

Protect IBM Z and IBM LinuxONE Workloads with TrendAI™ Deep Security™

Automated security, compliance, and proactive defense for your mission-critical systems

The security challenge

Enterprises face growing pressure to protect increasingly complex, interconnected infrastructures while navigating evolving compliance requirements. AI-driven attacks are accelerating faster than traditional defenses can adapt, exploiting blind spots across hybrid environments. In our [State of AI Security Report, 1H 2025](#), we revealed that 93% of security leaders expected to face daily AI-powered attacks in 2025, highlighting just how quickly automated threats are advancing.

IT organizations often work in technology silos. Storage, server, and cloud teams use separate toolsets, creating fragmented controls and inconsistent policies. The result is higher cost, greater operational complexity, and reduced agility when speed and cohesion are essential. Organizations need a solution that closes security gaps, ensures compliance, and strengthens resilience without compromising performance.

IBM Z® and IBM® LinuxONE provide a trusted, high-performance backbone for critical workloads. Strengthen and protect it with unified detection, compliance automation, and centralized visibility with TrendAI™ Deep Security™. Modernize securely, reduce complexity, and achieve measurable improvements in efficiency and protection.

Protection features

- Scan and detect threats across files and entire file systems
- Uncover dormant threats evading real-time monitoring via deep forensic analysis
- Support regulatory alignment without impacting performance through automated security checks

Key benefits

- Accelerate threat detection with AI-driven insights for faster risk identification
- Simplify security operations with seamless IBM Z and LinuxONE integration
- Secure systems proactively with quantum-safe encryption
- Protect innovation with readiness for AI workloads
- Preserve IBM Z and LinuxONE performance while prioritizing robust protection
- Reduce audit complexity by automating compliance checks

Proactively secure AI workloads with Deep Security

Deep Security delivers intelligent anti-malware protection, with no reboot or downtime required, for IBM Z and LinuxONE mainframes. Leverage integrated AI and analytics for comprehensive system-wide scans and deep forensic analysis, helping you uncover hidden threats. In addition, support regulatory alignment without impacting performance through automated compliance checks.

Designed for demanding environments, Deep Security empowers your teams with robust, real-time threat detection and response. Consolidate tools from distributed IBM Z or LinuxONE environments into one unified platform, helping you stay ahead of adversaries.

Strengthen your IBM Z and LinuxONE integration

IBM Z and LinuxONE help you modernize and reduce costs by consolidating workloads into a secure, high-performance environment. They deliver efficiency, reliability, and protection for the most critical applications while providing a foundation for long term innovation.

Through IBM Z® and IBM® LinuxONE, get access to advanced security with built-in predictive capabilities. For organizations running critical workloads, IBM Z and LinuxONE are designed to provide a resilient, high-performance foundation for long-term reliability. Build on this foundation with Deep Security by unifying security capabilities across environments, simplifying your security operations and enabling meaningful cost savings. Enforce AI governance and proactively manage risk through real-time telemetry.

Key capabilities

- Detect anomalies in real time with AI-powered threat detection via the Telum II processor in IBM Z and LinuxONE
- Identify irregularities before they escalate into breaches with real-time transactional analysis
- Protect data at rest, in motion, and in use against future quantum threats with quantum-safe cryptography in IBM Z and LinuxONE
- Proactively manage risk through real-time telemetry
- Enforce responsible AI use across hybrid environments through AI governance
- Visualize, prioritize, and mitigate risk proactively with real-time insights

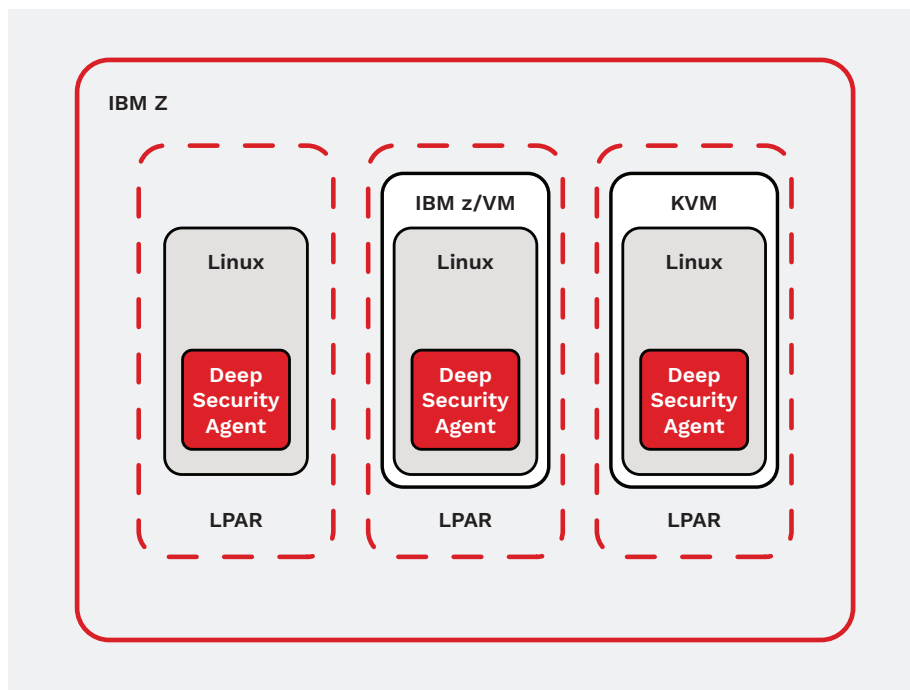


Figure 1: Technical diagram

Stronger together

Integrate Deep Security with IBM Z and LinuxONE to unify your security posture across mainframe, Linux, and cloud environments. Reduce complexity, streamline compliance, and support containerized and AI-driven workloads without sacrificing speed or scalability. Through this partnership, gain layered protection built to be future-ready and operationally efficient.

Integration benefits

- Boost resilience by combining IBM predictive capabilities with advanced threat defense from TrendAI™
- Unify your security posture across hybrid environments for consistent protection
- Simplify regulatory oversight through automated compliance checks
- Reduce complexity and operational cost through centralized management and automation
- Support and protect containers and AI-driven workloads while preserving performance

About TrendAI™

TrendAI™, a business unit of Trend Micro and global AI security leader, makes the world safer for digital information exchange across enterprises, governments, and organizations. Powered by security expertise and innovation, TrendAI™ leverages artificial intelligence to protect over 500,000 enterprises and millions of individuals across AI, cloud, networks, endpoints, and devices. AI Fearlessly.

[TrendMicro.com](https://www.trendmicro.com)

Copyright ©2026 Trend Micro Incorporated. All rights reserved. Trend Micro, TrendAI, and Deep Security are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.
[SB00_DeepSecurity_IBMZ_LinuxONE_260317US]

For details about what personal information we collect and why, please see our Privacy Notice at [TrendMicro.com](https://www.trendmicro.com)

Industry leadership

Gartner

Named a Leader: 2025 Gartner Magic Quadrant™ for Endpoint Protection Platforms (EPP), 20th time in a row



100% MITRE ATT&CK
Technique coverage

OMDIA

Leader in Global Vulnerability
Research and Discovery since 2007

Key certifications

- Common Criteria EAL2+
- FIPS 140-2 validated
- Microsoft Certified Partner
- Certified for SAP NetWeaver VSI 2.0 and HANA
- VCE Vblock Validated
- Virtualization by VMware

**Protect your mainframe
workloads**

Learn more at [trendmicro.com](https://www.trendmicro.com)

Connect with your IBM Z and LinuxONE account manager or TrendAI™ representative to obtain licensing, and download Deep Security software [here](#).