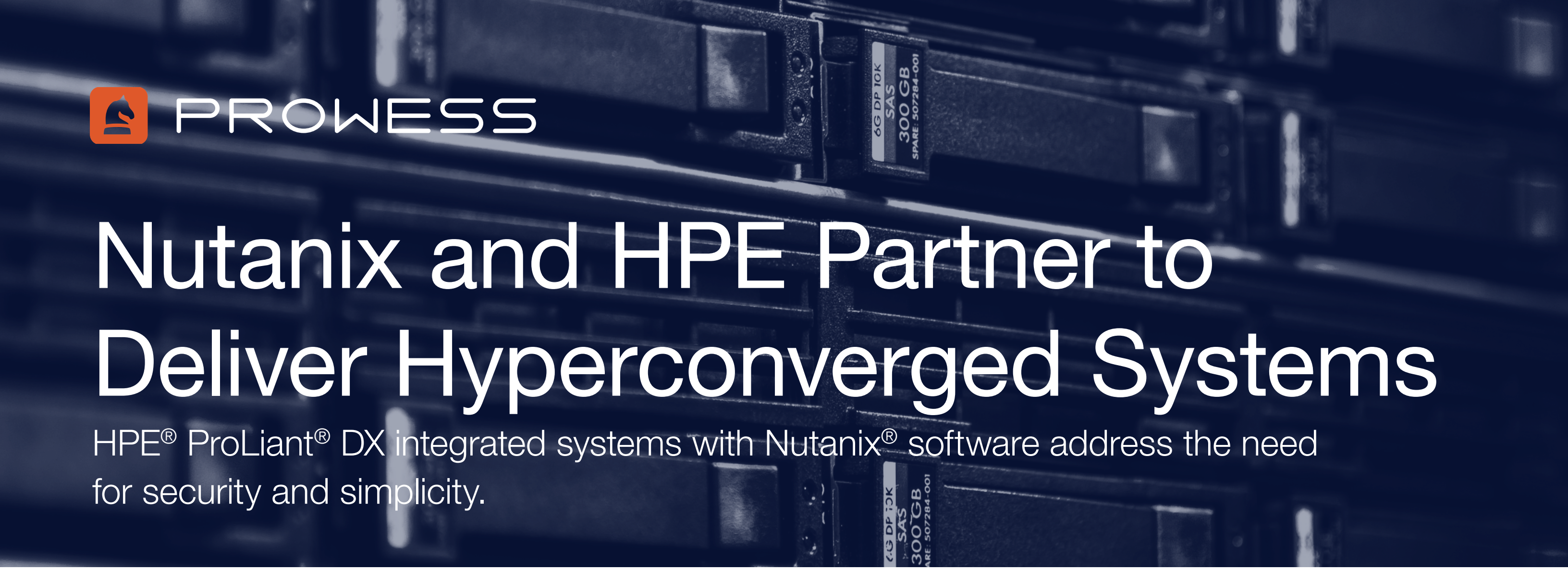

Nutanix and HPE Partner to Deliver Hyperconverged Systems

HPE® ProLiant® DX integrated systems with Nutanix® software address the need for security and simplicity.

The End of an Era

Legacy infrastructure—with separate servers, storage, and network components acquired piecemeal over time from various vendors—has become burdensome to IT departments. Expensive to purchase, complex to manage, and difficult to protect, these legacy systems often require the support of multiple teams of specialists just to stay running smoothly and free from attacks. However, when IT departments act as their own system integrators in this way—taking on the job of ensuring the compatibility and integration of components from various high-tech providers—unforeseen challenges tend to arise with the security, complexity, and costs associated with the system as a whole.

For starters, customer-integrated systems are not often tested together thoroughly, which increases their "attack surface" for intruders, and makes them inherently more vulnerable to threats. To make matters worse, the complexity of legacy systems can make it difficult to find the specialists needed to maintain them.[1] And finally, legacy infrastructure is often costly. In one survey of IT and finance leaders, 77 percent said a major obstacle to innovation in the company is "spending too much keeping the lights on."[2]

Facing these challenges, IT organizations are increasingly turning to hyperconverged infrastructure (HCI) as a more secure, simple, and cost-effective approach to managing and scaling infrastructure. HCI delivers servers, storage, and virtualization software components that are all pre-integrated in a single solution.

Among many other advantages, HCI solutions tend to be more secure than legacy infrastructure. The tightly integrated and pre-tested nature of an HCI system presents a smaller attack surface, thereby lowering the potential for vulnerability introduced through misconfiguration or human error. Also, in comparison to data centers in which each server is chosen independently, HCI can offer better protection against attacks targeting below the operating system (OS) when all nodes are guarded by a root of trust based in hardware.

Highlights

- Traditional IT infrastructure is expensive to acquire, complex to manage, and difficult to protect.
- IT organizations are increasingly turning to hyperconverged infrastructure (HCI) as a more secure, simple, and cost-effective approach to managing and scaling infrastructure.
- Nutanix has partnered with HPE to offer a line of all-in-one HCI integrated systems based on HPE® ProLiant® and Apollo servers with Nutanix® HCI software preinstalled.
- Nutanix and HPE together handle the job of defending these integrated systems from the variety of threats that IT systems face with sophisticated security measures from bottom to top.
- Tools and features from HPE simplify the management of firmware and hardware components, and Nutanix brings simple, comprehensive management of the virtualized environment from one dashboard.

HCI is also simpler to manage throughout its lifecycle. HCI virtualizes everything, manages all resources centrally, and allows you to scale to meet any need by simply adding more nodes, without the need to analyze workload requirements and assign specific resources. Supporting HCI can also be less expensive than supporting legacy infrastructure because it requires fewer administrators and specialists.

Despite the significant advantages of HCI, HCI solutions in practice might, at times, fail to live up to their promise of improved security, simplicity, and total cost of ownership (TCO). For example, customers can make the mistake of acquiring HCI software separately from hardware, resulting in an installation procedure that does not lead to a truly unified, integrated solution that simplifies management and lowers costs. Many HCI solutions outside of the HPE and Nutanix offering also lack the security features throughout the entire hardware and software stack that are necessary to protect it from modern attacks.

Introducing HCI Systems Based on Nutanix Software and HPE ProLiant DX Servers

Nutanix, a leader in HCI software, has partnered with HPE to offer a line of all-in-one HCI integrated systems based on highly secure HPE® ProLiant® and Apollo servers. This paper examines how well these Nutanix® and HPE® integrated systems fill the gap and deliver on the promise of security and simplicity.

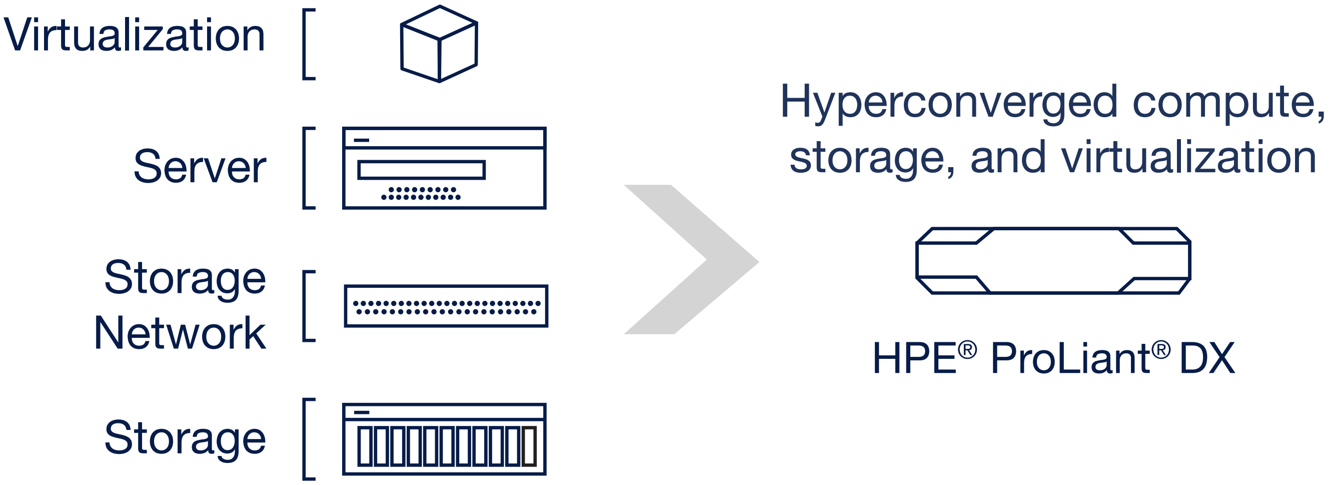

Figure 1. The Nutanix and HPE hyperconverged system includes everything in one box

Security

The scale of cybercrime has become enormous. According to the FBI, cybercrime cost more than $3.5 billion in the US in 2019, while other estimates place the cost of ransomware alone at more than $9 billion.[3] No wonder security is what keeps IT decision makers awake at night. This section examines how Nutanix and HPE each handle the job of defending their integrated systems from the variety of threats that IT systems face.

Nutanix Security

The Nutanix® AHV® hypervisor (the foundation of Nutanix HCI software) is hardened by design, adhering to the principle of least privilege and delivering a true defense-in-depth model. Its custom security baseline conforms to the requirements of the US Department of Defense (DoD). Meeting these high security standards enables Nutanix to be compliant in bidding on contracts with the US DoD.

Nutanix combines features such as two-factor authentication and data-at-rest encryption with a security-development lifecycle. These features are integrated into product development to help meet the most stringent security requirements. Nutanix systems have been certified to meet strict security and guidelines across a broad set of evaluation programs.

The Nutanix security strategy rests on three strong pillars:

- Nutanix HCI design is fundamentally more secure than mix-and-match infrastructure, because it eliminates untested attack surfaces in the gaps between components. All the HCI storage, compute, and virtualization software are tightly integrated and tested with security-configuration best practices applied by design; and patches are thoroughly tested across the storage, compute, and virtualization software elements to help ensure they are fully compatible and error-free before they are sent to the customer.
- The Nutanix Security Technical Implementation Guide (STIG) is more than a guide or best-practices document; it's machine-readable, and Nutanix software uses it to automatically configure itself to a hardened standard. Nutanix automates the regular health-checking of the applied STIG, and if the system configuration is not compliant, the software will reapply the baseline settings.
- Nutanix® Flow microsegmentation secures east-west traffic inside the perimeter to prevent any breach from propagating within the virtual environment. Nutanix Flow provides granular control and governance of all traffic into and out of a virtual machines (VM) or groups of VMs.

Nutanix software provides superior security against perimeter threats and against propagation of damage at the VM and application level in the event of a breach. There are new kinds of attacks, however, that no software can protect against. These target vulnerabilities at the firmware level, below the level of the operating system or hypervisor. The best protection against these firmware-level threats is to be secured in the silicon.

HPE® Silicon Root of Trust

Today's servers can run more than a million lines of firmware code before launching the operating system. This firmware attack surface is becoming a more frequent target for attacks because the firmware code operates in a privileged position. If compromised, a breached system can go for months without being detected.[4] Third-party penetration testing of HPE firmware confirms the impressive strength of its defense, which is founded on HPE's Silicon Root of Trust.[5]

> "The Silicon Root of Trust from Hewlett Packard Enterprise (HPE) has been designated a 2019 Cyber Catalyst cybersecurity solution. … Cyber Catalyst participating insurers rated the HPE Silicon Root of Trust highest on the criteria of differentiation, performance, viability, efficiency, and flexibility."
>
> **— Marsh[6]**

Silicon Root of Trust protects against firmware attacks and exposes previously undetectable firmware and malware threats. It can recover itself to a known secure state, with trusted firmware, and without manual intervention.

The key to Silicon Root of Trust is that all firmware is scanned and monitored through a series of integrity checks that initiate from a silicon fingerprint. When the server is manufactured, a digital fingerprint is created. Every time the system boots up, that digital fingerprint is compared to the firmware, and if they don't match, the system is smart enough to know that the firmware has been corrupted. The server won't boot. In addition, the system can regularly check the firmware to make sure no one has tampered with it, and it can even recover to a known-good state.

Once authenticated, the chain of trust is then passed upward to the UEFI/BIOS, the operating system bootloader, and the hypervisor, as shown in Figure 2.

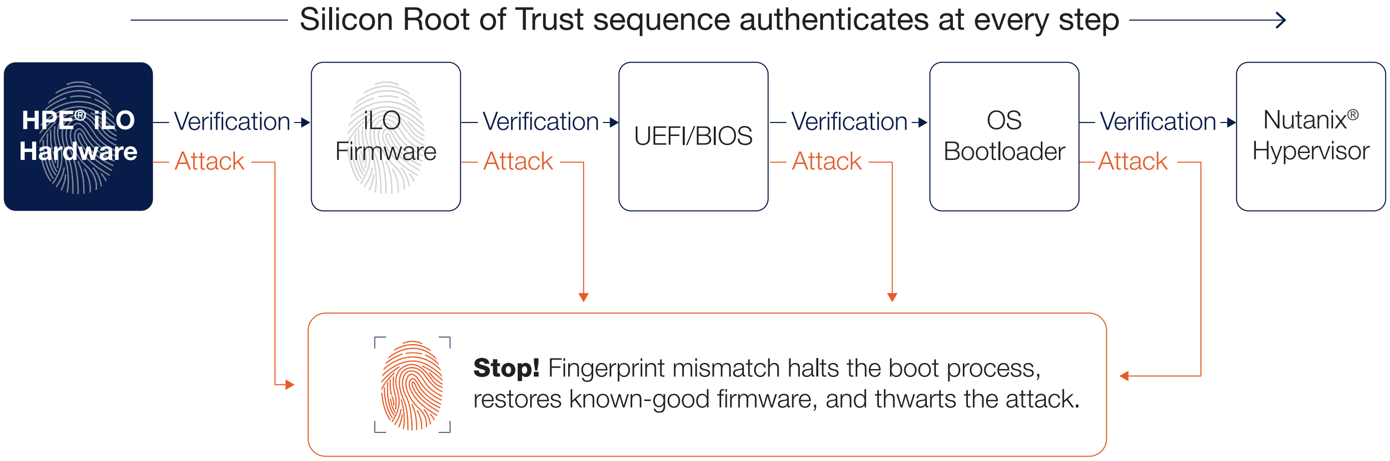
Silicon Root of Trust sequence authenticates at every step
HPE® iLO Hardware
Verification
Attack
iLO Firmware
Verification
Attack
UEFI/BIOS
Verification
Attack
OS Bootloader
Verification
Attack
Nutanix® Hypervisor
Stop! Fingerprint mismatch halts the boot process, restores known-good firmware, and thwarts the attack.

Figure 2. HPE® Silicon Root of Trust

Other HCI systems use roots of trust and chains of trust, but HPE Silicon Root of Trust provides the following distinguishing features:

- Only HPE manufactures its own custom application-specific integrated circuit (ASIC), the HPE® iLO 5 chipset, with the fingerprint burned into the silicon right in the fabrication facility. This unbreakable connection between the silicon and firmware protects the system starting early in the production process, and continuing through supply-chain shipping and distribution to the customer's final location.
- Silicon Root of Trust verifies all the firmware not only at boot time but daily. This includes firmware for iLO, complex programmable logic devices (CPLDs), innovation engines (IEs), server platform services (SPS), UEFI/BIOS, and option ROMs.
- Not only does Silicon Root of Trust identify a fingerprint mismatch and prevent booting up, but it also recovers automatically from a compromised firmware event by reverting to a known-good, secure state.

HPE systems include many security features in addition to Secure Root of Trust, including a single security dashboard, Commercial National Security Algorithm (CNSA) security modes, data collection for forensic evaluation, one-button secure erase, and secure VM isolation, among others. Because of this high level of security, HPE has been awarded the Cyber Catalyst Designation by Marsh, a leading insurance broker and risk advisor—which can mean better terms and conditions for cyber-insurance policies with participating insurers.[6]

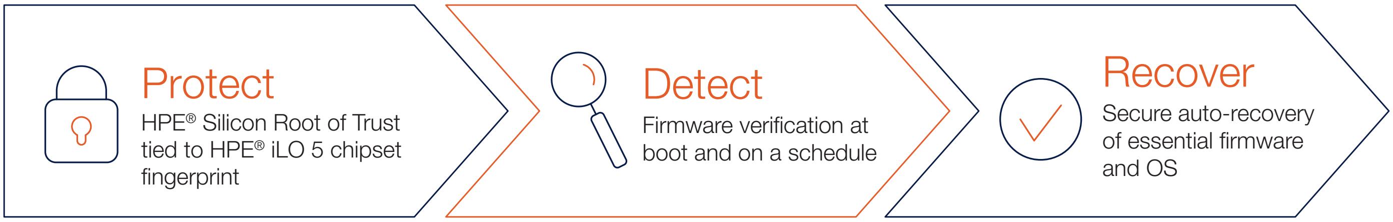
Protect
HPE® Silicon Root of Trust tied to HPE® iLO 5 chipset fingerprint
Detect
Firmware verification at boot and on a schedule
Recover
Secure auto-recovery of essential firmware and OS

Figure 3. HPE firmware security strategy: protect, detect, and recover

Simplicity

HPE ProLiant DX integrated systems include a number of tools and features that simplify the management of firmware and hardware components, along with a growing artificial intelligence (AI) element that automates maintenance tasks and moves toward a self-driving infrastructure. Nutanix® Prism® brings simple, comprehensive management of the virtualized environment from one dashboard. Together, HPE and Nutanix co-engineered this integrated HCI system to enable one-click lifecycle management from the VM down to the firmware and hardware.

HPE Infrastructure Automation with HPE® InfoSight® for Servers

HPE® InfoSight® for Servers provides a solution for customers challenged by the cost and complexity of managing IT infrastructure. InfoSight brings AI and predictive analytics to the data center to protect from system failure and security risks.

Data is collected from millions of sensors on hundreds of thousands of servers across the globe, tapping into the health and performance monitoring capabilities of iLO and Active Health System (AHS). This global data is then analyzed to predict and prevent problems locally before business operations can be disrupted.

The InfoSight for Servers wellness dashboard proactively monitors and identifies infrastructure issues, and it provides email notification for parts failures, security events, and software issues, including the firmware and drivers, in addition to the OS.

Support cases can be created within InfoSight to provide support teams with access to all the AHS files collected from the servers to expedite support resolution.

Nutanix® Prism® for Simplified Lifecycle Management

Nutanix pioneered HCI development and has been positioned as a Leader in the Gartner® Magic Quadrant® for HCI for three years running, most recently in November of 2019.[7]

Nutanix Prism provides a single screen that allows IT admins an easy way to manage infrastructure and Nutanix virtualization environments from end to end: Prism provides a single screen that allows IT administrators to manage infrastructure and virtualization, gain access to operational insights, and fix problems—all with a few clicks.

Prism is designed for an uncluttered experience with an intuitive user interface (UI) that simplifies and streamlines common data center workflows, eliminating the need to have different management tools for different tasks. Prism enhances productivity through features such as:

- **Instant search:** Integrated search enables users to query and perform actions quickly.
- **Capacity planning:** The predictive analysis engine in Prism forecasts the capacity needs of applications running on a Nutanix cluster, giving the IT team the ability to proactively understand and plan for infrastructure needs.
- **Customizable operations dashboard:** The visual dashboard gives an at-a-glance summary of the state of the application and infrastructure.
- **Integrated management:** Infrastructure management, operational insights, and problem remediation are all integrated for simplicity.

As a result of these features, organizations can use Prism to inventory their infrastructure in minutes, identify what needs to be updated, and reliably upgrade both Nutanix and HPE components accordingly. Directly through Prism, Nutanix life-cycle management provides one-click upgrades for Nutanix core software of the Nutanix® Acropolis® operating system (AOS), Nutanix® Cluster Check (NCC) and Nutanix® Foundation provisioning software, in addition to one-click firmware updates for the HPE ProLiant DX platforms, including HPE iLO, BIOS, solid state and hard disk drives, host bus adapters (HBAs) such as the HPE® Smart Array controller, and networking interface cards (NICs).[8]

Performing system software updates is a simple and non-disruptive process that is fully cluster-aware. In order to ensure high availability, the life-cycle manager runs pre-checks to confirm that it is picking a "healthy" node for upgrades. After upgrades, checks are run again at the node and cluster level to ensure a "healthy" state before moving on to upgrading the next node. From the Prism dashboard, users can simply click and download the desired software version from the cloud. The new software installation is automatically orchestrated across all nodes. Each node is first evacuated by moving its VMs and workloads to other nodes, then upgraded and rebooted as necessary. The complete verification of the upgraded system against Silicon Root of Trust is completed before workloads are returned to the node.

In addition to the easy manageability of the system using Prism, other Nutanix features that simplify administration include:

- Nutanix systems are hypervisor-agnostic, though the Nutanix AHV hypervisor is included at no cost. Each node in a cluster runs a hypervisor (Nutanix AHV, VMware ESXi™, or Microsoft® Hyper-V®), and the Nutanix software runs on a VM called the controller VM (CVM), which operates on every node in the cluster.
- Data-path redundancy ensures high availability in the event a Nutanix CVM becomes unavailable or needs to be brought down for an upgrade. If a CVM becomes unavailable for any reason, Nutanix CVM auto-pathing automatically re-routes requests to a "healthy" CVM on another node. This failover is fully transparent to the hypervisor and applications.
- Nutanix offers award-winning technical support that gets you quickly to the expertise you need, and it has a cooperative support agreement with HPE for support issues that might be hardware-related.

ROI on the Bottom Line

The hardened security and simplified manageability offered by Nutanix with HPE ProLiant DX integrated systems does more than just make life easier for IT teams. It improves the agility and ability of IT to respond to changing business needs, and it reduces maintenance cycles, unexpected downtime, and costly security breach responses. This means a net advantage on the business bottom line in terms of return on investment (ROI).

Based on customer interviews, IDC calculates that Nutanix customers will achieve average annual benefits of $13.44 million per organization in 2020 (approximated to $46,876 annual benefit per 100 employees/IT end users), which would result in an average five-year ROI of 477 percent.[9]

This return is achieved by:

- Making use of an agile, scalable, cost-effective, and high-performing IT platform to enable employees to improve business results
- Minimizing the effects of unplanned downtime on businesses, thereby contributing to greater productivity for business units and reduced revenue losses
- Needing less IT staff time to manage and support compute and storage resources, and better developing and deploying applications to staff and customers
- Establishing more cost-effective IT infrastructures and reducing licensing and other ongoing operational costs

Learn More

- HPE ProLiant DX systems integrated with Nutanix: **www.nutanix.com/hpe**
- HPE InfoSight: **www.hpe.com/us/en/solutions/infosight.html**
- Nutanix Prism: **www.nutanix.com/products/prism**
- HPE infrastructure security: **www.hpe.com/security**
- Nutanix infrastructure security: **www.nutanix.com/products/acropolis/security**

[1] According to Enterprise Strategy Group (ESG) research, 38 percent of organizations have a problematic shortage of existing skills in IT architecture/planning, with 33 percent indicating a problematic shortage in IT orchestration and automation. Source: ESG. “Industry Analyst Viewpoint: HPE ProLiant DX Appliances Powered by Nutanix.” Commissioned by Nutanix. October 2019. **www.nutanix.com/go/hpe-proliant-dx-appliances-powered-by-nutanix**.

[2] David Rowe. “Biggest Obstacle to Innovation, IT Leaders Say: ‘Keeping the Lights On.’” Rimini Street blog. June 2018. **www.riministreet.com/blog/biggest-obstacle-to-innovation-keeping-the-lights-on**.

[3] Computer Business Review. “Cybercrime Cost Business $3.5 Billion in 2019, Says the FBI: It’s Likely a Massive Underestimate.” February 2020. **www.cbronline.com/news/cybercrime-cost-fbi**.

[4] According to a FireEye survey, the median dwell time before an intrusion was detected between October 1, 2018, and September 30, 2019, was 56 days, which represents an improvement over previous years. Source: FireEye Mandiant Services. “M-Trends 2020 Special Report.” 2020. **https://content.fireeye.com/m-trends/rpt-m-trends-2020**.

[5] ”World’s most secure” claim based on InfusionPoints penetration testing of a range of servers from a range of manufacturers in 2017. Source: HPE. “HPE unveils the world’s most secure industry standard servers.” June 2017. **www.hpe.com/us/en/newsroom/press-release/2017/06/hpe-unveils-the-worlds-most-secure-industry-standard-servers.html**. For more details on the InfusionPoints testing, see: InfusionPoints. “InfusionPoints’ work featured at HPE Discover Europe.” **www.infusionpoints.com/insights/news/infusionpoints-security-testing-and-research-featured-hpe-discover-2017-europe**.

[6] Marsh. “Silicon Root of Trust — Cyber Catalyst Designation.” 2019. **www.hpezone.com/assets/pdf/HPE-Silicon-Root-of-Trust-Cyber-Catalyst-2019-Fact-Sheet.pdf**.

[7] Nutanix. “Nutanix—a 3-Time Leader!” **www.nutanix.com/go/gartner-magic-quadrant-for-hyperconverged-systems**. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[8] ESG. “Industry Analyst Viewpoint: HPE ProLiant DX Appliances Powered by Nutanix.” Commissioned by Nutanix. October 2019. **www.nutanix.com/go/hpe-proliant-dx-appliances-powered-by-nutanix**.

[9] Nutanix. “Organizations Leverage Nutanix Enterprise Cloud as Scalable, High-Performing, and Cost-Effective Infrastructure Foundation.” **www.nutanix.com/viewer?type=pdf&lpurl=/go/nutanix-enterprise-cloud-tco-roi**.

The analysis in this document was done by Prowess Consulting and commissioned by Nutanix and HPE. Prowess and the Prowess logo are trademarks of Prowess Consulting, LLC.