

HPE



eBook



HPE PROLIANT COMPUTE GEN12

For those who can't afford failure



The state of cybersecurity

Modern cybersecurity is a moving target.

No matter your industry or tech infrastructure, there are several elements at play that threaten the short- and long-term stability of your organization:

- **Attackers are growing more sophisticated and prevalent**
- **Compliance regulations are constantly shifting and evolving**
- **Audits are becoming increasingly more difficult to pass**

And it stands to reason that the biggest companies are the biggest targets where these things are concerned: They have the most to lose from a successful attack, or from falling out of compliance.

That's why it's vital to implement a technology platform that is secure by design, with built-in security, compliance, and resilience protocols end to end, from HPE's factories to your cloud.

Whether you work in finance, healthcare, infrastructure, or another of today's leading industries, your organization is a target because bad actors know **you can't afford failure.**

The good news? HPE knows that too. And we're here in your corner, ready to help you fight back.

Let's explore several cybersecurity use cases that will show you how to counter modern threats from every angle.



Top 10 most attacked sectors in 2023¹



Financial



Healthcare



Government

Professional Services

Retail

Industrial Services

Technology

Education

Manufacturing

Insurance





Financial services: the threat landscape

Sophisticated cyberattacks. Insider threats. Regulatory breaches. Changing compliance requirements.

Financial services organizations are engaged in a multi-pronged battle against sophisticated cyberattacks and constant compliance and regulatory shifts.

Your industry is particularly vulnerable because attacks, breaches, or violations can involve not just your institution's infrastructure, but your end customers.

Furthermore, these threats are attacking your most important workloads:

- Core banking platforms
- Fraud detection systems
- Payment processing gateways
- Regulatory reporting
- Front office systems and/or investment platforms

\$1.5 trillion

Combined amount earned by cybercriminals annually from attacks.²

30.9%

Total percentage of all attacks against the online payment and financial (banking) sectors in Q1 2025.³

33%

Increase in the total number of wire transfer BEC attacks observed in Q1 2025 compared to the previous quarter.³





Proactive protection for financial services

Ensure data integrity and compliance while scaling for high transaction volumes with HPE ProLiant Compute Gen12.

Backed by world-class Zero Trust security, HPE ProLiant Compute Gen12 servers proactively secure you and your customers or members' data while maintaining compliance and scalability.

How?

- **New HPE iLO 7 Silicon Root of Trust**
- **Embedded secure enclave for advanced encryption key storage**
- **Secure boot**
- **Runtime firmware verification**
- **Data encryption**
- **Trusted Platform Module (TPM)**



Our security and compliance protocols begin long before HPE ProLiant Compute Gen12 servers start helping your financial services firm with advanced workloads. HPE's Trusted Supply Chain practice requires that all hardware and firmware components undergo rigorous validation and traceability, ensuring security and consistency across the entire HPE portfolio.

So, partner with the organization that has security at the source. HPE protects your servers across all entry points, provides stronger encryption key storage, and offers seamless compatibility with leading security solutions like Commvault and Thales.

HPE ProLiant Compute Gen12: The server for financial services firms that can't afford failure.

What is "Silicon Root of Trust?"

Silicon Root of Trust is firmware technology that integrates security directly into the hardware level of HPE servers. It detects changes being introduced by cyber attackers and disables the server, so malicious code never penetrates and allows operation to quickly regain its original state.

66%

of high-performing organizations say it's a necessity for their tech infrastructure to leverage chips and/or certificates to alert them if a system is compromised during delivery.⁴





Healthcare: the threat landscape

Healthcare organizations are always preparing for what's next.

Providing quality patient care means navigating an ever-changing web of HIPAA and other compliance regulations while handling highly sensitive data.

Healthcare is particularly vulnerable because attacks, breaches, or violations can put not only your infrastructure at risk, but also the safety, privacy, and trust of your patients.

And these increasingly advanced cybersecurity threats can attack your most critical workloads:

- Electronic health records (EHRs)
- Clinical applications and imaging systems
- Patient monitoring devices
- Regulatory compliance reporting

Only **20%**

of organizations feel they are “highly effective” at keeping up with the modern threat landscape.⁵

74%

of ransomware attacks were aimed at hospitals.⁶

\$265 billion

is the estimated annual cost of ransomware to victims by 2031.⁷



When a small mistake becomes a big breach

A simple misconfiguration led to the accidental exposure of over a million patient records. Sensitive data was shared with a third party, triggering lawsuits and forcing the organization to notify patients and staff—even though there was no evidence the data was misused. For critical industries, the smallest slip can have massive consequences.⁸

If your organization is living in constant fear of a data breach and its impact on operations, revenue, and reputation, you can't focus on what matters the most: **Your patients.**





Secure sensitive patient data

You need a technology infrastructure that goes as above and beyond for cybersecurity as your healthcare organization does for patients.

HPE ProLiant Compute Gen12 proactively protects your data and systems from even the most sophisticated cyberattacks while ensuring HIPAA compliance. How?

- **New HPE iLO 7 Silicon Root of Trust**
- **HPE secure encryption**
- **Runtime firmware encryption**
- **Trusted Platform Module**
- **Secure management of all servers with [HPE iLO 7](#) and [HPE Compute Ops Management](#)**

The advanced, end-to-end capabilities of HPE ProLiant Compute Gen12 servers will secure you and your patients' sensitive data across all entry points. Our servers also offer seamless compatibility with leading security solutions, including Commvault, Thales, and Veeam.

It's time to safeguard against digital and physical attacks both outside and inside your organization with servers that are built from the ground-up with security in mind. HPE ProLiant Compute Gen12 embeds security and compliance at every phase of the server lifecycle, meeting the demands of healthcare providers now and in the future.

HPE ProLiant Compute Gen12: The server for healthcare organizations that can't afford failure.

What is HPE iLO?

HPE Integrated Lights-Out (iLO) is a unique, embedded ASIC technology and the core foundation for the intelligence of HPE ProLiant Compute.

HPE iLO is key to making the server operational with simplified server set up, hardened security features, system health monitoring as well as power and thermal control.





Public sector & critical infrastructure: the threat landscape

There is a very real human cost to cyberattacks and data breaches.

Disrupting public sector organizations, including those overseeing critical infrastructure, utilities, and defense, can halt essential services and threaten national security.

That means lives are on the line when it comes to your most important systems:

- Citizen services platforms
- Public safety and emergency systems
- SCADA systems
- IoT platforms
- Command and control (C2) systems
- Incident response systems
- Data integration platforms
- Geospatial intelligence

Moreover, critical infrastructure systems are foundational to public safety and national security. Organizations like yours often operate in highly classified environments, which means an internal breach, either intentionally or through employee error, can have just as catastrophic of an effect on your security and compliance posture.

~15%

of data breaches were tied to supply chain vulnerabilities in 2024.¹

52%

of organizations say identifying and authenticating IoT devices that access their networks is critical to their security strategy.⁴

16%

Only 16% of respondents in that same survey said they were highly confident that they knew all users and devices connected to their network at all times.⁴



Cyberattack Disrupts Government Operations

A cyberattack shut down Nevada state offices, websites, and phone lines for two days, forcing services offline while state and federal investigators scrambled to respond. Emergency services stayed online, but the disruption rippled across critical state operations.⁹





Meet public safety threats head-on

Protect your public sector organization and stay ahead of advanced persistent threats, physical tampering, unauthorized access, and other modern attacks.

With technology that counters evolving attacks and adapts to shifting regulations at every turn.

HPE ProLiant Compute Gen12 servers are the first industry standard servers to meet FIPS 140-3 Level 3 requirements, ensuring compliance with the most stringent regulations. That means end-to-end protection against the most insidious threats to public sector organizations, including ransomware, Denial-of-Service (DoS) attacks, and physical threats.

How?

- New HPE iLO 7 Silicon Root of Trust
- Secure networking
- Hardware-intrusion detection
- Military-grade encryption
- Role-based access controls
- Data availability
- Audit logs
- Zero Trust architecture

HPE ProLiant Compute Gen12 is post quantum ready to defend against tomorrow's threats, with compliance built-in, as the first to support NIST and CNSA 2.0.

Your organization is foundational to public safety and security, and you deserve a technology infrastructure that is built with security and compliance at the source.

HPE ProLiant Compute Gen12: The server for public sector organizations that can't afford failure.

What is "Zero Trust?"

Zero trust is a modern security model that never assumes trust—every user, device, and application must be continuously verified. By granting only necessary access and monitoring all activity, organizations reduce risk and protect their data.

Compliance built-in



FIPS 140-3

Federal Information Processing Standards publication 140-3 Level 3 certification



CNSA 2.0

Commercial National Security Algorithm





Security starts at the source

Don't be the next headline

- Russian hacking cartel attacks Costa Rican government agencies¹⁰
- TitleMax parent to pay \$12 million to settle data breach¹¹
- Largest water utility company in the U.S. targeted in cyberattack¹²
- Cyberattack forces closure of Nevada state offices for two days¹³
- Supply chain cyber attack hits UBS and Swiss banks¹⁴

Cybersecurity threats are unrelenting. That's why you need server protection that is just as unrelenting, from the manufacturing stage through end of life.

With HPE ProLiant Compute Gen12, next level security is built-in to safeguard every phase of the server lifecycle from manufacturing to end-of-life.

- **New HPE iLO 7 Silicon Root of Trust** ensures that every layer of firmware and software loads securely, providing an unbreakable chain of trust. This protects servers against firmware attacks, ensuring the highest level of data integrity and system reliability.
- **HPE Trusted Supply Chain** ensures that all hardware and firmware components undergo rigorous validation and traceability to prevent tampering or manipulation, ensuring nothing is altered from design to manufacturing to your facility.
- **HPE has a long history of designing and deploying platform security for the most secure operating environments across the most highly regulated industries.**

Make sure you're leveraging the newest, most sophisticated HPE ProLiant servers yet, so your organization remains well-equipped to counter modern cyberthreats now and in the future.



Because no matter what industry you work in, we know that **you can't afford failure.**

HPE: When you can't afford failure

We use the power of AI, cloud, and networking to help you move faster, work smarter, and achieve more. With deep expertise and bold ingenuity, we empower organizations to turn data into foresight, elevate performance, and drive real-world impact—at scale.

[Learn more →](#)



Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00151592enw

HEWLETT PACKARD ENTERPRISE

hpe.com



-
- ¹ StationX, 100+ Data Breach Statistics and Trends for 2025
 - ² Astra, 90+ Cyber Crime Statistics 2025: Cost, Industries & Trends
 - ³ APWG, Phishing Activity Trends Reports
 - ⁴ Ponemon Institute, The 2025 Global Study on Closing the IT Security Gap
 - ⁵ Ponemon Institute, The 2023 Global Study on Closing the IT Security Gap)
 - ⁶ Astra, 80+ Healthcare Data Breach Statistics 2025
 - ⁷ Cybercrime Magazine, 90+ Cyber Crime Statistics 2024: Cost, Industries & Trends
 - ⁸ TechTarget Network, Novant Health Notifies 1.3M Patients of Unauthorized PHI Disclosure
 - ⁹ CNN, Cyberattack forces closure of Nevada state offices for two days
 - ¹⁰ Russian hacking cartel attacks Costa Rican government agencies, The New York Times
 - ¹¹ TitleMax parent to pay \$12 million to settle data breach, Bloomberg Law
 - ¹² Largest water utility company in the U.S. targeted in cyberattack, NBC News
 - ¹³ Cyberattack forces closure of Nevada state offices for two days, CNN
 - ¹⁴ Supply chain cyber attack hits UBS and Swiss banks, Digwatch

