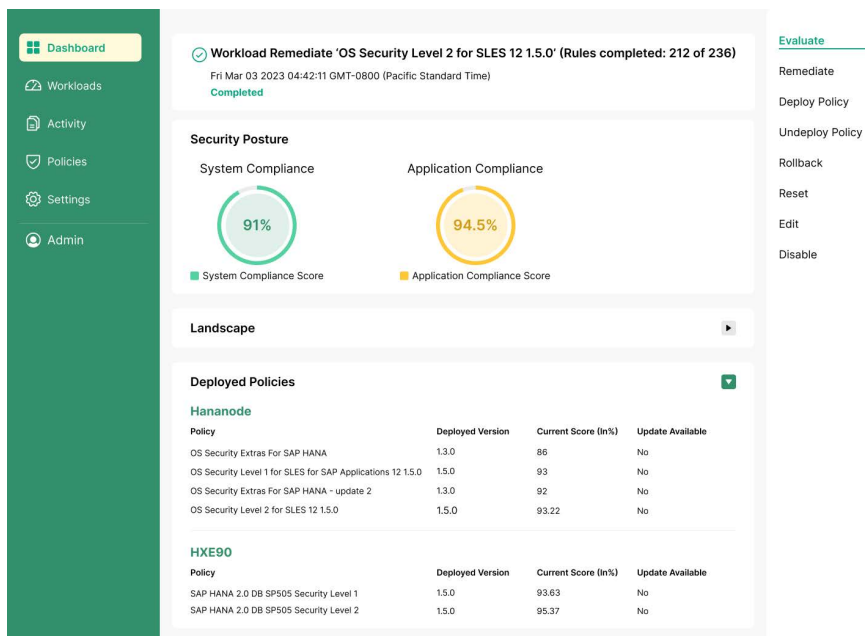


# WASL - Workload Aware Security Layer

## Automated Security and Compliance for SAP HANA and Linux

- Enterprise-grade protection for your most critical workloads
- 90% compliance for over 1,500 rules with one click
- Secure your SAP environment for a fraction of the total system cost and avoid millions of dollars due to data breaches and fines
- Reduce security hardening time from weeks to minutes!



Cyberattacks are a growing concern for organizations of all sizes and industries. Despite implementing robust security measures, there is always a risk that threats will bypass defenses and infiltrate information systems. These attacks not only result in financial losses and operational disruption, but also cause significant damage to a company's reputation. Organizations are faced with complex challenges around protecting their most vital assets—mission critical data. Most organizations store their mission critical data in SAP HANA databases and use applications and workloads built on SAP HANA. Therefore, security and compliance are paramount for these workloads.

### SAP HANA Challenges

**Complexity** - SAP HANA is a complex system with multiple components and layers, making it difficult to secure.

**Data breaches** - SAP HANA stores large amounts of sensitive data, it is a prime target for cyberattacks.

**Lack of visibility** - Getting a comprehensive view of the security status of the SAP HANA environment is challenging, making it hard to identify and respond to threats.

**Limited resources** - Many organizations struggle to allocate sufficient resources to SAP HANA security, whether it's staff, budget, or technology.

**Compliance** - Organizations need to meet a variety of regulatory requirements, such as GDPR, HIPAA, and PCI-DSS. Ensuring that SAP HANA is compliant is a significant challenge.

**Third-party vulnerabilities** - SAP HANA is often integrated with other systems and third-party software, these integration points introduce vulnerabilities that could be exploited by attackers.

**Insider threat** - The risk of malicious or accidental actions by authorized users, such as employees or contractors, is a major concern, especially with the rise of remote work.

### What We Solve

**Workload Aware Security Layer (WASL)** powered by XYPRO, reduces security implementation times from weeks to minutes! WASL is not only the smart technical solution, but the financially responsible one. Without WASL, HANA security implementation can cost your business thousands of dollars a day, with weeks, or even months, spent manually setting up security, compliance, and ongoing monitoring with expensive consultants. WASL's automated hardening eliminates human error and enables compliance to industry-standard Center for Internet Security (CIS) benchmarks and the SAP HANA® security guide with a **single click**.

WASL is a cutting-edge security solution that automatically configures, monitors and remediates security for SAP HANA database and workloads and Linux operating systems. With WASL, comprehensive results direct action and provide in-depth insights into your workload's security. It is the first integrated tool **purpose-built to secure SAP HANA**.

WASL installs quickly, delivers up to 90% compliance out of the box to Linux and SAP HANA application standards, presents results in a browser-based dashboard and generates actionable reports.

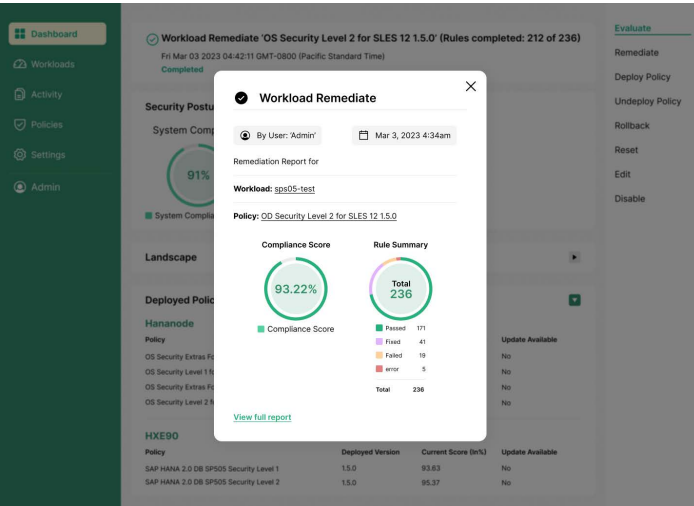
Security compliance for multiple SAP HANA environments, as well as Red Hat® Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) servers can be managed from a single, easy-to-use dashboard.

# Automated Security and Compliance

## A Better Approach From a Reliable Partner

With decades of expertise in securing the most critical and demanding global IT environments, XYPRO Technology presents this unique security compliance solution for Linux and SAP HANA workloads. WASL provides efficient, industry-standard compliance at the operating system and application levels.

Other products in the market rely on security services or require expensive manual effort. WASL automates security compliance, and reduces deployment time for Linux operating systems and SAP HANA workloads from weeks to minutes.



## Features and Benefits

WASL's powerful features keep your systems secure and compliant on an on-going basis:

### One-Click Security

- Push-button security with default profiles for operating systems (SLES/RHEL) and SAP HANA workloads
- Compliance with Center for Internet Security (CIS) benchmarks and SAP Security Reference Guide

### Purpose Built for SAP HANA workloads

- Automated security compliance—assessment and remediation keep compliance current
- Instant, one-click rollback to reinstate previous state

### Continuous Compliance

- Customizable templates, modify existing policies, or import newer policies
- Integrate existing hardening scripts and processes

### Superior ROI

- Achieve the fastest time to value for SAP HANA applications, saving time and cost
- Reduce the risk of sanctions and fines while maintaining compliance
- Secure your SAP environment for a fraction of the system cost.

### WASL Supports

- RedHat Enterprise Linux 7.x, 8.x, 9.x
- SUSE Enterprise Linux 12.x, 15.x
- SUSE Enterprise Linux for SAP HANA 12.x, 15.x
- SAP HANA 1.0, 2.0
- Microsoft Windows Server - Coming Soon!

### WITHOUT WASL

compliance levels less than 50%



SAP HANA + CIS Security Benchmark  
Compliance

SAP HANA security guide

(800+ pages) takes months to implement

### XYPRO WASL



Security compliance solution  
for Linux-based workloads

### WITH WASL

compliance levels reach 90% and above



SAP HANA + CIS Security Benchmark  
Compliance

1500+ pre-defined hardening rules,  
configurable and automated in one click!

Learn more at  
[xypro.com/wasl](http://xypro.com/wasl)

  
**Hewlett Packard  
Enterprise**

  
**SAP  
Partner**

  
**Red Hat  
Business Partner**

  
**XYPRO**  
Mission Critical Security

XYPRO Headquarters  
4100 Guardian St., Suite 100  
Simi Valley, California 93063 USA

Talk to us +1 805 583 2874

[XYPRO.com](http://XYPRO.com)