PUTTING ZERO TRUST TO WORK IN THE POST-QUANTUM ERA

HOW A CHANGING THREAT LANDSCAPE IMPACTS SERVER DEPLOYMENTS

SUMMARY

The ever-evolving nature of the cyber threat landscape ensures that new threats will keep emerging. While zero trust is a stated goal of every computer security incident response team (CSIRT), governance, risk, and compliance (GRC) unit, security operations center (SOC), and other IT target organization, it is seemingly unachievable. This is perhaps even more true in an era when AI is exploding, and post-quantum cryptography is moving from idea to reality.

While many security teams focus on multiplanar cyber threats with extended detection and response (XDR) platforms, the lowest operating level (ring 0) is often overlooked or assumed to be protected. However, it is here where the operating system kernel and drivers run with the highest privilege level, making it a particularly tempting target.

This research brief will explore the current cyber threat landscape and the impact AI, quantum, and other emerging technologies will have on cyberattacks and data hijacking today and in the future. Additionally, it will highlight what enterprise IT organizations can do at organizational, operational, and technical levels to create a strong security posture. Finally, this brief will demonstrate how HPE delivers the anchor for zero trust with its Gen12 platform, powered by its Integrated Lights-Out (iLO) 7 management chip.

THE EVERGREEN THREAT LANDSCAPE

Cyber threats have existed since we started connecting computers. In fact, in 1971, the Creeper program was created and successfully spread from computer to computer across ARPANET (the precursor to the internet) as an experiment in self-replicating programs. Decades of malware ensued.

More recently, ransomware has emerged to extort organizations for money or other purposes. In 2013, CryptoLocker was the first ransomware to employ military-grade (2048-bit) encryption for financial gain. While some may see the estimated $3 million extorted as insignificant, this ransomware propelled the cybercriminal movement and spawned the ransomware-as-a-service (RaaS) cottage industry.

Copyright © 2025 Moor Insights & Strategy

The cyber threat landscape is evergreen, continually evolving to evade the protections organizations put into place. While Creeper was simply an experiment to see if a program could replicate, later examples of well-known malware such as NotPetya relied on stolen digital signatures and evasion techniques, making them virtually impossible to detect. Like rootkit attacks, NotPetya attacked the master bot record with the sole purpose of absolute destruction.

The Current Cyber Threat Landscape — A Snapshot

While AI has dominated recent tech headlines, it is easy to overlook the continuous growth of the cybersecurity market. These interesting statistics help frame the current state of cybersecurity:

- Studies from Cybersecurity Ventures predict that cybercrime will cost the world economy $10.5 trillion annually by 2025,[1] with crime involving blockchain or cryptocurrencies (cryptocrime) accounting for $30 billion.[2]
- The primary attack vector for malware and ransomware is phishing, representing approximately 80% of reported cybercrimes.[3] While this number is stunning, the use of AI to hyper-personalize these attacks to mimic trusted individuals will make phishing even more dangerous in future years.
- The average length of a data breach is approximately 322 days. However, when AI is used to assist in cyber resilience, the time it takes to detect and contain vulnerabilities is reduced to 214 days. While delivering a reduction of 108 days (33%) is impressive, the duration that systems are open to data exploits is still alarming.
- While we think most cyberattacks are related to the more conventional "hacker breaches network through phishing" vector, the supply chain has proven to be a real vulnerability. In 2024, roughly 15% of data breaches were tied to supply chain vulnerabilities (including third-party software).[4]
- The lack of skilled IT professionals makes the grim outlook on security more dire. In 2024, a study from Cybersecurity Ventures identified 3.5 million open cybersecurity jobs worldwide.

[1] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, 13 November 2020.
[2] David Braue, "Cryptocrime To Cost The World $30 Billion Annually By 2025," Cybercrime Magazine, 19 April 2022.
[3] Nivedita James Palatty, "90+ Cyber Crime Statistics 2025: Cost, Industries & Trends," Astra Security, February 6, 2025.
[4] Gary Smith, "100+ Data Breach Statistics and Trends for 2025," StationX, 10 December 2024.

Copyright © 2025 Moor Insights & Strategy

With this data in mind, it is unsurprising that Moor Insights & Strategy (MI&S) finds technical and business leaders' optimism about AI's promise dampened by the more extreme threats the technology poses.

AI, Post-Quantum Cryptography, and the New Wave of Cyber Warfare

While AI is being deployed in the defense against cyberattacks, it has also emerged as a powerful new offensive cyber weapon for hackers looking for advantages in ransomware and malware. Unsurprisingly, AI is being used in several ways, with three of the more interesting being:

- *Advanced evasion:* Machine learning algorithms help ransomware mimic normal system behavior and automatically mutate code to evade detection by the security platforms employed by IT organizations.
- *Intelligent encryption:* AI can optimize encryption techniques based on available resources and data types, making decryption extremely difficult.
- *Self-learning malware:* Perhaps most insidious, autonomous malware can adapt to its environment and alter its behavior dynamically to bypass security measures.

While malware such as NotPetya and WannaCry were already very complex in profile and behavior, this new generation of AI-fueled malware makes protecting data exponentially more complicated. As such, it occupies the attention of CISOs and security organizations everywhere.

As AI has upped the malware game, quantum computing almost seems like science fiction. Yet it is quickly moving from concept to reality as both established giants like IBM and startups like Quantinuum and the HPE-backed IonQ are turning theory into practice, having already released multiple quantum processors.

Cloud providers have also entered the fray. For example, AWS enables organizations to consume quantum instances through its Braket service, which delivers the hardware, software, and integration to other services such as S3.

This all highlights that while quantum computing may be nascent, it is coming — and bringing with it a new set of challenges for cybersecurity. For example, quantum computers running Shor's algorithm can efficiently solve the complex math used in public-key cryptographic schemes such as RSA Diffie-Hellman. The logical result is quite apparent: Encrypted keys and secrets, once considered unbreakable, will be exploitable by bad actors using quantum.

Copyright © 2025 Moor Insights & Strategy

If this seems like something to be worried about several years from now, think again. One of the more diabolical approaches from hackers is the “harvest now, decrypt later” attack, in which hackers steal encrypted data and store it for when quantum technologies are mature enough.

Because of AI and post-quantum cryptography, MI&S sees the current cyber threat landscape as more challenging for enterprise IT than ever before.

HPE AND THE SECURE PLATFORM

HPE launched silicon root of trust as part of the 2017 debut of the 10th Generation ProLiant server protected by iLO 5 (MI&S delivered a detailed breakdown of this groundbreaking innovation in this research report). Silicon root of trust was invented to enable server platforms to boot into a known good state by creating an immutable fingerprint in silicon. This fingerprint, burned into iLO during manufacturing, includes the validated firmware and drivers that load in ring 0 before a server OS has even started to boot.

In addition to assuring that each of the millions of lines of code that run in a server’s pre-boot execution environment are authentic and unmanipulated, iLO verifies five essential firmware components:

1. *HPE iLO firmware*: Initializing iLO first ensures the system controller is secure and operational, enabling it to act as the foundation for all other firmware verification.
2. *System UEFI/BIOS firmware*: The UEFI (or BIOS) ensures all hardware is functioning correctly and trusted. It also prepares the server to locate and load the bootloader.
3. *System ROM firmware*: The system ROM works with UEFI/BIOS to ensure the hardware initializes securely. It also contains instructions for initializing components on the motherboard.
4. *Option ROMs*: Any additional hardware, such as network adapters or GPUs, have ROMs that contain required firmware.
5. *Bootloader firmware*: The OS bootloader loads the operating system kernel into memory. Prior to execution, the bootloader is validated against the immutable fingerprint stored in memory.

After the OS has booted and while the server operates, iLO uses AI-driven analytics (such as user and entity behavior analytics) and continuously scans firmware to ensure

Copyright © 2025 Moor Insights & Strategy

a pristine operating environment. If anomalies are detected, organizations can utilize tools within iLO to respond by identifying and removing the threat and restoring the server to a last known good state.

While this restoration capability began in ProLiant Gen10 with the iLO Amplifier Pack, it has since evolved to leverage newer technologies, such as UEFI, iLO 6, and advanced maintenance capabilities. This evolution is in response to the ever-changing threat landscape. As expected, HPE has evolved its portfolio with iLO 7 to take on the newest cyber threats.

Secure Supply Chain — Zero Trust Begins in the Factory

As previously noted, supply chain exploitation is real. More than that, it is perhaps the most insidious attack vector because enterprise IT organizations inherently trust the servers, infrastructure, and software they receive directly from a manufacturer.

However, the SolarWinds Orion IT vulnerability, disclosed in 2020, forced IT organizations of all sizes to view their software supply chain more skeptically. Likewise, the alleged embedding of chips and BIOS manipulation at a hyperscale server vendor, which was widely reported in 2018, led to more caution among datacenter architects.

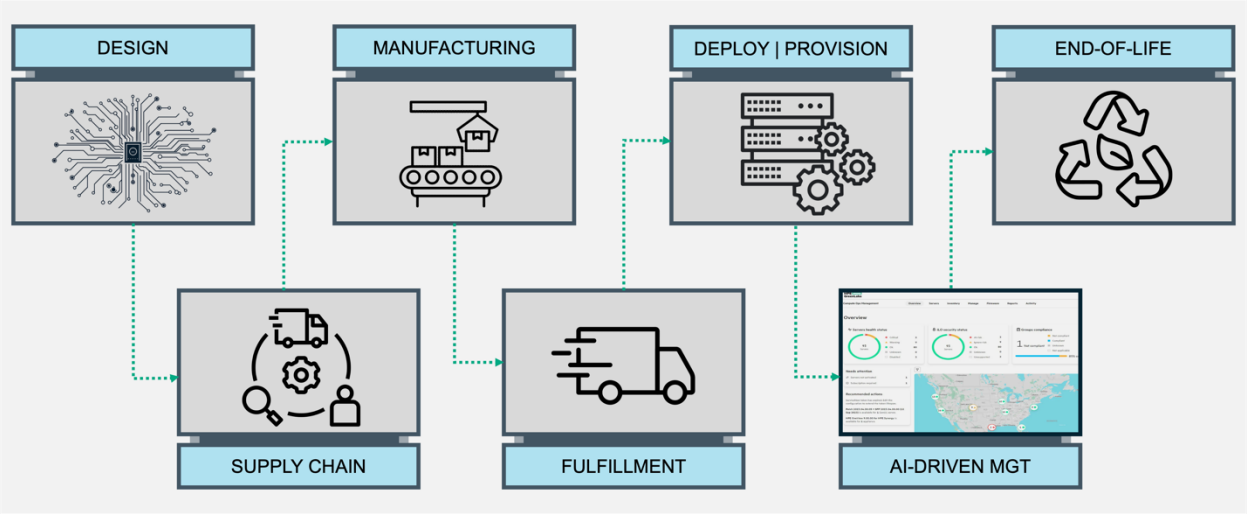
These incidents prompted a focus on a chain of trust that begins with the supply chain. In 2019, HPE launched its secure supply chain initiative to ensure that every component used to design, build, and run its servers comes from known and trusted sources validated through constant monitoring.

The chain of trust continues through the manufacturing process via HPE's secure manufacturing initiative. As part of this initiative, HPE servers are built in a highly secure facility with advanced features such as chassis intrusion detectors and configuration locks that prevent tampering during the build-out and delivery process.

Finally, chain of trust anchors a zero-trust environment with the previously detailed secure boot process and a continuous attestation that ensures operating environments are locked down — from the silicon up.

Copyright © 2025 Moor Insights & Strategy

FIGURE 1: SECURE FROM CONCEPT TO END-OF-LIFE



HPE creates a chain of trust from design to end-of-life.
Source: Moor Insights & Strategy

This focus on security across a server's lifecycle is critical for datacenter security. A secure chain of trust that begins long before server deployment prepares an operating environment, from the smallest startup to the largest hyperscaler, for the threat landscape of today and tomorrow.

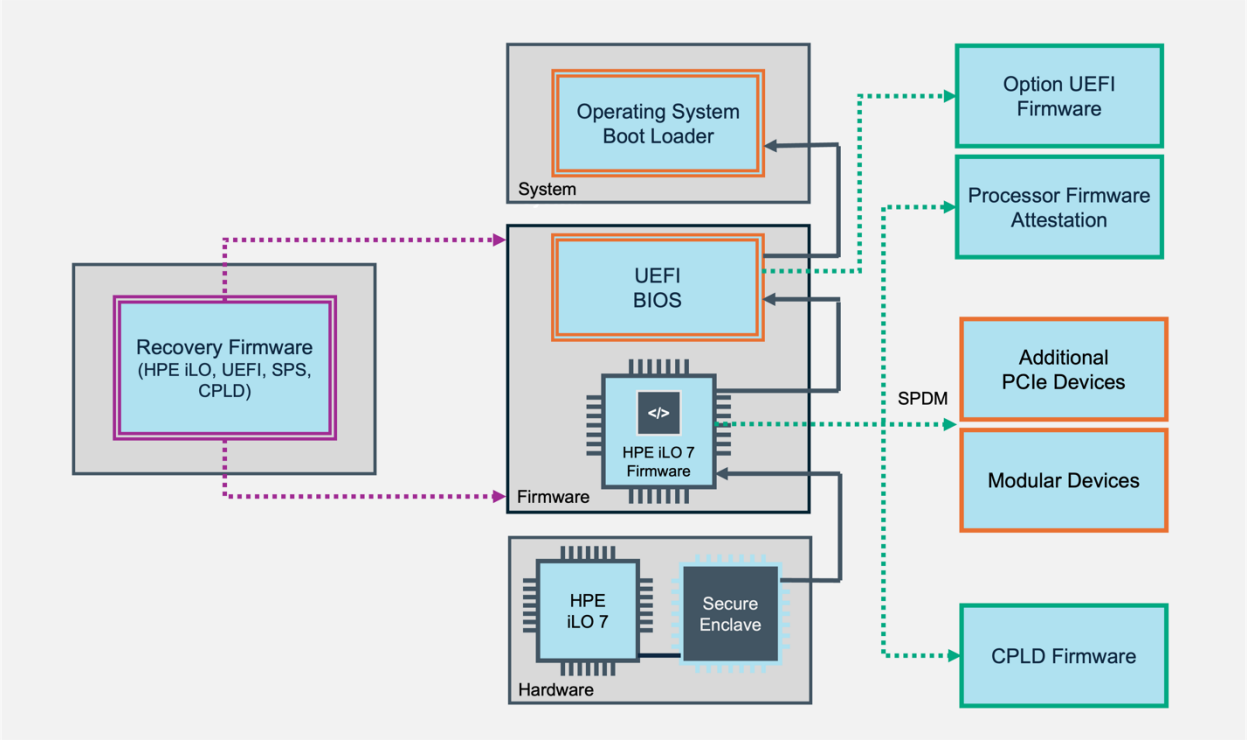
iLO 7 AND COM — SECURITY FOR THE POST-QUANTUM ERA

In ProLiant Gen12, MI&S sees HPE continuing to innovate by introducing iLO 7 and an enhanced security posture. Further, the combination of iLO 7 with the company's Compute Ops Management (COM) delivers the underlying technology and operational management of security needed in the enterprise.

Security begins in design. With iLO 7, HPE has taken its secure boot process and delivered multilayered protection through Secure Enclave, a discrete security chip built within the iLO baseboard management controller with quantum-resistant algorithms designed to protect keys, passwords, and security configuration information.

Copyright © 2025 Moor Insights & Strategy

FIGURE 2: SECURE BOOT WITH ILO 7 AND SECURE ENCLAVE



iLO 7 with Secure Enclave protects against post-quantum threats.
Source: Moor Insights & Strategy

It is worth noting that HPE ProLiant Gen12 servers adhere to the most stringent security standards, including FIPS 140-3 Level 3 certification. The FIPS 140-3 Level 3 standard introduced a new level of security required for tamper-resistance and stricter control of cryptographic modules. This standard is often applied to high-security environments such as governmental and finance-related compute. MI&S cannot identify any other industry-standard server that has achieved this certification.

The ProLiant Gen12 servers also support NIST and CNSA 2.0 quantum resistance requirements. These standards set requirements for algorithms to be deployed to resist both classical and quantum attacks. CNSA 2.0 has four quantum resistance requirements focusing on symmetric encryption, asymmetric key exchange, digital signatures, and hashing algorithms. Just as with FIPS 140-3 Level 3, MI&S cannot identify any other industry-standard servers that align with these stringent requirements.

While iLO 7 can deliver a secure boot environment for HPE ProLiant Gen12 servers, the industry-standard SPDM (Security Protocol and Data Model) attestation is also

Copyright © 2025 Moor Insights & Strategy

incorporated to continuously verify the integrity of the server's devices throughout the lifecycle. This is done by continuously validating each device's state against a cryptographically secured baseline.

The ability to actively monitor and manage the security of the distributed computing environment is critical to maintaining a secure operating environment. This is where COM particularly delivers value. From a single console, IT security professionals can quickly respond to incidents and employ automated controls to ensure compliance with organization standards.

It is evident to MI&S that security is a critical pillar of HPE's strategy. While many view security through the lens of post-server deployment, HPE has designed and built the foundational elements of a zero trust environment.

Five Must-Do's for a Post-Quantum Safe Environment

The risk created by a post-quantum environment is rooted in math. At some point, quantum computers will be able to quickly perform the complex math required to break the cryptographic methods underpinning current cybersecurity platforms. With this threat on the horizon, IT organizations must begin establishing a quantum-resistant/quantum-safe environment.

Five critical early steps are:

1. *Understand your current environment.* Perform an audit of all encryption mechanisms employed across the environment, including networking, software, and devices. Include audits of edge environments, where vulnerabilities are perhaps the greatest. This allows security professionals to develop a baseline from which to operate.
2. *Be crypto-agile.* Where possible, design systems so that cryptographic algorithms can be replaced with minimal disruption. Enabling systems to transition more seamlessly to NIST-approved post-quantum algorithms such as ML-KEM (key exchange) and ML-DSA (digital signatures) will minimize the cost and resources required to evolve.
3. *Follow the standards.* The U.S. government (and other regulating bodies around the globe) has been proactive in responding to quantum computing. Follow guidance regarding algorithms to deploy.

Copyright © 2025 Moor Insights & Strategy

4. *Start testing today.* Algorithms such as ML-KEM and ML-DSA are available for organizations to experiment with today. Do not wait for quantum computing to become mainstream.
5. *Evolve your zero trust mindset.* Build quantum resistance into the zero trust architectures deployed today. Zero trust evolves based on new threats such as quantum. This requires organizations' deployed technologies to evolve as well.

MI&S has found the Post-Quantum Cryptography Alliance from the Linux Foundation to be a good resource for enterprise IT organizations to learn and stay informed about operating in the post-quantum compute environment.

Zero trust in the post-quantum era begins with the infrastructure deployed. This known secure state must be validated and (securely) handed off up the operating stack to ensure that the zero trust environment is maintained from the server, across the datacenter, to the edge, and in the cloud. With ProLiant Gen12 platforms, MI&S sees HPE as uniquely positioned to deliver the foundation of the zero trust environment.

Call to Action

Cybersecurity can be described as a complex game of chess, where pawns can morph into bishops and rooks can morph into queens. In the time it takes vendors to respond to a new enterprise IT security threat, several new and more challenging threats can emerge that impact even more organizations.

As the threat landscape has evolved from crude and simple schemes to malware that can go undetected for nearly a year, the next phase of AI and post-quantum threats is exponentially more dangerous. While malware sophistication and attack methods increase at seemingly breakneck speed, a zero trust architecture rooted at the foundational levels of infrastructure is critical. It is not simply a marketing slogan for security, but the embodiment of deep levels of protection that guard against the threats of today and tomorrow.

HPE has a long history of designing and deploying platform security and has been an anchor vendor for the most secure operating environments across the most highly regulated industries. With the HPE ProLiant Gen12 server platform, the company has extended its protections through iLO 7, Secure Enclave, and COM. Combining these innovations with its secure supply chain, the company stands alone in its adherence to and certification for the most stringent requirements from regulatory bodies.

Copyright © 2025 Moor Insights & Strategy

While performance is critical to the modern enterprise, absolute performance should not come at the expense of security. Because of this, MI&S believes the HPE ProLiant Gen12 platform requires serious consideration from IT organizations of all sizes that are building and deploying applications for today and tomorrow.

For more information, please visit: hpe.com/iLO

Copyright © 2025 Moor Insights & Strategy

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Matt Kimball, Vice President and Principal Analyst, Datacenter Compute and Storage

PUBLISHER

Patrick Moorhead, CEO, Founder and Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be mentioned in context, displaying the author's name, title, and "Moor Insights & Strategy." Non-press and non-analysts must receive prior written permission from Moor Insights & Strategy for any citations.

LICENSING

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared without Moor Insights & Strategy's prior written permission.

DISCLOSURES

HPE commissioned this paper. Moor Insights & Strategy provides research, analysis, advice, and consulting to many of the high-tech companies mentioned in this paper. No employees at the firm hold equity positions with any of the companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy 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 Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, 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 opinions only 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 Moor Insights & Strategy. Company and product names are used for informational purposes only and may be trademarks of their respective owners.