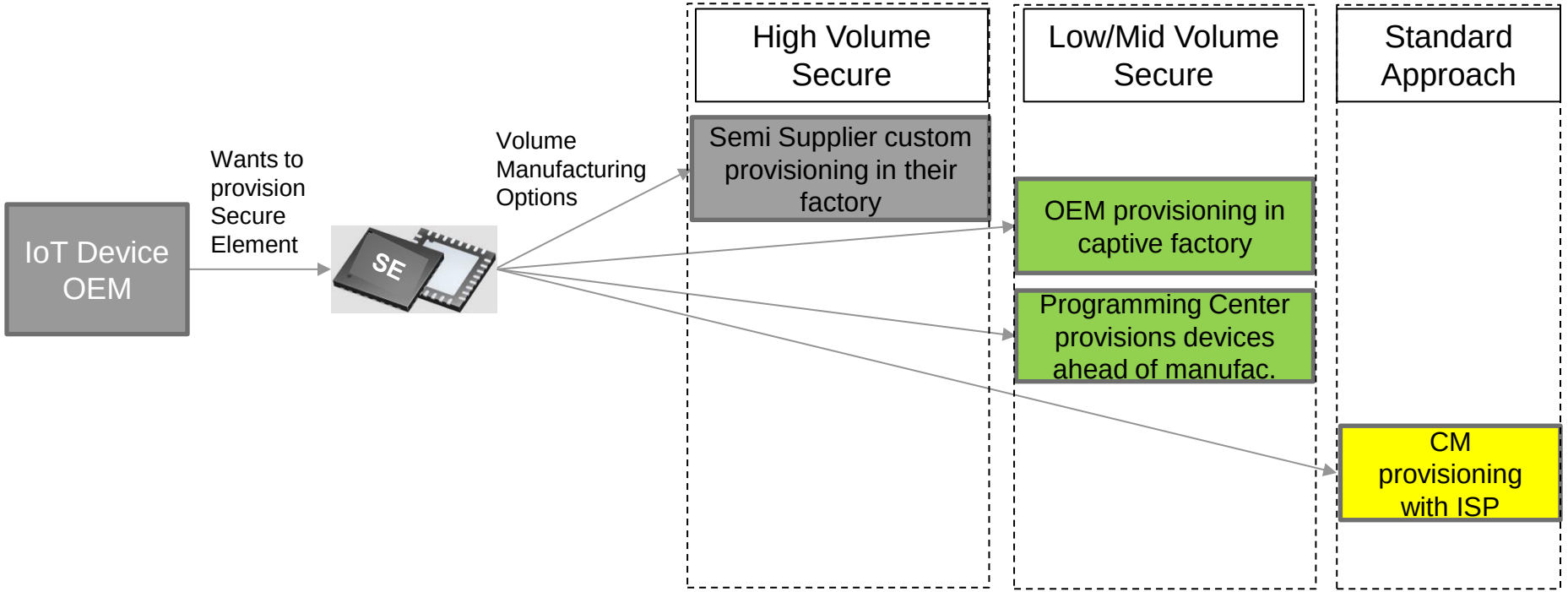
- **Secure Elements Completed:**
  - IFX: Optiga Trust E, Optiga Trust X
  - Maxim DeepCover DS28C36
  - Maxim DeepCover DS2576
  - NXP A70, A71
- **Secure MCUs Committed on Roadmap**
  - Renesas Synergy S5D9
  - Cypress PSoC 6

Plus More to Come

SentriX™ Programming System

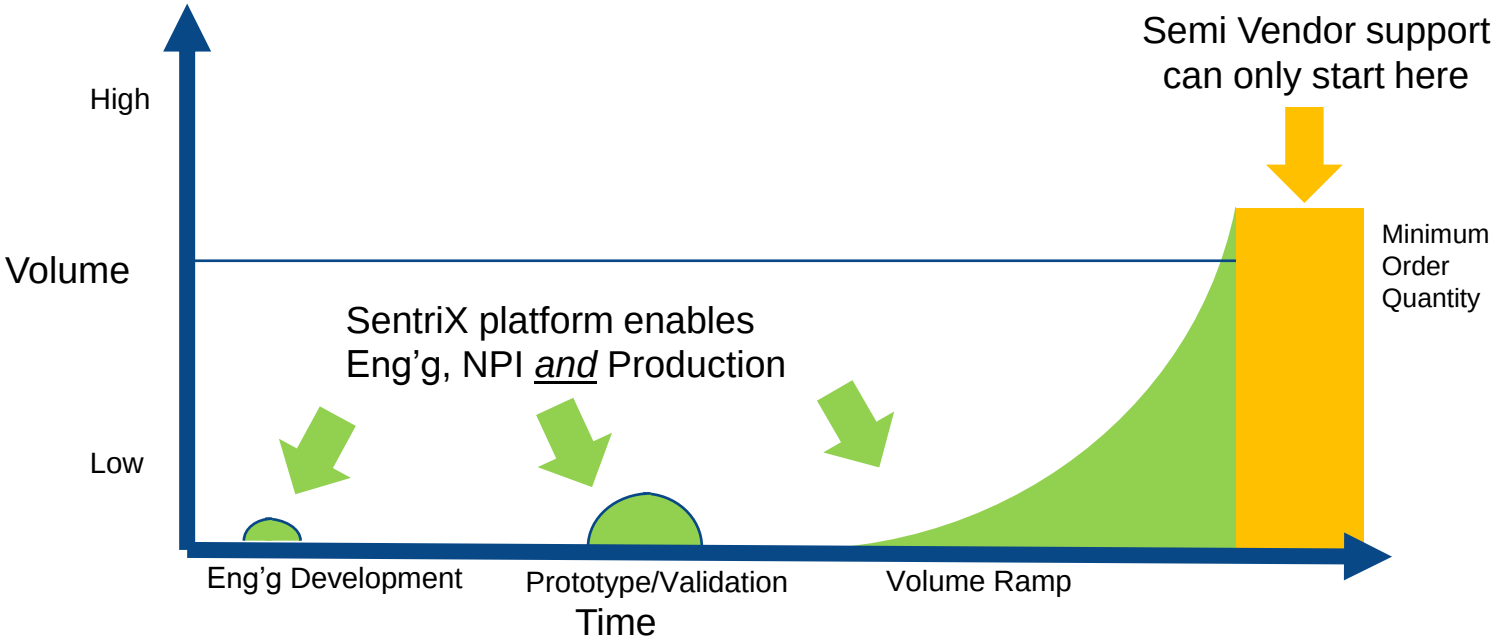
Production Availability: Now

Limited Options for Secure Element Provisioning



- **We are co-travelers with the semi suppliers and programming centers**

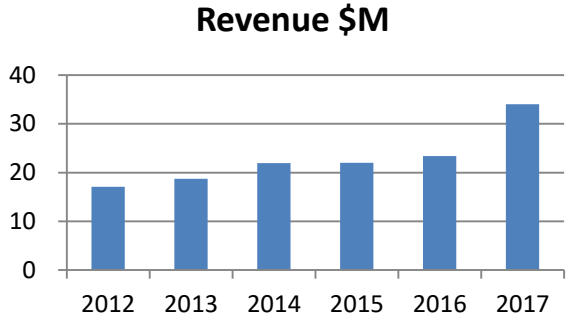
SentriX™ Supports the Full Product Lifecycle



SentriX Platform enables security programming through the engineering and prototype phases of development as well as the volume ramp

Servicing Customers Globally in Growing Markets

- Data I/O (NASDAQ:DAIO) is the global leader in device programming
- Global footprint with headquarters in Redmond, Washington and offices located in Shanghai, China and Munich, Germany
- 45% growth in Automotive electronics orders in 2017 with eight of the top nine automotive electronics companies buying from Data I/O



Sample Customers

Automotive

Panasonic, ALPINE, DENSO, Continental, BOSCH, HARMAN/BECKER AUTOMOTIVE SYSTEMS, DELPHI, Visteon, FUJITSU TEN, KOSTAL

Wireless

LG, TCL, HUAWEI

IoT/ Industrial/Consumer

amazon.com, Microsoft, Google, Honeywell, Schneider Electric, TOSHIBA, INSTA, WATLOW, hp, Danfoss, Schindler, SIEMENS, Miele

Programming Centers and EMS

JABIL, PLEXUS, PEGATRON, AVNET, FLEXTRONICS, btv technologies, eps, FOXCONN, wistron