HPE Enables Zero Trust Security Architecture With Project Aurora

Introduction

Enterprise IT organizations are more vulnerable than ever. The threat landscape continues to grow in terms of attack surfaces and vectors and willing conspirators. Data is the target. And infrastructure – the environment that houses, processes, and moves that data – is how to exploit an organization.

The problem is multi-planar. Attack vectors are granular, and the methods used by bad actors to infiltrate and exploit datacenters are increasing in complexity, rendering malware virtually undetectable in today's complex and highly distributed environments.

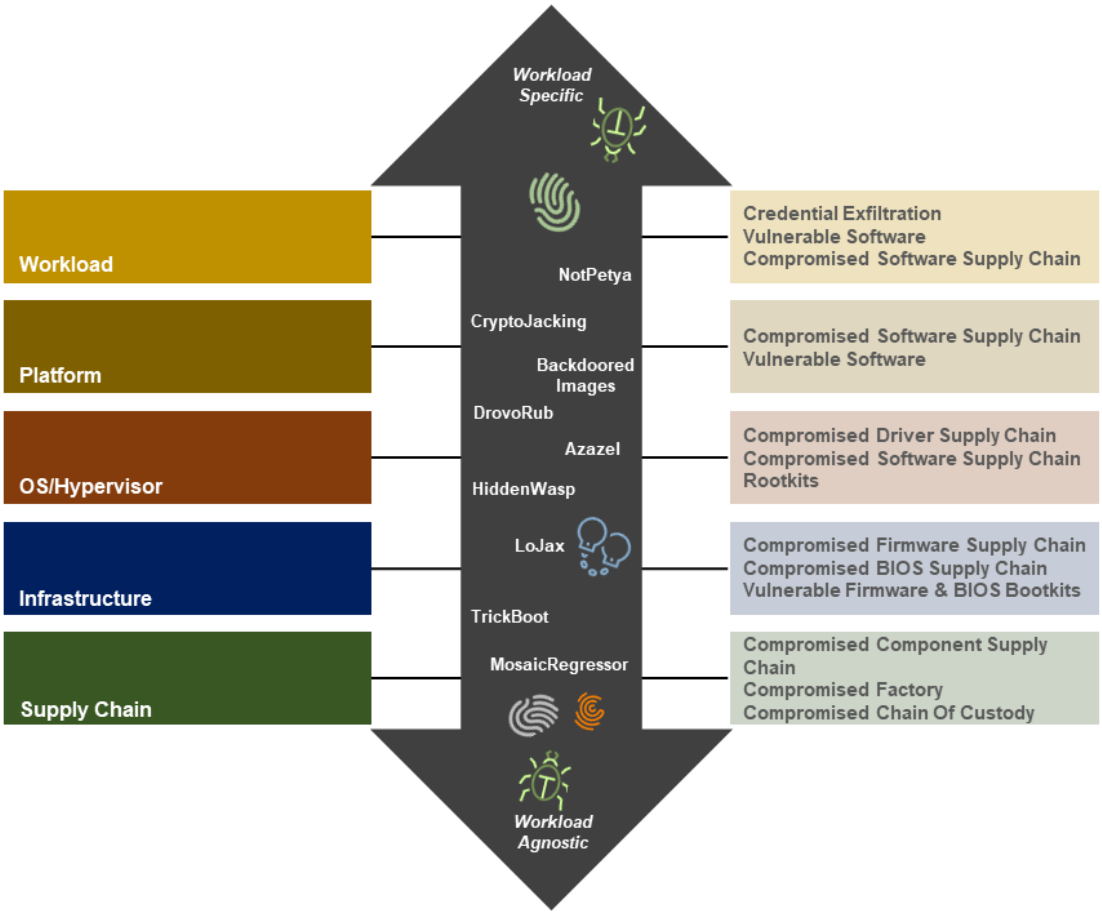
The motivations of bad actors vary from profit-seeking, loosely federated groups of hackers encrypting enterprise data to organized state actors trying to drive social engineering and political agendas. Some work to steal data and intellectual property to gain competitive advantage, while others are proliferating a new kind of warfare on a cyber battlefield.

A new approach to protection is needed – multi-planed security capabilities to defend against multi-planed threats. Further, this approach must be intersecting, creating a chain of trust that spans from the lowest levels of silicon to the workloads and data that reside on the servers to the infrastructure that powers the modern business.

This paper explores the threat landscape faced by organizations today and demonstrates how companies like Hewlett Packard Enterprise (HPE) enable zero trust architectures. HPE is extending its security strategy with the introduction of Project Aurora, which is set to deliver new cloud-native, zero trust security to HPE's edge-to-cloud architecture.

We will discuss how Project Aurora's security capabilities will embed within HPE GreenLake cloud services – starting with the HPE GreenLake Lighthouse – the security building blocks that will automatically and continuously verify the integrity of the hardware, firmware, operating systems, platforms, and workloads.

FIGURE 1: THE THREAT LANDSCAPE



Source: Moor Insights & Strategy/HPE

SETTING THE STAGE – THE GROWING THREAT LANDSCAPE

The average ransomware attack lasts 24[1] days before it locks data and extorts organizations for payment. That's nearly a month for software to root and proliferate across an organization. In that time, ransomware becomes firmly entrenched, and the locks put on data are virtually impenetrable.

More complex malware attacks, like those designed to infiltrate an organization and steal data, are even more insidious. In 2020[2], the average breach took 207 days to

[1] M-trends Special Report, 2021, Fireeye Mandiant Services
[2] https://www.ibm.com/security/data-breach

identify and 280 days to contain – months in which organizations can be completely dismantled or a nation's most valuable data shared with its adversaries.

The reason malware continues to sit undetected for longer and longer is simple – it is becoming increasingly sophisticated. The most insidious types of attacks are rootkits and bootkits, low-level attacks on the kernel or the firmware below the kernel. These types of attacks comprise multiple elements – one element used to prevent detection and another that gains privileged access (hence the term "rootkit") to perform functions such as implanting malware or spyware or stealing data.

DECONSTRUCTING THE THREAT – IT'S A MULTI-PLANAR CONSTRUCT

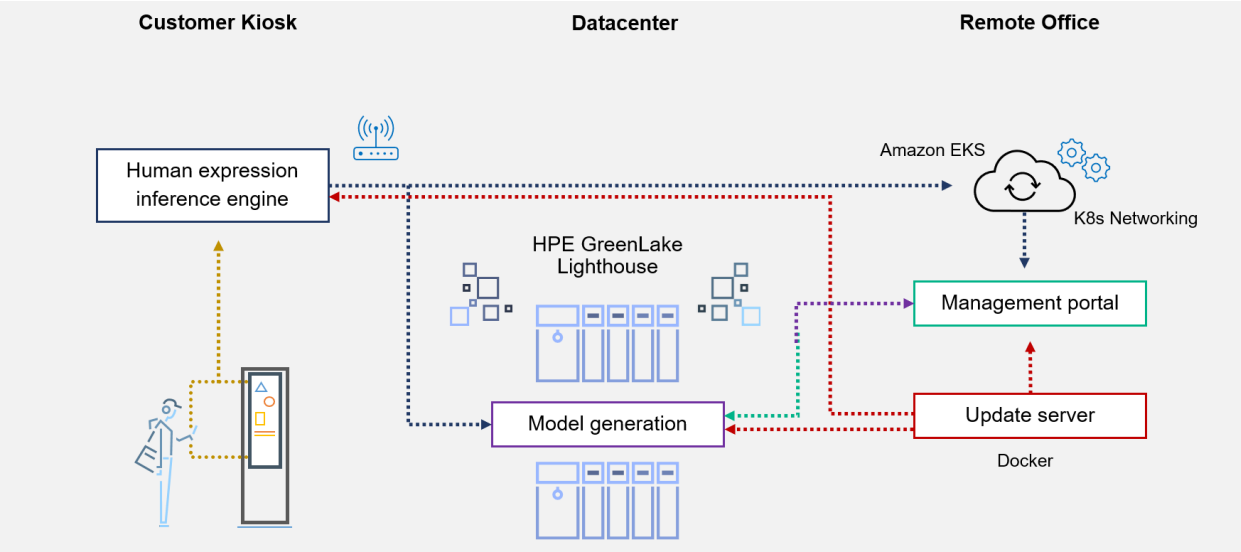
In terms of attack surfaces, the problem is multi-planar. On one vector, hardware is deployed in the wild to capture, process, and transform data. This process, often unattended and always more vulnerable, involves "things" (sensors, cameras, controllers, etc.), storage devices, servers, and networking on the edge. These environments connect to core datacenters and the cloud for deeper processing, storage, and archival.

The other vector is the environment that resides on the "things" – firmware, BIOS, operating systems and drivers, virtualized and cloud-native environments, and applications and data.

As mentioned, the edge and all that make up the edge are connected to the core datacenter and the cloud. The complexity of this can be challenging – a virtual playground for hackers of all stripes. The question becomes, how can an organization effectively protect itself? Is it even possible?

Protecting infrastructure and data is entirely possible. However, the approach to securing must align with the threat, meaning it must be multi-planed. Security must span the entire life cycle of infrastructure, and it must extend from the lowest levels of silicon to the cloud. Even before servers, storage, and gear are assembled, materials and components must be attested. Likewise, even before infrastructure is booted, environments must be measured and assured of authenticity. And as operating systems and applications generate meaningful data and produce results, continuous measuring and attestation of the environment are critical to maintaining integrity. Project Aurora from HPE embraces these concepts with its comprehensive security vision.

FIGURE 2: THE MODERN APPLICATION



Source: Moor Insights & Strategy/HPE

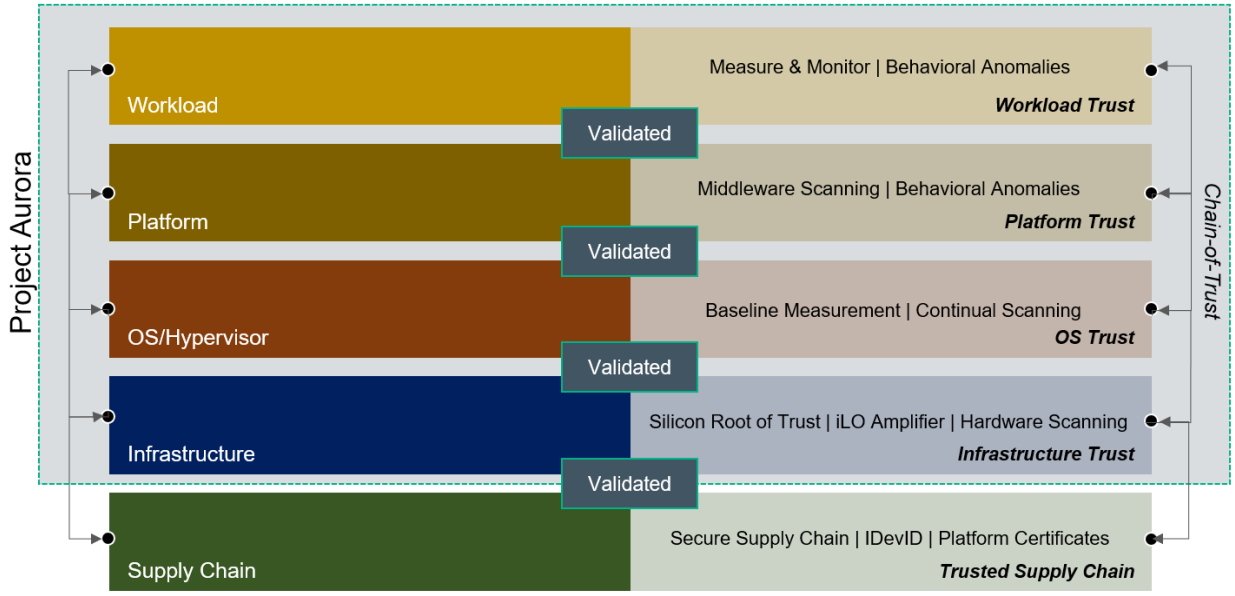
PROJECT AURORA – ENABLING A ZERO TRUST ARCHITECTURE FROM THE EDGE TO CLOUD

Your environment is only as secure as the most vulnerable element. That vulnerability may be a server residing on the edge or an application that must interface with a third-party microservice, even temporarily.

Or that vulnerability could be introduced into your environment before a server is even assembled. Supply chain exploits are not only common, but also well documented. Accounts of servers sold into the market with compromised baseboard management controllers (BMCs) and basic input/output systems (BIOSs) fill the internet.

Project Aurora is a series of intersecting security solutions designed to protect an organization's entire environment – infrastructure, communications, applications, and data from the edge to the datacenter to the cloud. In addition to the intersection of these security solutions, Project Aurora establishes a chain of trust from the silicon root to workloads and data. While Project Aurora may be a newly announced initiative from HPE, it is clear to Moor Insights & Strategy (MI&S) that this results from many years of consideration, design, and execution.

FIGURE 3: PROJECT AURORA BUILDING BLOCKS



Source: Moor Insights & Strategy

With Project Aurora, HPE creates a stack of building blocks for deployment at the edge, in the datacenter, and in the cloud. These security building blocks intersect with one another, requiring a secure validation before a handoff can take place – from power on to boot sequence to the loading and running of workloads.

Let's dig deeper into HPE's overall security portfolio by discussing how it currently protects infrastructure.

- Secure Supply Chain: HPE achieves and assures a secure supply chain through a few methods.
  - First, the company's supply chain team ensures the integrity of every material and component that makes up infrastructure in the field. HPE assigns personnel to supply chain providers, where on-site inspections complement in-depth auditing. This assures that the components are authentic and not exposed, in addition to being of high quality.
  - HPE has also invested in secure manufacturing capabilities, a service that MI&S does not see with other vendors. For organizations with a lower risk threshold, HPE can manufacture servers in secure facilities with employees who have passed more exhaustive background checks. Once on-site, infrastructure is validated as authentic and matching the secure factory

manifest through HPE Platform Certificates and cryptographic signatures (IDevID).

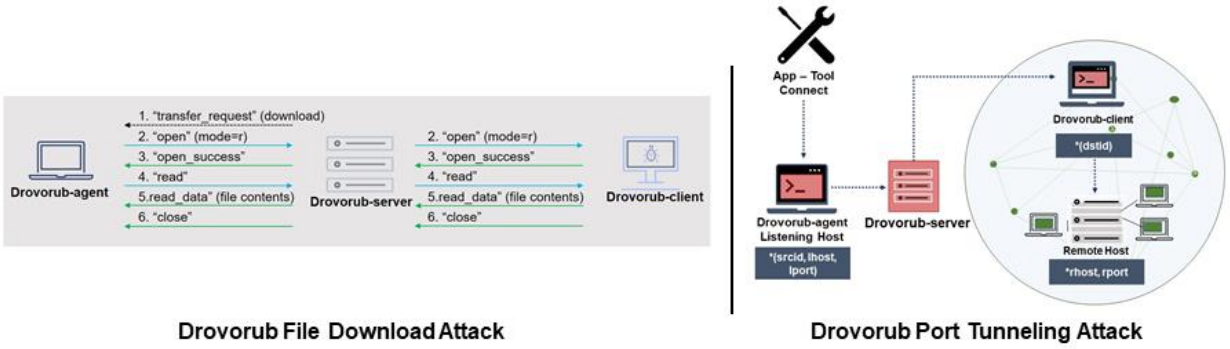
The attestation that takes place through the secure supply chain enables the establishment of a chain of custody. As such, a validation and secure handoff takes place with Project Aurora, driving secure operations up the stack through four services:

- **Infrastructure trust –** HPE's Infrastructure trust service performs several functions.
  - Silicon root of trust (HPE custom silicon), measures and attests to the firmware and over 4 million lines of code executed before a server (or other infrastructure) boots an operating system. This attestation assures that the infrastructure has its components and that the drivers and other supporting software are pristine.
  - Further, HPE's Integrated Lights Out (iLO) management controller works with silicon root of trust to continuously assure these files remain in good working order and track any changes. If an attack is detected, iLO has the tools to immediately isolate the malware within the firmware and restore infrastructure to its last known good state.
  - Once HPE infrastructure is booted to a known good state as attested by silicon root of trust, a secure handoff takes place, and hardware is continually scanned and measured throughout its operational life. Infrastructure trust looks for deviations, insertions, or other abnormalities. If it detects such a change, Project Aurora sends an alert to operators, at which time corrective measures can be activated through iLO Amplifier Pack or other tools.
  - HPE also secures infrastructure through protections built into components, such as encrypted drives and networking protections. The company is securing data and communications along the north-south and east-west vectors through protections at the very lowest levels of infrastructure.
- **OS trust –** Protecting the operating system begins with protecting the kernel. As previously discussed, rootkit attacks can be difficult to detect, and once detected, recovery can be a complex task. Project Aurora is extremely effective at the detection of rootkit attacks. During a secure and measured boot, a baseline measurement is taken of the kernel. This measurement is sent to HPE's iLO and used for continual scanning of the kernel. If, during the monitoring, a delta is detected, a violation is logged and a security event is generated. This event will lead to a remediation from HPE's iLO Amplifier pack or the IT organization's preferred toolchain.

- **Platform trust –** Protecting platforms - the containers, services, and middleware that supports multiple workloads is critical because this is where data can be easily exploited. This middleware will be deployed across multiple devices and servers in many environments, allowing for tainted platforms to spread easily across a distributed system. Further complicating this is the ready availability of such exploits; less-sophisticated bad actors can easily gain access to tools on the dark web for use against targets.
    - Project Aurora's platform trust uses security scanners to monitor the activity of platform components for behavioral anomalies such as file access patterns, memory access, system calls, and syscall profiles. Anomalies will trigger alerts that feed into security operations.
    - In the future, platform trust will include SPIRE (SPIFFE Runtime Environment) to attest and issue cryptographic identities, enabling assured secured communications even across unsecured networks.
- **Workload trust –** The inherent risk in protecting workloads comes from the fact that many applications are continuously changing or are homegrown and less likely to be thoroughly considered and designed for security. And much like Platform trust issues, distributed workloads can easily spread an exploitation, leading to data exfiltration from other workloads and applications – even security software. Project Aurora in this example can "watch the watchers." Further, in this era of digital transformation and DevOps methodology, speed and time to value are of the essence. This can often lead to less-than-thorough regression testing and audits, allowing vulnerabilities to go undetected.
    - Workload trust gives greater assurances that workloads are subject to the correct security policies. Further, scanning and monitoring infrastructure can look for signal baseline deviations from expected workload behavior patterns. Such deviations can trigger events that feed into security operations, much like platform trust.
    - Workload trust will leverage SPIRE to attest and issue cryptographic IDs to workloads, facilitating secure communications over unsecured lines.

When looking at HPE's approach to security, each component of Project Aurora stands as best-of-breed and can solve the needs of an enterprise wanting to protect its assets. But what truly separates Project Aurora is the intersection and orchestration of these services, tied by a validated chain of trust that removes vulnerabilities and gaps in coverage. MI&S believes this makes HPE's security strategy exponentially stronger, and there still much more work to do.

FIGURE 4: DROVORUB ATTACKS



Source: Moor Insights & Strategy

DROVORUB – A CASE STUDY

To best illustrate the power of HPE's security portfolio and Project Aurora, consider how it would defend against one of the more notorious Linux malware attacks known as Drovorub. Described by many as the "Swiss Army knife" of malware, this kit has proven very effective at evasion while enabling file transfers (to/from), port forwarding, and remote shell capabilities. Interestingly, Drovorub is the subject of a 39-page Cybersecurity Advisory by the United States National Security Agency (NSA) and Federal Bureau of Investigations (FBI) despite no published attacks. The advisory points out that the GRU (Russian military intelligence) is deploying Drovorub. Further, industrial automation giant Schneider Electric (and others) have released advisories on how to defend against Drovorub.

The Drovorub client resides on the attacked infrastructure and enables file transfers, shell access, and port forwarding. It also includes the Drovorub-kernel module, providing rootkit-based stealth functionality. It is this Drovorub-kernel that renders the client undetectable, enabling it to wreak havoc on an organization.

Per HPE, the company recreated Drovorub based on documentation publicly provided by the NSA and FBI. In its internal testing, Project Aurora detected the Drovorub-kernel in an average of three seconds. The worst-case scenario for detection was 10 seconds. This is compared to an average of 280 days to remedy the average malware attack – three seconds versus 280 days.

PROJECT AURORA REPRESENTS MORE THAN A SET OF SECURITY SERVICES

Project Aurora capabilities are being designed to deliver a security platform that provides end-to-end security from silicon to the workload and edge to the cloud. To achieve such a security profile, environments must be continually measured, attested, and verified – from initial boot to end of life.

While the benefits of Project Aurora are simple to understand, it is essential to remember that such comprehensive security is the result of an organization-spanning strategy rooted in a zero-trust philosophy with security as a guiding principle in the design, manufacturing, deployment, and support of infrastructure. This zero-trust philosophy is where HPE shows leadership.

HPE has demonstrated a commitment to building and delivering solutions and services designed to secure the data center. Since the acquisition of enterprise networking and security firm Aruba in 2015, the company has developed and acquired IP that drives secure environments – from infrastructure to networking to applications and data. The company's latest acquisition of security startup Scytale is particularly significant as it enables Project Aurora to secure applications and data in the cloud-native environment.

HOW PROJECT AURORA IMPACTS BUSINESS

Project Aurora vastly reduces an organization's risk profile – its most obvious benefit. Data breaches in the United States cost $8.64 million[3] on average. In addition, organizations that fall victim to such attacks can suffer immeasurable reputational hits – particularly in industries such as healthcare and finance.

Other benefits should not be overlooked. By deploying applications and services to the HPE GreenLake Lighthouse and taking advantage of Project Aurora, IT organizations can reduce the budget and resources required to manage infrastructure.

Utilizing the security solutions and services that Project Aurora will deliver also enables IT organizations to simplify security strategies, tactics, and procedures. The cybersecurity market is filled with thousands of point solutions, many of which must be deployed and managed individually. The cost and complexity of such environments can be overwhelming.

[3] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Additionally, Project Aurora can bring a uniformity of security across the edge-to-datacenter-to-cloud environment. Having the same security solutions in each environment delivers seamless and automated integration for the data journey – from point of origination to archival. IT staffs have the benefit of built-in security that "just works" across the hardware and software stacks, and the user experience is uninterrupted.

How does Project Aurora evolve?

Project Aurora is a comprehensive security solution for today's cyberthreat landscape. As an experienced IT person knows, that landscape will shift, with tomorrow bringing new threats. MI&S fully expects HPE to evolve Project Aurora's services to stay ahead of unknown attack vectors and increase coverage to support all attack surfaces.

Further, we expect HPE will populate all of its infrastructure with Project Aurora, from iLO to identity management built into its Aruba portfolio, to the measuring and attestation of the OS and applications residing on the HPE Edgeline, Nimble Storage, and Apollo product families.

As HPE proves out Project Aurora on the newly announced HPE GreenLake Lighthouse, MI&S anticipates the company will enable these capabilities to additional HPE GreenLake cloud services and its Ezmeral software platform, securing infrastructure deployed "on-prem." HPE is a company that listens to its customers, and one would expect these embedded and integrated capabilities will be in demand from virtually every enterprise.

Finally, MI&S believes HPE will drive partnerships and support an open ecosystem that can enable even greater levels of security through complementary technologies. Securing the edge-to-cloud is increasingly complex as architectures evolve and new applications and application architectures are deployed. Because of this, HPE has embraced the open-source community, and we would expect to see the same openness and embrace of open standards for Project Aurora.

Call to Action

The security threat landscape is ever-evolving and increasingly complex. Cyberattacks are more frequent than ever, and the stakes are getting higher. And as more high-profile attacks are publicized and ransoms are paid, bad actors are more motivated than ever.

While one attack is being addressed, two more seem to make themselves visible. And nobody knows how many servers, switches, storage devices, and other infrastructure have been impacted. Malware sitting undetected for months on end can damage an organization.

With such a sharp increase in attacks and the sophistication and insidiousness of modern ransomware and malware, IT organizations cannot continue to simply react. Instead, they should rely on tools, solutions, and services to detect such attacks and plants in real time, mitigating such threats.

Organizations must protect their infrastructure, operating environment, applications, and data on one plane. On another plane, they must protect the movement of that data from the edge to the datacenter to the cloud (north-south) and from device to device within the datacenter (east-west). And finally, this protection must extend for the entire life of the infrastructure, from the sourcing of components to secured recycling.

HPE's Project Aurora, complemented by its current security portfolio, takes a multi-planed approach that directly aligns with the threats posed in the industry. Infrastructure, operating system, platform, and workload trust capabilities are a perfect extension to the security portfolio the company has already developed (e.g., secure supply chain, Silicon Root of Trust).

Cybersecurity is complex and ever evolving. Every vendor in the IT solutions space rightfully recognizes this and works toward creating solutions that can meet the threats of today and stay ahead of the threats of tomorrow. HPE has demonstrated its commitment with Project Aurora, laying a foundation to provide a platform-agnostic way to define and enforce zero trust security policies.

For organizations where security is a top priority, MI&S believes HPE's GreenLake Lighthouse secured by Project Aurora should be given serious consideration.

For more information on Project Aurora, visit www.hpe.com/security/ProjectAurora

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 mentioned in context, displaying the 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 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 regarding 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 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.