SUSE

From Risk to Resilience

Elevating SAP Security Beyond the OS Layer

The Challenge

SAP landscapes are central to global business operations, but they face mounting cybersecurity risks. While many organizations already run SAP HANA on Linux, many still host SAP application servers on Microsoft Windows.
This mixed setup exposes businesses to:

- **Windows vulnerabilities:**
  Frequent critical flaws and forced downtime for patching.
- **Complex patching cycles:**
  Both OS and SAP application patches create exploitable windows.
- **Regulatory pressure:**
  Direct accountability under frameworks like the EU NIS-2 Directive.

At the same time, attackers are leveraging AI to automate exploits, while SAP itself has suffered vulnerabilities rated at CVSS 9.9–10.0, proving risks exist well beyond the OS.

Why SUSE Matters

SUSE Linux Enterprise Server (SLES) for SAP Applications helps close a critical security gap by eliminating reliance on Windows servers.

Key benefits include:

SAP Endorsement:
SAP itself runs 100,000+ VMs and its HANA Enterprise Cloud on SLES for SAP Applications.

Continuous uptime:
SUSE Linux Enterprise Live Patching applies kernel updates without restarts or downtime.

Automated security:
SUSE Multi-Linux Manager enforces consistent patching and compliance.

Certified trust:
Common Criteria EAL4+ certification and secure supply chain measures.

Resilience built in:
Trento embeds HA best practices, while confidential computing encrypts data at rest, in transit, and in use.

The Bigger Picture

Migrating from Windows to SUSE is not just a technical upgrade — it is part of a broader transformation. Executives must weigh:

- **Risks of Inaction:**
  Persistent Windows vulnerabilities and compliance penalties.
- **Risks of Action:**
  Migration complexity, hidden costs, and business disruption.

A holistic strategy goes beyond OS migration:

Prioritize SAP application security:
Patch vulnerabilities quickly and monitor continuously.

Adopt zero trust:
Enforce least-privilege, MFA, and microsegmentation.

Leverage AI-driven defense:
Detect and respond to threats in real time.

Conduct full TCO analysis:
Factor in hidden migration costs and long-term savings.

The Executive Takeaway

Security is not a product — **it is a process.** Transitioning to SUSE Linux Enterprise Server for SAP Applications closes a significant vulnerability gap and aligns with SAP's own operational strategy. But *true resilience* demands a modern security posture built on **zero trust, AI-enabled defense, and executive-level risk management.**

SUSE is a critical foundation for securing SAP in a rapidly evolving threat landscape.

To learn more visit:

https://www.suse.com/products/sles-for-sap/

SUSE