Today, data security and integrity are top of mind for businesses across the globe. With an ever-increasing rate of cyberattacks, IT organizations are faced with a complex set of challenges around protecting one of the businesses most vital assets—critical data.

Consider the following questions:

• Are you completely confident of the security compliance of your data center?
• Is your data center compliance level current?
• Do you fully understand the risks your data is in?

A recent study shows that over 70% of global organizations are not prepared to handle a sophisticated cyberattack.

Even if you understand the security risks your data faces and have been vigilant about them, more often than not you might be relying on:

• Time-consuming and error-prone manual processes, which cannot be scaled throughout the data center
• A heterogeneous set of utilities that are not easy to work with or manage
• Third-party services that, in turn, are reliant on either of the above

COMMON CHALLENGES IN SECURITY COMPLIANCE

Even if you understand the security risks your data faces and have been vigilant about them, more often than not you might be relying on:

• Time-consuming and error-prone manual processes, which cannot be scaled throughout the data center
• A heterogeneous set of utilities that are not easy to work with or manage
• Third-party services that, in turn, are reliant on either of the above

A BETTER APPROACH FROM A RELIABLE PARTNER

With decades of expertise in powering the most critical and demanding IT environments in the world, Hewlett Packard Enterprise is strengthening its server offerings with a unique security compliance solution—HPE Workload Aware Security for Linux® (WASL).

HPE WASL is designed to provide efficient, industry-standard compliance at the operating system and application levels. Unlike other products in the market that rely on security services or have solutions that require a lot of configuration effort, HPE WASL automates the security compliance process to industry standards. With HPE WASL, you can reduce the security compliance deployment time for Linux operating system instances and SAP HANA® workloads from days to minutes.

SECURING YOUR LINUX AND SAP HANA ENVIRONMENTS

Security threats to your mission-critical data are more imminent than ever before

To focus

• Reduce security compliance time from six weeks to six minutes
• Up to 90% compliance with default policies
• Secure your environment for less than 1% of total system cost and avoid millions of dollars on data breach

SAP HANA deployments compliance

Many global organizations rely on SAP HANA for their database needs. The out-of-box distributions can be less than 50% compliant with security standards. With Tailored Data center Integration (TDI) deployments on the rise, the responsibility to prove SAP® security compliance shifts to the customer. HPE WASL provides compliance to the published 400+ page SAP HANA security guide with a default policy performing 90 security compliance checks and yielding detailed HPE WASL reports showing compliance with TDI implementations.

The detailed reports of HPE WASL not only provides compliance to the SAP HANA guidelines with its default policies but also used to prove the compliance effectively. HPE WASL works with both the appliance and TDI implementation models.

SAP HANA deployments compliance

Many global organizations rely on SAP HANA for their database needs. The out-of-box distributions can be less than 50% compliant with security standards. With Tailored Data center Integration (TDI) deployments on the rise, the responsibility to prove SAP® security compliance shifts to the customer. HPE WASL provides compliance to the published 400+ page SAP HANA security guide with a default policy performing 90 security compliance checks and yielding detailed HPE WASL reports showing compliance with TDI implementations.

The detailed reports of HPE WASL not only provides compliance to the SAP HANA guidelines with its default policies but also used to prove the compliance effectively. HPE WASL works with both the appliance and TDI implementation models.

A recent study shows that over 70% of global organizations are not prepared to handle a sophisticated cyberattack. And the costs are huge—average cost of cyber crime is $13 million. Add to that a more difficult to measure, but very real costs of loss of business-critical data, customer trust, and reputation. With the frequency of these cyberattacks increasing by each passing second, currently standing at approximately 5 million data records each day, you need to take action to protect your data.

Whether you are a financial institution, a retailer, a healthcare provider, or a federal organization—maintaining customer and organizational data safety is paramount.

1 2019 Hiscox Cyber Readiness Report
2 The Cost of Cybercrime. 2019
3 breachlevelindex.com/
### POWERFUL, INTUITIVE, COST-EFFICIENT DEPLOYMENT

Double the guard: HPE WASL secures the operating system across Linux distributions in HPE x86 servers and application layers such as SAP HANA.

High degree of compliance with single click operations

HPE WASL is designed to minimize manual intervention and effort, and offers single-click capabilities to:

- Add new nodes
- Assess the current security compliance level
- Deploy policies
- RemEDIATE
- Rollback the remediation

All these actions are non-intrusive and require no downtime.

### Intuitive and fast

We understand that time to production is very important. HPE WASL optimizes the time to compliance from weeks to minutes. And it does all of this without any downtime.

Default policies of HPE WASL are designed to offer ~90% compliance, or higher. The rest requires some manual inputs in order to implement them.\(^8\)

### Ensuring industry-standard compliance

HPE WASL automates the rules laid out by:

- Center of Internet Security (CIS) for Linux at the operating system level
- SAP as SAP HANA security guideline at application level

It then turns them into default policies and serves as a reassurance of the security levels. HPE WASL also maintains easy-to-comprehend logs and generates detailed actionable reports, which help users understand and make necessary changes if required.

### Simplified management

HPE WASL is a GUI-based tool and offers simple management. Keeping ease of management at its core, it has a central security management station (SMS), which monitors and takes actions across your data center.

### Cost-efficient solution

HPE WASL offers cost-effective per-instance licensing model, saving you in:

- Administrative overhead to manually ensure the security compliance of each node every time
- Lost business opportunity due to downtime or delays in readiness to production
- Cost of dreadful data breaches
- Cost of non-compliance

### Customizable solution to suit your individual environment needs

We, at HPE, understand that one size does not fit all and you might have your environment-specific security requirements based on other applications that you use or guidelines that you adhere to. Therefore, HPE WASL, at its core, is designed to be extensible and customizable.

You can:

- Modify existing policies or
- Import newer policies

This extends support to your unique security or application-specific requirements. If you are interested in having the security compliance of your environment assessed, reach out to your HPE representative for a product demonstration.

### LEARN MORE AT

hpe.com/servers/wasl

---

\(^8\) HPE internal study, December 2019

\(^9\) The SLES 15 OS policies will be updated when the associated CIS benchmark is published.