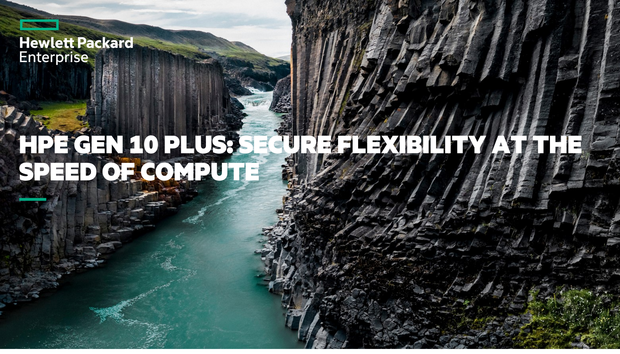


Hewlett Packard Enterprise

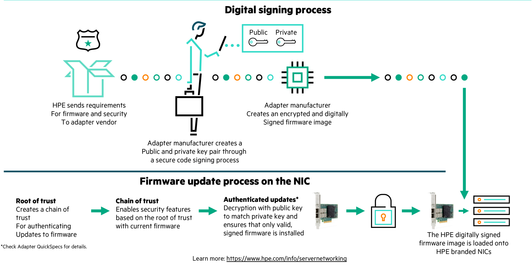
HPE GEN 10 PLUS: SECURE FLEXIBILITY AT THE SPEED OF COMPUTE

THE MOST EFFECTIVE CYBER SECURITY PROTECTION—INSIDE THE SERVER

	Protect	Detect	Recover
Feature	• Root of Trust/Chain of Trust • Authenticated Updates	• Secure Boot • Device-level Firewall	• Audit Logs • Sanitization
Value/Benefit	• **Root of Trust** enables a **chain of trust** for **Authenticating updates to firmware via signature validation**. This blocks installation of rogue or corrupted firmware and ensures that the executing firmware is trusted. • **Authenticated Updates** brings cryptographic keys onto the NIC (for HW Authentication) to protect user and configuration data from unauthorized access and verify digitally signed firmware.	• **Secure Boot** safeguards the system and ensures no rogue drivers are being executed on start-up. • **Device-level Firewall** blocks any unmanaged access to memory or storage. This ensures that on-device firmware and configuration data can only be accessed by authorized agents.	• **Audit Logs** are a forensics capability that provides traceability into authenticated firmware updates by capturing changes in standard system logs. • **Sanitization** (Secure User Data Erase) renders User and configuration data on the NIC irretrievable so that NICs can be safely repurposed or disposed.

Learn more: https://www.hpe.com/info/servernetworking

HOW THE NIC SAFEGUARDS—INSIDE THE SERVER

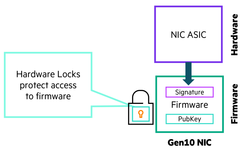


*Check Adapter QuickSpecs for details.

Learn more: https://www.hpe.com/info/servernetworking

ROOT OF TRUST

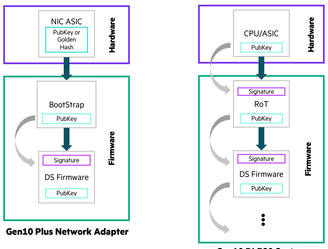
	Protect
Features	• Root of Trust/Chain of Trust • Authenticated Updates
Value/Benefit	• **Root of Trust** enables a **chain of trust** for **Authenticating updates to firmware via signature validation**. This blocks installation of rogue or corrupted firmware and ensures that the executing firmware is trusted. • **Authenticated Updates** brings cryptographic keys onto the NIC (for HW Authentication) to protect user and configurationuration data from unauthorized access and verify digitally signed firmware.



- HW Locks preclude modifications to FW except via authorized FW
- Factory installation of known good FW
- Once valid FW installed, only valid signed FW can be installed

Learn more: https://www.hpe.com/info/servernetworking

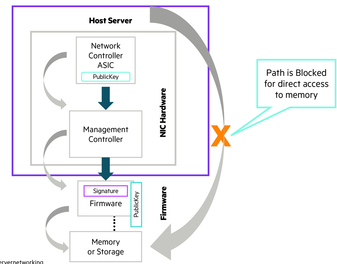
GEN10 PLUS ROOT OF TRUST (ROT) SYSTEM AND NETWORK ADAPTER



Learn more: https://www.hpe.com/info/servernetworking

GEN10 PLUS SERVER WITH SECURE NIC

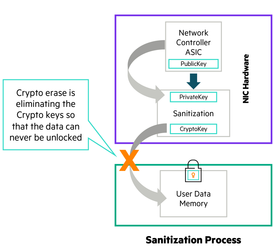
	Detect
Features	• Secure Boot • Device-level Firewall
Value/Benefit	• **Secure Boot** safeguards the system and ensures no rogue drivers are being executed on start-up. • **Device-level Firewall** blocks any unmanaged access to memory or storage. This ensures that on-device firmware and configuration data can only be accessed by authorized agents.



Learn more: https://www.hpe.com/info/servernetworking

GEN10 PLUS SERVER WITH SECURE NIC

	Recover
Features	• Audit Logs • Sanitization
Value/Benefit	• **Audit Logs** are a forensics capability that provides traceability into authenticated firmware updates by capturing changes in standard system logs. • **Sanitization** (Secure User Data Erase) renders User and configuration data on the NIC irretrievable so that NICs can be safely repurposed or disposed.



Learn more: https://www.hpe.com/info/servernetworking

For more information on HPE Gen 10 Plus, please contact us today.