Hewlett Packard Enterprise | intel

Brochure

Confidence at the core

With industry-defining protection that's built into the silicon, Hewlett Packard Enterprise builds the world's most secure servers.[1]

Get started >

[1] Based on external firm conducting cybersecurity penetration testing of a range of server products from a range of manufactures, May 2017.

Table of contents

Revolutionary technology rises to the top

Hardware-forged security should be a market differentiator and for world-leading defense, retail, and federal security agencies, it already is. Here are just a few real-world stories of large-scale early adopters.

Keeping enemies at bay
Recently, HPE worked with a European defense agency that was introduced to our Silicon Root of Trust technology. This particular defense customer had been paying huge sums of money each year to develop and deploy the same type of protection that HPE delivers free of charge with the **HPE Integrated Lights Out (iLO) 5** silicon-based security.

After a few presentations and conversations about the HPE cryptography, the defense agency immediately bought hundreds of **HPE Gen10 Servers**. They also purchased the HPE trusted platform module (TPM), the chassis intrusion detection device, the secure encryption license, and the HPE iLO license for each and every HPE ProLiant Gen10 server.

HPE continues to actively communicate with this valued customer, who is now helping to guide some of our future security designs based on the advanced security threat trends they see in the defense industry.

Continued on next page >>

In the shadow of innovation

The threat landscape is a dark mirror on technology advancements

How do you keep your eye on a target that's always moving, shape-shifting, and putting on new disguises? It's a little bit like staying focused on the latest trends in cybersecurity and it's a challenge for even the most security-conscious IT organizations on the planet.

But that shouldn't come as a surprise to IT professionals. **Threats and tactics have evolved** with just as much speed and innovation as the technology landscape itself.

Each time a new IT trend takes shape, hackers and cybercriminals find ways to exploit it. **Cloud computing**, the **Internet of Things (IoT)**, and mobile devices—all promise massive advantages to business and all offer a golden opportunity for those who seek to benefit from them illegally.

From this angle, it may be tempting to approach threat management based on the unique vulnerabilities of each new tech trend—biometrics for mobile devices, edge software solutions for IoT, and strategic application migrations for cloud. But by the time your organization has begun to address those exploits, others will be launched.

<< Continued from previous page

Protecting consumer trust
In the U.S. retail landscape, HPE provided technical training on our advanced Gen10 security features. A large retail enterprise sent nine of its employees to the HPE security training to see what significant advances we are delivering in its server product line.

After the full-day training session, the retail customer's employees were so impressed with the HPE Gen10 security model that they bought thousands of **HPE ProLiant servers** and have pending orders for several thousand more.

Safeguarding federal information
In the U.S. Federal sector, one large agency issued proposal requests that required such strict adherence to true silicon-based security that only HPE was able to meet their requirements.

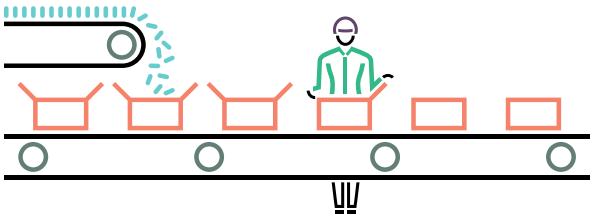
Federal customers are often very cognizant of security advancements and, generally, require IT products with the most advanced protection. Since only HPE has true silicon-based protection and the ability to not only detect intruders but also recover from any malware or compromised firmware code, we were immediately awarded the sale of several hundred HPE ProLiant Gen10 servers.

Watch Patrick Moorhead discuss why companies should pay more attention to firmware threats.

It's no longer a question of "if" your organization will be attacked. It's all about when. Security threats follow new innovations like shadows. They are inseparable and inevitable. And attacks that involve the human element—such as email phishing scams, carelessly guarded USB storage devices, or passwords left out in public—will always be problematic.

Attackers will strike wherever there are weaknesses and opportunities. Recently, hackers have had well-publicized success exploiting firmware in everything from home IoT devices to routers and even data center servers.

And while we can't stop attacks from occurring, there might be better ways to prevent attackers from getting what they want. The good news is that suffering because of a breach is completely avoidable.



Security in the silicon and supply chain

Firmware-level protection that safeguards infrastructure

It's time for a new way to think about security that goes beyond the firewall, beyond software, to protect the heart of your infrastructure where it counts the most—at the heart of your server infrastructure.

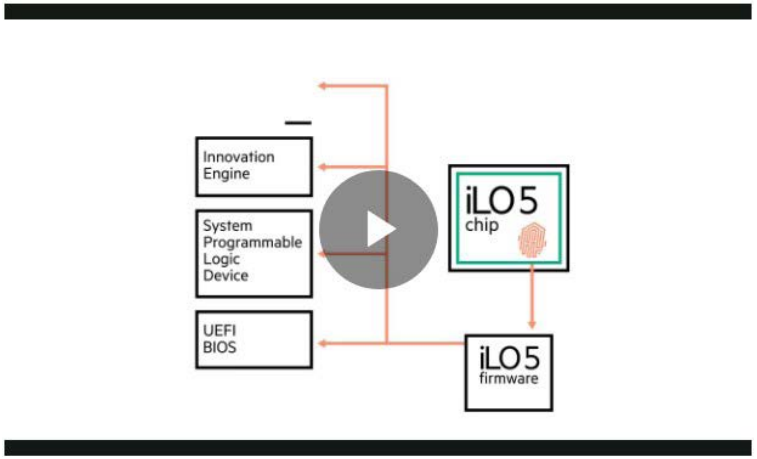
With HPE Gen10 Servers, we offer the first industry-standard servers that include a Silicon Root of Trust built directly into the hardware itself. This binds all the essential firmware—UEFI BIOS, complex programmable logic device, innovation engine, and management engine—into the silicon before the server is even built. And we're working with Intel® on the security features of its latest Intel® Xeon® processors to build an ecosystem that puts security first.

Think of it as an immutable fingerprint embedded in the silicon of the HPE iLO chip. For years, HPE has delivered a suite of remote management and monitoring features from its custom HPE iLO chip. Across our HPE Gen10 product line, we're introducing HPE iLO 5, which enables firmware to be authenticated as far back as the supply chain.

When the server boots up, the firmware looks for the unique fingerprint buried in the silicon to see if it matches the firmware fingerprint. Once the silicon fingerprint is verified, the rest of the essential firmware is allowed to boot and scan itself, looking for a bad code along the way.

If at any point, a hacker has inserted a virus or compromised code, the runtime firmware verification capability will detect it immediately and the customer is alerted.

Once a breach is detected, customers have three options. The server can be recovered to the last known good state of firmware, restored to factory settings, or, alternatively, the customer can choose not to recover so security teams can take the server offline to perform forensics.



Learn how the HPE iLO 5 chip, with Silicon Root of Trust, protects HPE servers from attacks, detects potential intrusions, and enables secure firmware recovery.

Why aren't our competitors doing this? HPE designs its own silicon and firmware, while the competition relies on off-the-shelf firmware. Our investment in your security is what differentiates Silicon Root of Trust from other manufacturer's claims of a hardware root of trust.

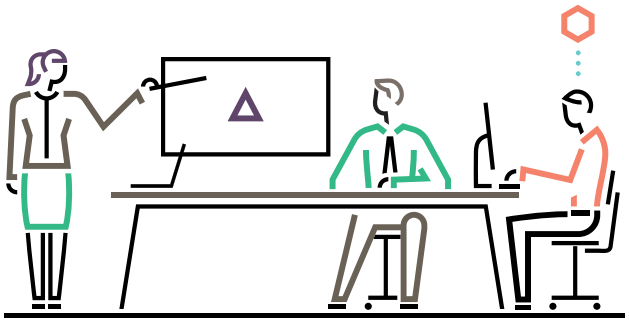
Together, the firmware and the silicon create a bond that cannot be broken. That bond is forged at the very beginning of our build process and carries through every element of the HPE supply chain.

At every touch point—from materials suppliers to logistics and transportation services, from production and assembly to warehousing and distribution—our suppliers are required to comply with our policies, as well as ISO standards and the Defense Federal Acquisition Regulation Supplement.

And we assure supply chain compliance through risk-based security audits, program monitoring, inspections of electronic parts, component traceability, and material control processes.

When analyzing potential threats, don't forget to consider who may have interacted with your server before it was installed in your data center. We have. And it's another reason you can trust HPE.

But don't just take our word for it.



Two generations ahead of the competition

How HPE differentiates and delivers deep security

We put HPE Gen10 Servers with Silicon Root of Trust head-to-head with the competition in an intrusion test by **InfusionPoints**, an independent cybersecurity solutions expert.

InfusionPoints approached the test from the perspective of a black-hat attacker, according to Jason Shropshire, Senior Vice President and CTO at InfusionPoints.

For Shropshire, the fact that HPE was even willing to put its Gen10 servers alongside its competitors made a lasting impression. “Nobody else is really doing this—comparing the security of their products like this in a black-hat setting. There’s a lot of benchmarking and performance testing, but this was a really unique hardware-level test,” Shropshire says. “It tells me HPE is taking this very seriously. But they knew what they had, and they came in with a lot of confidence.”

Shropshire and team specifically looked at the kinds of attacks they could make against the BIOS or other firmware on the servers. “As advances have been made in operating system and platform security, attackers have really turned their focus toward platform firmware and embedded systems,” Shropshire explains. “They’re looking at gaining persistence and if they can’t gain a foothold on the application or the operating system, they’re going to look for other vectors.”

Before a typical server even finishes booting up, the firmware runs a million lines of code. That’s where software scanners can’t detect malware and that’s where hackers are trying to go.

Learn how HPE built the Silicon Root of Trust and the most secure industry-standard servers.

So how did HPE Gen10 Servers stack up?

"Our team conducted numerous tests: including attacks against physical interfaces, platform firmware, and network interfaces. Initial test results show that the HPE Gen10 Server takes a significant step that puts it up to two generations ahead of their competitors," Shropshire reports. "Specifically, we believe that HPE's introduction of Silicon Root of Trust will set a new standard in providing auditable control of the integrity of platform firmware. HPE's overall forward-leaning security culture touches all phases of the Gen10 platform lifecycle including design, implementation, and maintenance."

It's a validation of three years of research and development for HPE that sees us in not just a unique position in the market, but a strong thought leadership position in the security landscape.

"One of the things that impressed me about HPE's approach is their good corporate citizenship with Gen10," Shropshire explains. "They're making a platform that's going to implement tens of thousands of IP addresses—those systems will be much more secure, and won't be able to become an attack platform for attackers."

Value for every vertical

Deep security regardless of industry or business size

So how can HPE help your enterprise, government entity, or small-to-medium business respond to firmware-level attacks? The HPE Gen10 product line offers security at the silicon and supply chain level regardless of the server line you purchase.

For enterprise and government agencies, we offer HPE ProLiant **rackmount servers**, **HPE BladeSystem server blades**, and HPE Apollo Systems high-density and **high-performance computing (HPC) servers**. For smaller businesses and remote branch offices, the HPE ProLiant ML series tower servers offer the same Silicon Root of Trust as the more powerful servers.

In government

These HPE Gen10 security advances have seen increased interest in the government sector. A recent review by **FedTech Magazine** shows how HPE ProLiant DL380 Gen10 Servers can secure nearly any Federal IT environment.

By offering a flexible range of configurations, the HPE ProLiant DL380 Gen10 can be deployed as part of a private cloud, anchor VM delivery, facilitate secure container environments, store database applications, and process **Big Data** transactions.

And HPE iLO 5 technology offers **four different levels of security**, based on customer needs and industry regulation. By default, HPE Gen10 Servers ship in production mode but can be upgraded to high-security mode for increased encryption sophistication, Federal Information Processing Standards (FIPS) mode for federal processing standards, and Commercial National Security Algorithm (CNSA) mode, which offers the highest level of cryptographic algorithms that meet standards set by the National Security Agency.

In retail

In today's online marketplace, more than 90% of login attempts at retail sites are made by hackers. More than 2.3 billion usernames and passwords were reported stolen in 2017, leading to potential losses of $50 million each day. Even with fraud prevention measures intact, actual losses are estimated at $5 million per day or $1.6 billion per year.[2]

And it's not just about stealing passwords. At the enterprise level, retailers are doing a lot more than processing transactions online—they're moving products around the world and sourcing new and existing materials with sophisticated enterprise resource planning (ERP) systems while trying to protect crucial employee and customer information.

It's where security differentiators built into HPE Gen10 Servers become business differentiators for retailers who succeed or fail by customer loyalty.

In logistics

Getting materials and products from one place to another is a lot more complex than it sounds. In human history, just about every mode of transportation has become vulnerable to crime in one way or another. And in today's intricate threat landscape, it's about a lot more than theft.

At each touch point, each factory, each transfer, each warehouse, and each delivery there exists an opportunity for bad actors to make unwanted modifications to products on their way to the end user. It's a pervasive problem and HPE has taken great strides to understand, as well as overcome so we can protect and validate our own secure supply chain.

Embedding secure solutions into the silicon of HPE Gen10 Servers has given a major logistics and delivery service enough confidence to deploy **HPE servers** in its data centers.

Everywhere else

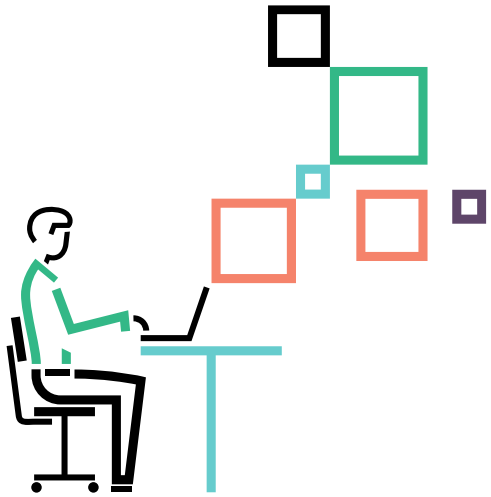
While security breaches can cause nuisance, fines, and loyalty issues for the enterprise, those same threats can have devastating effects on small and medium-sized business (SMB).

In fact, most SMBs can't survive a significant breach with their business intact—60% will go out of business after six months. It doesn't help that more than 70% of attacks target small businesses. And about half of all small businesses have already experienced a cyberattack.[3]

By building firmware validation directly into our silicon, HPE is trying to make security as fundamental as possible, and that's good news for SMBs who often don't have IT budgets and staff to fight the security battle day to day. If we can simplify security at its most basic level, we can help you outsmart the next attack.

[2] **2018 Credential Spill Report, Shape Security**, July 2018

[3] **60 Percent of Companies Fail in 6 Months Because of This, Inc. Magazine**, May 2017



Protecting what's next

HPE builds the world's most secure servers, but that's not all.

Security threats to your business data and systems are steadily increasing, with attacks being more complex and attack surfaces shifting from network perimeter, software, and applications to the physical platform itself.

Network firewalls, antivirus scanning, and even security monitoring tools aren't enough, because they can't detect firmware tampering. HPE is committed to increasing the security level in all three critical pillars of the environment—protect, detect, and recover—so customers can be confident that their infrastructure is secure from threats, even at the firmware level.

With a deeper, immutable level of trust that is part of the silicon, HPE is the only manufacturer of industry-standard servers with security that's two generations ahead of the competition.

Need guidance on your security journey? **HPE Pointnext** offers design and implementation services to further extend and complement the built-in security features in the HPE Gen10 Servers.

Let HPE help you protect your business, your customer, and what comes next.

Resources

- Video: **How to Prepare for and Recover from a Ransomware Attack**
- Article: **IoT and Edge Computing: The Wild West of Cybersecurity**
- White paper: **Server infrastructure security solutions for GDPR compliance**
- Video: **Defeat hackers before they attack: Europol and the FBI on best practices**
- Video: **How secure is your server? | Defending against hardware hacking**
- HPE iLO product page: **HPE Integrated Lights Out server management software**
- White paper: **Comprehensive Server Restoration**

Learn more at
hpe.com/security

Share now

Get updates

a00068331ENW, March 2019