

AI FACTORY FIREWALL

SECURING AI INFRASTRUCTURE WITH CHECK POINT AND NVIDIA

CHECK POINT™

NVIDIA

Cyber Security in the Age of AI

As organizations worldwide build AI factories, they face unprecedented challenges in protecting this infrastructure. AI factories are purpose-built for the intensive computational needs of AI workloads, supporting AI reasoning, agentic AI, and model training that powers the next wave of AI innovation.

The rapid evolution of AI applications from conceptualization to experimentation to production has created a complex landscape where traditional security measures fall short. AI factories excel at empowering AI model creation and deployment, from data ingestion to training, fine-tuning, and high-volume inference.

Protecting AI applications and the sensitive data they use demands a proactive approach to security. AI infrastructure security solutions need to address the unique vulnerabilities and threats faced by generative AI models, neural networks, and the substantial computational resources required for AI workloads.

AI Cloud Security Needs and Challenges

Data Exfiltration
Protecting intellectual property such as training data and AI/ML models from being exposed or stolen is a significant requirement. Ensuring that sensitive data remains secure is crucial for maintaining the integrity and confidentiality of AI projects.

Data Poisoning
Preventing attackers from manipulating training data to control model outputs is essential. Data poisoning can lead to vulnerabilities that could compromise the model's validity and effectiveness.

Denial of Service (DoS)
Mitigating attacks that degrade the performance of AI infrastructure is vital. DDoS attacks can significantly reduce the efficiency of AI systems, causing operational disruptions and making servers unavailable for genuine users. The performance reduction can lead to increased costs and revenue loss for AI-driven applications and model development.

Model Inversion
Model inversion occurs when attackers use the model's output to infer sensitive information about the input data. This technique poses significant challenges for enterprises deploying AI systems, as it can undermine data privacy and enable malicious actors to exploit vulnerabilities in critical applications.

Safeguarding AI Investments
Security incidents may require re-training of AI models, which can significantly impact business investments in AI data centers. These represent substantial investments, and a security breach could potentially double those costs. Moreover, if someone steals the model, they're also stealing intellectual property—the culmination of the research, development, and competitive advantage. Retraining the data post-incident is also painstaking and time-consuming, often requiring carefully obtaining and cleaning vast datasets.

Access Control
Implementing stringent access controls to AI infrastructure is more critical compared to general-purpose data centers due to the significant investment associated with training AI models. Ensuring that only authorized individuals can access and control AI resources is a fundamental aspect of securing AI applications.

Securing AI Cloud Infrastructure with Check Point and NVIDIA

Check Point AI Factory Firewall integrates with NVIDIA BlueField DPUs to secure AI infrastructure at scale, providing industry-leading threat prevention while ensuring peak AI performance. The collaboration enables service providers and enterprises to develop and deploy AI models and applications in a secure environment:

Validated on NVIDIA RTX PRO Servers

AI Factory Firewall is now open for enterprise deployment, validated on NVIDIA RTX PRO servers. This validation demonstrates enterprise-ready security for critical AI workloads including AI model development, agentic AI applications, and inference, built on NVIDIA BlueField technology. Organizations can confidently deploy AI Factory Firewall on NVIDIA RTX PRO servers today.

Ready for Next-Generation AI Infrastructure

AI Factory Firewall is designed to run on both NVIDIA BlueField-3 and, eventually, the newly announced NVIDIA BlueField-4, which delivers 6x the compute power and 800 Gb/s throughput. This next-generation platform supports 4x larger-scale AI factories and delivers 2x performance for AI inference and storage processing, ensuring your security infrastructure scales with AI innovation and meets the demands of gigascale AI factories.

Key Capabilities of AI Factory Firewall

Robust Defense Against AI-Driven Threats

- Network Threat Prevention includes a next-generation firewall with identity-based access control, intrusion prevention, and anti-malware
- Host-level protection mechanisms prevent local code execution and privilege escalation attacks
- Unique, industry-leading security capabilities powered by NVIDIA Cyber Security AI platform

Security Without Compromising Performance

- Run AI training and other complex use cases at peak performance while maximizing security
- To ensure optimal performance, security processes run on NVIDIA BlueField DPUs, which are isolated from the host and AI workloads
- NVIDIA DOCA Argus immediately detects and stops runtime attacks to minimize potential impact and risk, enhancing the security posture of the AI infrastructure
- Validated on NVIDIA RTX PRO servers for enterprise AI workloads including model development, agentic AI applications, and production inference

Seamless Integration with Scalable Management

- Standard orchestration tools enable easy deployment across diverse AI environments at scale
- Leverage multi-tenanted management with pre-defined security policies designed for AI
- Eliminate the need for manual agent installation on individual hosts, simplifying large-scale implementations

Safe Simulation and Validation with NVIDIA DSX Air

- Cloud-based simulation environment reducing AI data center transformation risk and cost for large-scale AI factories
- Supports thousands of GPUs, modeling the full NVIDIA stack: networking, DPUs, NVLink, and software
- Digital twin enables pre-production cyber security testing, ensuring validated security from token one

Future-Ready Infrastructure

- Security functions run seamlessly on upcoming NVIDIA BlueField-4 DPUs with significant performance gains
- Unlock new levels of infrastructure acceleration, efficiency, and cyber security

See AI Factory Firewall in Action

- Get more info on how to take your AI cloud security to the next level
- Schedule a demo of AI Factory Firewall today to discover how the Check Point and NVIDIA collaboration safeguards your AI infrastructure
- Learn more at www.checkpoint.com/ai/cloudprotect

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

© 2026 Check Point Software Technologies Ltd. All rights reserved.