Microchip Trust Platform Fits Hardware, Misses Behavioral Continuity

by Nick Clark | Published April 25, 2026

What Microchip Trust Platform Provides

Microchip's Trust Platform (built around ATECC608, ATECC509, and successor secure elements) provides hardware-grounded device identity for IoT, automotive, industrial, and consumer-electronics applications. The platform's value proposition is making secure-element integration accessible: customizable provisioning services, integration-friendly form factors, and a price point that supports IoT deployment economics.

Microchip's broader product portfolio (8-bit through 32-bit microcontrollers, Wi-Fi and Bluetooth radios, automotive networking) makes Trust Platform part of an integrated offering for connected-device manufacturers. The platform serves the broad mid-market of connected-device manufacturers who need authentication-grade hardware without the engineering overhead of building secure-element integration from scratch.

Why Mid-Market IoT Needs Continuity Architecture Most

High-end secure-element customers (defense contractors, automotive OEMs with deep security teams, regulated medical-device manufacturers) build custom integration to fill architectural gaps. Mid-market connected-device manufacturers — Microchip's principal customer base — typically don't have the engineering capacity to build behavioral-continuity layers above secure-element foundations.

The architectural gap matters most where customer engineering capacity is least. Mid-market IoT devices ship with secure-element-grade key storage but software-grade trust handling. The cumulative deployment of behavioral-continuity-missing devices produces the cybersecurity exposure that emerging regulations (NIS2, EU Cyber Resilience Act, FDA medical-device cybersecurity guidance) increasingly target.

How a Continuity IC Reaches the Mid-Market

The continuity-identity processor IC integrates with Microchip's Trust Platform as additional silicon. The integration is naturally additive: existing Trust Platform customers gain continuity-based identity by integrating the additional IC; the existing key-storage and signing primitives remain.

For Microchip's customer base, the integration provides what the customers themselves cannot reasonably build. The behavioral-continuity layer that high-end customers build custom becomes silicon-integrated for the mid-market. Connected-device manufacturers ship with continuity-based identity that previously required custom engineering.

What This Enables for IoT Cybersecurity

The mid-market IoT cybersecurity exposure that current architecture produces becomes structurally addressable. Devices ship with continuity-based identity that doesn't require per-customer engineering investment. The compliance pathway for

emerging regulations (NIS2, Cyber Resilience Act, FDA cybersecurity guidance) maps directly to what the integrated architecture provides.

Microchip's competitive position benefits from being the secure-element vendor that brings continuity-based identity to the mid-market. The patent positions the primitive at the layer where mid-market IoT cybersecurity has had the largest structural gap — and where the regulatory pressure to close the gap is most rapidly increasing.