Secure MCUs For the IoT

Insights into Digital Security Technologies

ABIresearch
for visionaries

Industry Demand

What stakeholders want:

- Secure connectivity for general purpose, low-power, mass-market devices to enable remote management and monitoring
- SMCU-based offerings that can integrate easily with existing IoT services and cloud platforms
- Appropriate hardware and associated software to allow for identification, authentication, integrity & confidentiality
- Secure programming, provisioning, onboarding & lifecycle management
- An emerging market of secure MCUs packaged with software development platforms

What vendors are offering:

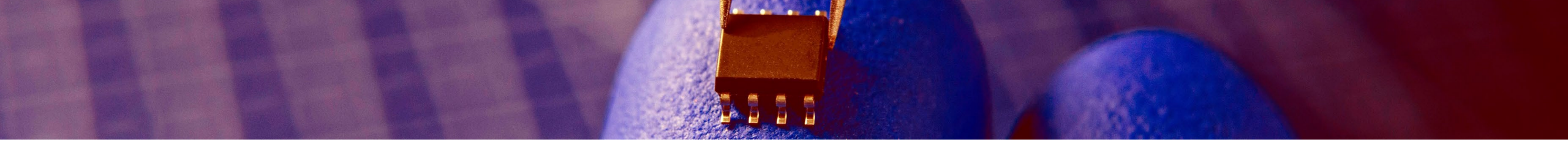
- New class of general purpose secure MCUs for the IoT (emerging in 2017)
- Primarily based on Arm Cortex M4 cores (M0 - M7 variations as well, especially for dual core offerings) & Arm V7M architecture
- Newer offerings out this year based on Arm Cortex M23 & M33 and Arm V8M with TrustZone TEE (M35P with tamper resistance built-in)

Competitive Offerings:

Vendor Ecosystem

MEDIATEK	life.augmented	REDPINE SIGNALS®
maxim integrated™	MICROCHIP	CYPRESS® EMBEDDED IN TOMORROW™
nuvoTon	NXP	RENESAS

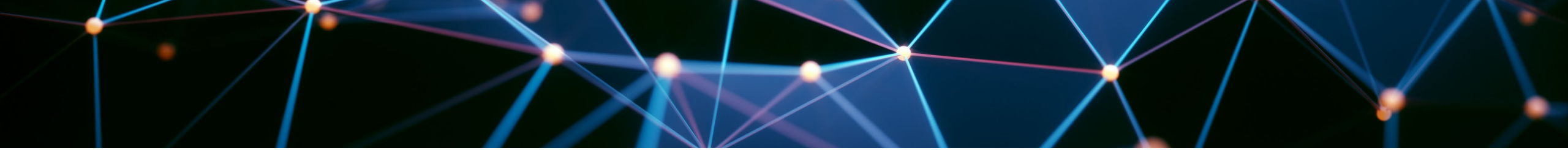
Note other application-specific MCUs include Infineon Aurix (automotive), Goodix GM6256 (fingerprint), TI Simplelink (Wi-Fi)



Technology Highlight:
Hardware

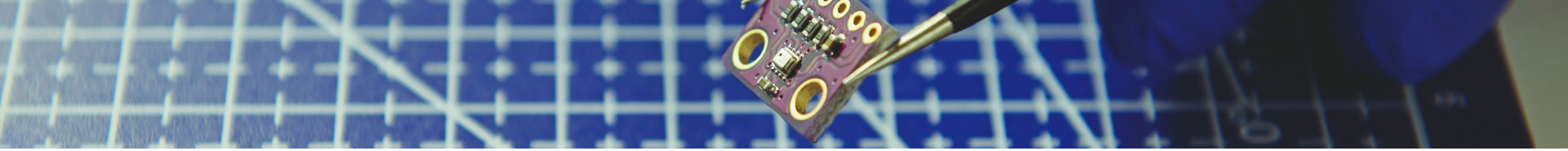
SECURITY PROCESSOR	ROOT OF TRUST	SECURE EXECUTION ENVIRONMENT	CRYPTOGRAPHY
• Security Subsystem • Internal Crypto Engines • Co-processor (dual core)	• Secure Boot • Unique ID (128-bit) • PUF	• Arm Trusted Firmware-M • Trustonic Kinibi-M • Microsoft Pluton Security Subsystem (Azure Sphere) • TrustZone TEE • Hardware Firewalls	• Symmetric (AES, DES/3DES) • Asymmetric (ECC, RSA, DSA) • Hash Functions (SHA) • TRNG, PRNG

SECURE MEMORY	TAMPER RESISTANCE	CERTIFICATION
• Secure key / certificate storage • Flash readout protection • Memory Protection Unit • Hardware Firewalls • Peripheral Protection • OTP Flash, e-fuse block	• Time-stamped • Anti-tamper pins • Voltage, clock, temp, optical, glitch detection • CRC, ECC, Parity, Watchdog • Zeroizable memories	• Arm Platform Security Architecture (PSA) • NIST FIPS 140-2 • NIST Cryptographic Algorithm Validation Program (CAVP)

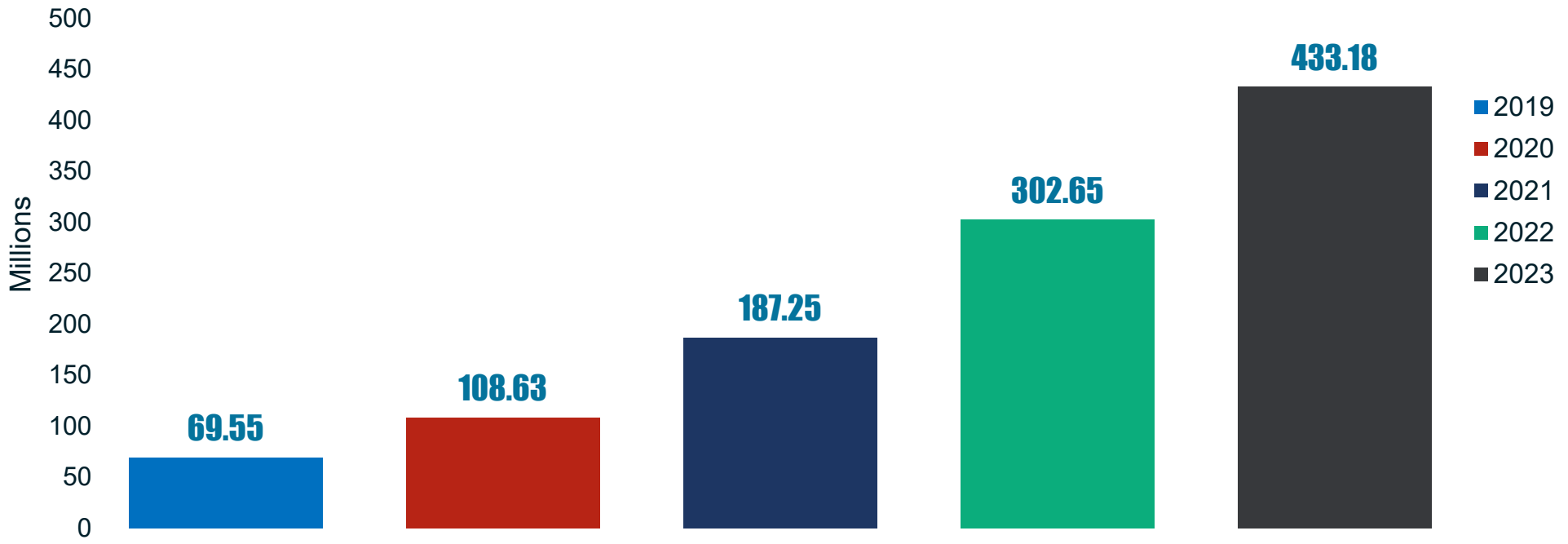


Technology Highlight:
Software and Services

SOFTWARE DEVELOPMENT	INTEROPERABILITY WITH 3RD PARTIES	ONBOARDING & PROVISIONING	LIFECYCLE MANAGEMENT
• Proprietary: MCUXpresso, PSoC Creator, X-Cube, NuSMP, Synergy SP	• Software, network, communications, key management	• Cloud Enrollment (Azure, AWS, Google) • 0-touch Provisioning • Remote Attestation • Certificate-based Authentication	• Secure FOTA updates • Security Monitoring • Security Analytics • Troubleshooting, Failure Reporting, etc.
• 3rd party: Eclipse, Visual Studio, Azure Sphere APIs & SDK, Arm Keil MDK, IAR Embedded Workbench, Modbus Toolbox, PSA APIs, Zerynth, Percepio, trustonic SDK, IDE Atmel Studio, Segger Mebedded Studio	• Arm Mbed OS & TLS • WolfSSL • Segger emCrypt • Pluton Key Management • Amazon FreeRTOS • AWS and Google Cloud IoT Core (both use x.509	• Arm Pelion • Azure Sphere Security Service • Trustonic end-to-end solution support • Data I/O SentriX secure provisioning platform • SecureThingz Key Provisioning	• Arm Pelion • Azure Sphere Security Service • Secure Thingz Secure Deploy Architecture • Arm Trusted Firmware-M



Global Shipments of Secure MCUs



- Shipments start around 2018 (sub 50 million), 2019-2023 CAGR 58%
- 2019-2020 slight pressure on growth from current manufacturing recession & uncertain political climate (i.e. US trade/tariff pressure on China & EU), & newness of technology
- Uptick from 2021 onwards with maturing market demand, movement from early adopters to mass market, additional security features, lowering ASPs (esp. for M4 cores) & increased competition

Target Markets and Applications

Smart Cities & Buildings

Commercial Building Automation, Smart Parking, Smart Street Lighting, Environmental Monitoring, Video Surveillance, Enterprise Access Points

Utilities & Industrial IoT

Agriculture, Industrial Equipment, Hospital and Other Healthcare Equipment, Electricity Metering, Water and Gas Metering, Smart Grid Equipment, Renewable Energy, Aerospace, Defense

Smart Home

Home Automation Controllers, Smart Home Devices, Smart Appliances, Smart Home Lighting Units

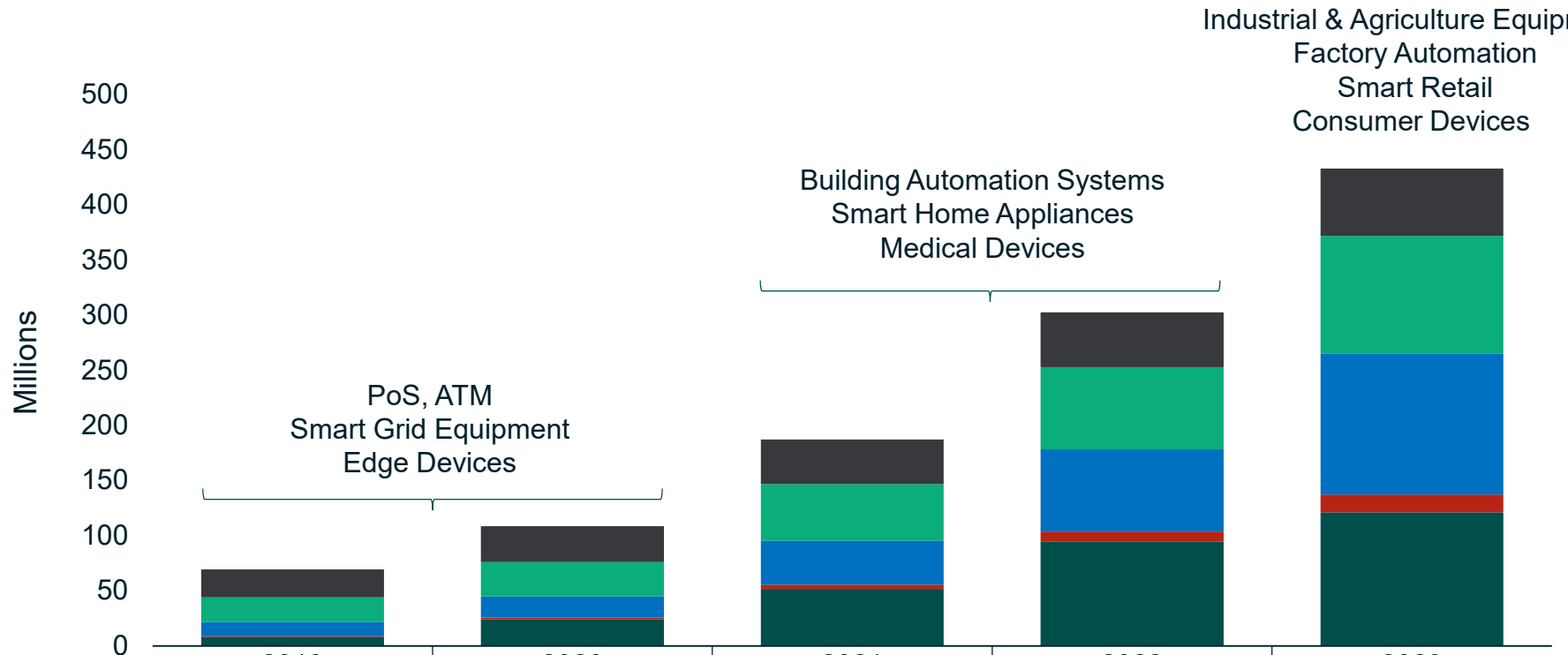
Wearables

Health and Medical, Sports, Fitness, and Wellness Devices, Smartwatches, Smart Glasses

Other

POS, ATMs, Kiosks, Vending Machines, Digital Signage, Asset Tracking, Inventory Management, Beacons, Robotics

Shipment Forecast of Secure NCUs by Sector



	2019	2020	2021	2022	2023
Other	25.41	32.60	40.42	49.75	61.02
Utilities and Industrial IoT	22.36	30.99	51.33	74.63	107.17
Smart Cities and Buildings	13.08	19.29	39.97	74.63	127.72
Wearable	0.88	1.48	3.70	8.89	15.99
Smart Home	7.82	24.27	51.82	94.76	121.29

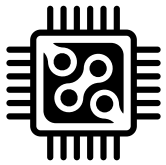
Market Outlook

Adoption

Success will depend on cost & usability of hardware & development platforms but especially on the service/cloud connectivity piece.

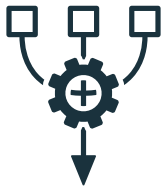
Competition

Emerging cross-over between microcontrollers and application processors will increase competition, pushing dual core offerings, such as NXP iMX, Samsung Exynos i (T200, T100, S111), leveraging Arm Cortex A & M (for dual core).



Technology

New Cortex M33 for next generation of Secure MCUs to facilitate TrustZone use, but additional tamper resistance to be served by the Cortex M-35P in the following generation.



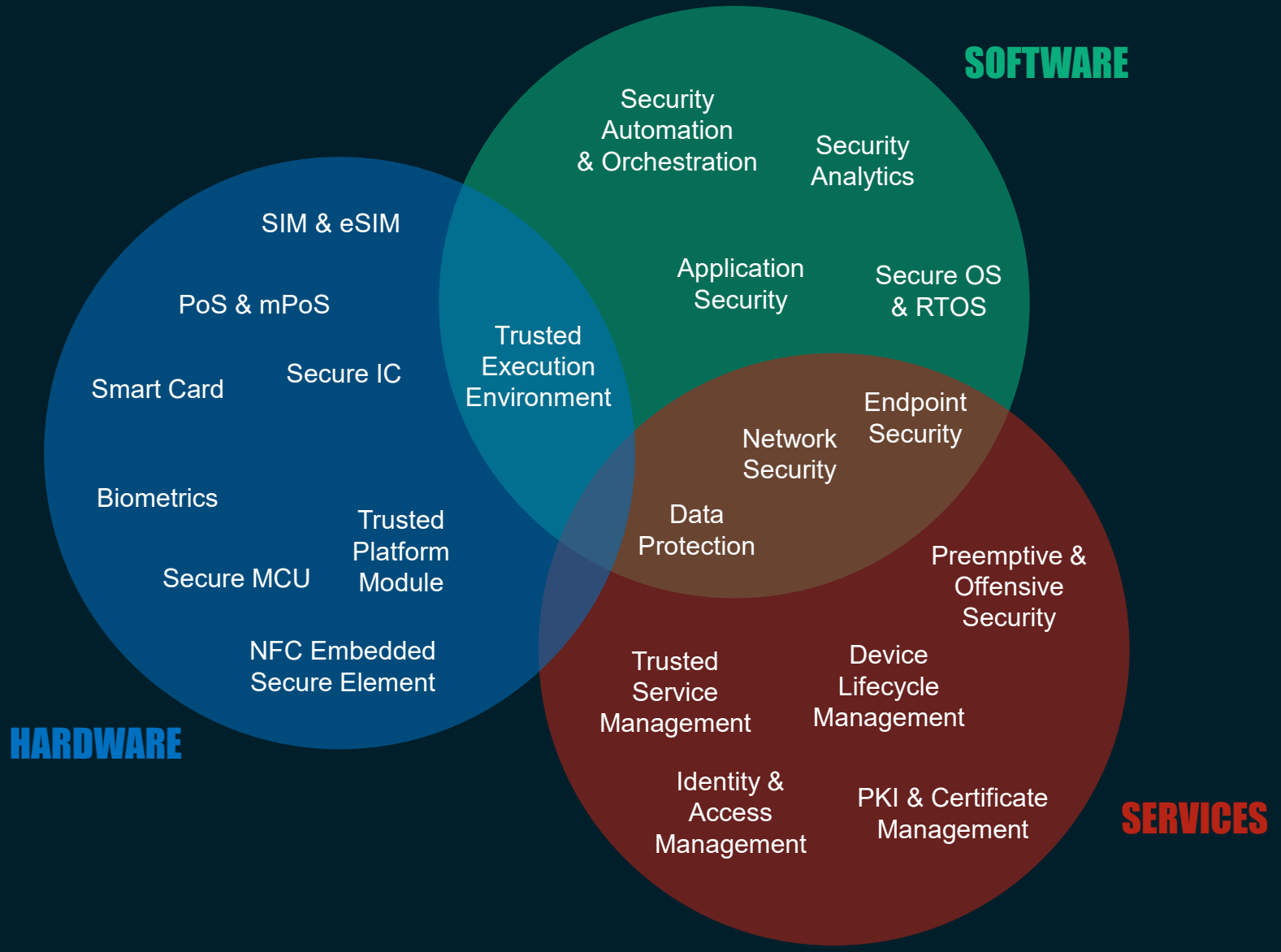
Bottlenecks

Secure provisioning services are still costly & technically challenging to implement, with the main obstacle around key management for less than 100k devices. Future offerings could focus on providing pre-provisioned secure elements with fixed configuration use cases for cloud authentication at low-cost.

Deep Digital Security Insight

Coverage

ABI Research's Digital Security Research Service offers end-to-end market coverage from information and communication technologies to operational control processes.



What Makes Our Research Different?

Best-in-class Market Data

We have the most comprehensive secure IC & smart card market data coverage.
No other research firm can match the detail of our datasets.

Close Vendor Relationships

We maintain close relationships with the top vendors in the secure hardware space,
ensuring that we have direct and accurate insight into shipment numbers.

First to Publish on Emerging IoT & OT Security

ABI Research was the first to identify and publish on a number of new market opportunities, including M2M security, critical infrastructure security, automotive cybersecurity, medical device security, IoT security, blockchain IoT applications, and secure MCUs.

LEARN MORE