Radware and SUSE Partner for Secure, Scalable Edge Solutions

A Growing Need for Edge Computing, Security, and Compliance

Organizations across the globe are undergoing rapid digital transformation, driven by the need for a flawless customer experience, security, high availability, and operational efficiency. The adoption of edge computing has become a strategic imperative, allowing organizations to process data closer to the source—be it in stores, warehouses, or distribution centers—enabling low-latency applications such as AI-driven customer analytics, autonomous checkout, and personalized marketing.

However, as businesses expand their digital footprint at the edge, they must also navigate an increasingly complex cybersecurity landscape. With more distributed infrastructure, security threats such as data breaches, ransomware attacks, and compliance violations pose significant risks. Organizations in industries including retail, eCommerce, financial services, healthcare, and government must ensure that their edge environments are high-performing, secure, and compliant with industry regulations such as PCI DSS, HIPAA and GDPR.

SUSE and Radware are joining forces to provide a scalable infrastructure with embedded security, designed specifically for today's IT environment. Radware application protection provides comprehensive, adaptive protection for applications and APIs for both Kubernetes and non-Kubernetes environments. Radware DDoS protection and SUSE solutions enhance resilience and ensure availability under attack.

Challenges at the Edge

While edge computing offers immense benefits, it also introduces significant challenges for enterprises. Managing a distributed edge environment requires a scalable and flexible architecture that can securely handle thousands of endpoints across multiple locations. The complexity of deploying, monitoring, and securing workloads at the edge increases the risk of cyber-threats and compliance issues

Organizations must address latency, data sovereignty concerns, ensure secure payment processing, and safeguard customer data while maintaining high availability and performance. Additionally, IT teams must overcome operational challenges such as integrating legacy systems with modern applications, automating security enforcement, and ensuring business continuity in the face of evolving threats.

SUSE Edge and SUSE Rancher Prime: A Scalable, Secure Platform for Edge Deployments

To address these challenges, SUSE provides a robust edge computing platform through SUSE Edge and SUSE Rancher Prime, offering businesses a scalable, secure, and easily managed solution for deploying and managing edge applications and workloads.

SUSE Edge delivers lightweight, highly available Kubernetes distributions that optimize edge infrastructure, enabling retailers to efficiently run containerized applications across thousands of locations.

SUSE Rancher Prime, SUSE’s industry-leading Kubernetes management platform, simplifies cluster orchestration and governance, ensuring seamless operations across diverse edge environments.

With SUSE’s edge solutions, organizations can automate deployment, enforce security policies, and centrally manage their distributed infrastructure, reducing complexity and operational costs while enhancing agility and innovation.

Radware Security: Strengthening Enterprise Edge Protection and Compliance

Radware’s security solutions add a critical layer of protection to SUSE’s enterprise edge offerings, ensuring secure delivery and high availability of low-latency applications while maintaining compliance with stringent regulatory standards. Radware’s Web Application and API Protection (WAAP) and Distributed Denial-of-Service (DDoS) protection safeguard edge environments from cyber-threats, preventing data breaches and service disruptions. Additionally, Radware Bot Manager helps mitigate automated fraud, securing online transactions and customer interactions.

As businesses adopt edge computing to enhance customer experiences and streamline operations, client-side protection has become a critical component of their security strategy. This is especially vital for organizations that must meet compliance requirements like PCI DSS, HIPAA, and GDPR.

Unlike traditional security measures that focus primarily on network and server-side threats, client-side protection ensures that the customer-facing components of a retailer's digital ecosystem—such as web applications, mobile apps, and online payment forms—are safeguarded against sophisticated cyber-threats. Client-side protection is provided by Radware's Cloud Web Application and API Protection (WAAP) solution.

By integrating Radware's advanced threat intelligence and real-time attack mitigation into SUSE Edge deployments, businesses can achieve proactive security enforcement, protect sensitive payment data and comply with PCI DSS and GDPR regulations. This joint solution empowers organizations to embrace digital transformation with confidence, ensuring seamless, secure, and compliant edge operations.

Using behavioral-based machine learning algorithms and AI-powered security event cross-correlation, Radware provides real-time, adaptive protection that is automatically refined as threats change. Radware Kubernetes Web Application and API Protection (KWAAP) together with SUSE Rancher Prime and SUSE Security provide a full-stack Kubernetes management and security solution that meet the needs of today's enterprises and service providers.

Conclusion

The partnership between Radware and SUSE offers a comprehensive, secure, and scalable solution for organizations in all industries seeking to leverage edge computing while mitigating security risks and compliance challenges. By combining SUSE Edge and SUSE Rancher Prime with Radware's industry-leading security solutions, organizations can accelerate innovation, enhance customer experiences, and protect critical data and applications across distributed environments. This joint solution ensures that organizations can meet the demands of today's digital-first economy while safeguarding their business from emerging cyber-threats.

And to ensure that enterprises can innovate at the speed of business while minimizing risk, Radware KWAAP is pre-certified to interoperate with SUSE Rancher. See link below.

Learn about Radware KWAAP's certification with Rancher

Click here

Need more information?

Contact Radware

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.