HPE Locks Down Server Security

New security levels for more complex environments & increased threats

Executive Summary

Security is a looming issue for businesses. The threat landscape is increasing, and attacks are becoming more sophisticated. Emerging technologies like IoT, mobility, and hybrid IT environments now open new business opportunity, but they also introduce new risk. Protecting servers at the software level is no longer enough. Businesses need to reach down into the physical system level to stay ahead of threats. With today's increasing regulatory landscape, compliance is more critical for both increasing security and reducing the cost of compliance failures. With these pieces being so critical, it is important to bring new levels of **hardware** protection and drive security all the way down to the supply chain level. Hewlett Packard Enterprise (HPE) has a strategy to deliver this through its unique server firmware protection, detection, and recovery capabilities, as well as its HPE Security Assurance.

Today's Customer Needs

Technologies like cloud infrastructure, the Internet of Things (IoT), mobility, and software-defined infrastructure can deliver many benefits, including better agility, more innovation, deeper customer relationships, and better business economics. But with those benefits come significant challenges to protect critical data, as these complex ways of using IT expose businesses to more threats. Previously, many believed that a strong perimeter, with limited client and data access, was all that was required to protect IT assets. But as new ways of doing business are extending IT out beyond the datacenter, the need to protect and secure from a new perspective is paramount.

When IT controlled all compute, setting security was less complex. Cloud technology changes that dynamic. Although cloud providers deliver SLAs for data service, most do not have the same service level agreements for security. Data access is changing through mobility and cloud, with more distributed east-west traffic and a less hierarchical structure than the more tightly controlled models of the past. In the new world of hybrid IT, the lines are blurred and the perimeter is fluid, changing with the needs of the business. IoT, for instance, is quickly changing the security focus from a pure software discussion into a **hardware and firmware** discussion because of the proliferation of devices that must now be comprehended. Enterprise protection must happen from the edge to the core to the cloud.

Copyright © 2017 Moor Insights & Strategy

Security continues to be one of the most important aspects of protection for businesses today. But it is not just about keeping people out; the focus needs to be on protecting the assets of a company. A 2016 Ponemon Institute report on the cost of cybercrime estimated that the 720 million daily hack attempts led to $455B in costs for 2016 alone. More startlingly, 60% of the small businesses that suffer a cyber-attack go out of business within 6 months. The $9.5M average annualized incident cost is on the rise, increasing an estimated 21% over the previous year, due mostly to denial of service attacks, malicious code, and web-based attacks.

Threats are escalating. “Smash and grab” crimes of opportunity have changed to more methodical, longer-term attacks that can compromise a company for weeks or months. This dynamic indicates that not only are larger, more sophisticated criminal elements involved, but also more rogue nation states are turning to cybercrime.

Ransomware is on the rise. At least 14 hospitals were attacked in 2016 and San Francisco’s MUNI transport system was compromised in a high visibility attack. This threat is expected to grow sharply with Ransomware as a Service (RaaS) creating an explosion of potential attackers and lowering the barriers to entry for cybercrime. Businesses are especially vulnerable to ransomware, because they can more quickly pay with deeper pockets than consumers, making them a better target.

Not all security threats are focused on malicious actors. Sometimes the danger is more benign. Government regulations are another part of the security puzzle, as failure to properly secure data can have an additional financial toll on businesses. The European Union’s General Data Protection Regulation will go into effect in May 2018, requiring notification “without undue delay” along with sanctions of up to €20M or up to 4% of revenue, adding costs to a cybercrime incident. In the US, industries like healthcare have regulations like HIPAA that govern the storage, handling, and security of data, and the payment card industry has PCI-DSS to cover how transactions are secured. Combining the cost of an attack with the cost of regulatory punishment escalates the financial impact, putting a sharper focus on the potential financial pain of a cyberattack.

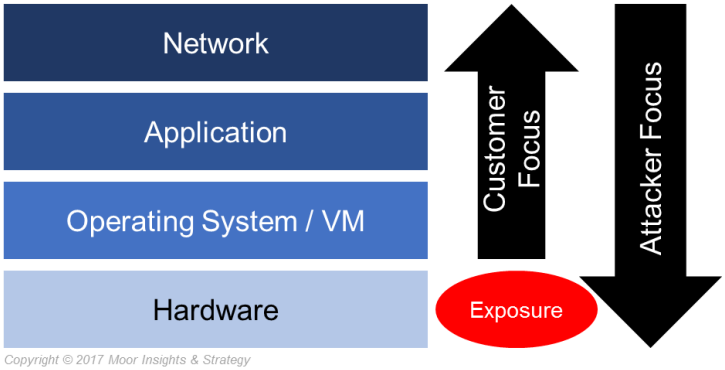
HARDWARE IS MORE EXPOSED TODAY

Many may see security as a software-led discussion. However, the conversation needs to begin much lower, **at the hardware level**, if businesses are interested in truly securing IT. Hardware-level security issues can create a large blind spot for organizations, as issues could hide for weeks, months, or years before being discovered, because most tools assume that hardware is secure. The recent Mirai and

Copyright © 2017 Moor Insights & Strategy

Dyn attacks were gigabit-level DDoS attacks driven by IoT devices. These events highlight that attacks are starting to move down the stack, targeting firmware and hardware instead of the more watched application software and operating systems. Hardware is more difficult to protect, because it is traditionally isolated from security monitoring / intelligence. In most security monitoring, the hardware is "assumed secure" which can be a major miscalculation. This situation is slowly changing but not fast enough. McAfee, for instance, now checks firmware in its BIOS scans, but it only occasionally compares the current BIOS snapshot to the original.

FIGURE 1: HARDWARE IS THE NEWEST VECTOR FOR ATTACKERS



Source: Moor Insights & Strategy

Exploits that sit in firmware are more insidious, because the system and the OS are not generally designed to enable privilege to higher layers, creating a hidden exposure once the hardware is compromised. Missing an enemy when sweeping a site presents an opportunity to be attacked from the rear where an army is exposed. Hardware and firmware-level exploits could hide for a long time before being discovered and can be pre-programmed to exploit resources at a predetermined date in the future.

The supply chain is an equally vulnerable arena for hardware. Cisco suffered intercept issues with shipments that were accessed in transit and altered. Supermicro servers in the Siri development lab at Apple were found to have malware on them that had been introduced directly from its server manufacturer's own website. Even server, storage, and security giant IBM had to admit that malicious exploits were accidentally shipped on USB flash drives used for enterprise system configuration. This indicates a chain-of-custody issue for the manufacturer regarding its supply chain or potentially those who were supposed to sign off on the validity of the product. Hard drives may also be a target. Kaspersky uncovered a firmware hacking tool that enables the firmware of a hard drive to be compromised. Because most hard drive manufacturers do not

Copyright © 2017 Moor Insights & Strategy

cryptographically sign the firmware installed on drives, this creates yet another opening for a compromise. These issues highlight the fact that not all exploits are accidents; businesses need to also look at the integrity of the supply chain as part of their security.

As mobility rises within the enterprise, these devices also introduce plenty of risk into the equation. Recently CheckPoint identified malware in the vendor-supplied ROM on Android phones that were sent to a communications company, potentially impacting hundreds of thousands of devices.

Dealing with hardware and firmware vulnerabilities needs to be addressed, but it will take time, just as seatbelts and airbags took time to permeate the automotive market, first as a premium option and eventually as a mandated standard safety requirement.

With Hardware as the Target, OEMs Need to Change

There is currently a low bar in the industry for hardware security, which is why attackers are turning to hardware and firmware for their exploits. While harder to accomplish, once compromised there is less likelihood of detection. Google recognized the importance of security and demanded it at the hardware level. Google's own internally designed security processor is custom silicon that it developed specifically because the industry was not keeping pace with the vulnerability complexity.

While there is some hardware variance in the industry, HPE estimates 20% of the platforms in the market share enough common hardware components to enable a large pool for attack. Firmware, the lowest level of the platform, is also the most vulnerable, because many manufacturers share firmware and BIOS code from their ODM design houses. This code is the lowest level of system operation and is incredibly complex, with over 1 million lines to execute just to initialize and boot the server.

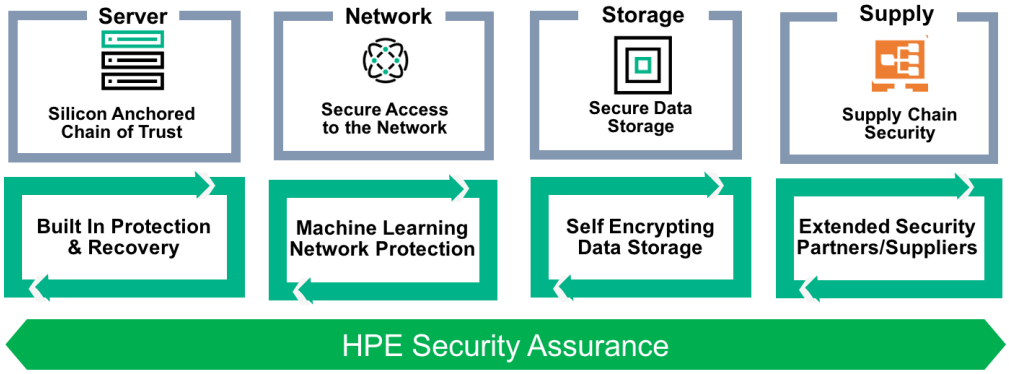
IT should take a special look at where these components come from within their supply chains, because currently there is much sharing in the industry and less custody of control by many manufacturers. Companies like HPE hold strict control over their firmware code, but across the industry such control is more of an exception than a rule. Additionally, once the server leaves the manufacturer, what is the chain of custody for that product in the channel? Both are serious issues that must be assessed as part of the security audit for any new platform standardization exercise.

HPE has defined its security framework around its idea of Security Assurance, which focuses on a broad set of security capabilities and strategies that protect systems. Protection comes from hardening the hardware, using intelligence to better detect

Copyright © 2017 Moor Insights & Strategy

anomalies, adding encryption down to the component level, and then securing through its partners and supply chain. HPE believes this strategy helps enable the highest levels of security.

FIGURE 2: THE HPE SECURITY ASSURANCE STRATEGY



Source: Hewlett Packard Enterprise

HPE BOOSTS SERVER SECURITY WITH SILICON ROOT OF TRUST

HPE began with one of the strongest security statements when it introduced its 9th generation platforms. As the 10th generation comes to the market, HPE increased the physical security, claiming that these new servers are the most secure in the market.

Each HPE platform has a root of trust that is burned into the silicon components on the motherboard, making it literally impossible to compromise, because the system cannot boot without this circuitry. This silicon root of trust begins with the HPE iLO management controller, which is an HPE-specific design, much more advanced than the more generic and lower cost Aspeed BMC popular with many other vendors.

HPE iLO's intellectual property is owned solely by HPE, and it owns the firmware as well, with a strict process for both access and sign off on changes. This is a large differentiator that HPE can deliver, because it designs and produces its own products. Even the software operating environment for iLO is different. iLO utilizes HPE-controlled software tools, making it more difficult to compromise relative to the more generic Linux-based tools that most other vendors use for their management controllers.

HPE focused on the National Institute of Standards and Technology (NIST) security framework of protect, detect, and recover when building its unique silicon root of trust capability into 10th generation servers.

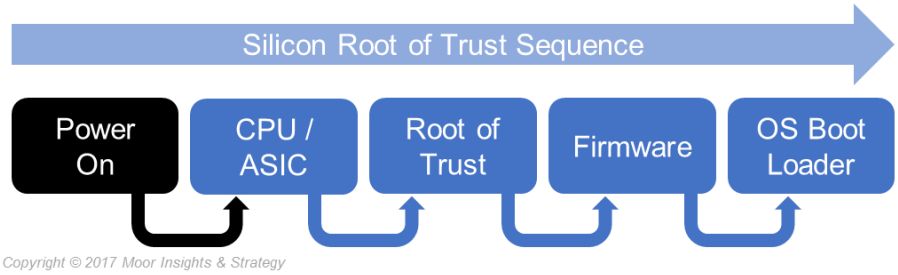
Copyright © 2017 Moor Insights & Strategy

Protection against firmware attacks is enabled by a silicon-anchored chain of trust. At boot, the iLO is the first device initialized. The system cannot continue without that first handshake to iLO, setting this HPE-specific device as the basis for the entire secure initialization. The handshakes continue to extend the protection throughout the chain, all the way up to the operating system and applications, ensuring a clean handoff of known good credentials with a continuous protection stream.

Detection is enabled in this design through HPE's unique daily automatic scanning of the firmware. Upon discovery of compromised firmware code or malware, which is normally invisible to most other systems, the server will launch into recovery mode.

Recovery, if needed because of any anomaly, enables the system to automatically recover firmware back to a previous authenticated state. In an unprecedented level of security, even that previous state is checked for integrity. Any issue there forces a reset back to the original factory firmware which is held in yet another different location.

FIGURE 3: SILICON ROOT OF TRUST SEQUENCE



Source: Moor Insights & Strategy

Further enhancements to HPE systems' physical security are delivered through Enterprise Secure Key Management, which is a complete management solution to secure storage, server, and cloud together. As enterprises move more compute towards the edge, businesses will find greater value in being able to drive security consistency across their distributed enterprises. To protect data at rest, 3Par storage features self-encrypting drives, and HPE Secure Encryption works through the SMART Array Controller to automatically encrypt data at rest. This feature helps bring businesses into compliance for regulations like Sarbanes-Oxley, HIPAA, and others through the hardened encryption and ability to store / manage keys remotely.

To protect the network and deliver network access control, the HPE/Aruba ClearPass Policy Manager identifies devices, enforces policies, and protects the network. Niara, a recent purchase for HPE, integrates into these tools, using advanced monitoring and

Copyright © 2017 Moor Insights & Strategy

behavior analytics to track user, device, and system behavior, more rapidly identifying and responding to anomalies. Niara enables the ability to watch machine-to-machine interaction to identify suspicious activity that could be tied to hardware.

IN-DEPTH CERTIFICATIONS & COMPLIANCE

HPE goes further than most with its quest to bring more certifications to its platform, enabling businesses to deploy with confidence that they are in full compliance with security regulations and advanced standards. To back its claim of the most secure servers available, HPE points to the following collection of security compliance certifications and integration with leading security tools:

- The Commercial National Security Algorithms (CNSA), used for handling top secret information
- US FIPS 140-2 validation of cryptographic modules
- HPE equipment with NIST 800-53 controls, providing a secure baseline. Customers can leverage this to pursue compliance with ISO27001, HIPPA, DFARs, and NERC
- Because HPE meets requirements like FIPS and Common Criteria, it helps facilitate customers' achieving Federal Risk and Authorization Management Program (FedRAMP) with Authorization to Operate (ATO) certification
- Common Criteria for Information Technology Security Evaluation
- Security Information and Event Management (SIEM) integration for advanced scanning of audit logs through a unique connector in ArcSight as well as syslog interface input with Splunk

All combined, these certifications show that not only is HPE building secure servers but it is also working with governments and regulatory bodies to ensure compliance with the critical standards businesses require for security compliance.

HPE ADDRESSES THE SUPPLY CHAIN

A secure supply chain is a critical element of cybersecurity. HPE has a strategy to focus on security first throughout its entire supply chain, helping protect against compromise at each juncture. Through this focus, HPE works to reduce the risk of exposure to threats such as counterfeit materials, malicious software embedded in products, and other untrustworthy components throughout its supply chain. HPE vets component vendors against anti-counterfeiting laws and sources only from TAA (Trade Agreements Act) designated countries.

Copyright © 2017 Moor Insights & Strategy

Supply chain protection reaches down into the actual firmware code. HPE's internal processes strictly dictate who can access firmware, who must sign off on firmware, and how it is handled. Because HPE develops a significant amount of its own designs, it is in a better position to limit supply chain exposure, boosting platform security.

HPE assurance is delivered across multiple levels, as it works with partners to enable more end-to-end security. When HPE buys third-party devices to integrate, it still writes its own software and drivers to have secure control over the product and process. HPE digitally signs all device drivers for extra assurance when updating, and HPE works with its OS vendor partners to guarantee that each partner signs its software and drivers as well. Finally, to help ensure the security of its supply chain, HPE works with third-party organizations to do verification testing throughout its entire supply chain, including penetration testing where applicable.

HPE Pointnext Helps Enables End-to-End Security

To help accelerate digital transformation, HPE has introduced HPE Pointnext to help make hybrid IT easier and assist in powering the intelligent edge.

The wide portfolio of security services can engage at the strategic level for:

- Advisory and digital transformation
- Architecture design and integration services to remediate gaps
- Transform or modernize edge to the core to the cloud security infrastructure
- Architect, design, and implement a completely hardened infrastructure environment, including network- and storage-related security and data protection
- Design and implement security and incident management solutions for rapid detection and response of iLO alerts and verification check notifications

At the tactical level, Pointnext can deliver:

- Professional and operational security assurance services
- In-depth coverage to address risk and compliance management
- IT service continuity
- Operational and infrastructure security
- Data protection and access control
- OS, hypervisor, and application hardening in accordance with specific policy and regulatory requirements such as PCI DSS
- Design and implementation of 2- and 3-factor authentication solutions

Copyright © 2017 Moor Insights & Strategy

MI&S PERSPECTIVE

Threat complexity is changing, and businesses need to look seriously at their security strategies. Too often, businesses assume purchasing from a top-tier vendor guarantees the highest levels of compliance. As we dig into the details about products, processes, and supply chains, we see this is not always the case. This fact should lead any standardization decision down the **security** path much earlier in the process.

Historically, threats have multiplied faster than prevention technology. With PCs, virus scanning of the OS was enough, but eventually malware and application infection became the issue. Now ransomware is the newest threat, reaching all the way down to the system level. We see system-level compromise as the newest server threat now.

We also see denial of service on the rise, with the threat profile changing the attack outcome from temporary to permanent in some cases. Within the industry there is often disagreement about acronyms, but we use the following nomenclature:

- **Denial of Service (DoS)**: An attack where a server is overloaded with traffic or the firmware is compromised, rendering it inaccessible (for a period of time). Additionally, a server with compromised firmware could still be available to users but also available by an attacker who uses it for nefarious purposes, allowing the compute process to happen but in an altered state.
- **Distributed Denial of Service (DDos)**: An attack on a server from multiple locations where it becomes very difficult to identify the source of the attack, because requests are coming from many locations.
- **Permanent Denial of Service (PDoS)**: The server (or device) is compromised, typically at the firmware level, where recovery is not possible, rendering the device useless with no way to bring it back into operation; most commonly called a “brick”. New tools are even seeking out insecure IoT devices and bricking them to reduce risk of attack. (Some refer to this as “Destructive Denial of Service”, but that carries the same acronym as the distributed attack.)

These three categories all cover accessibility to systems and are different from data theft or information loss (such as the Target case), which can either be the direct purpose of an attack or be an outcome / side effect of the denials of service.

Previously, system-destroying malware like Stuxnet was highly specialized, very expensive to create, and very targeted in its attack, destroying a very specific model of centrifuge in a single location, for instance. Now the business world faces ransomware which moves beyond simply holding the data or system access hostage and now holds

Copyright © 2017 Moor Insights & Strategy

the physical system itself hostage. With the ability to replicate ransomware tools easily and cheaply, businesses need to step up their security by ensuring protection, detection, and recovery all the way down to the system level.

This is a time for looking deeper into the vendors and their supply chains, which begins by asking how well you know your partners. Additionally, as threat profiles continue to change and supply chain becomes more critical, there needs to be a "Good Housekeeping Seal of Approval" that can be applied to supply chain best practices to help ensure better security visibility. It is probably only a matter of time before we see the first case of a nation state or terrorist organization sending people to work within manufacturers to directly subvert products. Businesses must be on guard.

CALL TO ACTION

Business environments have become more complex, and threats have become more sophisticated. The traditional means of security are still valid and important, but they are not enough to tackle today's new challenges. Because a chain is only as strong as its weakest link, businesses need to look more holistically at their products, processes, and supply chains to ensure the best security.

Those who believe they have a strong security strategy may be missing out on key aspects. They should constantly be asking the question, "HOW secure?" Those who are not asking the question may not be truly secure. The roots of security reach back into the design and supply chain, they do not start when the product arrives on the dock.

HPE has one of the most comprehensive strategies, focusing on protecting, detecting, and recovering within its products. The long list of certifications helps bring the confidence that deployed products will adhere to security and regulatory compliance. All of this is part of the HPE Security Assurance that reaches all the way back into the supply chain to help ensure secure and robust products. MI&S recommends that companies embarking on platform standardization projects consider HPE, as its approach to security assurance positions it significantly ahead of the competition.

Copyright © 2017 Moor Insights & Strategy

IMPORTANT INFORMATION ABOUT THIS PAPER

AUTHOR
John Fruehe, Senior Analyst at Moor Insights & Strategy

PUBLISHER
Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

EDITOR / DESIGN
Scott McCutcheon, Director of Research 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 cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by 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 in any form without Moor Insights & Strategy's prior written permission.

DISCLOSURES
This paper was commissioned by Hewlett Packard Enterprise. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any 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 considering new information or future events.

© 2017 Moor Insights & Strategy. Company and product names are used for informational purposes only and may be trademarks of their respective owners.