Trusted security by design

HPE ProLiant Gen11 servers — compute engineered for your hybrid world

Deploy with confidence, gain peace of mind

As threats to your data, assets, and resources continue to expand and accelerate, securing your organization’s hybrid compute infrastructure is more critical than ever before.

To enable security with performance at scale, your enterprise needs support within every layer of your data infrastructure from edge to cloud. Rather than face escalating security threats alone, you can work with Hewlett Packard Enterprise to adopt a holistic defense-in-depth approach — starting by modernizing your compute with HPE ProLiant Gen11 servers.

With HPE ProLiant Gen11, security is built into each server’s DNA:

• From silicon to software via the silicon root of trust from HPE
• From factory to cloud using a trusted supply chain
• From generation to generation by continually adding new security capabilities to address ever-evolving cyberattacks

Trust HPE ProLiant Gen11 edge to core security posture to protect your:

• Infrastructure, including servers, storage, and networking
• Workloads, such as applications, virtual machines, containers, and databases
• Data, regardless of where it resides within your IT landscape

Security is fundamental

By integrating security directly into the hardware level of HPE ProLiant Gen11 servers, the silicon root of trust from HPE firmware technology makes it impossible to tamper with the servers during manufacturing. With verification embedded in their silicon chips, HPE ProLiant Gen11 servers will always boot in a pristine and immutable state.

The silicon root of trust from HPE

• Protects a million lines of firmware code from malware and ransomware with a digital fingerprint that is unique to the server
• Secures more than 4 million HPE servers around the world

Figure 1. Diagram illustrating the HPE ProLiant Gen11 silicon root of trust
The fundamental security components of HPE ProLiant Gen11 servers include:

- **Platform certificates** that detect tampering and verify that your server remains completely unmodified between manufacturing and delivery.
- **Initial Device Identifiers (IDevIDs)**, which are cryptographic identities that provide secure, zero-touch onboarding without human intervention, enabling automatic provisioning and access management for integrated applications.
- **Trusted Platform Module**, adding another layer of authentication.
- **HPE GreenLake for Compute Ops Management**, keeping your infrastructure up to date with the latest firmware and security patches.

**Security is uncompromising**

Beyond the silicon, HPE ProLiant Gen11 servers authenticate platform components against potential entry points of security threats. For example, storage controllers and network interface cards are verified and authenticated using HPE iLO 6. This version of HPE iLO features new authentication using the Security Protocol and Data Model (SPDM) certification — a key security capability designed to ensure each component’s integrity.

Striving to achieve continuous innovations for best-in-class security, HPE ProLiant Gen11 servers extend protection beyond compute by reaching across the HPE partner ecosystem and through the HPE GreenLake edge-to-cloud platform.

**Security is protected**

A trusted and protected infrastructure begins with a secure supply chain. HPE Trusted Supply Chain is an option that provides you with optimized protection and confidence for your HPE ProLiant Gen11, from trusted suppliers to manufacturing facilities and while in transit for delivery. Now available worldwide — including NA, LATAM, EMEA, and APJ regions — HPE Trusted Supply Chain security includes more workloads and is available with AMD and Intel-based HPE ProLiant Gen11 servers.

Assuring security compliance

Global supply chain operations compliance is assured through risk-based security audits, program monitoring, inspection of electronic parts, component traceability, and material control processes. These extreme practices help prevent, monitor, detect, analyze, and report incidents of confirmed counterfeit, and malicious taint to all HPE products—providing you with peace of mind, knowing that your HPE ProLiant Gen11 servers will arrive unharmed and untampered by any nefarious actors.

Extending server protection with HPE GreenLake

To protect your hybrid cloud environment, HPE GreenLake provides fundamental zero trust lifecycle management for all your HPE ProLiant Gen11 servers, delivered as a secure SaaS application that is continuously managed and improved by HPE.

When you extend your protection by running HPE ProLiant Gen11 servers via the HPE GreenLake platform, you receive:

- **End-to-end** security features from your devices to the cloud
- **Security** triggers throughout the supply chain
- **Service** delivery from HPE professionals you trust

Learn more at [HPE.com/security/compute](HPE.com/security/compute)

---

1. HPE iLO 6 follows SPDM to create an integrated and cost-effective approach to management.