

A Data Center that Serves Your Critical Missions

Engage efficiency to ensure that your data is secure and working in tandem with new technology

Old Technology. Retiring Engineers.

For decades, your trusted engineers have held your legacy systems together with the technological equivalent of duct tape and bailing wire. But now they're starting to retire.

To keep your organization moving forward, your hardware and software systems must employ the latest technologies. But perhaps even more important, those technologies must be based on the skillsets possessed by the new generation of engineers.

It has never been efficient or cost-effective to prolong the life of your obsolete data center. The right time to make changes for the future is now. Make a strategic move toward seamless, innovative, and secure technology to maintain data integrity in the 21st century.

No Time Like the Present...

- **Increase Efficiency:** Major advances in both hardware and software will enable you to continue using your legacy data and systems within a fully modern environment.
- **Migrate Archaic Software:** Repackage your old but critical software so the new hardware can supercharge its performance.
- **Let Someone Else do the Work:** Use the cloud to relieve space constraints, save money, simplify maintenance, and access the latest gear.

High Performance Computing (HPC)

Today's HPC solutions let even modestly sized organizations benefit from the latest Big Data, AI, and Data Center advances.



**Hewlett Packard
Enterprise**

Containerization

Containerizing your legacy software dramatically improves system performance and security while freeing you up from obsolete hardware and associated maintenance costs.



Cloud Computing

With a FedRAMP-certified HPE ProLiant cloud solution, all firmware is certified and updated automatically, relieving your team of that expensive and time-consuming chore.





Speed: Organizations like the National Renewable Energy Laboratory (NREL) and Sandia National Laboratories use lightning-fast HPCs to model complex systems more efficiently. These systems have become increasingly affordable thanks to innovations such as the use of networked Arm processors.



Innovation: The new containerization paradigm creates multiple isolated OS user-space instances. Each one looks like a separate computer from the point of view of programs running in it. However, programs running in a container can only see the contents and devices assigned to that container. This improves security and efficiency, particularly through the containerization of legacy apps.



Scalability: The hybrid cloud solution (with on and off premise components) will allow you to minimize maintenance costs, increase efficiency, while still following government security rules. The cloud simplifies operations and gives agencies freedom to grow unencumbered, in accordance with their missions.

Data Center Technology in Motion

Westwind and HPE partnered with Sandia National Laboratories to deploy the Astra platform, the fastest Arm-based supercomputer in the world. Arm processors previously had been used exclusively for low-power mobile computers, including cell phones and tablets. A single Astra node is roughly one hundred times faster than a modern Arm-based cell phone, and Astra has 2,592 nodes.



Ready for a data center?

Connect with us at info@wwcpinc.com.

Put Your Technology in motion — 866-345-4720





Automate security compliance management

HPE Workload Aware Security for Linux

What is HPE Workload Aware Security for Linux (WASL)?

HPE WASL, the foundation for a secure data center, is an intuitive one-click security compliance tool to secure the HPE and Linux systems (RHEL and SLES), as well as HPE and SAP HANA appliances/TDI. It provides a security policy framework to meet evolving security needs, based on industry standard, The Center for Internet Security® (CIS) benchmarks and application security guides. It is the industry's first software compliance tool to secure both SAP HANA and Linux infrastructure, that too in minutes.

Why is HPE WASL important?

HPE WASL brings a wealth of new capabilities and delivers a wide range of benefits for both business users and IT departments. HPE WASL helps business users in preventing any unauthorized or unintentional use. For IT, HPE WASL helps in monitoring the security posture of systems deployed and take corrective actions.

What's new in HPE WASL 1.3?

- Ease of migration 1.2 to 1.3
- Policy update and alerts
- SMS as virtual appliance
- Migrate to production version from 30-day evaluation version

Industry-standard support

- CIS Benchmarks for RHEL 7, SLES 12 Operating System
- SAP HANA Security Guide

Accidental or unintentional breaches constitutes over 50% of insider attacks through user carelessness or negligence as they are from deliberate malicious insiders. Over 50% of employees or IT privileged users with access to databases and file servers pose the biggest risk to organizations. The cost of a successful breach can range from \$100–500K.¹ Deterrence methods employed to configure the organization-defined guidelines can offer to protect the digital assets.

Save cost

- Eliminate need for specialized security professionals
- Avert heavy fines and legal cost of non-compliance
- Avoid costly third-party managed security services

Reduce complexity

- Secure multiple SAP HANA® and operating system instances in minutes not in weeks
- Always comply to changing application security guidelines
- Eliminate multiple tools to secure OS and application

Eliminate risk

- Automate server hardening, eliminate error-prone manual steps
- New policy alerting feature
- Single dashboard to measure cybersecurity posture and threat exposure

Mitigating risk of internal threats

One-click security

Secure in minutes

Continuous compliance

Comprehensive audit and actionable reports

Complete audit trail

Faster security ramp to production

Figure 1. HPE WASL value proposition

Automated security compliance for SAP HANA and Linux® OS

Purpose-built for SAP HANA

- Unique solution to secure SAP HANA database and the underlying operating system
- Comprehensive audit reports
- No separate training required for system administrators

Easy deployment

- Push-button security for operating system and SAP HANA workloads
- Ability to customize default security profiles shipped with the product
- Integrate existing hardening scripts and into custom security profiles

Shorten time to production

- Security compliance in minutes instead of days²
- ~90% out-of-box compliance for SAP HANA and operating system with default profiles³

Superior ROI

- Single-click evaluation and remediation operation
- Continuous compliance to organization guidelines
- Automated guidelines eliminates need for specialized knowledge

Modern

- Automatic security compliance with periodic scans on workloads to bring back into stated compliance level
- Provides a rollback option to reinstate to previous compliance state

¹ Insider threat report, Crowd Research Partners, 2018

^{2, 3} HPE internal lab test, June 2019

Supported workloads in physical or virtualized environment

- SAP HANA 1.0 SPS11
- SAP HANA 1.0 SPS12
- SAP HANA 2.0 SPS00
- SAP HANA 2.0 SPS01
- SAP HANA 2.0 SPS02
- SAP HANA 2.0 SPS03
- RHEL 7.2, 7.3, 7.4, 7.5, 7.6
- SLES 12 SP1, SP2, SP3, SP4
- SLES for SAP® Applications 12 SP1, SP2, SP3, SP4
- SLES 15*
- SLES for SAP HANA Applications 15*

Supported hardware platforms

- Any HPE x86-64 server

HPE WASL SMS requirements

- 16 GB lockable memory
- 30 GB disk space
- 4 cores minimum
- VMware ESXi™ 6.0, 6.5, 6.7

HPE WASL support

- HPE Foundation Care Service
- HPE Proactive Care Service
- HPE Proactive Care Advanced Service

How to order

Order HPE Workload Aware Security for Linux (WASL) through your HPE sales distributor.

- HPE Workload Aware Security for Linux (Basic) license is a low-cost offering for customers who want to assure security compliance for a Linux operating system instance only:
 - Q8K91AAE HPE WASL x86 Basic Instance E-LTU
 - Q8K91A HPE WASL x86 Basic Instance LTU
 - Q8K93A HPE WASL x86 Basic Media
- HPE Workload Aware Security for Linux (Advanced) license for SAP HANA appliance and TDI customers seeking application security compliance along with operating system security:
 - Q8K92AAE HPE WASL x86 Advanced Instance E-LTU
 - Q8K92A HPE WASL x86 Advanced LTU
 - Q8K94A HPE WASL x86 Advanced Media

Note: For SAP HANA scale-out implementation, an advanced license is required for the master node and basic license for each of the other nodes.

HPE WASL components

HPE WASL includes security management station (SMS) and node packages. SMS is a graphical user interface to centrally register, track compliance, and manage all the instances of servers and applications (called workloads) in the environment. SMS also provides role-based access control (RBAC) to meet a wide variety of security policies and procedures.

The node packages run on end-workload instance, performing operations such as evaluation and remediation by SMS. They are installed automatically on the target workload instance either during the workload registration or manually by the administrator.

HPE WASL can be ordered with a new system purchases or separately for existing server running Red Hat® Enterprise Linux 7 or SUSE Enterprise Linux 12. Physical delivery requires the software media to be ordered separately whereas electronic delivery includes a software download.

A license purchase includes one year 24x7 technical support and software updates service. Customer needs a valid support contract to get latest updates on HPE WASL and default set of policies.

Implementation services are available separately.

HPE WASL support information

Protect your business beyond warranty with HPE Support Services

HPE Support Services offer complete care and support expertise with committed response choices that are designed to meet your IT and business needs. With each support offer, customers can customize their reactive support level by selecting either 6-hour call-to-repair, 24x7 with 4-hour on-site response, or next business day on-site response.

Note: HPE and SAP HANA Appliance/TDI support contract do not cover WASL; a separate support contract for WASL is required.

Warranty

Hewlett Packard Enterprise will replace defective delivery media for a period of 90 days from the date of purchase.

© Copyright 2019 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. SAP and SAP HANA are trademarks or registered trademarks of SAP SE in Germany and in several other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware ESXi is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other third-party marks are property of their respective owners.

a00076420ENW, July 2019

AWS security program for cloud adoption

Securely adopting AWS at scale

Elements of the security practice

- **Logging and monitoring:** Visibility into issues as they arise
- **Encryption and key management:** Appropriate protection for your sensitive data
- **Access management:** Defined and established role-based access controls
- **Nearly continuous compliance:** Organizational visibility into compliance controls

“Engaging Natixis’ security, legal, and compliance personnel, Cloud Technology Partners, a Hewlett Packard Enterprise company, ensured that access to the AWS production environment was adequately protected, appropriate data governance mechanisms were in place, and full traceability of activities was available to fulfill regulatory requirements.”

— George Marootian, EVP, Head of Technology, Natixis.

AWS security practice

Our AWS security practice is developed by a group of architects, engineers, developers, and technology enthusiasts dedicated to defining, automating, and helping ensure secure environments on Amazon Web Services (AWS).

Following AWS, cloud security alliance (CSA), NIST, and other industry best practices, the security practice enables our clients to safely and confidently operate in compliant environments.

Gaining the benefits of cloud in a safe and secure manner requires successfully navigating a highly complex technical and regulatory environment. The security practice addresses the following challenges:

- **Infrastructure security and network protection**—Implement secure network components on AWS, including perimeter protection, VPC/subnet segmentation, and IDS/IPS capabilities
- **Data security**—Manage access and protection of sensitive data in the cloud
- **Identity and access management**—Establish appropriate mechanisms for user access to cloud environments based on the principle of the least privilege
- **Logging, monitoring, and audit trail**—Monitor the aspects of secure cloud operations and enable forensic capabilities
- **Governance, risk, and compliance**—Meet regulatory, audit, and legal requirements while retaining agility; enable nearly continuous governance and management practices
- **Industry standards**—Leverage AWS, cloud security alliance (CSA), ISO 270xx, and NIST guidelines to accelerate your cloud adoption journey

AWS security practice

We work with the world’s leading enterprises and financial institutions to solve their unique security, governance, and regulatory concerns when moving to the cloud. The security practice is a key component during the phases of the cloud adoption program providing a clear, safe, and secure path to end-to-end cloud adoption.

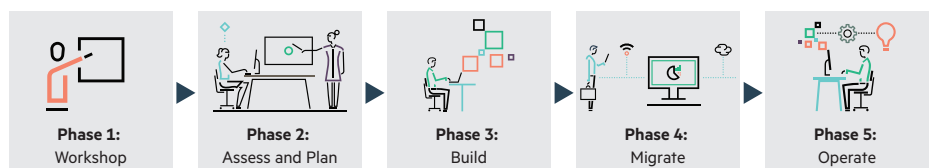


Figure 1. Enterprise cloud prescriptive approach

Client success story



Cloud adoption

How Natixis is pioneering cloud in the financial services industry—Natixis turned to HPE and AWS to securely support their future IT and business operational needs.

[Read the case study](#)

Security reinforcement

HPE Security Review Service for NonStop servers



Identify and address gaps in system security

HPE security consultants evaluate, analyze, and report on the security of your HPE NonStop servers. Our security consultants have extensive knowledge of HPE NonStop server and Safeguard access-control software. We work with your personnel to gather and analyze your data. Then, we recommend ways to enhance the security level of your system.

Upon completion of the security review, you will know the strengths and potential exposures of your current security implementation. A detailed report is

provided, comparing your existing security implementation to your company's policy and to HPE recommended guidelines for security.

HPE security consultants will meet with you and your staff to determine the appropriate form of data analysis for your system and your circumstances. Security constraints considered include data sensitivity, scheduling, system resources, and internal policies.

The analysis can take place at your site or off-site. Our service includes specific data extracted from your system on the following products: HPE NonStop Server, Safeguard, Pathway, HPE NonStop SQL, TMF, RDF, SNAX, and EXPAND. The typical security review service lasts approximately 12 to 15 days.





Service highlights

Features

- An extensive security analysis of your systems.
- Meetings with your staff at both the technical and management levels to discuss our results and findings.
- A confidential report that details our final conclusions and recommendations to improve the security of your systems. This report includes Safeguard Access Control Lists (ACLs) for each application group.

Benefits

- Identifies the strengths and weakness of the security on your systems
- Aids you in understanding how to identify potential security issues
- Helps minimize security review time with the use of automated tools
- Let's you take advantage of HPE built-in security features and best practices

HPE Security Standards and Compliance Assessment Service

SKU-based

Evaluate your organization's preparedness to protect your digital enterprise in accordance with ISO standards as well as prepare for compliance mandates.

An invaluable ISO/IEC 27001:2013 pre-certification review

HPE's Security Standards and Compliance Assessment Service is the perfect service to determine if your organization is on the correct trajectory toward certification.

HPE's own ISO 27001 (data center) certification experience as well as the knowledge of HPE's security consultants will guide your organization to a higher state of program maturity or certification should you desire.

Assessment focus areas

HPE's Security Standards and Compliance Assessment Service (full version) assesses and analyzes each of the following areas within the context of security and continuity:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- Systems Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Compliance

HPE Security Standards and Compliance Assessment Service

A sound security or continuity program begins with a strong foundation

Many organizations purchase multiple technologies to address their security and continuity concerns. However, experience teaches us that the root cause of many compromises and outages often start from overlooked gaps in controls and processes. In other words, a service-based approach to protecting your digital enterprise.

To find these gaps, HPE has developed an assessment approach that takes an objective look at an organization's security and continuity of operations resources and practices. We call this our P5 Model—People, Policies/Procedures, Processes, Products, and Proof. HPE evaluates the completeness of each of these control properties to determine the organization's overall InfoSec program capability.

Holistic view

A balanced control approach is the difference between success and failure

In order to understand your organization's security and continuity of operations program's capabilities, HPE uses a multi-dimensional assessment approach.

In conjunction with HPE's P5 Model, HPE evaluates whether control types and maturity are commensurate with your organization's attack surface. For example, do you have an overabundance of management vs. technical controls? HPE also evaluates your investments in technology in comparison to our unique defense-in-depth model to evaluate if you are over or under protecting against certain risks. One of the more insightful views provided is the information assurance perspective where HPE quantifies your controls as either detective, preventive, or corrective to determine if you have the right balance of control types.

Assessment framework

A standardized assessment requires a standardized control taxonomy

HPE selected the ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements standard to base its security and continuity of operations assessments.

- Fourteen (14) domains (ISO clauses)
- Thirty-four (34) disciplines (ISO second-level clauses)
- One hundred-fourteen (114) key controls

Solution brief

Hybrid assessment approach

HPE's Security Standards and Compliance Assessment Service can not only show you how you score according to the ISO 27001:2013 standard, but also provides insight into how your organization would score according to other well-known standards. Through a process called Equivalency Scoring, HPE can map your ISO 27001:2013 score to the following:

- Cloud Security Alliance (CSA) CCM
- CSA Big Data Working group
- HIPAA/HITECH
- PCI-DSS
- NIST 800-53
- CSA CIAQ (Mobility)
- Others

Assessment approach

Non-intrusive project approach

HPE uses a direct assessment methodology where first hand observations are used to evaluate displays of compliance consisting of personnel interviews, policy and procedures analysis, process/workflow review, technology assessment, and metrics evaluation. This approach surfaces the level of achievement of desired outcomes in a meaningful and diagnostic manner. We do our homework first, and then ask questions.

Service exclusions

The HPE Security Standards and Compliance Assessment Service excludes:

- Application security testing
- Penetration testing
- Vulnerability scanning

Service deliverables

The primary base service deliverables include:

- One (1) assessment report (summary)
- One (1) assessment spreadsheet (high-level gaps)
- Fourteen (14) interviews
- One (1) security awareness survey of up to (50) employees
- One (1) collaboration work session
- One (1) Equivalency Standard Score

- One (1) security breach calculation
- One (1) presentation of findings

HPE will provide project deliverables in Microsoft® Office products.

Service cost and duration

The HPE Security Standards and Compliance Assessment Service is available in a full and a "lite" version on a time and materials plus travel basis. The estimated project duration for the full service is four (4) to six (6) weeks, which allows time for client scheduling, control remediation research and personnel interview, analysis and reviews. Both the lite and full service can be scoped as required to fit customer needs. This service is orderable using the SKU HK411A1#004 and the appropriate number of Units of Service (UoS). Contact your TS Consulting pursuit Solution Architect for scoping and pricing assistance.

The HPE advantage

HPE Consulting Services has a wealth of experience in security and continuity technologies. Our consultants come armed with specialized methodologies and tools developed in-house and honed over many years. What's more, the global resources of the world's largest technology company back HPE security architects and consultants. HPE clients find our approach efficient, flexible, and collaborative.



505-345-4720 | WWCPINC.COM
SALES@WWCPINC.COM

**Hewlett Packard
Enterprise**

© Copyright 2016–2017 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. All other third-party trademark(s) is/are property of their respective owner(s).

4AA6-4688ENW, April 2017, Rev. 2



505-345-4720 | WWCPINC.COM
SALES@WWCPINC.COM

Simplify and save with the right cloud solution:

- Operated for you with cloud-native tools and expert services
- Common view of usage and cost
- Assists with workload placement and portability
- Expertise in each component, and a broad ecosystem of partners

Expertise from proven cloud leaders

With the addition of Cloud Technology Partners (CTP), HPE Pointnext Services gained significant IP and expertise in moving customers to the cloud. More than 400 customer engagements has led to the creation of proven methodologies and automation to help you move to cloud faster, maintain ongoing compliance and cost, and deliver business results faster—no matter where you are in your cloud transformation.

Simplify IT with a smarter hybrid cloud

HPE GreenLake Hybrid Cloud—cloud management services for your hybrid cloud

Nearly every enterprise is now in the process of moving to—or expanding their use of—cloud to speed the delivery of services, gain competitive advantage, and reduce operational costs. But without a doubt, cloud implementation has become complex and difficult for businesses to handle with only their internal IT resources. Many organizations realize that without the right expertise and cloud-native automation, they may expose themselves to undo risk and cost.

It's time for a simplified solution that helps you get the most from public cloud without high costs, a steep learning curve, and risks.

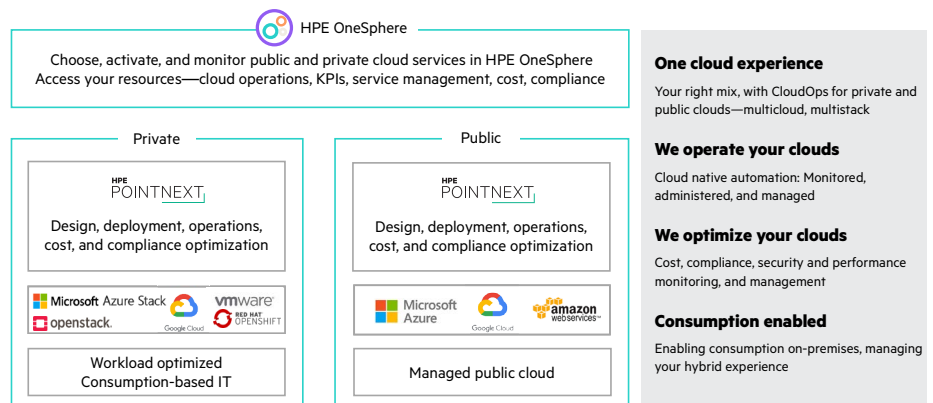
HPE GreenLake Hybrid Cloud delivers a managed cloud environment for your public and private clouds that automates cloud operations, with help to manage performance, cost, security, and compliance.

Starting first with services for Microsoft® Azure, and adding support for Microsoft Azure Stack and AWS, we will continue to add to the multicloud story over time.

A complete solution—managed in a way that works for you

Based on HPE best practices and intellectual property from Cloud Technology Partners (CTP), a Hewlett Packard Enterprise company, HPE GreenLake Hybrid Cloud helps speed time to value, lower costs, streamline operations, and help enable IT and regulatory compliance with purpose-built configurations that are designed, implemented, and operated for you.

Our cloud-native model means more automation, less “heavy lifting” by your team, and proper controls that help you start compliant and stay that way. With HPE GreenLake Hybrid Cloud, you can rapidly deploy a complete cloud solution, with the essential areas supported and operated for you. You are free to focus on applications and business outcomes while the experts from HPE Pointnext Services take care of the rest.



HPE GreenLake Hybrid Cloud: Cloud management services for your hybrid cloud



Key benefits

By moving to HPE GreenLake Hybrid Cloud, you can quickly realize the following key benefits:

Speed	Savings	Simplicity	Security
Faster time to value with proprietary cloud methodology and tooling	Lower costs using Continuous Cost Control services	Simplified IT, with cloud solutions planned, implemented and operated for you	Improved compliance capabilities with monitoring of over 1,500 IT, corporate, and regulatory controls
Increased speed of IT operations using cloud-native, automated model	More time to focus on strategic projects by offloading cloud operations	Single vendor support for your public and private clouds	Fifty percent reduction ¹ in time and effort to prepare for compliance audits
Accelerated design and implementation with expert services from HPE Pointnext Services	Reduced risk and labor costs by automating manual tasks	Proven HPE Pointnext Services expertise based on native cloud tools; infrastructure as code	Peace of mind with 24x7 remote monitoring and active capacity management

Why HPE for your hybrid cloud?

Your cloud program is one of the most significant technology shifts you'll face over the next decade. The sheer complexity of operating cloud services demands a new set of skills for both building and operating a secure, scalable, and compliant **hybrid cloud**. To help customers meet these requirements, the following services are incorporated into every HPE GreenLake Hybrid Cloud solution:

- **HPE design methodology**—Unique to HPE, the methodology is designed to help customers address security, operations, automation, resource management, cost control, compliance, and tooling.
- **Simplified CloudOps**—With processes and tools that are cloud-native, agile, and automated, the experts from HPE Pointnext Services help you address your security requirements and achieve continuous delivery and operations of cloud computing infrastructure, competitive performance and usability, and the scalability required to support your business.

- **Continuous monitoring**—The Continuous Compliance service provides a single source of verifiable information across governance, risk, and compliance (GRC)—enabling real-time monitoring and remediation. With automated monitoring of more than 1,500 controls, customers can reduce the time, cost, and complexity of audit preparation.
- **Continuous visibility and control**—The Continuous Cost Control service provides a holistic view of financial impact as you migrate to and operate in the cloud. Gain visibility across all your accounts and costs and map actual spend and reconcile costs back to business cases. Use monitoring and alerting features to analyze cost optimization and uncover potential savings.

Customers can achieve more than 50% cost reduction by using a managed service provider (MSP).

– Agile IT, How MSPs Can Reduce Your IT Spending By Over 50%, October 2016

HPE Pointnext Services

Implementing HPE GreenLake Hybrid Cloud is an excellent choice for driving up innovation, scalability, and flexibility while also driving down costs. With the addition of tailored services from **HPE Pointnext Services**, you can also minimize risk and resolve problems fast.

HPE Adaptive Management Services are included with HPE GreenLake Hybrid Cloud, delivering tailored services to support your entire cloud. You can rely on the skills, people, and processes of HPE Global Operations Centers to monitor and operate your infrastructure and applications, enabling you to focus on strategic initiatives and reduce IT complexity. Using the practices and tools implemented with HPE GreenLake Hybrid Cloud, HPE Pointnext Services provides services to run, scale, optimize, and support your production applications in the cloud.

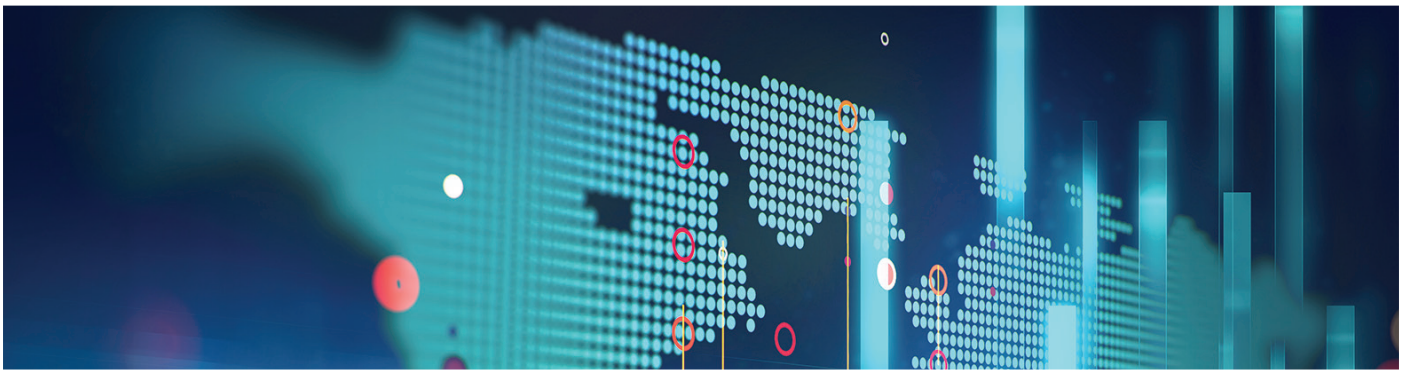
Learn more at hpe.com/greenlake



Hewlett Packard
Enterprise

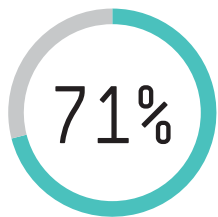
Protect more data, faster for less

HPE StoreOnce next-generation platform



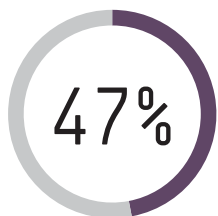
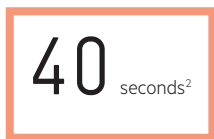
Transforming the simplicity, performance, and agility of your Hybrid IT data protection

Protecting data is increasingly challenging



of organizations can only tolerate less than one hour of downtime for high-priority applications before invoking a failover.¹

A company is hit by ransomware every



of organizations are not confident that their backup and recovery processes are sufficient for their hybrid environment.³

Data is your most valuable currency

We're living in an era of digital transformation, where the accessibility of emerging digital technologies enable you to reimagine your business in new ways—creating new experiences, new products and services, and new efficiencies. Data is the engine of your digital transformation and is your most valuable currency.

Your organization depends on data to be instantly available and secure—wherever and whenever you need it. And in an always-on world, the financial and business impact of unplanned downtime and data loss can prove catastrophic.

Data protection is increasingly challenging

As the value and business-criticality of data increases, the challenges of protecting data are tougher than ever. Exploding data growth and copy data sprawl, demanding service-level requirements, and an evolving threat and compliance landscape are putting pressure on costs and intensifying risk. What's more, as you transform to Hybrid IT, protecting applications across your data center and the cloud can prove increasingly complex.

It's time for a more intelligent approach.

Next-generation HPE StoreOnce

The new, next-generation **HPE StoreOnce system** provides a built-for-cloud data protection platform that can scale from small remote offices to the largest enterprises and service providers. Next-generation HPE StoreOnce can help you reduce cost, risk, and complexity with flash-speed protection in your data center, as well as deliver low-cost archive and disaster recovery in the cloud.

- **Help optimize cloud investment:** HPE StoreOnce with HPE Cloud Bank Storage delivers simple, efficient, and reliable backup to the cloud. It lets you seamlessly cloud-enable your storage, backup, and enterprise apps, as well as natively integrate your choice of cloud service provider without the need for a separate gateway or virtual appliance. You can reduce the time, cost, and network bandwidth for your cloud storage by 20X⁴ with highly efficient deduplicated data transfer as well as store encrypted, self-describing backup data for simple cloud disaster recovery.



HPE StoreOnce and HPE Cloud Bank Storage

¹ Real-world SLAs and Availability Requirements, ESG Master Survey Results, May 2018

² **Must-Know Ransomware Statistics 2017**, Barkly, June 2017

³ 2018 Frost & Sullivan survey of IT decision-makers

⁴ Assuming dedupe ratio of 20:1 as compared to a fully hydrated backup

Figure 1. Cloud backup made simple with HPE StoreOnce and HPE Cloud Bank Storage

- Take control of data growth:** A scalable portfolio of physical and software-defined HPE StoreOnce backup appliances provides you with up to 10X more capacity⁵ with a wide range of pay-as-you-grow capacity points and up to 104 PB⁶ in a single system. HPE StoreOnce makes every gigabyte of your storage go further with intelligent deduplication that reduces your backup costs and footprint by 95%⁷ on-premises and in the cloud. Guaranteed.⁸

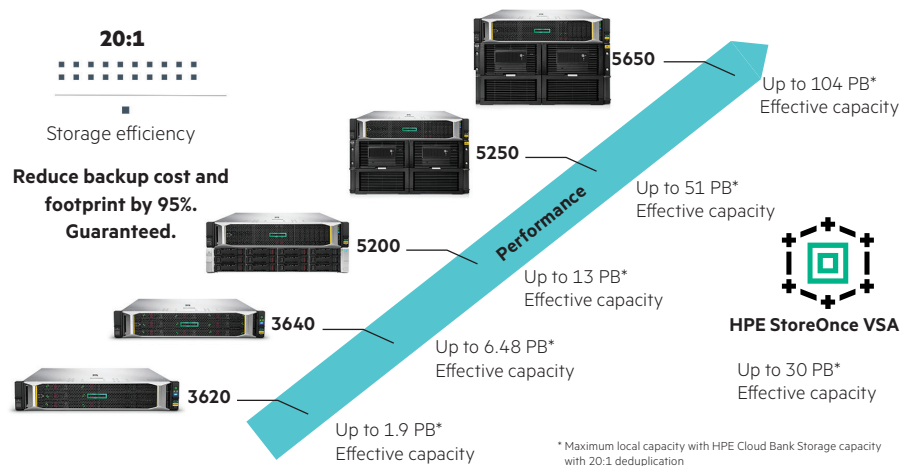


Figure 2. Take control of data growth with HPE StoreOnce next-generation platform

- Deliver on service-level agreements (SLAs):** HPE StoreOnce helps you break the backup window with up to 3X⁹ faster performance and industry-leading backup speeds of up to 288 TB/hour.¹⁰ Direct backup from your **HPE 3PAR** or **HPE Nimble array** to HPE StoreOnce with HPE Recovery Manager Central (RMC) delivers 23X faster backup and 15X faster recovery for your enterprise apps.¹¹ This backup comes with less cost and complexity, as well as having minimal impact on your production environment.
- Get comprehensive protection against any threat:** HPE StoreOnce gives you the confidence that your data is recoverable with a data protection platform that is reliable by design. Mitigate threats with 3-2-1 data protection¹² best practice, encrypted backups, data integrity checks, role-based access control, fast restores, and high availability storage of last resort. Make backups invisible to ransomware attacks with the highly reliable HPE StoreOnce Catalyst protocol.
- Reduce complexity:** HPE StoreOnce takes the time and stress out of data protection, reducing management time by 95%¹³ with multisystem and multisite visibility and management—from a single pane of glass. It empowers your application owners with self-service protection, enabling them to easily and efficiently control end-to-end protection for their applications—from the data center to the cloud—using familiar native user interfaces.

⁵ ⁹ HPE StoreOnce VSA 4.x vs. HPE StoreOnce VSA 3.x

⁶ Assuming 20:1 deduplication of protected data on local and cloud storage

⁷ Assuming dedupe ratio of 20:1 as compared to a fully hydrated backup

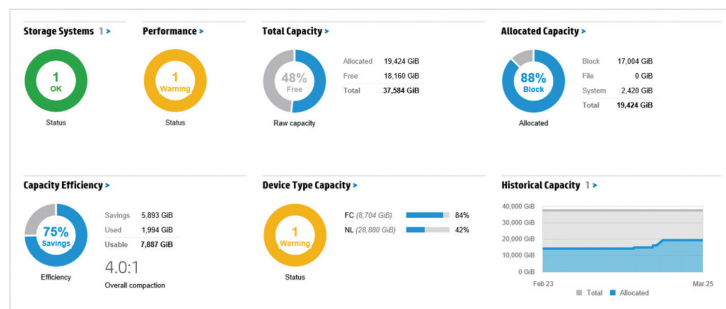
⁸ **HPE StoreOnce Get Protected Guarantee Program**

¹⁰ HA federated 8-node system using HPE StoreOnce VSA

¹¹ Based on HPE testing comparison between HPE RMC and traditional backup environments, June 2017

¹² The 3-2-1 data protection best practice prescribes that you have three copies of your data, on two different media types, with one copy kept off-site

¹³ Based on management of federation of 20 next-generation HPE StoreOnce appliances compared to management of 20 HPE StoreOnce Gen3 appliances independently (on cloud or on-premises)



Multisystem, multisite visibility, and management—from one single pane of glass

Figure 3. Monitor and manage your data protection with ease



- Experience agile software-defined protection for virtual and cloud environments:** HPE StoreOnce VSA extends the deployment options for StoreOnce with the agility and flexibility of a virtual appliance, removing the need to install dedicated data protection hardware. All the features of the purpose-built HPE StoreOnce systems are available in a software-defined backup target of up to 500 TB usable capacity, which can be configured in 1 TB increments. An HPE StoreOnce VSA license server simplifies license management for large or dynamic VSA deployments.

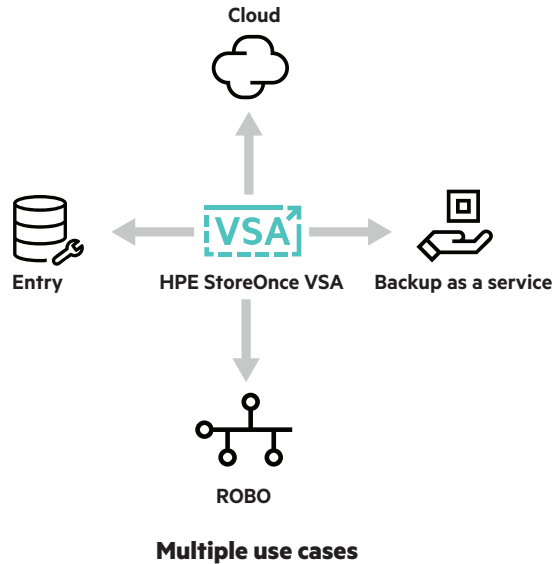


Figure 4. Software-defined protection for virtual and cloud environments

- Gain consumption-based backup on-premises:** Pay-per-use consumption models and **Flex Capacity** planning strategies with HPE GreenLake backup are now enhanced with next-generation HPE StoreOnce. Benefit from the advantages of the on-premises cloud with a usage-based billing model that aligns and grows with your business needs. Experience trouble-free data protection with a complete backup solution that is designed, operated, and implemented by **HPE Pointnext**.
- Protect your data your way:** HPE StoreOnce delivers investment protection and helps eliminate lock-in with a choice of physical or software-defined deployment, flexible-as-a-service consumption, and provides broad and deep integration across a rich ecosystem of market-leading ISV partners.

Summary

The next-generation HPE StoreOnce platform delivers end-to-end protection as you evolve to Hybrid IT—natively linking your primary, secondary, and private/public cloud storage. This lets you easily and efficiently leverage the economics and agility of the cloud for archive or disaster recovery, while continuing to use your on-premises infrastructure for fast and reliable operational recovery.

Next-generation HPE StoreOnce provides intelligent data protection for an all-flash, Hybrid IT world.



Brochure



Protect your digital enterprise

Hewlett Packard Enterprise Transformation Workshop

HPE
POINTNEXT

A new era requires new approaches

Today's businesses are more connected, context aware, digital, and data driven than ever. Consumer and enterprise customer experiences are melding seamlessly into one. Technology trends such as cloud computing, big data, social media, and mobility solutions create a faster, more affordable, and differentiated digital enterprise.

At the same time, internal and external risks and threats to your information are growing exponentially, and your organization is under increasing pressure to stay competitive, compliant with new regulations, and protected. Protecting the digital enterprise is more than protection from cyber-threats, it also includes the confidentiality, integrity and availability of your digital assets. Protecting your digital enterprise requires adaptive, predictive, and dynamic approaches across people, process, technology, and policies. Because a major key to your organization's success is speed to market, you depend heavily on secure and available information assets.

As one of the people responsible for protecting your organization's data, digital processes, and assets, your role is evolving as well. Organizations spend millions of dollars either because of these new threats, new compliance requirements, or technology changes. You need to move your organization forward and drive results by providing your employees and customers with secure and available access to information—anywhere, anytime, and with any device while keeping your budget under control.

Move forward with this Hewlett Packard Enterprise Transformation Workshop

Protecting your digital enterprise requires alignment with key IT and business decision-makers for a business-aligned, integrated, and proactive strategy to protect your hybrid IT infrastructure and data-driven operations, as well as enable workplace productivity. By focusing on digital protection as a business enabler, the HPE Transformation Workshop: Protect your Digital Enterprise is an excellent way to begin this process.

During this workshop, Hewlett Packard Enterprise will bring new perspectives on how your organization can transform from traditional static security and recovery practices to intelligent, adaptive models to keep pace with your business dynamics. We will explore your models and frameworks, as well as steps that will help take you from where you are today to reach your short- and long-term enterprise security and resiliency goals.

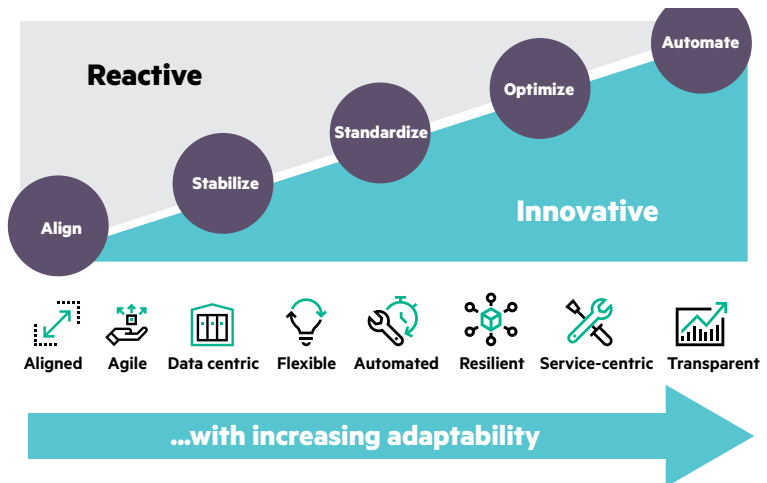


Figure 1: The Hewlett Packard Enterprise experience to protect your digital enterprise

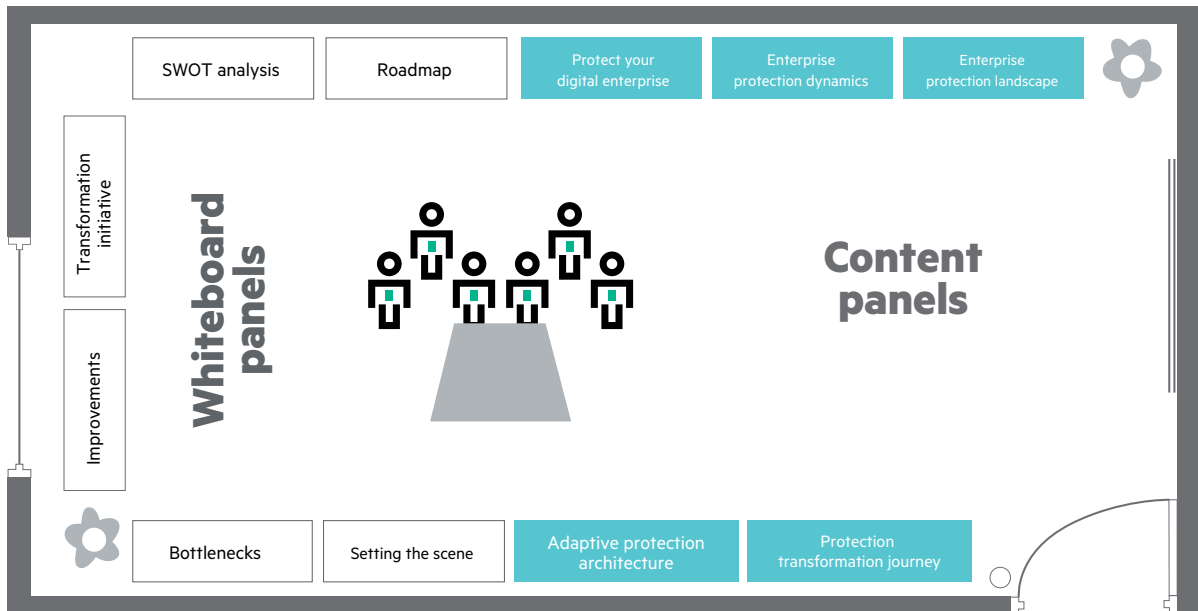


Figure 2: Whiteboard and content panels

HPE Transformation Workshop: Protect your Digital Enterprise

Explore enterprise digital protection strategies

Hewlett Packard Enterprise experts facilitate the workshop based on our knowledge and experience with new technology megatrends, risk and threat management, and protection models to help you align your business needs and priorities. This full-day workshop consists of a structured walk-through of visionary concepts and models for protecting the digital enterprise by exploring the following topics.

- Protect your digital enterprise
- Enterprise protection dynamics
- Enterprise protection landscape
- Adaptive protection architecture
- Protection transformation journey



Protect your digital enterprise

Explore internal and external drivers that require different approaches to keep pace with new styles of business and new styles of service delivery and consumption. Compare and contrast the current style of enterprise protection with an agile, future-state enterprise protection approach.



Enterprise protection dynamics

The speed of change from new technologies is placing new risks and pressures on the enterprise, increasing threats and regulatory compliance. IT megatrends such as the cloud, the Internet of Things (IoT), mobility, Big Data, and software-defined infrastructure (SDI) bring unique risks, threats and vulnerabilities.



Enterprise protection landscape

Explore what digital enterprise protection means to your organization and interdependencies that make up your digital protection landscape. Examine your organization's approach to prevention, detection, response, recovery and compliance.



Adaptive protection architecture

An adaptive enterprise protection vision requires the adoption of a holistic, integrated service management framework that takes into account security, business continuity/disaster recovery (BC/DR), and operational processes. Hewlett Packard Enterprise shares technology architectures that can jump-start an adaptive, integrated, and holistic enterprise protection strategy.



Protection transformation journey

During this journey, organizations can evaluate their enterprise digital protection program on the scale of being reactive to being more proactive and innovative. At each state, we explore actions that can be taken with the goal of achieving the ideal future state that supports the digital enterprise.

Seven reasons to join the HPE Transformation Workshop: Protect your Digital Enterprise

- Help ensure that your enterprise digital protection strategy aligns with your business needs and supports the New Style of IT
- Prepare for new threats, risks, and opportunities with new IT trends
- Rationalize and prioritize your security, governance, and resiliency initiatives
- Gain stakeholder buy-in and consensus
- Draw on best practices and Hewlett Packard Enterprise's project experience and methodologies
- Understand the current situation as well as your future aspirations clearly, and develop a high-level action plan
- Take a holistic approach to protecting your enterprise data—including people, process, technology, and governance



505-345-4720 | WWCPINC.COM
SALES@WWCPINC.COM

The first step towards adaptive enterprise protection

The ultimate outcome of the HPE Transformation Workshop: Protect your Digital Enterprise is to create a roadmap that aligns to your digital protection goals. It culminates with an interactive roadmap-building session to identify the key components in your enterprise digital protection transformation journey, including long-term goals, major transformational steps, constraints, and short-term opportunities to sustain and boost your transformation initiatives. After the workshop, we'll collect, summarize, and prioritize the outputs in order to create a shared goals and initiatives unique to your organization. This will provide a high-level transformation program roadmap that you can use to take the next steps.

Why Hewlett Packard Enterprise?

Hewlett Packard Enterprise delivers integrated IT security and assurance solutions based on internationally accepted security and availability standards—for example, ISO27k, European Network and Information Security Agency (ENISA), National Institute of Standards and Technology (NIST), and others. These standards guide you in managing business risk and making the most of your security and availability investments. Our capabilities, which span both traditional IT and hybrid IT environments, include consulting, education, and managed security services.

In addition to services, Hewlett Packard Enterprise also provides market-leading security products that enable operational security, application security, data protection, and network-level protection. Our selection of products include HPE ArcSight Security Information and Event Management (SIEM) solutions, HPE Fortify for application security, and HPE Voltage as well as HPE Atalla for data protection.

For more information

Talk to your Hewlett Packard Enterprise representative about signing up for an HPE Transformation Workshop.