Getac
Device Component Integrity (DCI)

Securing the Supply Chain from Production to Deployment

In an era where cyber threats extend beyond software to the physical hardware itself, supply chain integrity is paramount. Getac Device Component Integrity (DCI) is a comprehensive security solution designed to safeguard your enterprise devices against malicious tampering, counterfeit parts, and unauthorized modifications.

By adhering to **NIST SP 1800-34C compliance** for supply chain integrity, Getac DCI ensures that every critical component within your device is authentic, original, and verified. We build trust and reliability directly into the manufacturing process, shielding your critical systems from hidden backdoors and data risks before they ever reach the field.

The Challenge: Supply Chain Vulnerabilities

Modern enterprises face significant threats from the hardware supply chain, including:

- **Malicious Components:**
  Hardware or software elements embedded with malicious code capable of compromising system confidentiality.
- **Backdoor Attacks:**
  Unauthorized access points that allow attackers to bypass authentication and control systems remotely.
- **Counterfeit Parts:**
  Unverified, non-original components that lead to system failures, increased downtime, and potential safety hazards.

Getac DCI neutralizes these threats by establishing a verifiable chain of trust.

Key Benefits

- **Enhance Security**

Eliminate the risk of hardware tampering and counterfeit parts. DCI reduces supply chain vulnerabilities by ensuring that only authorized, original components are present in your device.

- **Build Reliability**

Authentic components guarantee consistent performance.
By verifying hardware integrity, we ensure stable system operations, avoiding the unexpected failures and downtime associated with substandard or fake parts.

- **Supply Chain Transparency**

Gain end-to-end visibility. DCI provides a verifiable record of component authenticity, offering transparency that protects users and validates the device's origin.

- **Reduce Costs & Risks**

Unverified parts are a liability.
By preventing accidents, system failures, and productivity loss caused by faulty hardware, DCI safeguards both personnel and assets, ultimately reducing long-term operational costs.

How It Works:
The DCI Lifecycle

Getac DCI operates through a rigorous "verify and validate" methodology, ensuring authenticity from the factory floor to your facility.

1. Order:
The customer places an order for DCI-enabled devices.

2. Build:
Getac manufactures the device, recording the specific identity of key internal components.

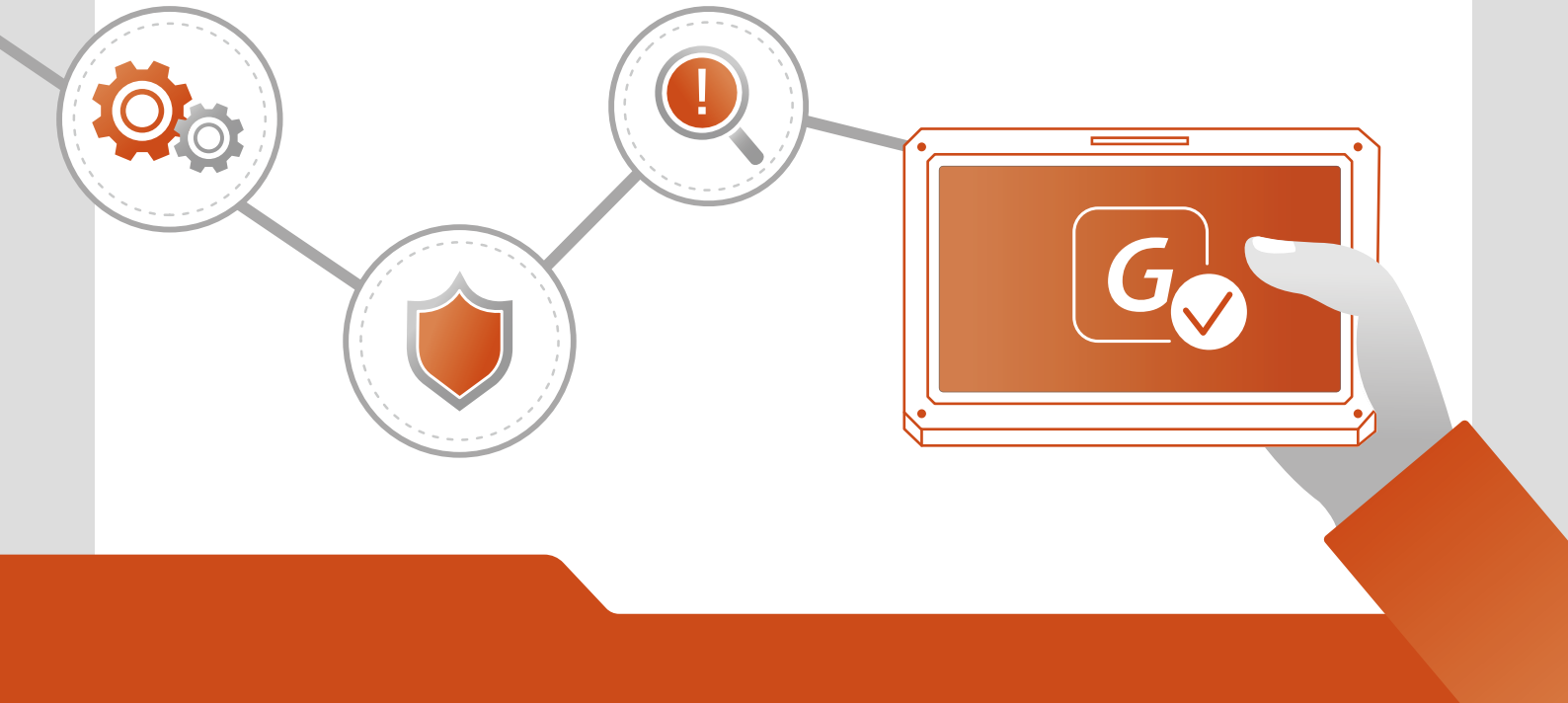
3. Collect & Create:
Component data is aggregated, and a Platform Certificate is digitally signed.

4. Store:
The signed certificate is securely stored to preserve integrity.

5. Deliver:
The physical device and the public keys are delivered to the customer.

6. Validate* :
Upon receipt, the customer verifies the device's authenticity using their infrastructure.

** Customers are required to deploy and manage their own server infrastructure.*



Getac's Role: Establishing the Chain of Trust

Getac acts as the root of trust, generating the cryptographic proof required to validate the hardware.

- **Certificate Creation:**

  For every DCI-enabled unit, we issue a unique **Platform Certificate** generated using Getac's private key. This ensures absolute authenticity and traceability.

- **Component Coverage:**

  The Platform Certificate captures specific details of critical components, including:

  - CPU
  - PCB Serial Number
  - BIOS Firmware Version
  - GPU
  - Trusted Platform Module (TPM)
  - Networking Modules
  - Memory and SSD

- **Secure Storage:**

  Certificates and public keys are housed within Getac's secure manufacturing and OTS systems to maintain integrity across the entire supply chain.



Customer's Role: Deployment & Validation

To fully leverage DCI, customers deploy and manage their own server infrastructure to validate incoming devices. This process utilizes the **HIRS (Host Integrity at Runtime and Start-up)** framework.

Infrastructure Requirements

This system consists of two main elements:

- **Validating Server (The HIRS ACA Server):**

  The customer utilizes the **HIRS ACA Server**, a web-based attestation framework designed to process Attestation Identity Requests (AIRs). This server validates each Platform Certificate against Getac's public keys. It confirms the device's legitimacy before it is allowed to join the network or process data.

- **Validating Client (The HIRS Provisioner):**

  This client-side component collects and validates hardware component data from the device itself, ensuring a tamper-free configuration.

By integrating this validation step, organizations maintain complete control over their hardware security posture, ensuring that only trusted, verified Getac devices are deployed in their operations.

Secure your foundation. Protect what matters.

Please contact your local Getac sales representative for further details.

GETAC TECHNOLOGY CORPORATION

5F, Building A, No. 209, Section 1, Nangang Rd.,Nangang Dist.,
Taipei City, 11568, Taiwan, R.O.C.
Tel : +886 2 2785 7888
globalmarketing@getac.com | www.getac.com

Copyright © 2026 Getac Technology Corporation and/or any of its affiliates. All Rights Reserved.

Getac
Rugged Mobile Computing Solutions