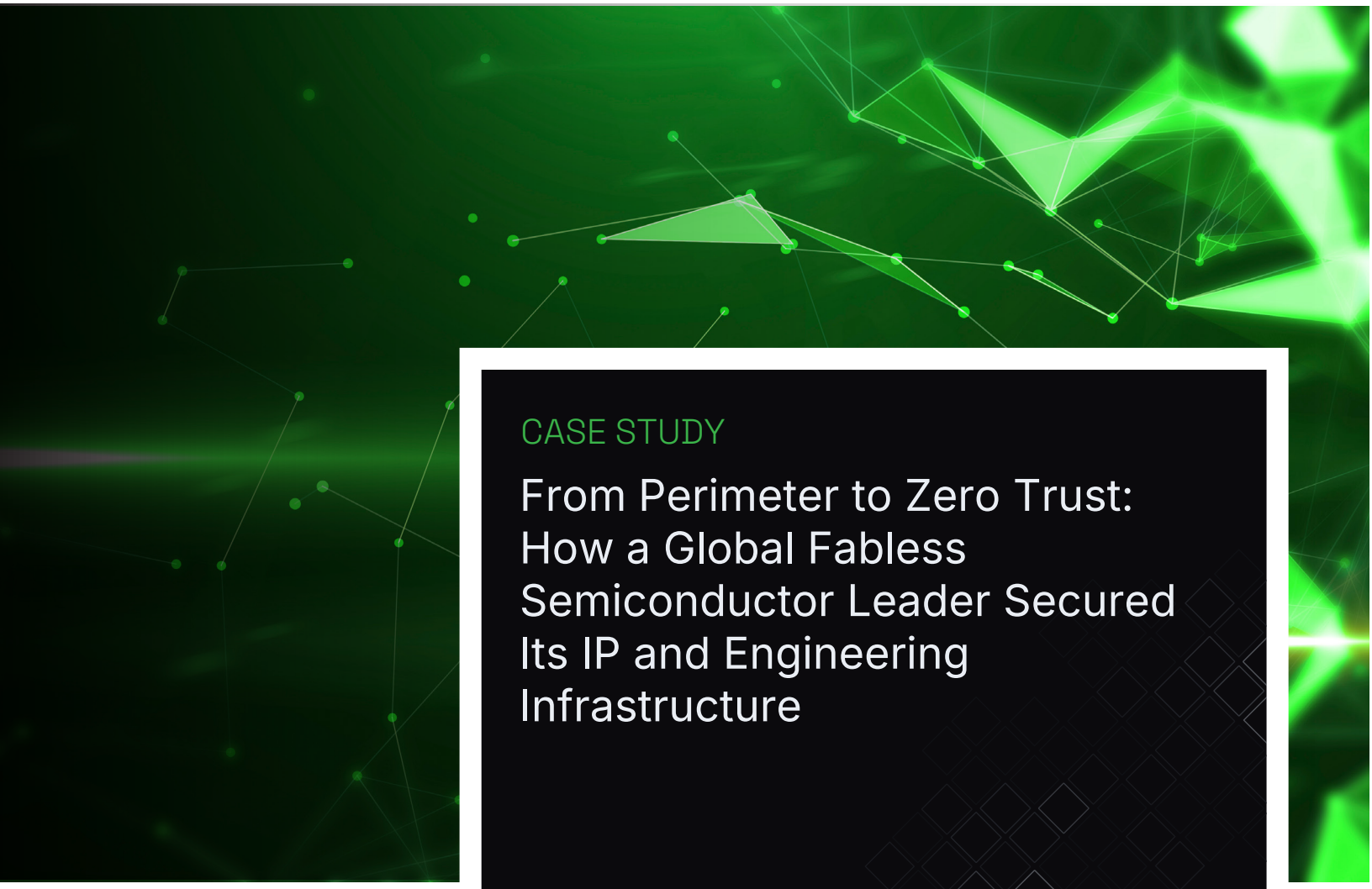
ARMATURE
SYSTEMS



CASE STUDY

From Perimeter to Zero Trust: How a Global Fabless Semiconductor Leader Secured Its IP and Engineering Infrastructure

Industry: Semi Conductor

May 2026

The Challenge

The client faced a convergence of threats that legacy perimeter-based security was never designed to handle.

IP Under Siege

As a fabless company, proprietary chip designs are the organization's only tangible asset. Without physical manufacturing as a fallback, a single successful exfiltration by a nation-state actor or persistent threat group represents an existential risk.

Vulnerable Overseas Nodes

International design centers and remote labs operated under inconsistent security configurations, creating regional blind spots that sophisticated threat actors could exploit to gain a foothold into the core network.

Firmware Integrity at Risk

The client's Root of Trust Signing Authority, the mechanism that digitally signs firmware to verify authenticity, lacked redundancy. A compromise or outage here would expose the entire product supply chain to tampering and counterfeit code injection.

Engineering Continuity Constraints

The architectural overhaul had to be executed within a very short timeframe without disrupting concurrent engineering development. Any loss of access to remote labs or data centers would directly impact the bottom line.

Uncontrolled Device Growth

A growing influx of IoT devices, lab test benches, and unmanaged hardware across factory floors created visibility gaps, shadow IT that bypassed security policy and expanded the attack surface.

The Partnership

The client is a premier fabless semiconductor innovator with a worldwide footprint and critical reliance on two global data centers. In the semiconductor industry, intellectual property is the lifeblood of the organization, because they do not manufacture chips themselves, the loss of proprietary designs to nation-state actors or persistent threat groups could result in catastrophic business consequences.

Armature Systems served as that partner, executing a complete network overhaul to support low-latency connectivity, path and transport diversification, and a comprehensive Zero Trust implementation, all while maintaining the integrity of their Root of Trust Signing Authority for digital firmware.

Our Solution

Armature Systems implemented a strategy centered on security ensuring the client could innovate at speed without compromising on protection.

1 NETWORK INFRASTRUCTURE: RESILIENCY & GLOBAL FABRIC

Armature focused on a high-availability architecture that ensures the engineering production line never stops.

Operational Continuity

Redundant, resilient topologies ensure constant connectivity. Mission-critical updates were executed only during strictly defined maintenance windows to prevent any impact on active design cycles.

Global Transport Diversification

A seamless, low-latency fabric was established between international design centers and the two core data centers. Path diversification ensures data moves securely across geographic borders even if a primary transport provider fails.

2 ZERO TRUST & RIGOROUS SECURITY ASSESSMENTS

ZTNA Implementation

The client transitioned from legacy access to an identity-centric Zero Trust model. Proprietary chip designs are now isolated and accessible only to verified users on healthy devices, preventing lateral movement by threat actors.

Network Security Assessments

Deep-dive firewall audits across the global footprint included rule base optimization to close high-risk gaps, geo-blocking to harden international sites against regional threat groups, and compliance verification across all configurations.

NAC Implementation & Auditing

A Network Access Control solution was deployed to automatically profile every device from a technician's tablet to a lab test bench and assign strict, role-based permissions. Exhaustive auditing ensures no device goes unmanaged.

3 ENGINEERING INTEGRITY & SECURE WORKFLOW

Redundant Root of Trust Signing Authority:

Armature designed and implemented a high-availability Root of Trust Signing Authority, ensuring the digital signing of firmware remains secure and available, protecting the supply chain from tampering and counterfeit code.

Micro-Segmentation of Remote Labs

Granular micro-segmentation limits the blast radius of any compromise in a remote lab, ensuring testing environments cannot be used as a bridge to reach sensitive IP vaults.

Identity-Driven Resource Isolation:

Access to high-value design tools and simulation clusters is dynamically gated by identity, preventing unauthorized access to silicon blueprints while maintaining the high-speed throughout engineering teams require.

The Outcomes

BEFORE ARMATURE		AFTER ARMATURE
Perimeter-based access Legacy trust model: anyone inside the network perimeter was implicitly trusted.	→ ZERO ACCESS	**Zero Trust Foundation** Every user and device verified continuously without any disruption to active engineering cycles
Exposed IP Lateral movement risk, a compromised remote lab could reach core chip design vaults	→ MICRO-SEG	**IP Locked Down** Chip designs invisible to unauthorized users, with no lateral movement path from labs to vaults.
Single point of failure Firmware signing had no redundancy leaving it vulnerable to tampering or outage	→ ROOT OF TRUST	**Supply Chain Secured** Redundant Root of Trust Signing Authority eliminates counterfeit code from entering the supply chain.
Shadow IT Individuals connected unauthorized switches & APS, creating invisible, unmanaged network segments.	→ NAC	**Full Device Visibility** NAC automates device profiling and blocks unauthorized hardware to eliminate all visibility gaps.

Zero Trust Foundation, Zero Disruption

The complete architectural transition to Zero Trust was executed within a compressed timeframe without a single disruption to active engineering cycles, all changes confined to pre-approved maintenance windows.

IP Locked Down

Micro-segmentation and identity-driven isolation ensure proprietary chip designs are invisible to unauthorized users, with no lateral movement path from remote labs to core IP vaults.

Supply Chain Integrity Protected

A redundant Root of Trust Signing Authority ensures firmware authenticity is continuously verified, eliminating the risk of counterfeit code entering the product supply chain.

Full Device Visibility Achieved

NAC deployment gave the client complete visibility and automated control over every device on the network, eliminating shadow IT and unmanaged hardware across global sites.

ARMATURE
SYSTEMS

ABOUT ARMATURE SYSTEMS

Armature Systems is a cybersecurity systems integrator that helps organizations design, build, and operate network and security programs across the full lifecycle.

We work hands-on alongside internal teams to deploy the right technology, build effective processes, and deliver measurable security outcomes across network, cloud, identity, compliance, and threat response.

Ready to modernize your security & network program?
Visit armaturesystems.com