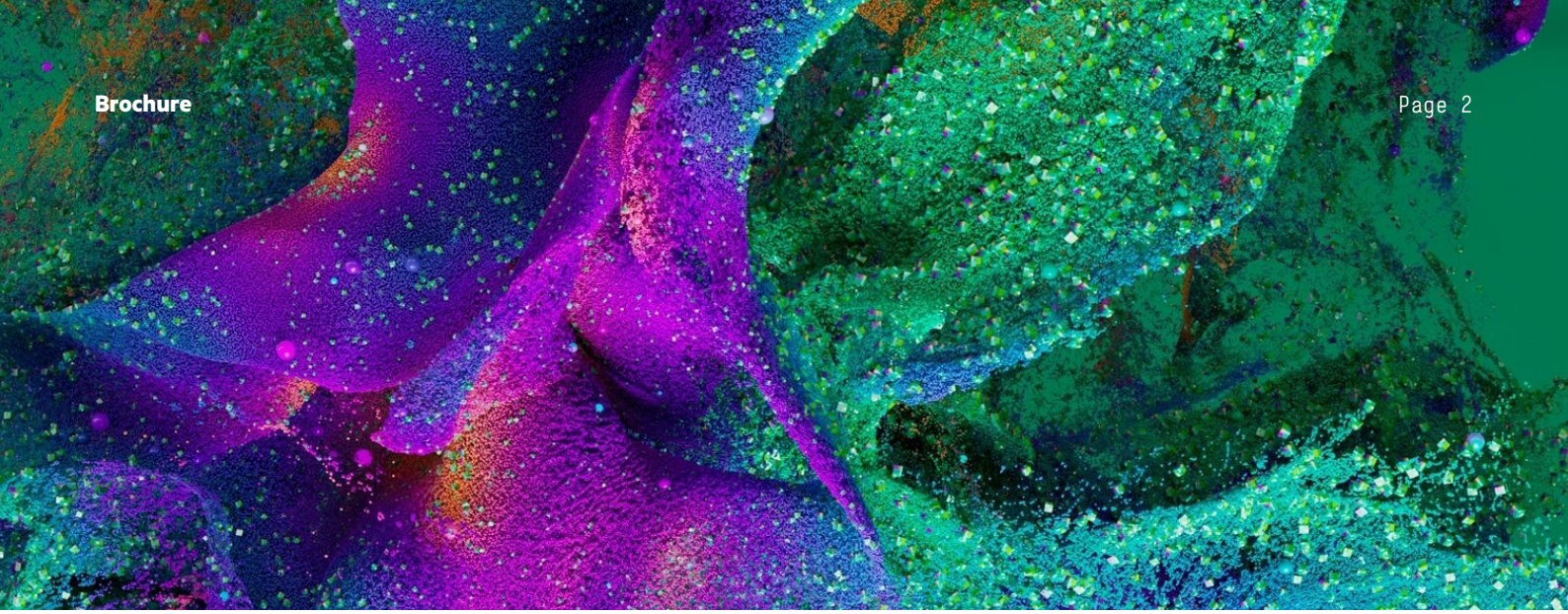
Brochure

Protection and compliance of your mission-critical SAP environment

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

HPE GreenLake



To focus

- Reduces security hardening remediation time from days to minutes
- Achieve up to 90% compliance with default policies
- Secure your SAP environment for a fraction of the total system cost and avoid millions of dollars due to a data breach

SAP HANA deployments compliance

Many global organizations rely on SAP HANA for their mission-critical 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.

SAP Workload Security solution powered by WASL enables compliance to industry standards and the published SAP HANA security guide with default policies performing over 90 security compliance checks.

Detailed reports provide proof of compliance to the SAP HANA default policy guidelines.

SAP workload security solution works with both the appliance and TDI implementation models.

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

Consider the following:

- Are you completely confident of the security compliance of your SAP® environment?
- Is your SAP hardening level current?
- Do you fully understand your SAP data risks?

A recent study shows that over 70% of global organizations are not prepared to handle a sophisticated cyberattack.[1] And the costs are huge—on average, a data breach costs your organization more than $4.24 million.[2] 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 and currently standing at approximately 68 data records each second of each day,[3] you need to take action to protect your data.

Common challenges in SAP security compliance

Even if you understand and have been vigilant about the security risks to your SAP databases, often you are relying on:

- Time-consuming and error-prone manual processes, which cannot be scaled to address the entire digital estate
- A heterogeneous set of point products that are not easy to work with or manage
- Third-party services that, in turn, are reliant on either of the above

HPE with SAP Workload Security solution powered by XYPRO Workload Aware Security Layer (WASL) enables compliance to industry standards and SAP HANA® security guide. The solution offers two onboarding service options, and hardening lifecycle services.

The solution verifies that the Linux® operating system, as well as the SAP HANA database and workloads are secured to formalized security benchmarks and guidelines. WASL delivers up to 90% compliance to Linux and SAP HANA application standards, installs in hours, and presents results in a comprehensive browser-based dashboard and generates actionable audit reports. WASL for SAP HANA and Linux x86 allows you to verify the SAP HANA database and Linux operating system instance for new and existing deployments.

[1] inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html

[2] ibm.com/security/data-breach

[3] dataprot.net/statistics/data-breach-statistics/

Features

Automated security compliance for Linux servers to SAP HANA guidelines

XYPRO WASL delivers security compliance for x86 Linux deployments based on industry-standard Center for Internet Security (CIS) benchmarks and can enable compliance to SAP HANA security guide with a single click.

Security compliance for multiple SAP HANA environments, as well as Red Hat® Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) servers can be managed from a single, easy-to-use dashboard.

Servers can be added and configured directly from the security management dashboard.

Achieve faster time to value, save time and cost

XYPRO WASL checks both the workload and the operating system for comprehensive security compliance.

The service delivers security compliance that saves time instead of having to read hundreds of pages of required SAP HANA documentation.

Automates updating process with over 1,000 automated rules that can be invoked by a single click, reducing the time to achieve compliance from weeks into minutes.

Incorporate your specific security requirements

XYPRO WASL provides the ability to add additional scripts or customization to the default rules.

You can easily propagate customization to multiple servers from the dashboard and quickly roll back changes with a single click.

Its role-based access control regulates ability to perform specific tasks on system and application based on the role of individual users.

Cost-effective licensing

XYPRO WASL provides a cost-effective licensing model to support hardening needs at the Tier 1 SAP HANA database tier and at the Tier 2 application tier. The licensing model allows security compliance on all the Linux installations in the whole enterprise regardless of how they are deployed.

The service also works with SAP HANA appliances and TDI deployments.

HPE Pointnext Services

Advisory and Professional Services brings breadth and depth of technical expertise enabling successful adoption of XYPRO WASL customized to your specific requirements, including knowledge transfer and establishing your first use case is ready for production.

As a part of better outcome model Advisory and Professional Services provides two onboarding service options. Each of these services provides:

- Installation, configuration, and validation of the WASL platform
- Gathering and analysis of customer unique hardening requirements
- A hardening assessment scan to determine the level of compliance of the target OS
- Evaluation and analysis of hardening assessment scan results
- Modifications to hardening profiles required to reach the optimal hardened state
- Hardening of the target operation systems
- Detailed reporting of pre- and post-hardening state of targets

1.HPE Hardening Service for SAP Workloads

The HPE Hardening Service for SAP Workloads can help you assess and harden the security state of your mission-critical SAP HANA (SAP Tier 1) platforms and its underlying OS, to your specific requirements and regulatory needs. Hardening both the OS and the SAP HANA platform enables confidence that your SAP HANA installation is ruggedized to meet attacks. This service provides onboarding and hardening services for up to five SAP HANA instances.

2.HPE Hardening Service for SAP Application Platforms

The HPE Hardening Service for SAP Application Platforms can help you assess and harden the security state of the OS for your mission-critical SAP application servers (SAP Tier 2) to your specific requirements and regulatory needs. This provides assurance that your critical SAP applications are running on a secure and attack-resistant operating system platform. This service provides onboarding and hardening services for up to 10 SAP application servers.

HPE Security Hardening Lifecycle services are also available for ongoing hardening process management, including SAP HANA environment readiness, verification, and upgrades for new XYPRO WASL releases, remediation support for non-compliance, and onboarding new platforms.

A better approach from a reliable partner

With decades of expertise in securing the most critical and demanding IT environments in the world, Hewlett Packard Enterprise, together with XYPRO Technology, have strengthened their mission-critical security offerings with a unique security compliance solution for Linux and SAP HANA workloads. 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 require significant manual effort, WASL automates the security compliance process. WASL reduces the security compliance deployment time for Linux operating system instances and SAP HANA workloads from weeks to minutes.

Value proposition

Secure SAP HANA environments

- Rapidly achieve and maintain industry and regulatory standards and meet business requirements
- Benefit from HPE's deep technical and delivery expertise for WASL and SAP HANA environments
- Comply with guidelines from Center for Internet Security (CIS) and SAP Security Reference Guide

Purpose built for SAP HANA workloads

- Comprehensive solution covering both Linux OS (SLES/RHEL) and SAP HANA applications
- Built-in compliance and audit reports

Easy deployment

- Push-button security with default profiles for operating systems (SLES/RHEL) and SAP HANA workloads
- Customizable templates, modify existing policies, or import newer policies
- Integrate existing hardening scripts and processes

Shorten time to production

- Reduces security hardening remediation time from days to minutes
- Instant one-click rollback
- ~90% out-of-box compliance

Superior ROI

- Achieve faster time to value, save time and cost
- Get single-click evaluation and remediation
- Reduce chances of sanctions and fines while maintaining compliance
- Automate guidelines, checklists, and specialized knowledge

State of art

- Automated security compliance—assessment and remediation, easily run at regular intervals to check and keep compliance current, provides a rollback option to reinstate previous state
- Simplified management with a browser-based graphical interface solution

If you are interested in having the security compliance of your SAP environment assessed, reach out to your HPE representative for details or a product demonstration.

Explore **HPE GreenLake**

Learn more at

hpe.com/security

xypro.com/wasl

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard Enterprise

© Copyright 2022 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.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. 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 (or an SAP affiliate company) in Germany and other countries. All third-party marks are property of their respective owners.

a50006887ENW