MOOR
INSIGHTS & STRATEGY

ZERO TRUST IS A LIFECYCLE EFFORT

INTRODUCTION

Securing infrastructure begins before one ever installs a server. This statement has never been more accurate – or less understood – which can leave organizations more vulnerable than ever.

The security attack vectors against organizations of all types and sizes have evolved considerably. As a result, IT organizations must expand their collective security aperture to consider the new challenges that arise from a highly distributed world where infrastructure is globally sourced and deployed in the most remote of locations.

Security is more than trusted platform module (TPM), access management, or identity management. While such technologies are essential, infrastructure and the platforms and workloads that run on it need more to be secure. To ensure proper security, IT must have full confidence that the servers it receives are entirely secure, right down to the components that populate the motherboard. Further, that confidence must span components from chain of custody to deployment through the end of life. And such security must be intersecting, meaning tools and methods must cascade down to the lowest levels, allowing no softness to be exploited.

Although this may sound impossible, it isn't – challenging, perhaps, but not impossible. This brief will describe how companies like Hewlett Packard Enterprise (HPE) deliver infrastructure security with a Zero Trust lifecycle approach.

SETTING THE STAGE – IT'S A DANGEROUS WORLD

In a data-driven market, data is the lifeblood of an organization. It is the crude that organizations refine into intelligence to drive them forward. Because of this, the value of data becomes, well, invaluable.

Further, data is being generated and stored at unprecedented rates from virtually everywhere. Every IT organization has read the forecasts from prognosticators talking about the zettabytes of data generated annually. More importantly, every IT organization is living this truth. With the digitization of the world economy, transformation projects look to make every connected device, every customer interaction, and every sensor on a machine a valued contributor of data. The “edge-to-cloud" mindset of many organizations delivers great amounts of intelligence and agility. However, the deployment of edge and cloud environments also increases risk profiles significantly due to the growing number of connection points. In a distributed world, security becomes a function of trust.

Organizations are more at risk than ever and trust is paramount. Those that wish to do harm – bad actors and nation-states – have employed different tactics to exploit data, including tactics that IT organizations have not yet accounted for or modeled around.

One of the more prolific attack vectors recently uncovered is a method known as "supply chain" attack, whereby bad actors exploit third-party hardware and software suppliers for gain. Consider an industry-standard rack server is built from up to 10,000 components. Further, consider the chain of custody of that server before it reaches a datacenter. The opportunity for the server to become compromised is a real threat that should concern every IT professional. From "chip clipping" and other means of manipulating hardware to insider threats of "spoofing" drivers and manipulating firmware, the threats are real and ever-evolving.

As such, organizations need to assure the authenticity and ongoing security of infrastructure well beyond traditional access and identity management. Security practices must be both holistic and eternal – from the proverbial cradle to the grave. And this is where HPE stands uniquely positioned in the market.

HPE'S SECURITY-FIRST VISION – AND TACTICS

Cybersecurity must be holistic and intersecting and span the lifecycle of the environment and data it protects. Zero Trust is a guiding principle that must drive the strategy and tactics of those developing security solutions and those consuming the solutions. An automated Zero Trust model that is rooted in hardware is key to increasing engineering velocity by standardizing and automating authentication flows.

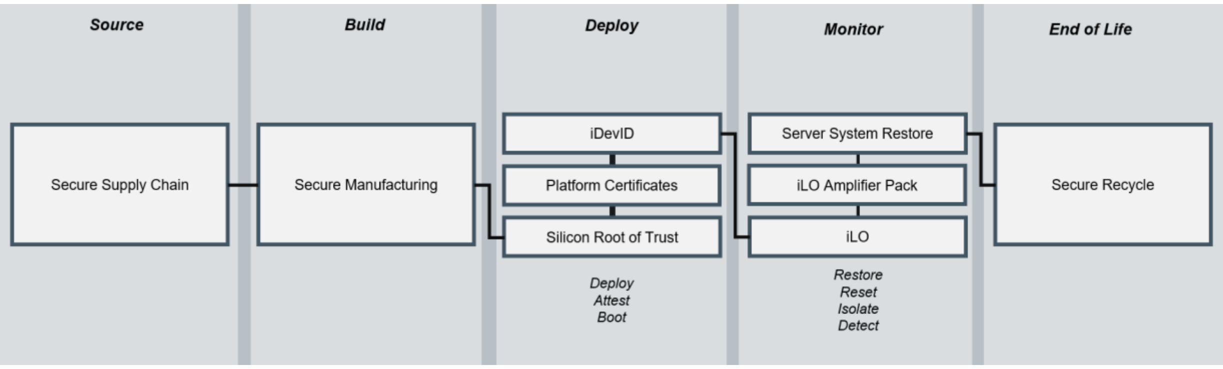
HPE appears to have taken its well-known innovative DNA and applied it to deliver a security practice unmatched in the industry. As Moor Insights & Strategy (MI&S) looks at HPE from outside the organization, there seem to be five pillars to the company's approach.

1. **Foundational Organization**– Establishing a separate security organization ensures a Zero Trust mindset across the entirety of the company – from supply chain to product design and development to manufacturing and beyond. The

founding of this organization drives MI&S's confidence in the company's ability to innovate in this area.

2. **Strategic Operations** – Building a security organization that spans the functions of a company only works if there is an activation of that organization's strategy. And this is another area where HPE seems to lead. It has operationalized this Zero Trust mindset, from sourcing materials and components to the manufacturing of servers through the lifecycle and the safe and secure recycling of infrastructure. MI&S has written extensively about how HPE delivers on secure supply chain here and here.

FIGURE 1: HPE'S OVERLAPPING LIFECYCLE SECURITY



Source: Moor Insights & Strategy

In addition to HPE's stringent means of verifying materials and components for its servers, it has initiated a program of secure manufacturing by performing the build process in a secure facility in the United States. For companies or organizations that require the highest levels of manufacturing integrity (e.g., government entities), these servers are the answer. While HPE has not publicly stated its intentions, one can envision a replication of this effort for other countries.

3. **New Technology Development** – HPE is known for being on the leading edge of new technology development and market introduction, which has undoubtedly been the case with security-related technology. An excellent example of homegrown innovation is its introduction of Silicon Root of Trust technology as part of the HPE ProLiant Gen10. Silicon Root of Trust is an HPE-exclusive technology that ensures the authenticity of firmware and the over 4 million lines of code executed by a server before boot. Ensuring the server boots from an immutable source at the lowest level of security possible provides the foundation

for a pristine operating environment.

HPE's Silicon Root of Trust also ensures that firmware and drivers are not hijacked, spoofed, or otherwise corrupted during server operations. If the technology detects an exploit during runtime, the it isolates the ransomware and removes it and restores the server to its last known operating condition (MI&S covered this here).

HPE has introduced two new solutions, Platform Certificates and Product Cryptographic Identity (known as IDevID), that drive assurances around platform authenticity as servers ship to a customer site. We will address these in greater detail below.

4. **Mergers & Acquisitions** – Sometimes, the best path to innovation is through acquisition. Not just because it enables a company to expand its portfolio, though this is undoubtedly a benefit; in addition, it brings intellectual property (IP) and the intellect behind that IP to the acquiring organization. And if managed properly, a company can leverage that IP across other products and services. This is another area where HPE has led, with two of its more prominent acquisitions being Aruba and Scytale.

   The company's acquisition of Scytale is very telling about its approach to security. Scytale is an authentication service that enables enterprise applications to share data securely. In a practical sense, think of cloud-native architectures that deploy microservices. This technology authenticates and secures each microservice connection across applications. It doesn't take much imagination to see how HPE can utilize such security technology across its technology portfolio.

5. **Ecosystem Engagement** – Finally, developing products from a collective Zero Trust mindset means nothing if IT consumers lack adoption. And market adoption only happens with enablement from the ecosystem. The company has found ways to leverage security technologies from AMD (Secure Encrypted Virtualization) and Intel (SGX) to protect customers more effectively.

   The ecosystem also extends to partners and players in adjacent industries. For example, the recognition of HPE's Silicon Root of Trust with designation as a Cyber Catalyst from Marsh and other leading insurers in the cyber risk space signals to businesses large and small that its servers can significantly reduce risk profiles. MI&S knows of no other server vendors whose security technology earned this designation. Marsh has also recognized Aruba ClearPass and Aruba Policy Enforcement Firewall with the Cyber Catalyst designation as HPE doubles down on the protection of devices, users, and networks at the edge from cyber threats.

While these five pillars of HPE’s Zero Trust security strategy are impressive, it is the intersection of these pillars – the complementary nature of them – that is perhaps most impressive. As stated earlier, bad actors are finding increasingly sophisticated ways to attack the most vulnerable infrastructure components. HPE’s approach appears to mitigate these vulnerabilities.

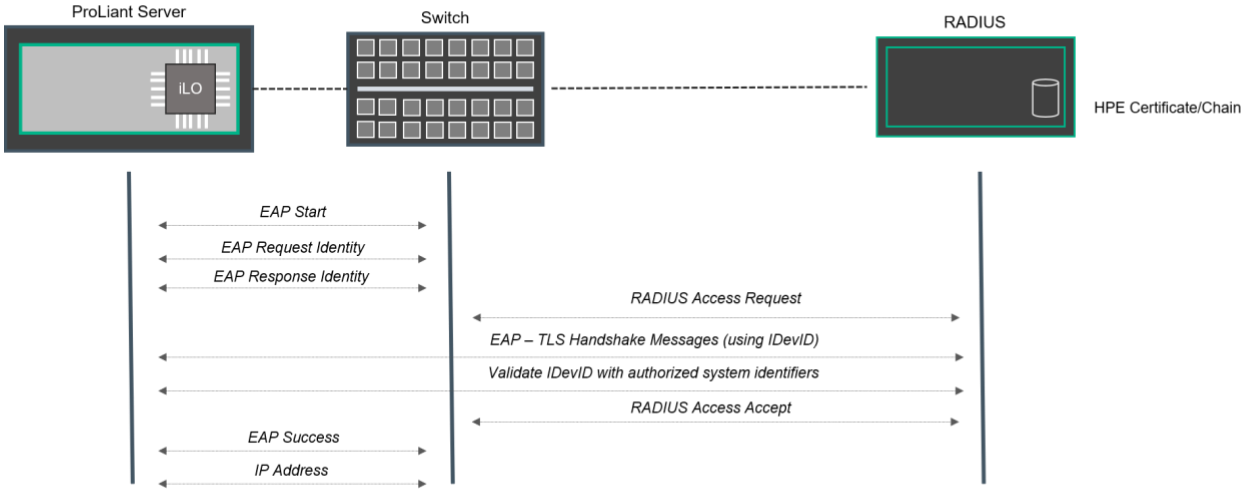
Addressing a New Front With Platform Certificates and Product Cryptographic Identity (IDevID)

As IT organizations shore up one security vulnerability, others seem to come into focus. Such is the case with HPE's strategy. As the company continued to execute its Zero Trust strategy, it quickly realized that there was the potential for infrastructure to be tampered with while en route to the customer. Perhaps a bad actor intercepts a server, somehow infiltrates a partner organization, or even joins an IT staff. So, how could a customer, upon deploying a server, ensure that what is inside is authentic and in good working order?

Enter HPE’s two latest additions to its security portfolio – Platform Certificates and Product Cryptographic Identity (IDevID). In combination, these two solutions enable the automation of secure server onboarding and management capabilities.

IDevID is the method for authenticating HPE’s Integrated Lights Out (iLO) management controller and the HPE system. When powered, iLO authenticates against an external RADIUS server. After this authentication is performed, the HPE server can self-identify on a network in an unattended fashion. This is especially helpful for environments that have large server installs, remote locations, and edge environments.

FIGURE 2: HPE CRYPTOGRAPHIC IDENTITY (IDEVID)



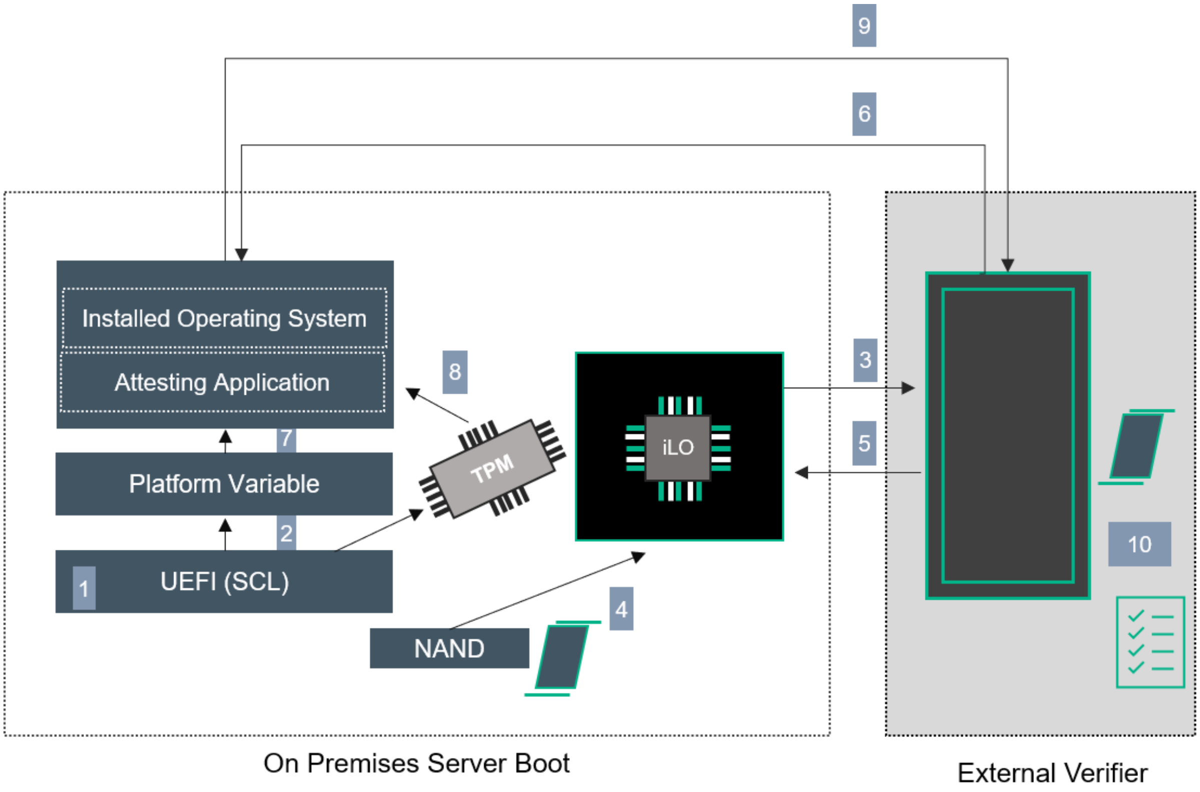
Source: Moor Insights & Strategy

Platform Certificates is the method by which an IT administrator can assure the authenticity of a server's components – from motherboard revision and ASIC IDs to CPUs, memory, and PCIe devices. In addition to assuring the current components in the server are the components that were in the server that left the factory, Platform Certificates ensures the software and firmware supporting those components are authentic and up to date.

How do Platform Certificates work? When manufacturing an HPE server, HPE creates a manifest of all its components. This manifest, or Platform Certificate, is digitally signed and stored on the server. When the customer receives the server and boots for the first time, the customer verifies their certificate in one of two ways – on-site by an HPE provided tool or through an external verification process. Either way, attestation occurs before an OS or any applications are loaded, assuring no attempt at manipulating the certificate can be made.

Considering the capabilities of Platform Certificates and IDevID individually should bring some reassurance to IT administrators concerned with protecting their data and operating environments. Perhaps most impressive is that these two solutions are part of a much larger security practice from a company that has turned its collective innovation engine toward solving security across the lifecycles of infrastructure and data.

FIGURE 3: PLATFORM CERTIFICATES



Source: Moor Insights & Strategy

THE IMPACT ON BUSINESS

The impact of employing a holistic cybersecurity strategy is multidimensional. Daily headlines about the large company that lost tens of millions of dollars due to a cyberattack seem to fill the news. Cyberwarfare is the new battleground from a national readiness perspective, and government infrastructure is attacked every minute of every day, with nation-states looking for any vulnerability.

These cases are not strawman arguments used to drive home a point about the importance of being ever-vigilant. Instead, these are real-world examples that have had documented and quantified financial and security impacts, such supply chain attacks whereby bad actors use third-party hardware or software as the vehicle for exploitation.

But these incidents don't just happen to multinational companies or large government entities. Enterprise organizations and midsized businesses are equally at risk, or perhaps more so, as they lack adequate budgets and resources. And because of this, HPE's approach to driving hands-free security for the lifecycle of infrastructure should make its servers a "must consider" for companies of all sizes.

Simply put, HPE's intersecting security should increase IT administrators' peace of mind as they embark on digital transformation projects, knowing that the vast amounts of data generated and stored from the edge to the cloud are secure.

CALL TO ACTION

The hype around the increasingly dangerous cybersecurity landscape is more than hype. It's real. Bad actors and nation-states employ various means to extract data for many reasons – financial gain, competitive edge, geopolitical advantage, and the like. As cybersecurity solutions close one attack vector, those bad actors find another.

Because of this market dynamic, IT organizations must constantly evolve their cybersecurity strategies to meet the most current challenges. In a previous research brief, MI&S outlined the three Ps of holistic security – products, process, and people. Products must be constantly evaluated and intersect to deliver gapless security. People must be trained and ever-vigilant. And processes must be established, updated, and continually tested.

The security-minded IT organization should look for IT solutions vendors that are equally security-minded. Solutions vendors that understand security stands on equal footing with performance, cost, and manageability.

With this understanding, MI&S believes any IT organization embarking on digital transformation or modernization projects should strongly consider HPE as data becomes the most valuable asset to an organization. HPE's relentless focus on Zero Trust, combined with its culture of innovation, has driven the company into a leadership position.

In a software-driven world where many consider compute to be a commodity, security is the new differentiator. And HPE currently wears the crown.

For more information, visit www.hpe.com/security

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Matt Kimball, Senior Analyst at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Principal 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 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

DISCLOSURES

This paper was commissioned by HPE. 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 in light of new information or future events.