$4B USD
in biometric banking technology by 2021

4B
global embedded security shipments by 2021

ABI Research's Digital Security market intelligence offers end-to-end market coverage from information and communication technologies to operational control processes. Our coverage, which includes data, trend, and forecast reports, examines leading-edge security technologies that mitigate complex risks including hardware, packaging, devices, appliances, software, platforms, networks, and services. We aim to provide organizations within the finance, government, defense, healthcare, energy, transport, and telecommunications industries with the information necessary to help them anticipate, preemptively prepare for, and proactively combat the growing proliferation of cyber threats.

TOP QUESTIONS WE RECEIVE FROM INDUSTRY INNOVATORS

- How can cybersecurity product vendors compete against service-based security offerings?
- What pressures will cybersecurity vendors feel due to the growing proliferation of cyber threats in the connected world?
- Why does cybersecurity need to happen at the product design level?
- How can, and why should, OEMs partner with cybersecurity vendors to ensure their connected products are secure?
- For OEMs, which cybersecurity vendor makes the most sense for my company to partner with?
- What other potential applications, aside from payments, can blockchain be used for?
- What offensive or pre-emptive cybersecurity steps can my company take to be ahead of our adversaries?
- How can established security vendors penetrate new IoT markets? What are the diversification opportunities?
- How can my company adapt traditional cybersecurity technologies to operational environments?
- What are the costs of cybersecurity implementations and exclusions?
- How do security demands differ across different verticals or sectors?

COVERAGE AREAS

- Enterprise technologies, including malware detection and analysis, threat intelligence platforms, security operations centers, next-gen penetration testing services, machine learning and behavior recognition, quantum encryption, cognitive security, and the future of cloud security (containers and serverless)
- IoT security standards development for application and network security
- IoT security for smart grids, biometrics in automotive and industrial settings, critical infrastructure and transportation, building automation systems, biometric-enabled payments, payments, etc.
- Smart card and ICs, including anti-counterfeiting and brand protection, mobile ticketing, companion devices, SIM cards, and e-SIM
- Security analytics and big data capabilities
- The future of cloud security
- Behavioral recognition and machine learning technologies

KEYWORDS

- Digital security
- Operational technology (OT)
- Blockchain
- BYOD mobile cloud
- Threat intelligence
- Zero days
- Advanced persistent threats (APT)
- Automation
- Cyber resiliency
- Identity of Things
- Encryption
- Authentication
- Cybersecurity
- Biometrics
- Cloud security
- Cyber attack
- Network compliance
- Malware detection
- Behavior recognition
- Network security
- Smart cards
- SIM cards
- e-SIM
- Industrial control systems
- Cyberespionage
- Data leak
- Cryptocurrency
- Phishing
- Insider threat
- Indicators of compromise
- Threat vector
- Attack surface

***Key Analysts**: Dan Shey, Michela Menting, Phil Sealy, Dimitrios Pavlakis, Jonathan O'Flaherty*