

HPE PROLIANT COMPUTE GEN12

Built to Defend



Why This Analysis Matters

As organizations increasingly adopt hybrid and cloud-native architectures, the line between physical infrastructure and cloud operations is becoming less distinct. With this evolution comes heightened expectations for server hardware to deliver robust, built-in security. Our objective was to assess how effectively HPE ProLiant Compute Gen12's platform with HPE iLO 7 addresses these modern challenges—and how it compares to both traditional hardware vendors and leading cloud providers.

Key Highlights of HPE ProLiant Compute Gen12 with HPE iLO 7 Security

Through our analysis, several standout security features in the HPE ProLiant Compute Gen12 / HPE iLO 7 ecosystem earned high marks:

Silicon Root of Trust: HPE's proprietary silicon root of trust protects against firmware tampering and supply chain compromise. Every HPE ProLiant Compute Gen12 server validates its firmware before booting, providing assurance from the very first line of execution.

Runtime Firmware Verification: HPE iLO 7 continuously checks firmware integrity while the system is running—an advanced feature rarely found in traditional server management tools.

Automatic Secure Recovery: In the event of a firmware compromise, the server can revert to a known-good version, ensuring continuity and integrity.

Zero Trust Integration: HPE's compatibility with modern identity and access solutions through HPE Compute Ops Management supports fine-grained, role-

based access control and full audit visibility, aligning with Zero Trust principles.

Comprehensive Telemetry and Log Integrity: With integrated hardware logging and tamper-proof auditing, HPE ensures that you see what happened—when it happened.



Figure 1 – HPE ProLiant Compute DL380 Gen12

How HPE Stacks Up

To better understand how the HPE ProLiant Compute Gen12 platform with HPE iLO 7 and HPE Compute Ops Management stands out in today's security-conscious IT landscape, we conducted a comparative analysis against other leading hardware vendors and major cloud service providers. Our evaluation focused on critical security capabilities such as firmware protection, secure recovery, access control, audit integrity, and alignment with Zero Trust principles.

The table below provides a breakdown of this analysis, highlighting where HPE leads, where others fall short, and why these distinctions matter for organizations looking to build or maintain a hardened, resilient, and compliant infrastructure. This comparison is designed to help decision-makers assess their options with security at the forefront.

Security Feature	HPE ProLiant Compute Gen12 + iLO7 + HPE Compute Ops Management	Other Hardware Vendors	Cloud Service Providers
Silicon Root of Trust	✔ Yes	• Partial or Vendor-Specific	✔ Yes
Runtime Firmware Validation	✔ Yes	✘ No	✔ Yes (Platform Specific)
Automatic Secure Recovery	✔ Yes	• Manual Intervention Required	• Limited
Secure Identity Federation / Role-Based Access	✔ Yes (With HPE Compute Ops Management)	• Basic User Control	✔ Yes
Hardware-Enforced Audit Logging	✔ Yes	• OS-Dependent	✔ Yes
Zero Trust Architecture Alignment	✔ Yes	• Emerging Support	✔ Yes
Continuous Compliance Monitoring	✔ Yes	✘ Not Native	✔ Native

Figure 1 – Analysis Comparison

What This Means for the Enterprise

Our analysis makes it clear—HPE is delivering a secure-by-design platform ready for today’s enterprise IT and SecOps demands. Whether in data centers, hybrid cloud, or at the edge, the HPE ProLiant Compute Gen12 servers with HPE iLO 7 combine security, compliance, and resilience in one powerful solution.

Paired with HPE Compute Ops Management, HPE offers centralized control and deep visibility—making it an ideal choice for organizations looking to strengthen their infrastructure without sacrificing agility.

Conclusion

At InfusionPoints, we recognize the importance of a proactive approach to cybersecurity, and HPE continues to demonstrate leadership in this space. Their commitment to undergoing independent security reviews of the HPE ProLiant Compute Gen12 server platform and HPE iLO 7 capabilities reflects a broader dedication to building secure, resilient, and future-ready infrastructure.

By focusing on security at every layer—from hardware and firmware to cloud-enabled management—HPE is setting a strong example of how innovation and trust can go hand in hand. Their openness to third-party validation and continuous improvement underscores a clear priority: delivering technology that’s built with security at its foundation.

About InfusionPoints

InfusionPoints is your independent trusted partner dedicated to assisting you in building your secure and compliant business solutions, testing your security controls and defending your consumer, employee, and supply chain information.

Important Facts about this Paper

PUBLISHER: InfusionPoints, LLC

INQUIRIES: Contact us if you would like to discuss this report, and InfusionPoints will respond promptly.

+1-336-990-0252

info@InfusionPoints.com

<https://www.infusionpoints.com>

CITATIONS: This paper can be cited by accredited press and analysts but must be cited in-context, displaying author “InfusionPoints, LLC”. Non-press and non-analysts must request prior written permission by InfusionPoints, LLC for any citations.

LICENSING: This document, including any supporting materials, is owned by InfusionPoints, LLC. This publication may not be reproduced, distributed, or shared in any form without prior written permission from InfusionPoints, LLC.

DISCLOSURES: This paper was commissioned by Hewlett Packard Enterprise (HPE). InfusionPoints provides security research, analysis, advising, consulting, and penetration testing to many high-tech companies in this space.

DISCLAIMER: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. InfusionPoints, LLC disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of InfusionPoints, LLC and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

InfusionPoints, LLC provides forecasts, and forward-looking statements, and trends in cybersecurity as directional indicators and not as precise predictions of future events. While our opinions are based on our current judgment based on available information and analysis, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinion as of the date of publication for this document.

Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

©2025 InfusionPoints, LLC. Company and product names are used for informational purposes only and may be trademarks of their respective owners.