

Moderne Infrastruktur, moderner Schutz: Serversicherheit für die Zukunft

Bauen Sie eine sichere Zukunft mit einer
Infrastruktur ab Chipebene



Ihr Unternehmen strebt nach Innovation und Wachstum. Dasselbe gilt jedoch für die Bedrohungslandschaft. HPE ProLiant Compute Gen12 Server mit HPE iLO 7 helfen Ihnen, aufkommende Risiken zu meistern, damit Sie sich auf das Wesentliche konzentrieren können.

Risiken einer alternden Infrastruktur

Lücken im Hintergrund, die in der Legacy-Infrastruktur möglicherweise übersehen werden:

- Firmware-Drift zwischen Updates
- Nicht validierte Komponenten von Drittanbietern
- Rootkit-Verhalten auf Chipebene
- Offline-Konfigurationsänderungen
- Manipulation von Anmeldeinformationen während Ausfallzeiten

HPE ProLiant Compute Gen12 mit HPE iLO 7 hilft, diese Lücken mit Out-of-Band-Sichtbarkeit zu schließen – selbst wenn das Betriebssystem offline ist.

Argumente für moderne Serversicherheit

Die heutige Bedrohungslandschaft ist besser getarnt. Diese Bedrohungen können aus unerwarteten Richtungen kommen und auf Taktiken zurückgreifen, die schwerer zu erkennen – geschweige denn zu stoppen – sind. Dabei zielen die Angriffe zunehmend auf Firmware und Lieferketten ab. Eine sichere Infrastruktur bedeutet, jeden Layer in jedem Moment des Lebenszyklus zu schützen und gleichzeitig mit den Compliance-Anforderungen und der betrieblichen Komplexität Schritt zu halten.

Doch herkömmliche Abwehrmaßnahmen wie Firewalls und Endpunkt-Tools sind nicht darauf ausgelegt, das zu berücksichtigen, was vor dem Starten des Betriebssystems oder bei Leerlauf der Server passiert. Und es ist zunehmend unrealistisch, dass manuelle Sicherheitsprozesse wie Patches, Updates und das Konfigurationsmanagement mit der Geschwindigkeit und dem Umfang moderner Betriebsabläufe Schritt halten können.

Das Ergebnis? Lücken, die in Hybrid- und Multi-Gen-Umgebungen unbemerkt wachsen.

IT-Entscheider stehen vor vielfältigen Fragen: Wie sichern Sie, was nicht immer sichtbar ist? Welche langfristigen Kosten entstehen, wenn die Compliance nicht mehr eingehalten wird? Wie modernisieren Sie die Infrastruktur, ohne neue Risiken oder Belastungen hinzuzufügen?

Der erste Schritt besteht darin, von der mehrschichtigen Sicherheit zum integrierten Schutz überzugehen – in die Plattform integriert, zukunftssicher und vom ersten Tag an aktiv.

Übernehmen Sie die Kontrolle – mit einer Plattform für durchgehende Sicherheit

Es wird immer schwieriger, die Sicherheit der Infrastruktur zu gewährleisten, wenn sich die Umgebungen über Standorte, Workloads und Bereitstellungsmodelle hinweg erweitern. Die Führungsrolle von HPE im Bereich Serversicherheit basiert auf jahrzehntelanger Innovation – von der Silicon Root of Trust über Secure Boot bis hin zur umfassenden Lifecycle Protection.

Mit HPE ProLiant Compute Gen12 wird diese Grundlage noch stärker. HPE iLO 7 stellt den nächsten Schritt in dieser Entwicklung dar und bietet IT-Teams leistungsstarke, integrierte Tools, um Bedrohungen frühzeitig zu erkennen, Richtlinien konsequent durchzusetzen und schnell zu reagieren, wenn etwas schief geht.

Anstatt die Sicherheit auf den Stack zu ergänzen, integriert HPE sie in jeden Layer. HPE iLO 7 läuft auf seinem eigenen isolierten Chip und bleibt auch dann aktiv, wenn das Host-Betriebssystem ausfällt. Dadurch erhalten Teams kontinuierlich Einblick in den Zustand, die Integrität und die Gefährdung des Servers.

Erweiterte Funktionen, die den Plattformschutz erhöhen:

- Secure Enclave-Architektur zur Isolierung von Verschlüsselungsschlüsseln
- Echtzeit-Dashboards zur Erkennung von Sicherheitsbedrohungen
- Konfigurationssperren und reine TLS-Verschlüsselung
- Gerätespezifische Firmware-Überprüfung
- Aktive Sicherheit auch bei ausgeschaltetem Server

Diese Funktionen bieten integrierte Intelligenz, die mit dem Schutz beginnt, noch bevor das Betriebssystem hochfährt.

Die neue Secure Enclave-Architektur speichert Anmeldeinformationen sicher und hilft, Manipulationen zu verhindern. Gleichzeitig erleichtern Echtzeit-Dashboards, gerätespezifische Firmware-Updates und Konfigurationssperren die Aufrechterhaltung sicherer Vorgänge im großen Maßstab.

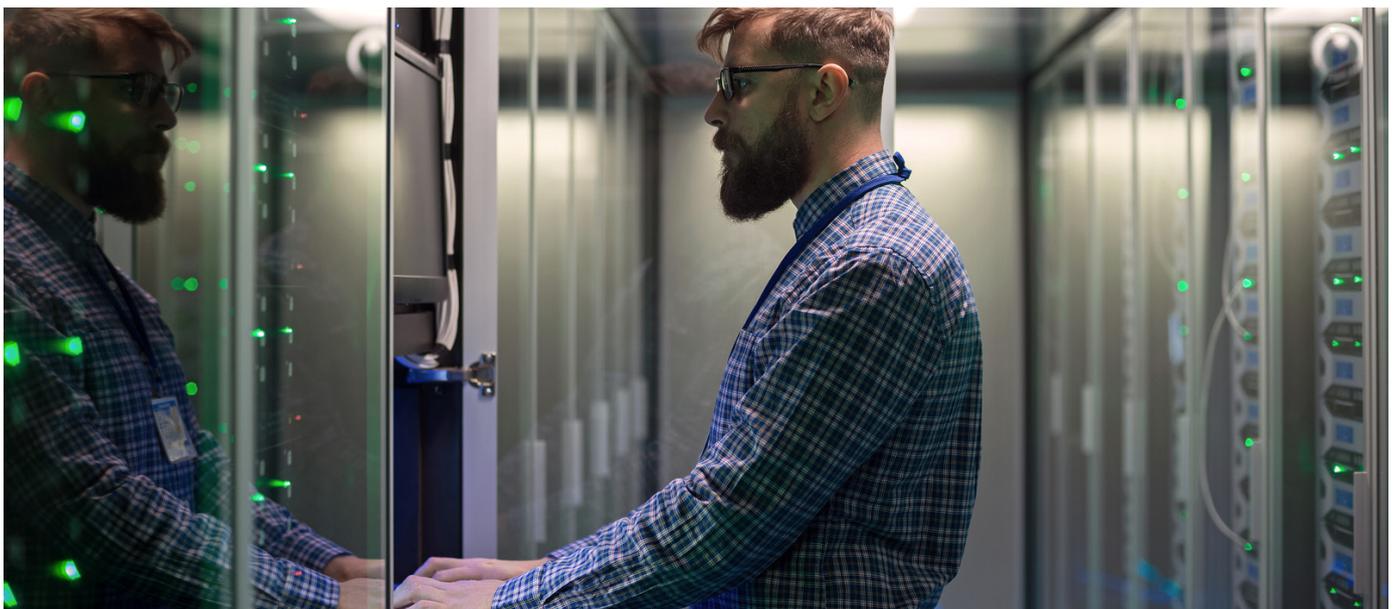
Durch die Zusammenführung von Hardware, Firmware und Verwaltung auf einer zuverlässigen Plattform können Sie die Modernisierung beruhigt durchführen, da Sie wissen, dass die Sicherheit bereits integriert ist und Sie vom ersten Tag an unterstützt.

Ein einfacher Weg zu starkem Schutz

Bei der Aufrüstung der Infrastruktur bestehen häufig Bedenken hinsichtlich Unterbrechungen, Inkonsistenzen oder dem Verwaltungsaufwand. HPE iLO 7 ist jedoch darauf ausgelegt, diesen Übergang zu erleichtern und die Aufrechterhaltung sicherer Vorgänge in gemischten Umgebungen zu vereinfachen.

Mit seinen Echtzeit-Dashboards, der gerätespezifischen Firmware-Validierung und der zentralen Kontrolle der Anmeldedaten gibt HPE iLO 7 den IT-Teams mehr Vertrauen in die Durchsetzung von Richtlinien und die Sichtbarkeit von Bedrohungen, unabhängig davon, wie schnell die Umgebung wächst.

Unabhängig davon, ob Sie neue Server hinzufügen oder schrittweise aktualisieren, unterstützt Sie HPE iLO 7 durch umfassendere Transparenz und strengere Kontrolle dabei, Ihre Sicherheit aufrechtzuerhalten und zu stärken.



Transformieren Sie Ihren Sicherheitsansatz – jetzt offensiv statt defensiv.

Die HPE ProLiant Compute Gen12 Server mit HPE iLO 7 bieten einen Schutz auf Plattformebene, der Risiken senkt, Abläufe optimiert und die Einhaltung von Vorschriften unterstützt – damit Sie sich auf die Zukunft konzentrieren können.

Weitere Informationen finden Sie unter

[HPE.com/iLO](https://www.hpe.com/iLO)

[HPE.com/ProLiant](https://www.hpe.com/ProLiant)



[HPE.com besuchen](https://www.hpe.com)

[Jetzt chatten](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise (HPE) ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Aus dem vorliegenden Dokument sind keine weiterreichenden Garantiesprüche abzuleiten. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen in diesem Dokument.

a00148191DEE

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

