Preparing for AI Data Center era

Company with AI Data Center

Tomas Vobruba | Lead Security Engineer, Check Point Slovakia

Jarná ITAPA 2026

Browser Extensions

SaaS Integrations

zoom

AI IS EVERYWHERE

IDEs/Dev tools

Web Apps

Desktop Agents

Customers Profile Building On-Prem LLM / SLM

Neo-Cloud, (ISP) Service Providers

GPU-as-a-Service (GPUaaS) platforms, multi-tenant.

Government / Defense / Public Sector

Sovereign AI, national security, air-gapped environments

Financial Services (Banks & Insurance)

Private inference, regulatory compliance, risk & fraud AI

Manufacturing / Industrial / Engineering

IP-driven AI, digital twins, engineering copilots, factory AI.

Healthcare & Life Sciences

Clinical AI, pharma R&D, patient data protection

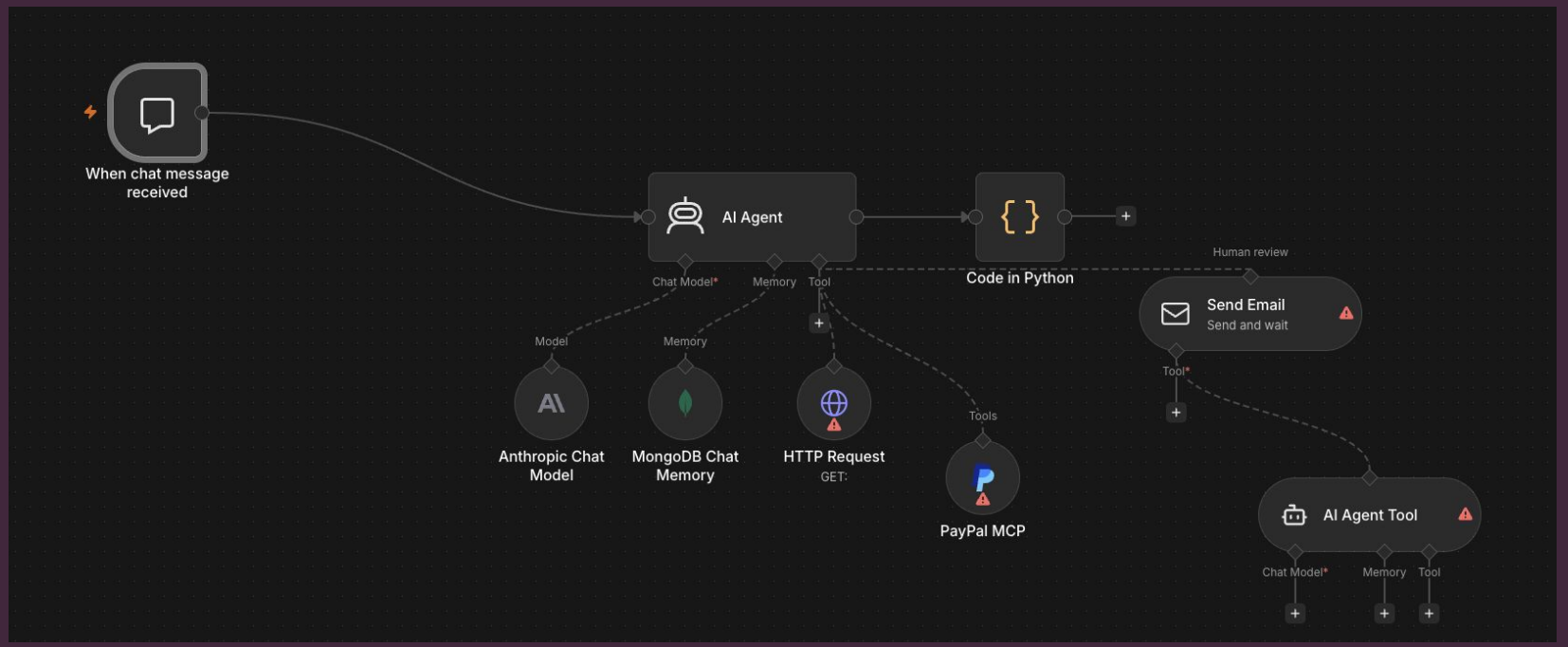
According to Gartner's server forecast, growth in the shipment of AI-optimized servers is driven **by enterprises and service providers** that are aiming to build future-ready AI data center facilities

Gartner

Source Gartner: Forecast Analysis: Data Center Sites, Worldwide

(18 Dec/2025)

Actual state of security of AI agents and AI datacenters



170

Described techniques in MITRE ATLAS

10

New risk categories in OWASP ASI Top 10 (2026)

08/2026

Compulsory testing of security and robustness via EU AI Act, čl. 9 a 15

512

New vulnerabiulities in open-source release projects

Proč agenti mění bezpečnostní model

Autonomie = nová proměnná. Agent jedná na základě svého oprávnění bez čekání na člověka — proto OWASP zavádí princip „least agency“.

Co dělá agenta jiným

- Plánuje a vykonává více kroků
- Volá nástroje, API, spouští kód
- Má paměť napříč sezeními
- Deleguje úkoly dalším agentům
- Nerozliší spolehlivě instrukci od dat

Excessive agency
víc autonomie, než je potřeba, zesiluje každou chybu

Goal / Behavior Hijack

ASI01 — nepřímý prompt injection v e-mailu, PDF, RAG obsahu

Tool Misuse

ASI02 — zneužití oprávněných nástrojů k neoprávněné akci

Identity & Privilege Abuse

ASI03 — eskalace přes nadměrná oprávnění agenta

Memory Poisoning

ASI06 — otrávení perzistentní paměti napříč sezeními

Insecure Inter-Agent Comm

ASI07 — útok přes nezabezpečenou komunikaci mezi agenty

Rogue Agents

ASI10 — drift chování, kolize, sebereplikace po kompromitaci

Zdroj taxonomie: OWASP Top 10 for Agentic Applications 2026 (ASI)

Lower

BARRIER TO PASS

Indirect prompt injection attacks (via files or websites) succeed with significantly fewer attempts than direct attacks, bypassing standard filters.

Source: Lakera Q4 2025 Agent Security Trends

60%

TARGET SYSTEM DATA

~60% of observed attack traffic attempts to leak system prompts—targeting the application's internal instructions and IP.

Source: Lakera Q4 2025 Agent Security Trends

15%

AUTONOMOUS DECISIONS

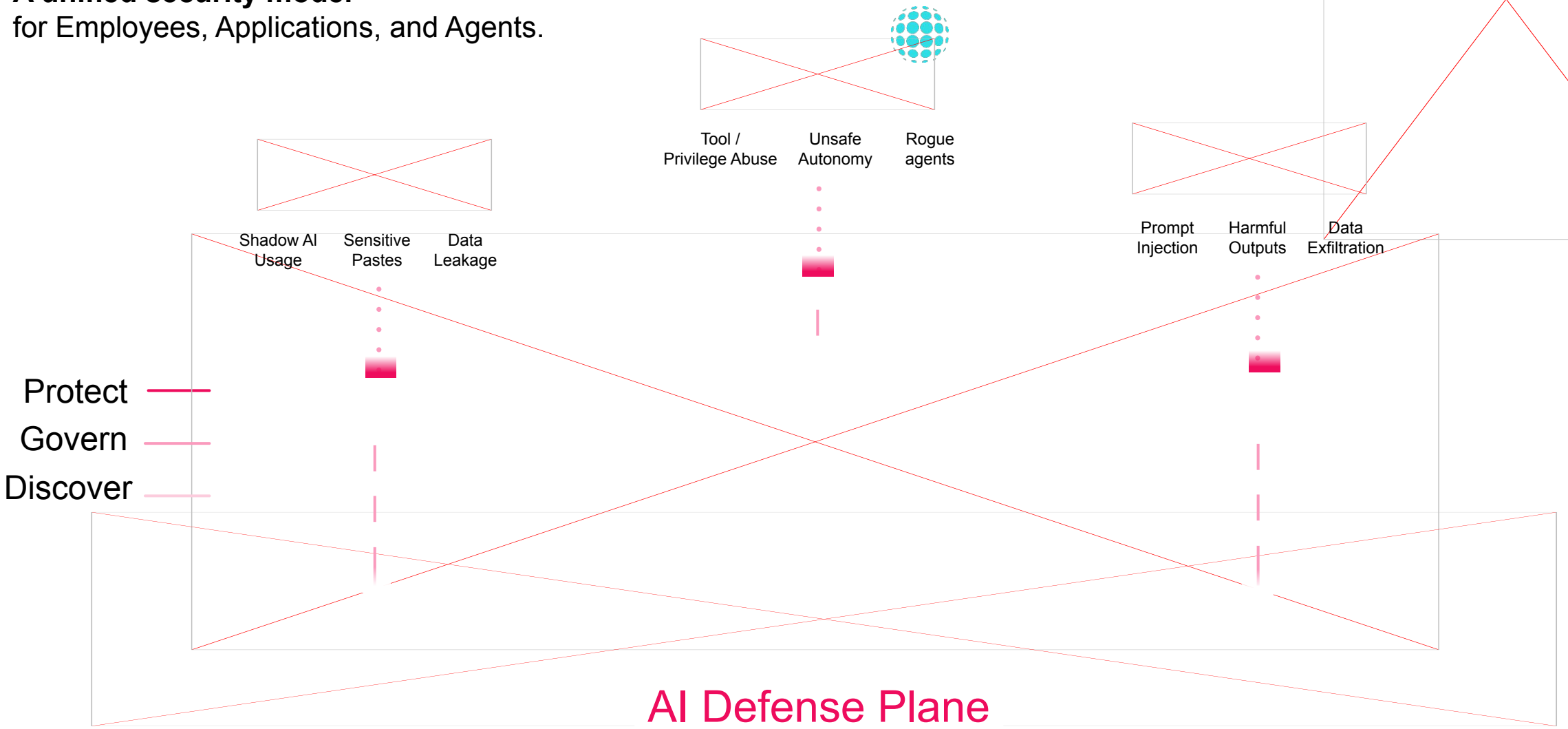
By 2028, 15% of day-to-day work decisions will be made autonomously by agentic AI—shifting the burden of trust from humans to machines.

Source: Gartner

Tool	What It Sees	What It Misses in AI
Network / WAF	Packets, HTTP requests	Prompt intent, reasoning paths
App Security	Schemas, validation	Indirect manipulation, context
DLP	Files, regex patterns	Semantic leakage in output
IAM	Roles, permissions	Unsafe autonomous sequences

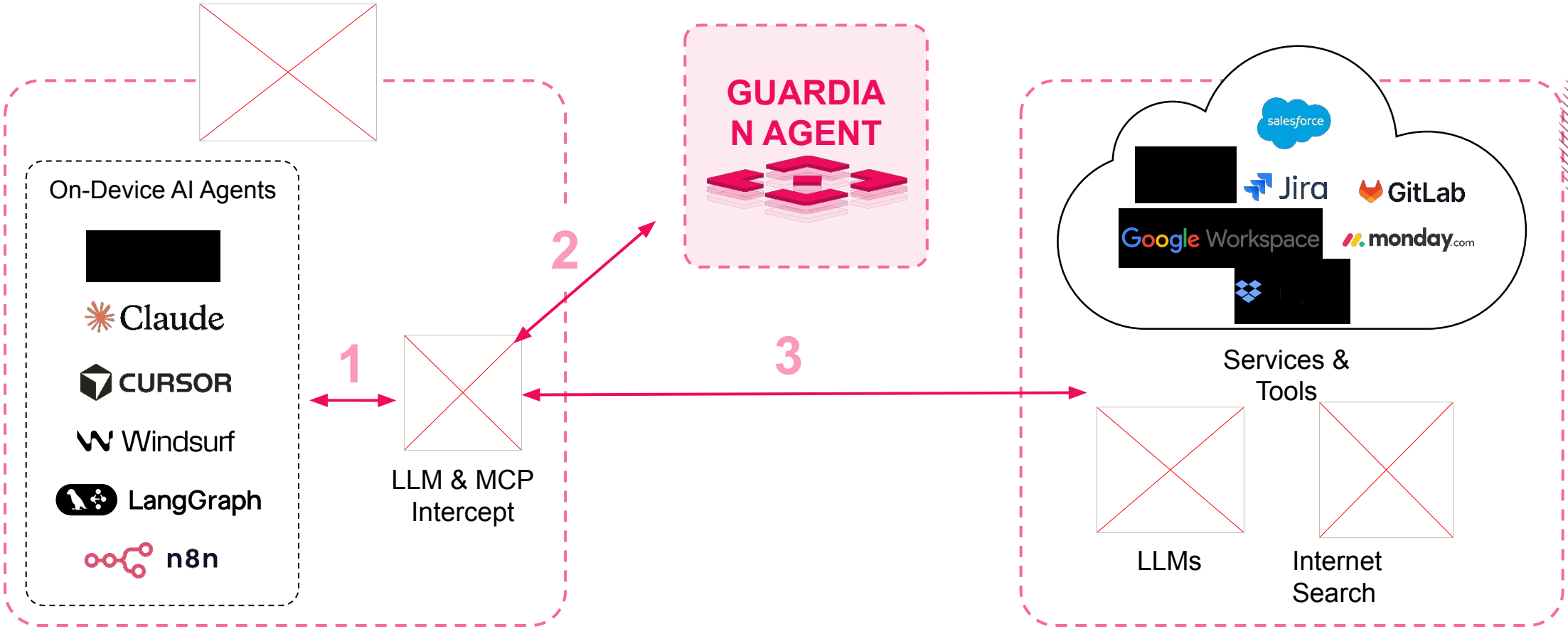
The Check Point AI Defense Plane

A unified security model
for Employees, Applications, and Agents.

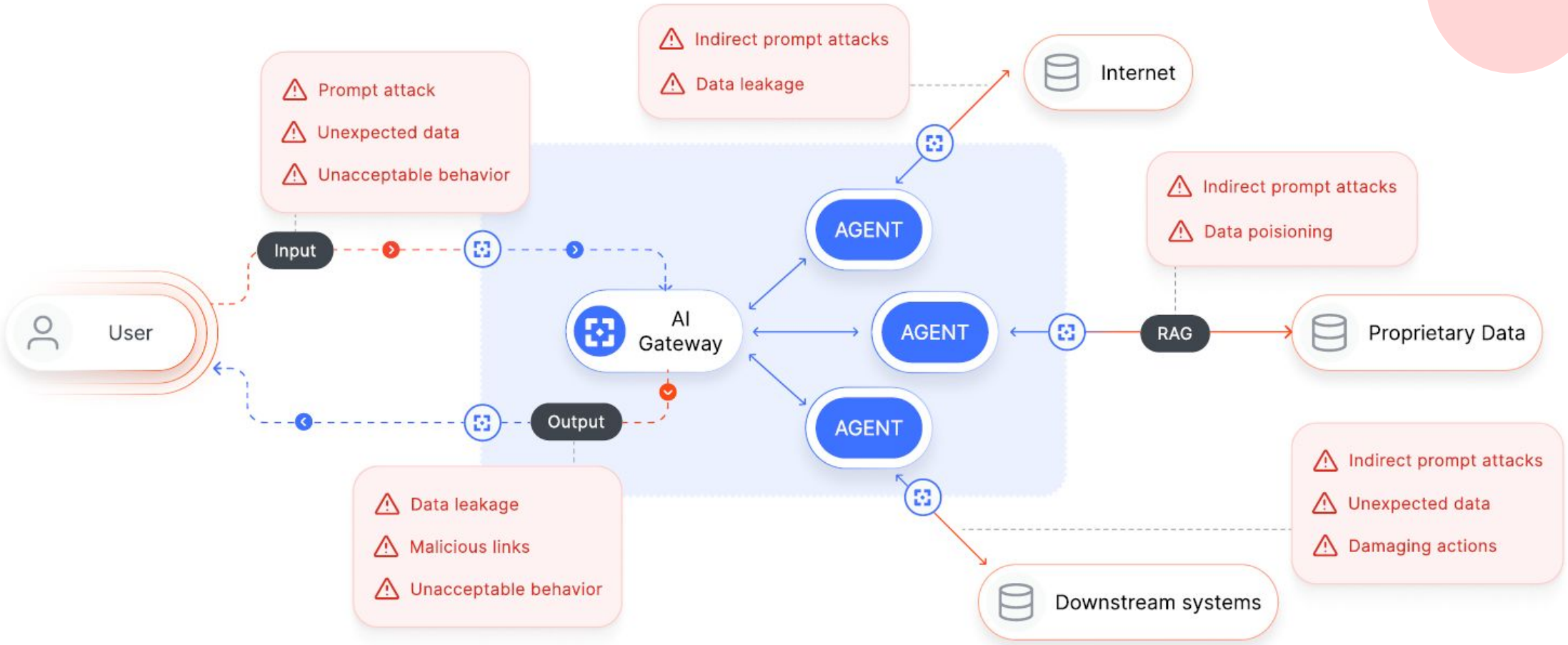


One platform. One lens. From employees to applications to agents.

Protect Agentic Use On Employee Devices



AI Guardrails: Agentic Patterns



AI Data Center Security:
Check Point Defense-in-Depth Stack

Comprehensive Network + Host + AI Level Security
Tailored Security at the network, host and prompt level designed for AI Infrastructure

Zero Impact on AI Performance
Running in BlueField-3 DPU with no impact on AI performance

Designed for cloud service providers
Dedicated security per customer
Easily manageable at scale

1. Perimeter & Network Security — Zone isolation, Remote Access, Egress filtering
- **Maestro Hyperscale NGFW**
- **ZTNA**

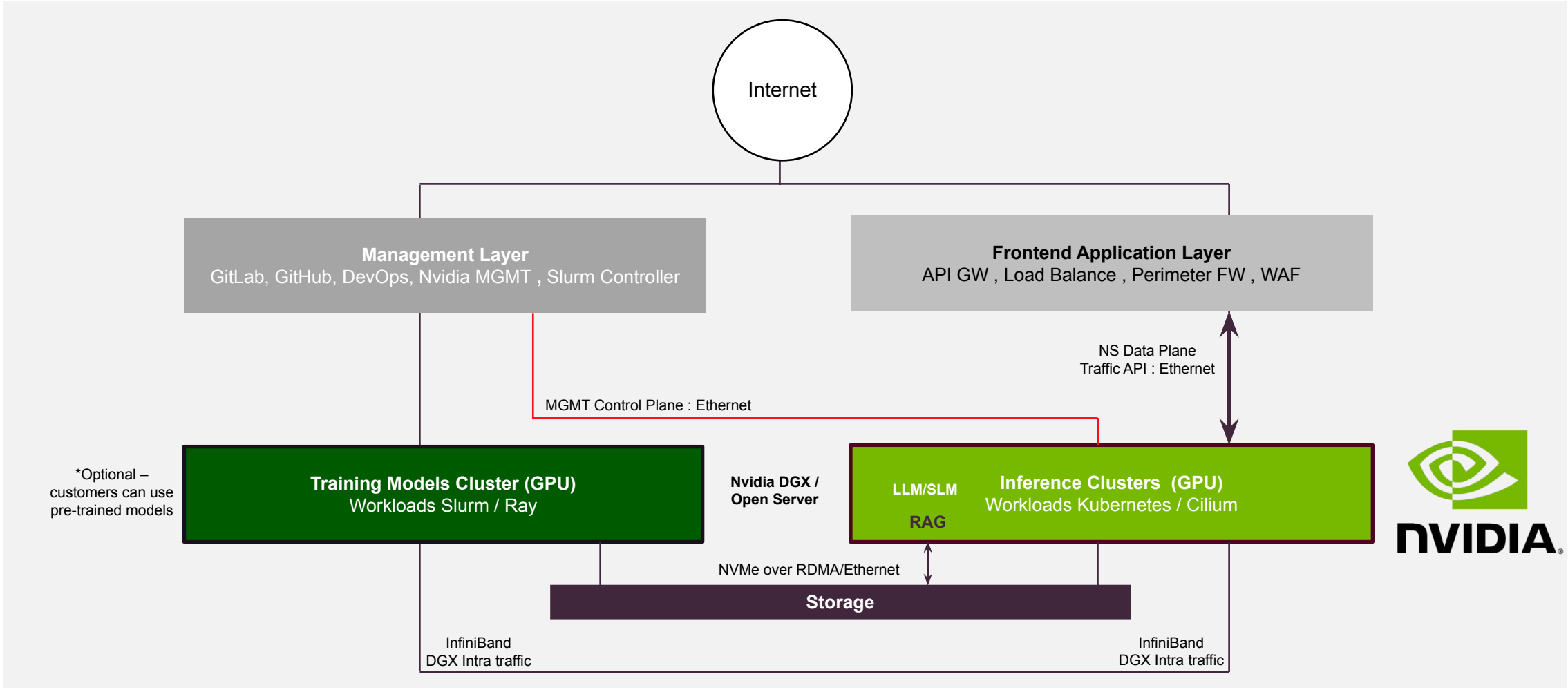
2. AI Native Application Security — Prompt injection, rate limiting, DLP
- **WAF + AI Security**
- **API Security + Guardrails**

3. Workload & Container Security — Zero Trust, runtime protection
- **Microsegmentation**
- **K8s Runtime Security**

4. Host Level Network Security (on every node) — Control & Data Plane protection , IPS, EW traffic security
- **Check Point NGFW + Nvidia BlueField-3 DPU**

5. Hardware-Accelerated AI Security (Integrated with Check Point) — Offloded inspection, AI workloads anomalies detection
- **Nvidia BlueField-3 DPU + DOCA + Check Point Threat Cloud**

Typical AI Data Center



Solution Blueprint

The AI Data Center Blueprint

Multi Layer: Data Center, Servers, Containers and Application

Internet
Users
DevOps

Maestro Hyperscale Firewall

Access Control, Zero Trust
Private Access, Threat Prevention

DevOps,
Operations/Management Plane

Users,
Data Plane

Server Segmentation
Access Control
IPS

Training Model Clusters

Firewall

Nvidia
DGX Server

Firewall

Nvidia
DGX Server

Apps + AI Inference

Firewall +
Prompt Security

Nvidia
DGX Server

Firewall +
Prompt Security

Nvidia
DGX Server

LLM GW

Prompt Security
(App Layer)

LAKERA

Inference Apps Containers

Micro segmentation

AI Native Application Security

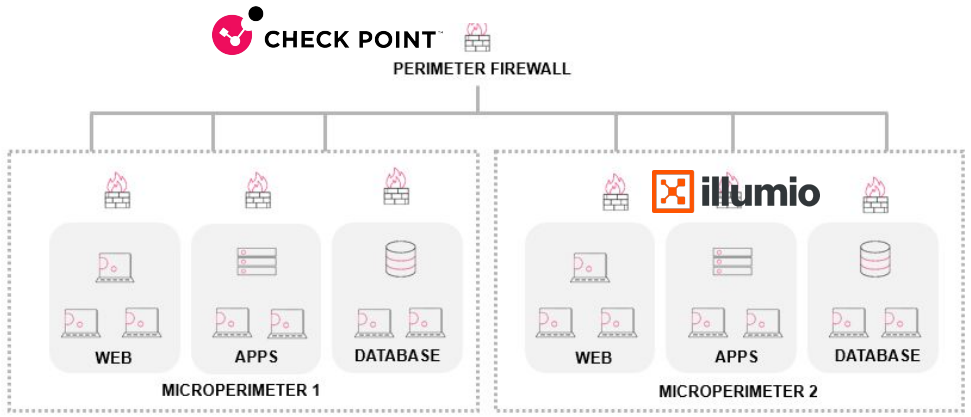
- **Cloud-native Web & API security solution** that provides precise threat prevention using contextual AI to protect your Apps against known and unknown threats, without relying on signatures.

1. **Perimeter & Network Security**
2. **AI Native Application Security**
3. **Workload & Container Security**
4. **Host Level Network Security (on every node)**
5. **Hardware-Accelerated AI Security (Integrated with Check Point)**

- Protects LLM APIs from prompt injection and jailbreak attacks
- Enforces safe and compliant use of LLMs through policy controls
- Monitors and restricts LLM tool and function usage
- Prevents sensitive data leakage in LLM responses

Workload & Container Security

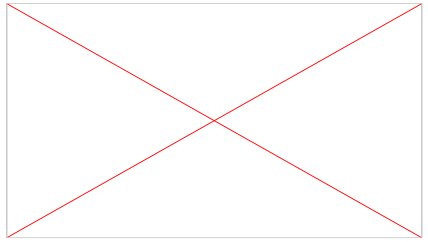
Check Point integration with Illumio can provide additional AI-driven insights to identify risks and attack routes, enabling quick containment at the container layer. It is also possible to accomplish similar micro segmentation using PVLAN and/or SDN technologies.

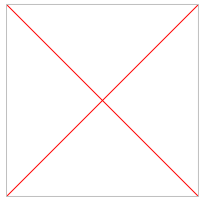


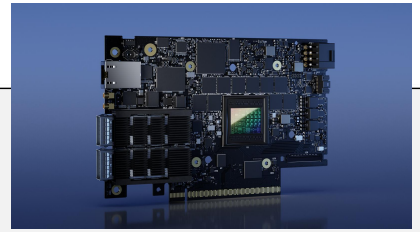
- **Collaborative approach to zero trust:** Protect critical assets with effective micro-segmentation across hybrid environments, simplifying and accelerating zero trust adoption
- **Lateral movement prevention:** Shield critical assets by identifying attack paths early and preventing threats from spreading laterally across the network
- **Advanced threat intelligence:** Leverage combined threat intelligence from both platforms to expose hidden threats and strengthen your security posture

1. **Perimeter & Network Security**
2. **AI Native Application Security**
3. **Workload & Container Security**
4. **Host Level Network Security (on every node)**
5. **Hardware-Accelerated AI Security (Integrated with Check Point)**

AI Host / GPU Level Protection







Server Resources

NVIDIA GPU

CPU

Host memory

BlueField-3 DPU

CHECK POINT

DOCA

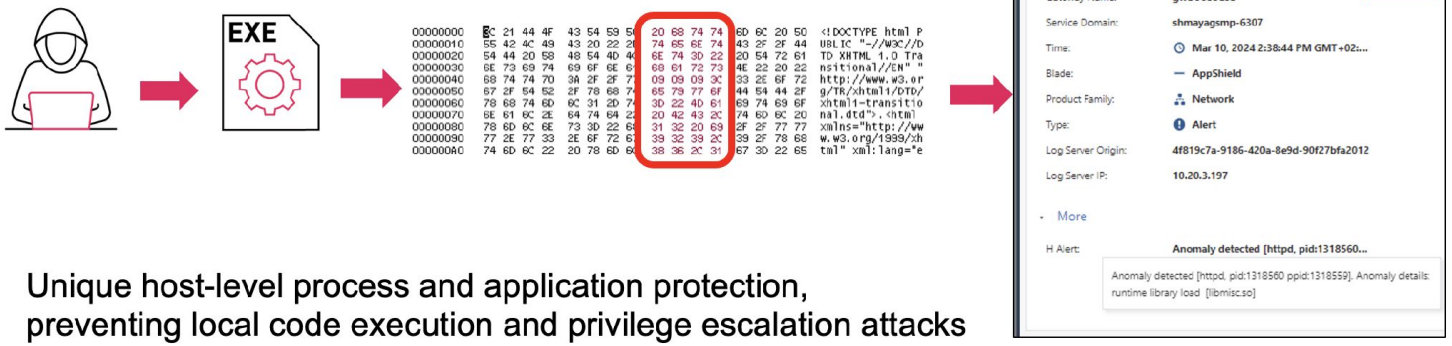
Argus

Independent of the host, invisible to attackers

Security functions run on DPU, so CPUs and GPUs are fully dedicated for AI

1. **Perimeter & Network Security**
2. **AI Native Application Security**
3. **Workload & Container Security**
4. **Host Level Network Security (on every node)**
5. **Hardware-Accelerated AI Security (Integrated with Check Point)**

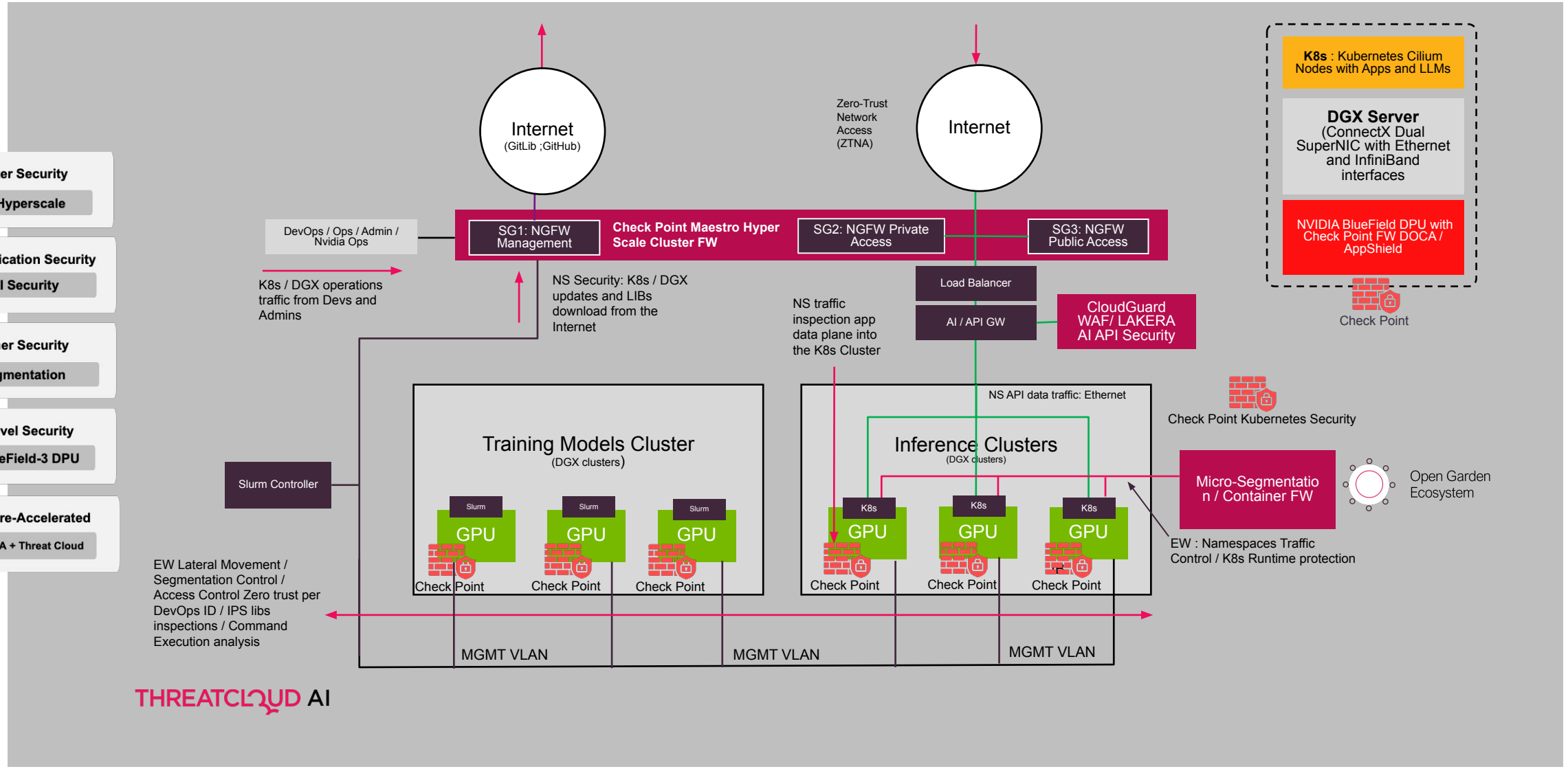
Hardware-Accelerated AI Security (Integrated with Check Point)



Unique host-level process and application protection, preventing local code execution and privilege escalation attacks

1. **Perimeter & Network Security**
2. **AI Native Application Security**
3. **Workload & Container Security**
4. **Host Level Network Security (on every node)**
5. **Hardware-Accelerated AI Security (Integrated with Check Point)**

Check Point AI DC Full Security Stack



https://catalog.ngc.nvidia.com/orgs/nvidia/teams/doca-checkpoint/containers/aicp?version=0.8.2

Thank You!