CRAFTING A COMPREHENSIVE APPROACH TO CYBERSECURITY

HPE UPS THE ANTE WITH NEW SECURITY CAPABILITIES – AND A NOD FROM THE CYBER INSURANCE INDUSTRY

INTRODUCTION – THERE'S NO HONOR AMONG THIEVES

It used to be that hacking was dominated by technically sophisticated individuals whose interests and pursuits were more oriented around "can I?" Even if the goals were less noble in nature, hacking used to require a level of technical sophistication. The world has changed. Individuals and organizations can access resources on the dark web to hack and attack the most sophisticated systems for gain with little to no prior technical knowledge or experience.

The emergence of edge computing in response to the proliferation of the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) generating unprecedented amounts of data further increases the risk of cyberattacks.

No silver bullet exists when it comes to securing data, nor is there an "easy button" when it comes to locking down the infrastructure and data that drives businesses and organizations of all sizes. Rather, a cross-organizational focus on security - a focus that includes people, process and products - is required to ensure a company's risk is minimized. Further, risk transfer (cyber insurance) is a critical element to mitigating the effects of cyber incidents.

This brief will explore these three pillars of cybersecurity and will explore how Hewlett Packard Enterprise has responded to the needs of its customers through technology and affiliations with partners and the cyber insurance industry.

THERE ARE A LOT OF BAD PEOPLE OUT THERE…

In today's hybrid world, infrastructure is exploitable and data is vulnerable. This is a fact. Even organizations with the most comprehensive approach to securing access to its network are exposed because the most exploitable resource in an organization is also its most valuable – the employee. Phishing emails have evolved from a Nigerian Prince promising riches to emails appearing as legitimate from partners and fellow employees. Before an employee realizes they are being exploited (if they realize), malware buries

itself deep in the infrastructure, and data is hijacked by a community that is more clever than ever.

The dark web is filled with offers to assist in the hijacking of data – or tools, programs and scripts that require minimal interaction for a person (or persons) with the wrong intentions to wreak havoc on organizations of all sizes. In fact, many of the tools used in hacking and ransomware attacks are funded and organized by nation-states and used by organized crime syndicates that find cybercrime more profitable than the drug trade.

If all of this is not enough, artificial intelligence (AI) is being leveraged by those who wish to do harm. Researchers at Columbia University were able to bypass Captcha using AI. Further, this same study found that AI increased phishing effectiveness attacks and assisted malware in evading detection by three layers of concealment and by only executing when its intended target is reached.

Cyberattacks and the hijacking data is not the exclusive domain of hacktivists, individuals or organized e-Crime syndicates looking to extort organizations. Nation-states are waging cyberwar on one another in attempts to destabilize markets, defenses, politics and, ultimately, society. The 2016 US presidential election is perhaps the most well-documented example of a concerted effort to damage a country's political structure. However, it was just another example in a decades-long political tit-for-tat in political warfare. Add this to the long list of nation sponsored cyberattacks targeting countries across the globe.

THE THREE PS

The cybersecurity IT professional who is not living in a state of paranoia is not taking their job seriously enough. The same can be said for any employee of an organization as it applies to the protection of intellectual property and data. Comprehensive security requires an investment in the creation of *processes* and procedures that assist security-aware *people* (employees), protected by the *products* and technologies that mitigate risk.

PEOPLE – THE FIRST "P"

While organizations of all sizes begin to awaken to the real threat of cybercrime and the cost associated with falling victim to a cyberattack, the realization that securing the perimeter is perhaps the most important lesson in forming a comprehensive cyber resilience plan. Even with the emergence of edge computing and the exponential growth in potential attack surfaces, any organization's weakest point is its employees.

FIGURE 1 – THE THREE P'S OF CYBERSECURITY

Source: Moor Insights & Strategy

What makes people an organization's cybersecurity weakness? Simply put, we are curious; we trust too easily, and we fall into a state of carelessness during the day-to-day grind of our jobs.

Even the most conscientious employees can fall victim to phishing attacks aided by AI to appear as legitimate. AI was found to increase the effectiveness of phishing campaigns dramatically by increasing the click through of (phishing) emails from 5% to a staggering 30%.[1,2]

Cyberattacks by way of phishing expeditions continue to rise. Likewise, some of the largest and well-known security breaches have been the result of an employee's missteps.

> *What is considered to be the worst breach of US military computers was the result of an infected USB stick intentionally left in a Department of Defense facility parking lot. This stick was picked up by an employee and inserted into a*

[1] https://www.secplicity.org/2018/08/27/artificial-intelligence-part-2-cyber-criminals-get-smart-with-ai/
[2] https://www.theatlantic.com/technology/archive/2016/08/the-twitter-bot-that-sounds-just-like-me/496340/

PC to retrieve the contents. The result of this curiosity/vigilance led to the creation of US Cyber Command.

An admin password scribbled on an HVAC contractor's sticky notepad led to the theft of tens of millions of customer credit cards from retail giant Target.

More than a decade after that attack on the US military, the average employee is still the greatest risk to an organization's security. Conversely, the trained and vigilant employee can be a strong first line of defense.

PROCESS – THE "HOW-TO" OF CYBERSECURITY

Regular employee training that focuses on security and protections against cyberattacks is a standard in any IT organization's security strategy. Effective training consists of interactive aids that allow an employee to fully understand what to look for and how to react.

The US military creates Standard Operating Procedures (SOPs) to guide and instruct personnel on how to be most effective in executing their duties. SOPs also instruct personnel how to react in the event of emergencies. To ensure readiness, exercises are regularly run to measure readiness and drive individual and organizational proficiency.

While the modern business operates far differently than the US military, taking such an approach to cybersecurity can pay great dividends. Educated and vigilant employees are the results of processes and procedures that drive such awareness.

Training should be a part of any employee's initial onboarding, with regular monthly sessions that are both interactive and personal. Telling an employee to look for suspicious emails is basic. Showing an employee what a clever phishing email looks like is better. Instructing an employee on how to check links for suspicious URLs – and how to report – is best.

Training should be supplemented by regularly scheduled exercises that both test the vigilance of employees and that test the readiness of the cybersecurity team. Organizations that commit to this level of security awareness will strengthen their most vulnerable resources greatly.

For example, a staged phishing exercise can assist in training employees in finding the vulnerabilities in an enterprise in a safe and proactive manner.

Products – the tools of Cybersecurity

Having the right products and technologies to minimize an organization's risk and support the real-time response and recovery – the third “P” in the cybersecurity triad - is critical to a holistic cyber-resilience strategy.

Moor Insights sees HPE as differentiated in its approach to securing infrastructure. The company’s portfolio spans edge to cloud, silicon to software and services to ensure it delivers a security solution that spans the lifecycle of infrastructure – from initial deployment to end of life.

Unpacking the HPE security portfolio

HPE's portfolio of security is both broad and deep, spanning silicon, hardware and software. But the HPE security solution actually begins before the ProLiant server is even unpacked. During the manufacturing process, HPE maintains strict control, cryptographically signing silicon and firmware.

Silicon-based security

When the server is racked, stacked and powered up and the HPE silicon comes alive, HPE silicon runs a hash that verifies the HPE firmware. The HPE firmware conducts a verification of the CPU and will stop the boot process if any malware is detected. Once the CPU is validated, it boots. Then, via the silicon root of trust, the server BIOS validates the option ROMs and the operating system boot loader. The result? An HPE ProLiant server that has booted to a pristine and immutable state. For a deeper view of HPE's Silicon Root of Trust, download the Moor Insights & Strategy research paper here.

Server system restore – real-time recovery from cyberattacks

Here’s a scenario - “the” call in the middle of the night. A breach has occurred. 1,100 servers are “bricked,” and the personal information of 150,000 customers is encrypted. An email has been received, demanding $200,000 in digital currency. While this sounds like a nightmare, according to an industry study, businesses have fallen victim to ransomware attacks every 14 seconds in 2019. By 2021, that frequency will increase, with attacks projected to occur every 11 seconds.

While Silicon Root of Trust ensures infrastructure boots to an immutable and pristine state and detects low-level attacks in real-time, the integration of Server System Restore makes HPE's security solution invaluable to organizations of all sizes.

Server System Restore makes recovery simple, secure and scalable. Whether an organization has one hundred, one thousand or ten thousand servers, IT administrators can configure Server System Restore to automatically:

- Remove corrupt firmware,
- Reinstall validated firmware (and apply proper settings),
- Securely restore operating systems,
- Restore applications, and
- Restore data.

Single click. Complete restoration. No ransom paid.

One Button Secure Erase – End of Life with Confidence

In many IT organizations, servers reach "end-of-life" and are either returned as part of a lease, recycled, donated or disposed of properly. Despite the attempts of professionals managing the end of life, bits of data more than likely still exist. In some cases, significant amounts of data can be gleaned through a variety of techniques by those looking to exploit a business.

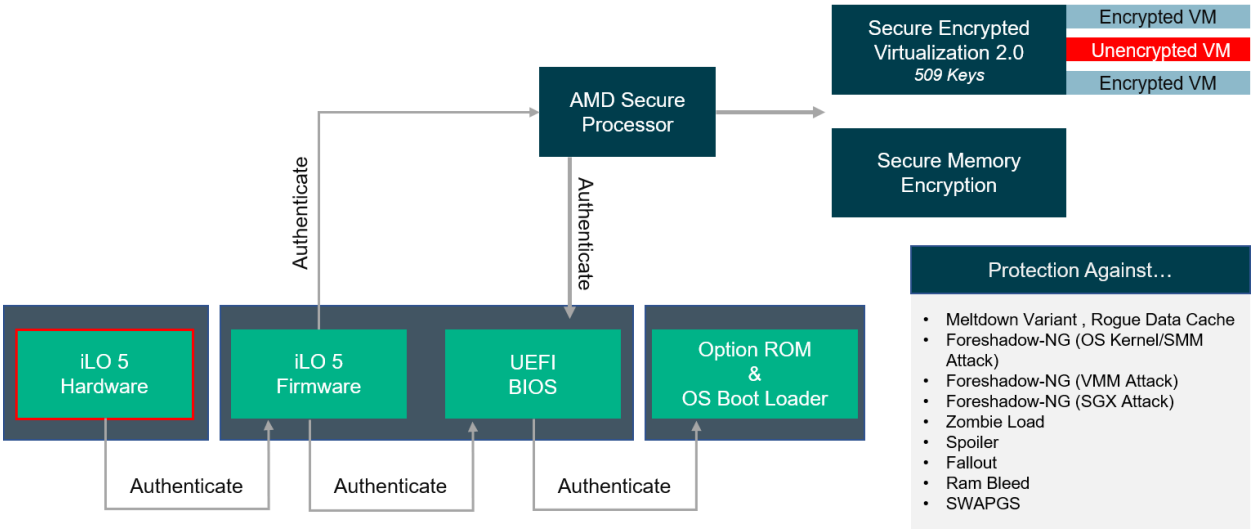
One Button Secure Erase is a feature that does exactly what its name implies – completely erases every byte of data that sits on an HPE server when retired by an IT organization. When that server is ready to be recycled or donated, IT organizations can have confidence there will be no traces of data or proprietary information. This is an invaluable feature for organizations and completes the cradle-to-grave lockdown of infrastructure and data that differentiates HPE in the market.

Leveraging Partnerships - HPE & AMD are better together

Like all server manufacturers, HPE has fully taken advantage of the security capabilities built into the AMD EPYC Processor. This includes physically encrypting memory through Secure Memory Encryption (SME) and encrypted virtual machines via AMD's Secure Encrypted Virtualization (SEV) technology.

Unique to HPE is the handshake that takes place between the two security solutions. During an EPYC-based ProLiant server boot, the EPYC CPU is authenticated by HPE's Silicon Root of Trust. Once authenticated, the EPYC Processor does a complementary authentication of the server BIOS. Once the server boots to a known good state, the EPYC CPU protects data at rest and at work through its SME and SEV technologies.

FIGURE 2 – HPE – AMD SECURE VIRTUALIZATION

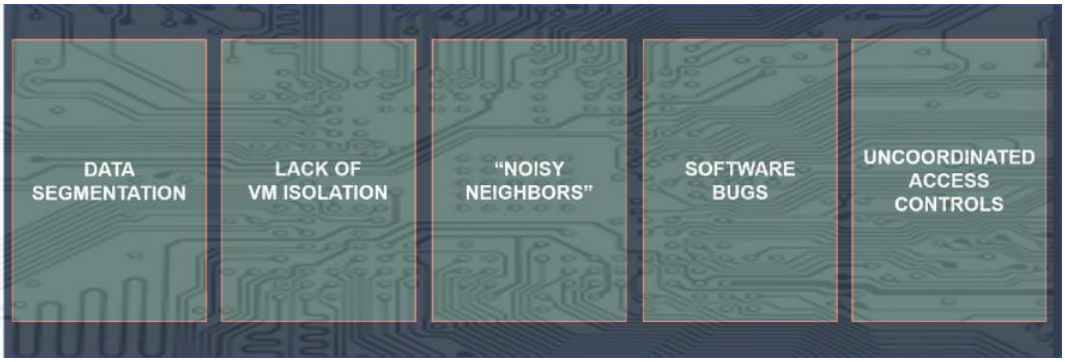


Source: Moor Insights & Strategy

LEVERAGING PARTNERSHIPS PART II - NEW SECURE VM ISOLATION WITH INTEL XEON

New to the HPE security portfolio is Secure VM Isolation, a jointly engineered technology that drives absolute isolation of virtual machines on Intel-based Gen10 ProLiant servers. This solution seems to be tailor-made for multi-tenant environments as it secures and isolates virtual machines from one another.

FIGURE 3 – MULTI-TENANT CHALLENGES

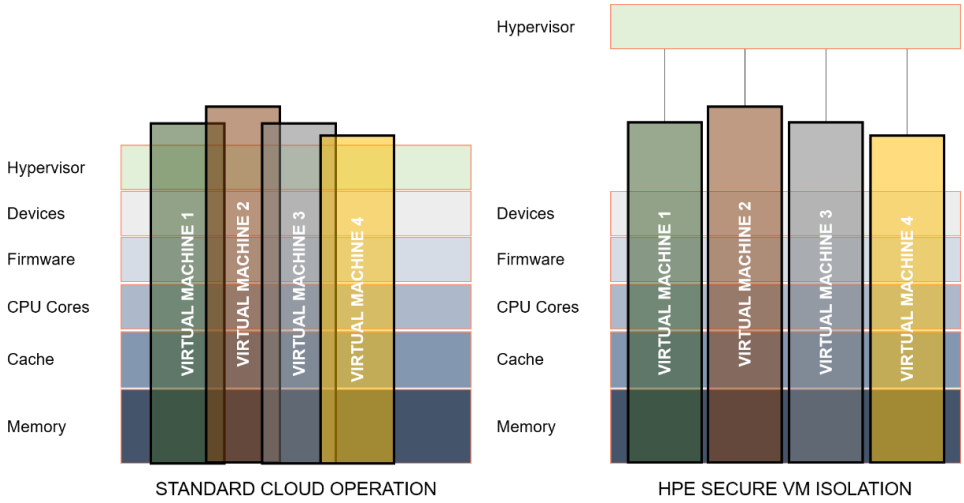


Source: Moor Insights & Strategy

Secure VM Isolation is built on a custom, hardened KVM hypervisor. After booting to a pristine operating environment, the trusted virtualized environment is launched. Virtual

machines receive dedicated compute and memory. This deployment locks "neighbors" from accessing a VM's resources, enabling security, reliability and consistency of performance.

FIGURE 4 – HPE – INTEL SECURE VM ISOLATION



Source: Moor Insights & Strategy

ENDPOINT PROTECTION IS KEY

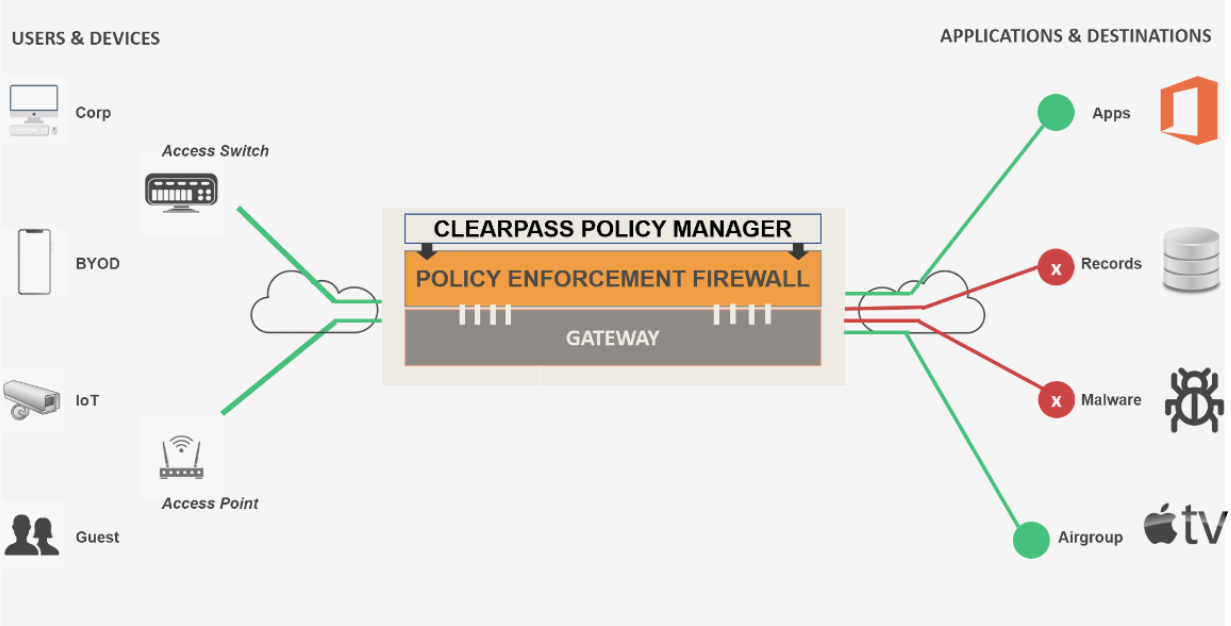
While HPE servers ship with arguably the tightest security controls in the industry, a complete security solution must account for endpoint devices as well. The Internet of Things (IoT) and Industrial Internet of Things (IIoT) have helped usher in the era of edge computing. The millions of new devices populating “the edge” present an opportunity for businesses to gain invaluable intelligence that can increase productivity and operational efficiencies.

While edge computing introduces many benefits to an organization, it presents even more risk as every device and sensor connected to the network presents a new potential vulnerability. One of the benefits of HPE’s acquisition of leading network company Aruba is a product portfolio that takes a “zero trust” approach to the market.

Indeed, Aruba is well known for its robust security capabilities in the area of networking connectivity—independent of whether the connection is wired, wireless, WAN or remote. As more companies look to expand and enhance edge environments, the potential security vulnerabilities introduced by IoT and IIoT will keep cybersecurity

teams awake at night. Aruba ClearPass Policy Manager combined with the Policy Enforcement Firewall, delivers Aruba's Dynamic Segmentation access control system. ClearPass Policy Manager authenticates users and devices and assigns a pre-determined role and IT access privileges associated with that role. Aruba's Policy Enforcement Firewall (PEF) utilizes identity-based polices and Layer-7 application visibility to deliver zero trust role-based access control at the point of connection. This removes the edge security gap that is typical with other network architectures and access control systems.

FIGURE 5 – POLICY ENFORCEMENT FIREWALL (PEF) ENFORCES DYNAMIC SEGMENTATION



Source: Moor Insights & Strategy

MARSH CYBER CATALYST DESIGNATION

Marsh, a leader in insurance brokering and risk management, announced the Cyber Catalyst designation for cybersecurity providers whose solutions, in the view of the leading cyber insurance providers, demonstrate an ability to reduce cyber risk for organizations. HPE's exclusive Silicon Root of Trust and Aruba's Policy Enforcement Firewall (PEF) both received this designation. Silicon Root of Trust was the only server hardware technology to be awarded the Cyber Catalyst designation.

WHAT IS THE CYBER CATALYST PROGRAM?

Created by Marsh and headed by Tom Reagan, a 15-year veteran of the industry, the Cyber Catalyst program brings together eight of the leading cyber insurers in the world with the common cause of identifying those cybersecurity solutions they believe can help organizations of all sizes.

The designation of Cyber Catalyst is awarded to cybersecurity solutions that participating insurers believe can have a meaningful impact in assisting organizations in reducing cyber risk. The insurers (Allianz, Axis, AXA XL, Beazley, CFC, Munich Re, Sompo International, and Zurich North America) conduct a comprehensive vetting of submitted products and services (with technology advice from Microsoft) to determine a products worthiness of designation.

WHY THE MARKET NEEDS THE CYBER CATALYST PROGRAM

No rational IT professional would say "I am completely confident in my organization's cyber resilience, and I never worry about my company's data being held ransom." Rather, the most vigilant IT security professionals live in a perpetual state of paranoia. Virtually every company struggles with securing its infrastructure and data.

The number of cybersecurity solutions providers claiming to have all the answers is seemingly countless. This market dynamic has made it difficult for the average IT organization to effectively research and evaluate the products and solutions that make the cyber resilience continuum – from prevention to recovery to lifecycle management.

The Cyber Catalyst program should bring some much-needed clarity to the cybersecurity market. IT consumers can make more informed decisions. This should lead to better-protected clients for insurers, who are motivated to write fewer checks. Additionally, IT organizations adopting products with the Cyber Catalyst designation may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

As this was the initial program cycle for Cyber Catalyst, over 150 solutions and products were nominated to the committee by a large number of companies. Out of the 150 initial submissions, approximately 135 were considered. After two rounds of presentations, the final pool of nominees was required to perform product demonstrations. In the end, 17 designations were awarded. Of the 17 designations, two belonged to HPE developed technology.

CYBERSECURITY IS COMPLEX – DON'T GO IT ALONE

Creating a comprehensive cybersecurity program that accounts for processes, people and products and solutions is difficult. Working with a third party to create the processes, navigate the technical waters and deploy a completely integrated solution is beneficial for several reasons.

There are a lot of qualified organizations that can bring the depth and breadth necessary to deliver a holistic cybersecurity strategy and its execution. Moor Insights & Strategy sees HPE Pointnext as uniquely qualified, as the organization brings best practices from consulting some of the world's largest organizations and a fully developed portfolio of technology – from hardware to software.

By working HPE Pointnext, organizations gain access to a suite of best practices that span assessment to deployment to testing and managing cybersecurity solutions. Additionally, the Pointnext team has developed best practices for different verticals, accounting for the nuances and regulatory requirements that drive technology and deployment decisions.

Finally, Pointnext can fully test and assure cybersecurity product readiness through a unique crowdsourcing technique. Hundreds of partners work to look for holes and gaps in the Pointnext developed solution – ensuring the tightest security.

CALL TO ACTION

The world of cybersecurity is becoming less safe daily. As hacking and exploitation tools become more sophisticated and highly publicized ransomware attacks hit the news on a seemingly daily basis, more and more bad actors are motivated to jump in the game.

Virtually every organization is at risk. Until the release of the HPE ProLiant Gen10 server platform, servers were at risk of low-level attacks that can spoof firmware and drivers and exist for months without detection – leading to siphoning of data or ransomware attacks.

IT organizations of all sizes would be well-served to take inventory of infrastructure to better understand the potential security holes that exist. Additionally, look at the processes that exist for ensuring cyber-readiness, including the on-going training programs for employees and regularly scheduled exercises to ensure organizational readiness.

IT organizations would be wise to consider HPE in delivering organization-wide cybersecurity solutions for many reasons:

- A security first mindset that spans the supply chain – from sourcing of components to the manufacturing of boards and systems.
- HPE-exclusive Silicon Root of Trust (S-RoT) delivers unparalleled security without compromising performance.
- HPE Server System Restore works with S-RoT to enable real-time response and recovery from the most insidious cyberattacks.
- HPE One Button Secure Erase completes lifecycle protection by securely erasing every trace of data from servers as they reach end-of-life.
- Proven track record of technology that can prevent malware attacks from taking root.
- A team of professionals in Pointnext who bring experience, technology and partnerships to ensure the tightness of security deployments across the globe and across industries.
- Validation of its unique capabilities via its Cyber Catalyst designation from Marsh.

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 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 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.