CL

8 Ways a Silicon Root of Trust Can Lay the Foundation of Security and Integrity for Your Business-Critical Servers

The security and integrity of your organization's business-critical servers are at the very foundation of your trusted computing infrastructure and trusted supply chain. Here are eight ways that leading solution providers are leveraging a **silicon root of trust** to help you protect your organization's servers from unauthorized changes throughout their lifecycle — from sourcing and manufacturing; to everyday bootup, updates, and execution; to eventual repurposing, retirement, or disposal.

☐	To provide servers with a **silicon root of trust**, a unique digital fingerprint (a *cryptographic hash*) is embedded in the server chip at the factory — which enables servers to anchor their secure boot process to an unchangeable (*immutable*), silicon-based source.
☐	Specialized services are available to ensure the **domestic sourcing**, **manufacturing**, and **provenance** of industry-standard servers that include the advanced security capabilities described below — built by vetted employees, in highly secure domestic facilities — up to the time they become an integral part of your organization's trusted computing infrastructure or trusted supply chain.
☐	To ensure the **authenticity and integrity of the server's firmware**, only firmware that has been digitally signed by its silicon root of trust will be allowed to load and run — making it virtually impossible for servers to execute compromised code (e.g., *malware*, *zero-day exploits*).
☐	If recovery from unauthorized changes to server code should be needed, firmware is **automatically restored** to a safe, previously known setting.
☐	To establish trust with **additional server components** (e.g., drivers, OS boot loaders) during the secure boot process, standardized mechanisms ensure that they too are authenticated and digitally signed.
☐	Built-in **monitoring** can automatically check essential server firmware at regular intervals (e.g., daily) — and alert your IT administrators for manual remediation, or automatically recover to a known good state.
☐	**Automation** of common server tasks (e.g., server provisioning; continuous, proactive monitoring of system health; server management; power and thermal control; and secure, out-of-band remote management) helps your organization's IT staff to support higher scale at lower total cost.
☐	By permanently erasing data and resetting security attributes, your organization's servers can be **securely repurposed, retired, or disposed of** when the time comes.

ABERDEEN STRATEGY & RESEARCH
ILLUMINATE. INSPIRE. IGNITE.

18573