UNIBEAM

# Securing IoT, One Device at a Time

IoT devices rely on SIM cards or eSIMs for secure communication, but these systems face serious security risks. Attackers can remove SIM cards from authorized devices, clone them, or exploit vulnerabilities in eSIM provisioning to impersonate devices, access networks, and cause a loss of confidentiality or degradation of data integrity. Traditional SIM systems also struggle to manage large IoT networks, creating risks during swaps and reauthentication. Stronger authentication solutions are essential to protect IoT ecosystems from these threats.

**That's why we created Unibeam IoT Authentication.**

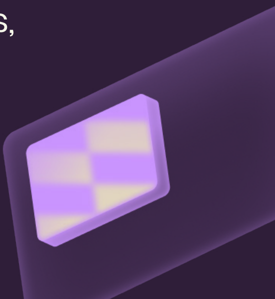
## Unibeam IoT Authentication: Bringing confidence and control back to IoT

Unibeam IoT Authentication takes device security to the next level by seamlessly binding SIM/eSIM cards to IoT devices. This ensures bulletproof protection against unauthorized access, cloning, and spoofing. And with our advanced payload encryption, your IoT data remains secure from end to end.

Unibeam delivers real-time monitoring, cryptographic safeguards, and scalable security. The result? Rock-solid data integrity, near-zero downtime, and more efficient, resilient operations.

## Why Unibeam IoT Authentication?

- Tamper-proof SIM device pairing- Unibeam "locks" every SIM/eSIM card to its specific IoT device, blocking unauthorized use - even if the SIM/eSIM is removed or cloned
- End-to-end data encryption- Sensitive IoT sensor readings are encrypted alongside Unibeam's unique SIM/eSIM-device binding, ensuring data privacy and integrity
- Real-time threat detection- With 24/7 monitoring, Unibeam detects unauthorized SIM swaps and spoofing attempts, providing instant alerts to mitigate risk
- Scalable security for large IoT ecosystems- For modest networks or millions of devices, Unibeam delivers robust, low-overhead security that ensures seamless, reliable management - at any scale
- Future-proof technology- Fully compatible with traditional SIMs and eSIMs, Unibeam evolves with advancing IoT technologies and emerging threats



## What Does Unibeam IoT Authentication Do?

For IoT ecosystems of any size, Unibeam IoT Authentication ensures that every SIM/eSIM is securely paired with its intended device - even in networks with millions of connections. Here's how:

- → Unbreakable Pairing- Each SIM/eSIM is locked to its device, preventing unauthorized access - even if the SIM/eSIM is removed or cloned
- → Ironclad Encryption- Sensitive IoT data (like sensor data) is encrypted at the source using unique encryption and binding technology
- → Bulletproof Data Integrity- All IoT data is protected against alteration or spoofing, keeping it private, intact, and secure from prying eyes
- → Constant Vigilance- Continuous monitoring of SIM/eSIM-device connections detects and alerts unauthorized activity or spoofing in real-time

Purpose-built for IoT deployments at any scale, Unibeam IoT Authentication tackles threats fast, minimizes downtime, and ensures that your devices and sensitive data remain untouchable.

## Behind the Scenes: How Does Unibeam IoT Authentication Work?

IoT device authentication ensures each device is securely identified and granted network access only if it is legitimate. For SIM-enabled IoT devices, this process verifies the SIM/eSIM card, its link to the device, and its interactions with the network.

This layered approach ensures that IoT devices are securely integrated into the network and protected from unauthorized access. How does this happen?

01 Bind Device to SIM/eSIM

Unibeam IoT Authentication identifies each IoT device by two key components: a device-specific ID (like its IMEI or a hardware-based cryptographic key), and a SIM-specific ID (like its IMSI). During the initial setup, the device's ID and the SIM's ID are securely paired, creating a trusted connection that serves as the foundation for Unibeam's authentication.

02 Authenticate

Unibeam IoT Authentication uses advanced cryptographic techniques for added security by ensuring the data's authenticity and integrity. Unibeam then validates these two key components to confirm the device's identity without exposing sensitive information during transmission.