SUSE

Today’s SAP Security Challenge: Moving from Risk to Resilience

SUSE closes Windows security gaps in your SAP infrastructure

Flyer

From Risk to Resilience

SUSE closes Windows security gaps in your SAP infrastructure

Today's rapidly expanding digital eco-systems provide organizations with many benefits. At the same time, they present important challenges, not least of which is rapid growth of cyber threats. This necessitates a robust security posture to protect sensitive data and maintain uninterrupted operations.

For the many organizations that depend on SAP systems, the common practice of running application servers on Microsoft Windows while using Linux for SAP HANA databases introduces critical security risks. The inherent vulnerabilities of Windows make it a preferred target for cyber-attacks ranging from viruses to sophisticated ransomware.

SUSE enables organizations to effectively avoid security risks and establish a truly resilient SAP infrastructure.

Windows in SAP Environments: A Real Security Challenge

Windows servers are commonly part of SAP solutions for reasons like their familiarity to IT staff, or existing investments in Windows technology that companies are reluctant to abandon. But the fact is that this loyalty to Windows opens the SAP system to significant security risks.

Windows systems and servers are frequently targeted by cybercriminals due to their large install base and inherent vulnerabilities. The complexity and frequency of required updates, coupled with Windows' lengthy patching process, are obstacles to timely security patches. This often leaves enterprise systems vulnerable to viruses, trojans, ransomware and spyware attacks for prolonged periods of time.

Moreover, Windows patches cannot be applied live. In mixed SAP environments, this means Windows application servers need to be brought down, which can only be done during planned maintenance windows. This causes patch application delays, that force you to take your business-critical SAP system offline for some time — downtime that disrupts business processes, leads to potential data loss and impacts overall productivity.

Bad actors are well aware of all these vulnerabilities, which points to the fact that Windows servers are simply less secure than they need to be for a truly secure SAP environment.

A Secure Alternative: SUSE Linux Enterprise Server for SAP Applications

The solution to the Windows security challenge is transitioning to SUSE Linux Enterprise Server for SAP Applications (SLES for SAP) – a secure, high-availability platform that eliminates the vulnerabilities associated with Windows servers. SLES for SAP is designed specifically for SAP environments, with optimizations that enhance both security and performance.

Further, it is easy to deploy, configure and protect the full SAP system stack quickly, reliably and confidently, on-premises and in the cloud.

These are just some of the ways SLES for SAP elevates security to the next level:

1. **Live Patching:** SUSE's cutting-edge SUSE Linux Enterprise Live Patching capabilities enable critical security updates and system patches to be applied in real-time without rebooting systems or restarting applications. The ability to apply important patches immediately ensures business operations are never interrupted and reduces vulnerability windows.
2. **Automated Patch Management:** SLES for SAP applications uses SUSE Multi-Linux Manager to automate patch management and configuration. This feature is available in the core, in the cloud, and on the edge. Easy to use from a single console, SUSE Multi-Linux Manager significantly reduces the risk of human error and ensures systems are consistently up-to-date and secure.
3. **Regulatory Compliance:** SUSE Linux Enterprise Server for SAP Applications meets the highest international security standards, including the Common Criteria EAL4+ certification. It also supports the requirements of NIS-2 and similar jurisdictional regulations. These comprehensive measures ensure compliance with stringent regulatory requirements and protect organizations from potential fines and penalties associated with data breaches.
4. **High Availability:** SUSE solutions are engineered to maximize system availability. But many IT professionals expect HA solutions to be complex to implement. That's what makes Trento, a feature of SLES for SAP, so valuable. Trento is a proactive monitoring tool that embeds best practices in code to ensure that SAP environments are continuously optimized, reducing the risk of unplanned outages. Users benefit from an open, cloud native Web console designed to run on a Kubernetes cluster.

Operational Excellence with Proven Security

SUSE's comprehensive approach to SAP security is not just about defending against potential threats, but also about enhancing the operational efficiency of SAP systems. By reducing the complexity and inherent risks of mixed infrastructure environments, SUSE helps streamline management and safeguard critical business processes.

- **Secure from the Core:** At the heart of SUSE's security philosophy is the principle of securing the infrastructure from the core. This begins with a hardened operating system that is resistant to vulnerabilities and extends through each layer of the application stack.
- **Data Protection and Confidential Computing:** Data is an invaluable asset that needs stringent protection. SUSE supports confidential computing techniques that ensure data is encrypted at rest, in transit, and in use. It enables the running of fully encrypted virtual machines in your SAP environments to provide multiple layers of protection against unauthorized access and breaches.
- **SAP-Specific Security Enhancements:** SUSE enhances SAP environments with tailored security measures such as the SAP HANA Firewall and integration of best-practice guidelines for system hardening. These specialized tools and protocols provide an additional layer of security tailored to the unique needs of SAP systems.

SUSE Delivers a Secure, Resilient SAP Infrastructure

In today's technology landscape, where cyber threats are increasingly sophisticated and regulatory demands are more stringent, the need for a secure, reliable and compliant SAP infrastructure is paramount. With over two decades of experience in the SAP ecosystem, SUSE is a trusted leader in providing secure, robust and compliant SAP solutions. Transitioning from a mixed Windows and Linux environment to a unified SUSE Linux Enterprise Server for SAP Applications dramatically enhances security, reduces operational risks and ensures continuous compliance.

Explore how SUSE can transform your SAP security landscape!

SUSE enables organizations to effectively avoid Windows security risks and establish a truly resilient SAP infrastructure.

Visit www.suse.com

SUSE 2025

SUSE Software Solutions
Germany GmbH

Frankenstraße 146
90461 Nürnberg
Germany

www.suse.com

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Innovate
Everywhere