



Safeguarding Critical Infrastructure with AI-Driven Cybersecurity

February 2025

Cybersecurity at the Crossroads

Critical infrastructure is facing an unprecedented level of cyber threats



U.S. utilities faced a nearly 70% jump in cyberattacks from January to August 2024 compared to the same period in 2023, underlining the escalating threat to critical infrastructure¹

Cyberattacks on critical national infrastructure have risen by 30% in 2024, with the US power grid being particularly vulnerable²

*The U.S. Department of Homeland Security (DHS) warns of escalating threats to US critical infrastructure in 2025
Homeland Threat Assessment³*

(1) [Check Point Research](#) | (2) [KnowBe4](#) | (3) [Industrial Cyber](#)

Navigating the Evolving Landscape of Critical Infrastructure Security

Outdated systems, converging networks, and increasing regulatory pressure create new challenges



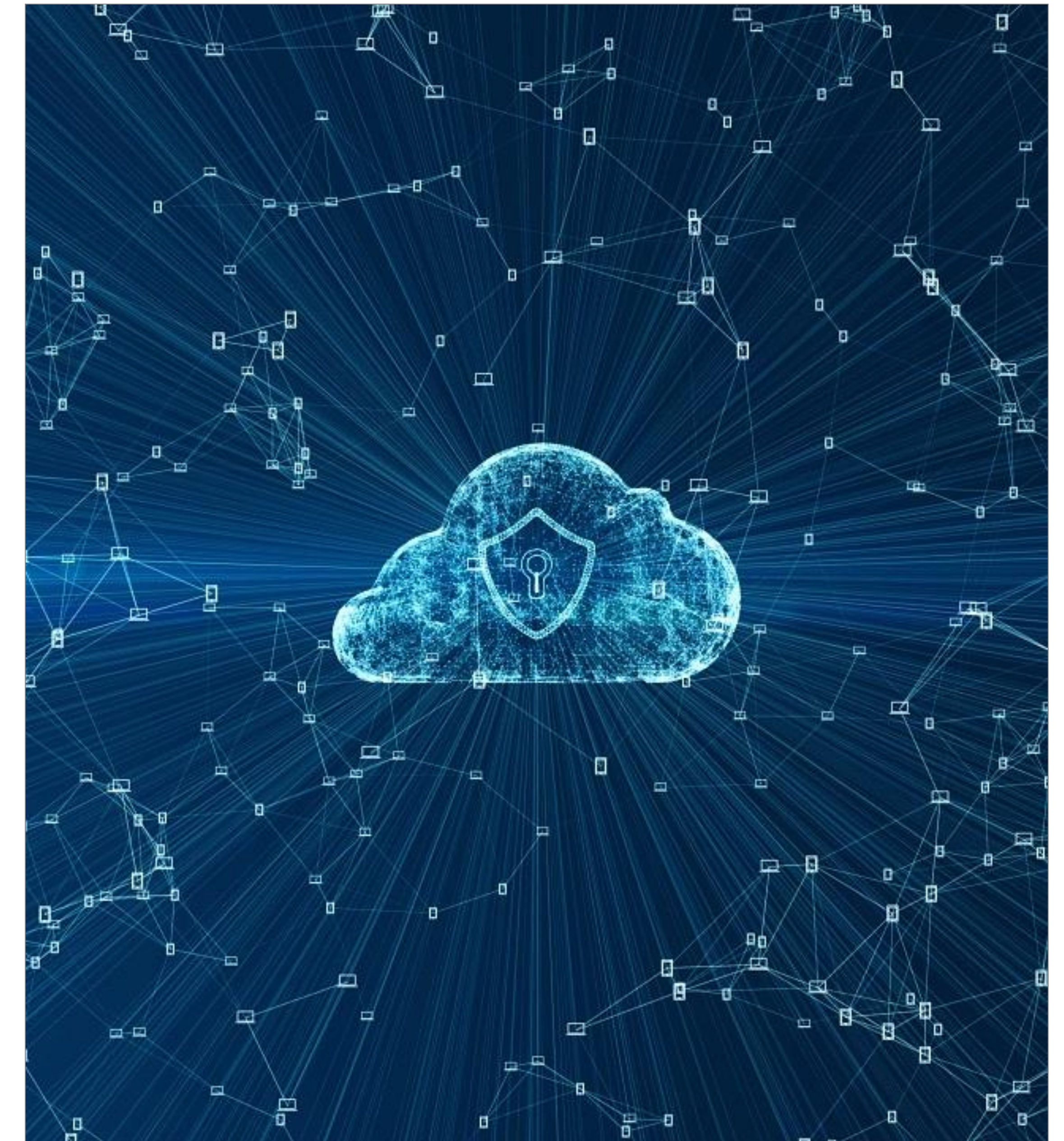
Legacy Infrastructure

Many OT systems are outdated, and run unpatched, legacy operating systems and protocols



IT/OT Convergence

Every ICS sensor, instrument, and device accessible over an IT/OT network is at risk of compromise



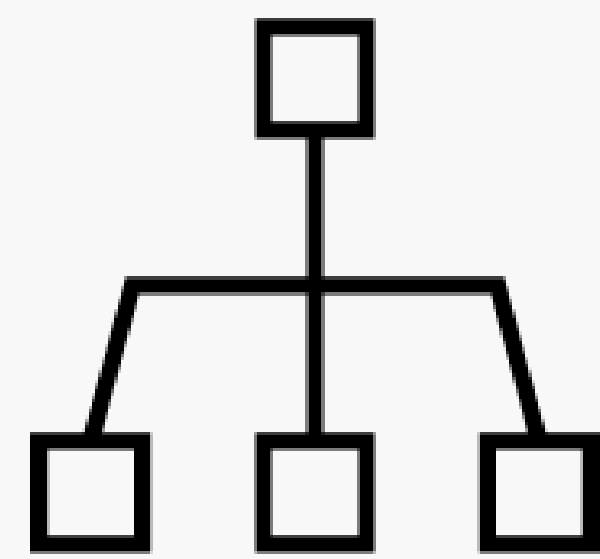
Heightened Regulatory Demands

New regulations mandate utilities to strengthen defenses against evolving cyber threats

Needs and Challenges for Securing Critical Infrastructure

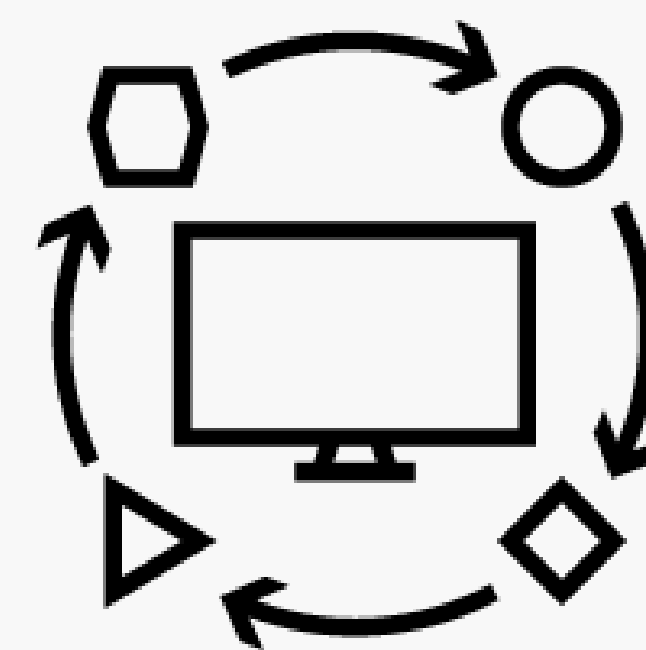
Traditional cybersecurity solutions fall short in protecting OT networks from escalating threats

Comprehensive Visibility



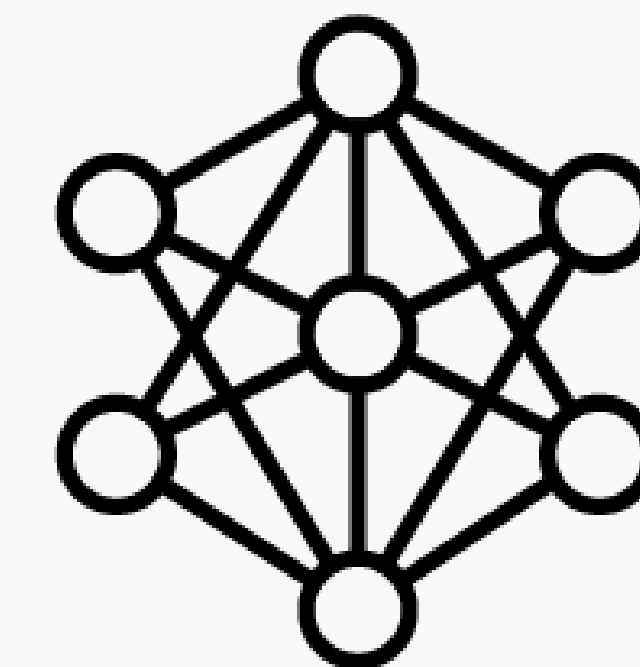
Existing security tools often lack full visibility into nodes, networks, and applications, limiting threat detection and response

Non-Disruptive Security



Traditional security controls are intrusive and may disrupt OT systems, compromising critical operations

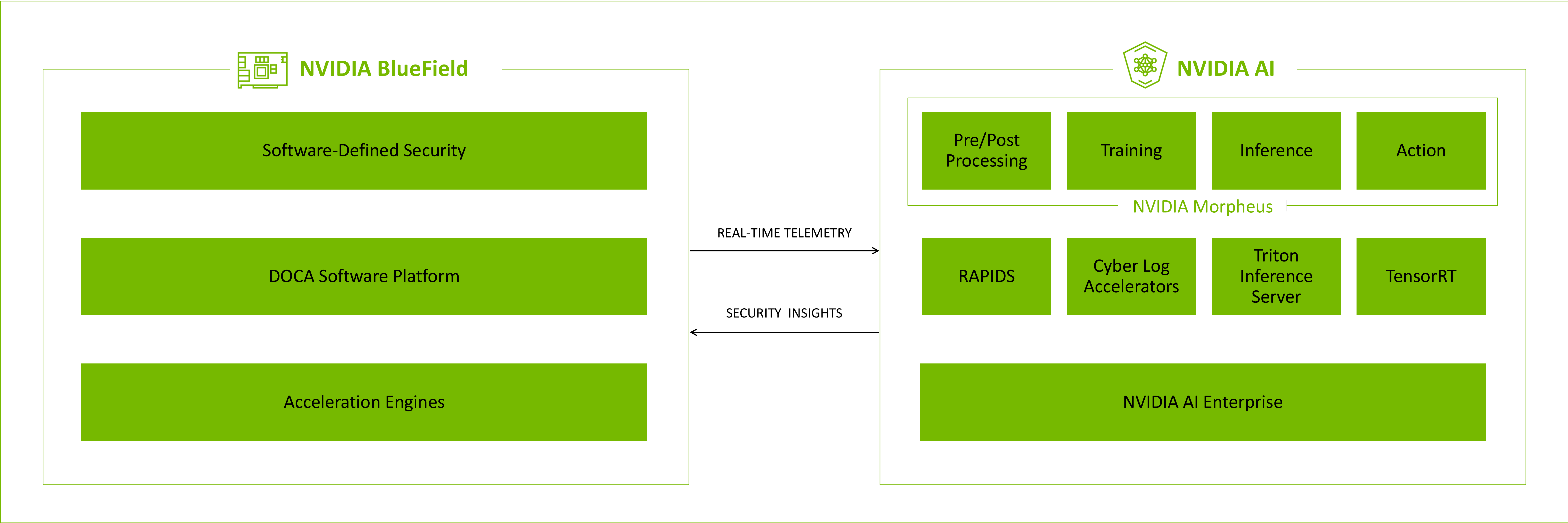
AI-Driven Analytics



AI solutions relying on partial data due to limited visibility fail to profile network behavior, detect anomalies, and stop emerging threats

NVIDIA Cybersecurity AI

Full-stack, accelerated computing platform for securing critical infrastructure assets



Powers accelerated AI-driven solutions to enhance your cybersecurity posture and secure critical infrastructure

Enhance Critical Infrastructure with NVIDIA Cybersecurity AI

Transforming OT security for the age of AI



New Class of OT Security

Deliver cutting-edge, real-time protection with comprehensive 360° visibility into hosts, networks, and applications



Seamless Integration

Achieve robust security without disrupting existing OT networks or hosts, simplifying and streamlining operations



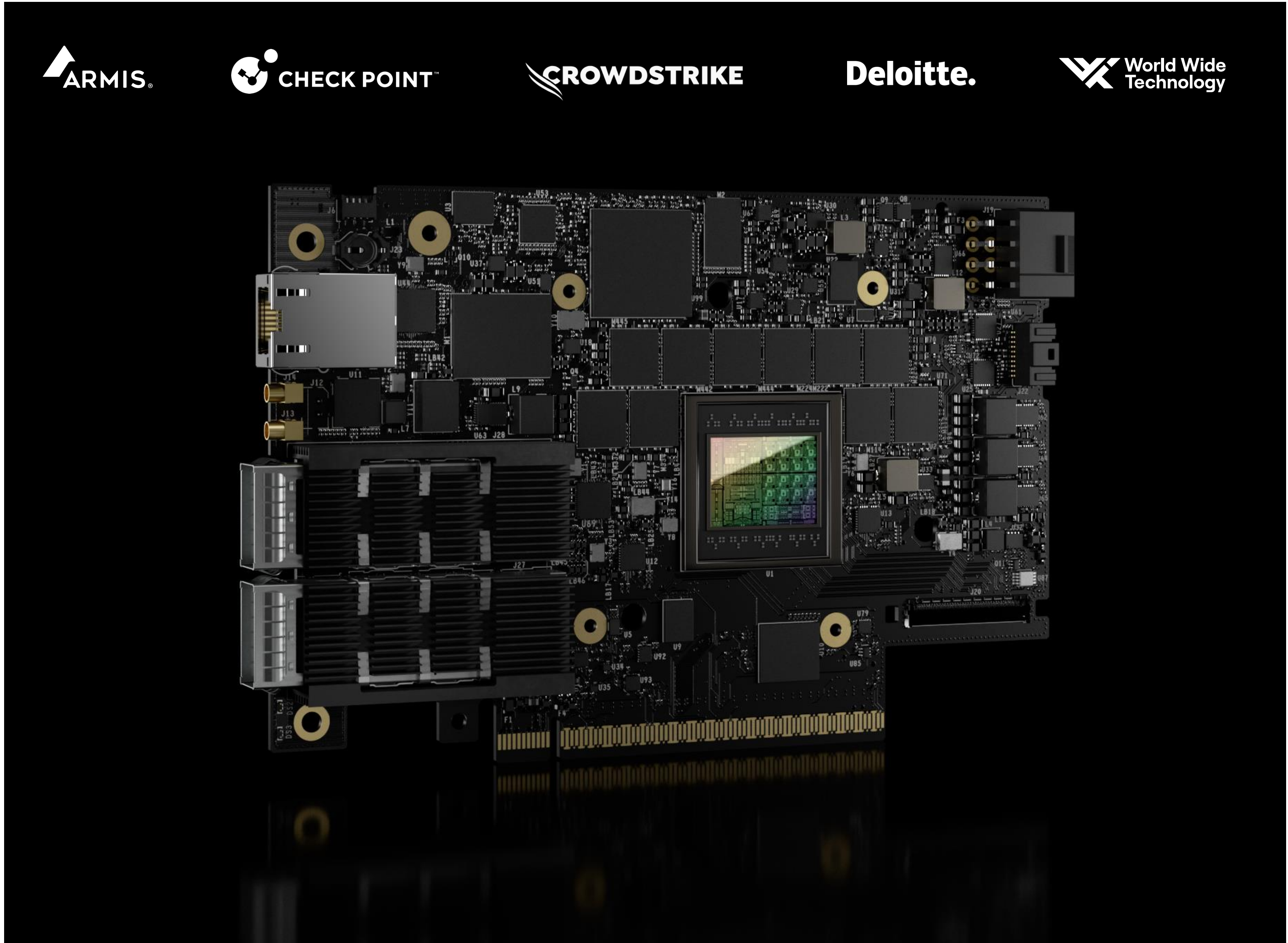
Built-in Security at the Edge

Push protection to every node with isolated, tamper-proof, out-of-band enforcement capabilities



AI-Powered Insights

Enhance security with AI-driven insights from NVIDIA Morpheus, enabling advanced threat detection and rapid response



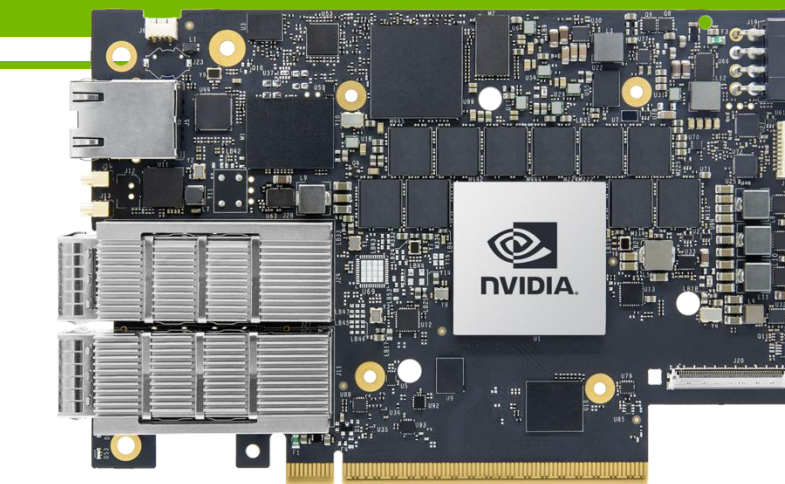
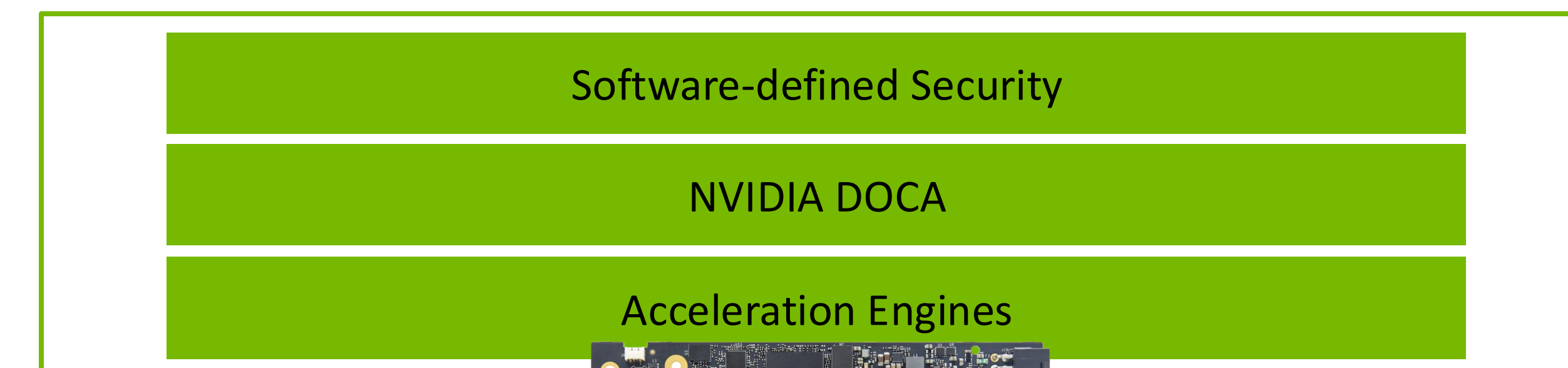
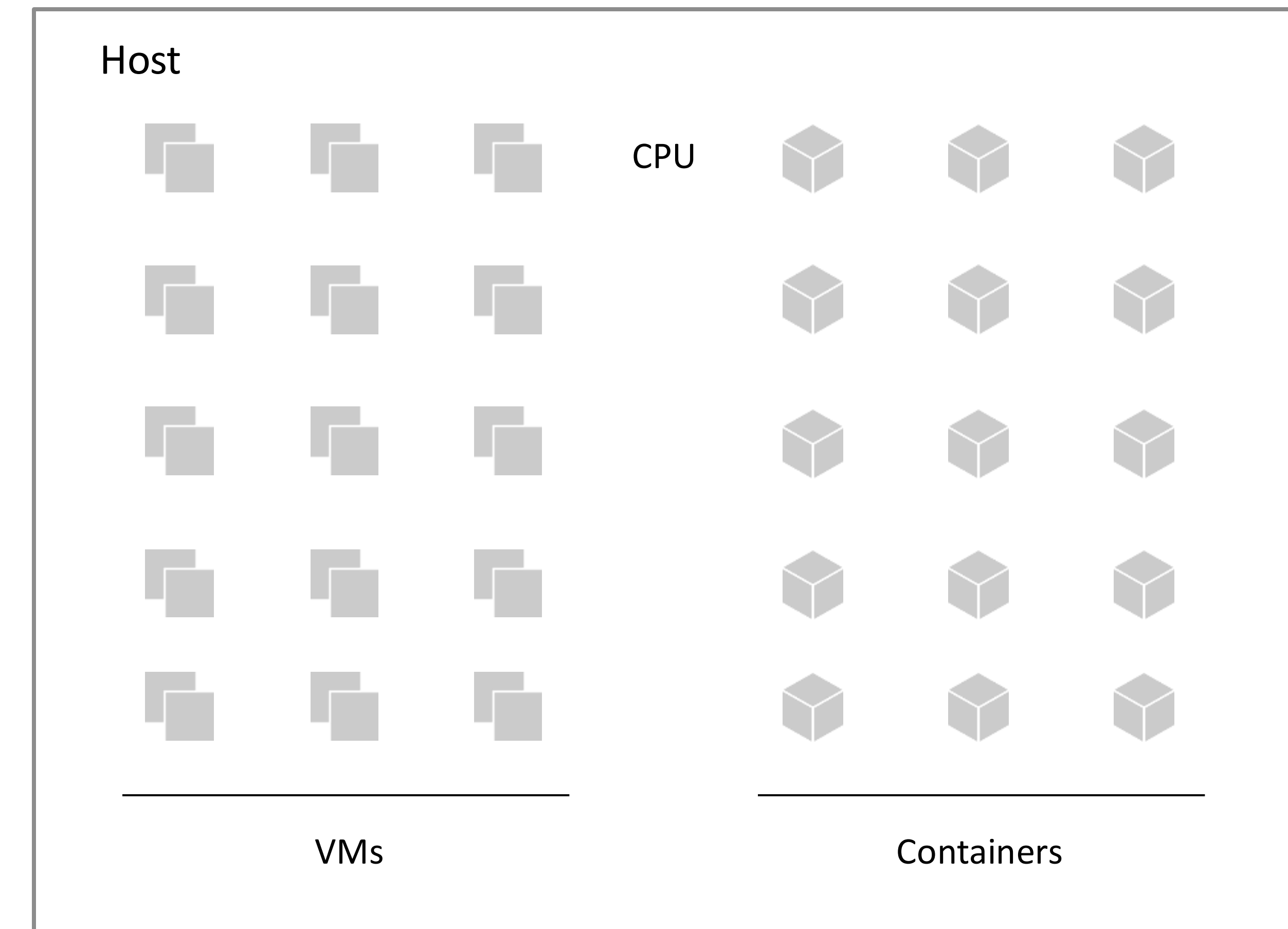
NVIDIA BlueField-3 DPU

Accelerated computing platform for Cybersecurity AI

NVIDIA BlueField-3 DPU

Accelerated computing platform for Cybersecurity AI

- Advanced SoC integrating high-speed NIC, 16 x Arm cores, DDR5 memory, with integrated eMMC and SSD storage
- Runs all major operating systems, VMs and containers
- Powered by NVIDIA DOCA software framework, accelerating data center infrastructure applications
- Non-intrusive device operating in zero-trust mode, appearing to the host as a standard NIC
- Enables security for every node with purpose-built hardware acceleration engines

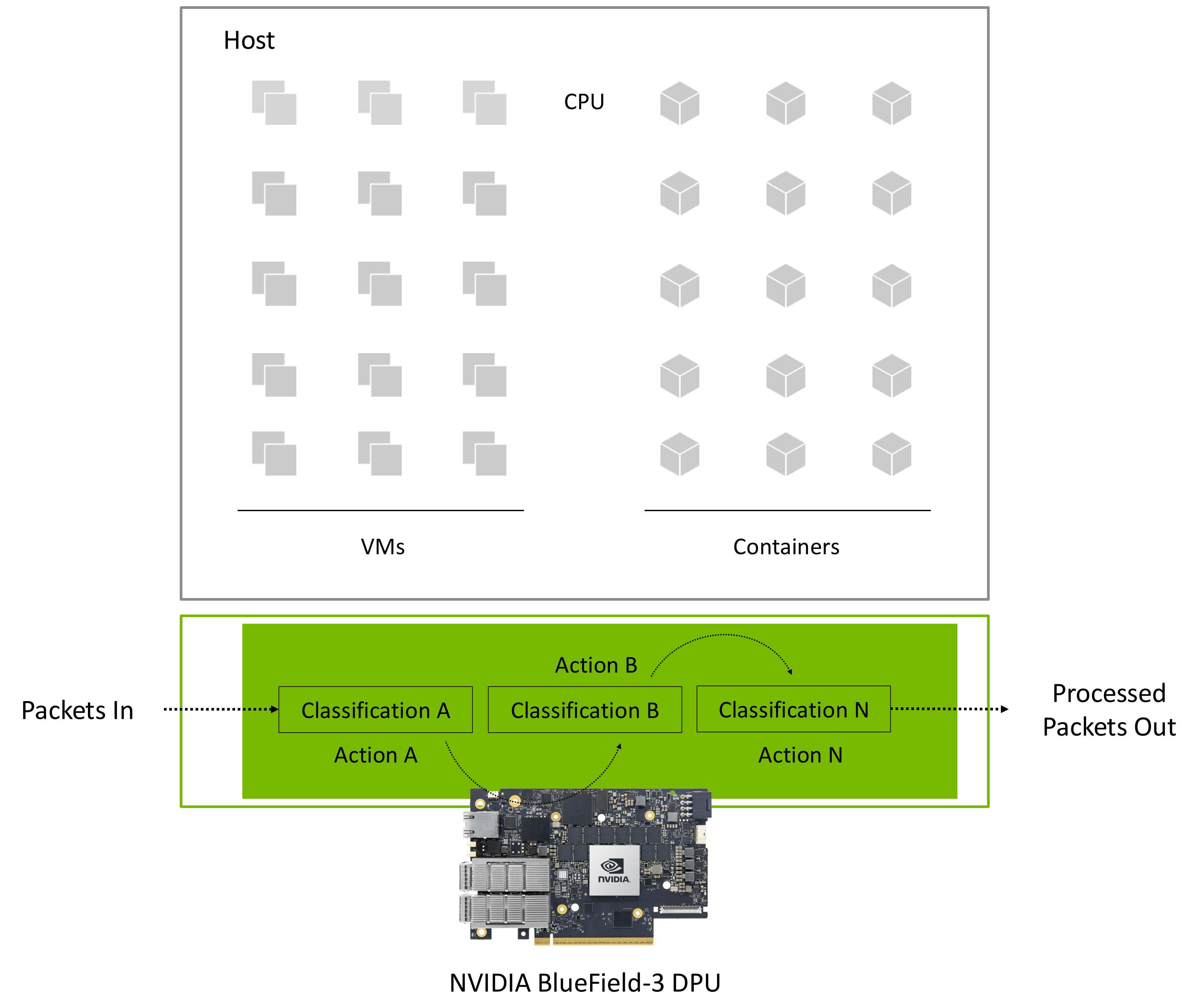


NVIDIA BlueField-3 DPU

NVIDIA OVS-DOCA

Virtual switch with built-in network segmentation and firewalling capabilities

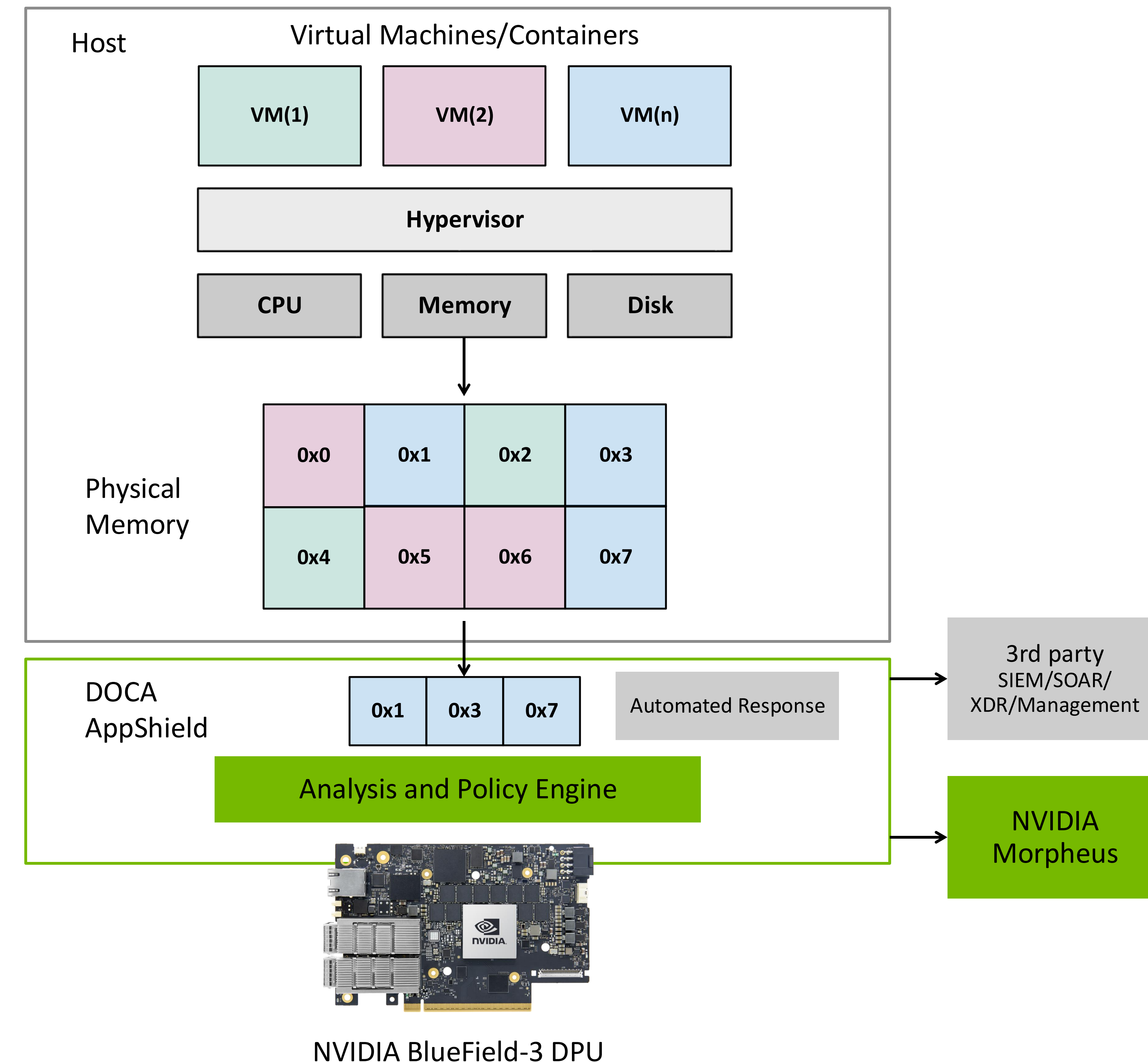
- Open vSwitch (OVS)-based switch, accelerated by NVIDIA DOCA
- Software-defined, highly optimized for security processing
- Fully programmable with flexible match and action engine
- Enforces network security policy in the BlueField hardware
- Operates independently from the host



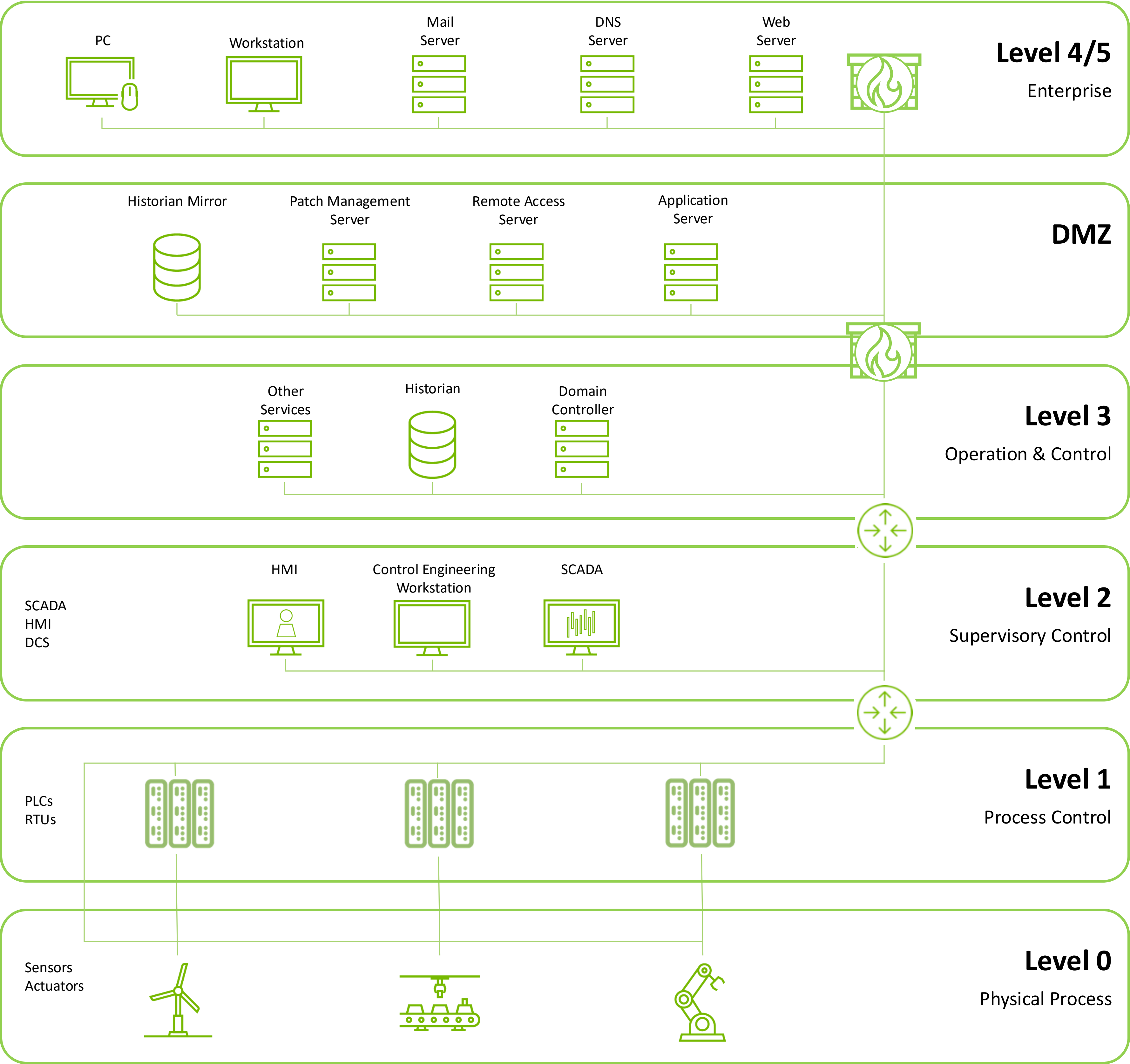
NVIDIA DOCA AppShield

Analyzes volatile memory snippets in real-time to deliver insights into the state of application workloads

- Provides real-time workload visibility by analyzing snippets of specific regions of volatile memory in real-time
- Immediately detects and stops runtime attacks to minimize potential impact and risk
- Robust security capabilities built into every node:
 - No agents
 - No integration with the compute workload
 - No performance impact
 - Autonomous operation
- Invisible to attackers as monitoring persists even if the host is comprised

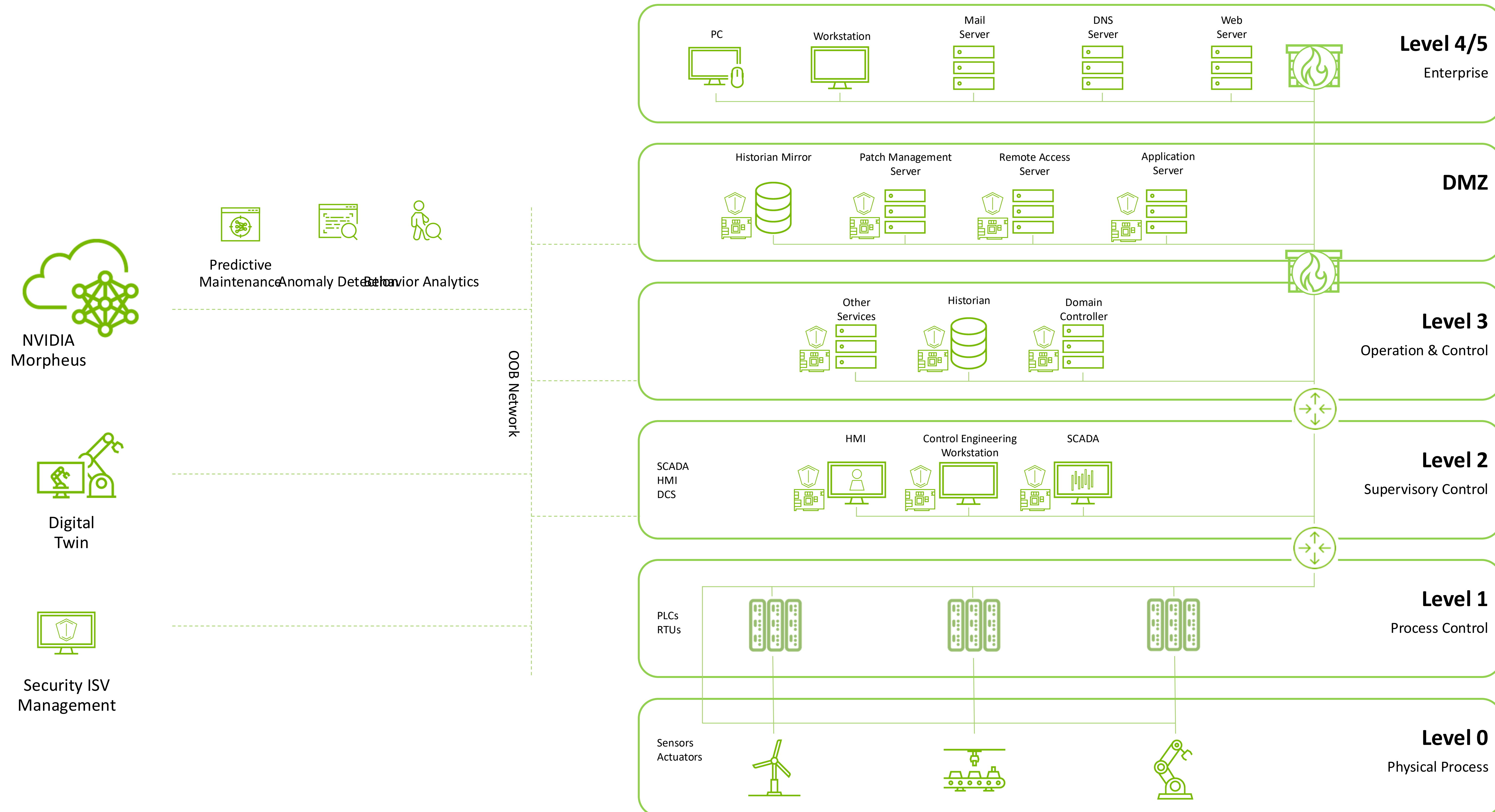


An Abstract of The Purdue Model



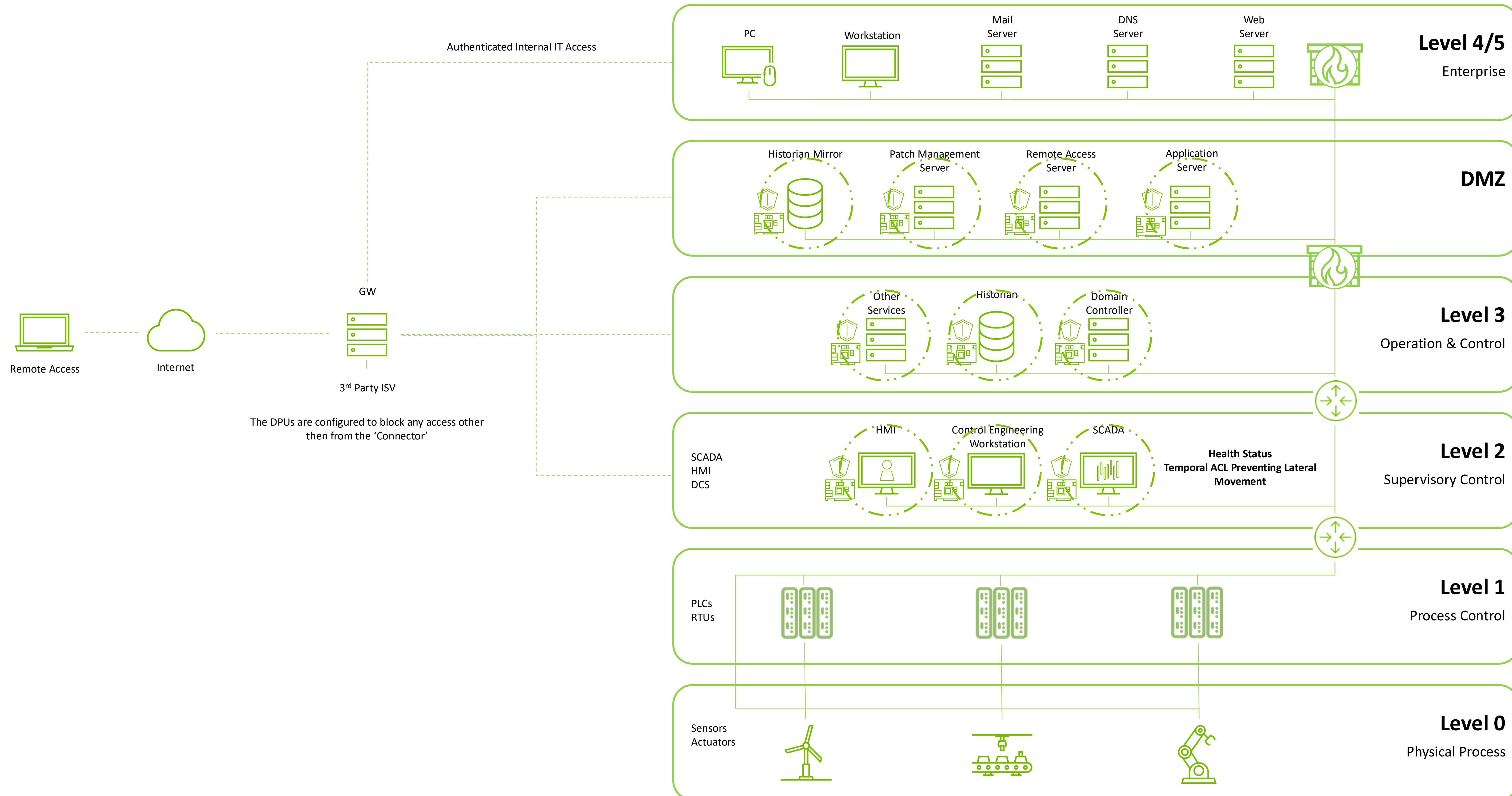
Safeguarding Critical Infrastructure

Powered by NVIDIA Cybersecurity AI



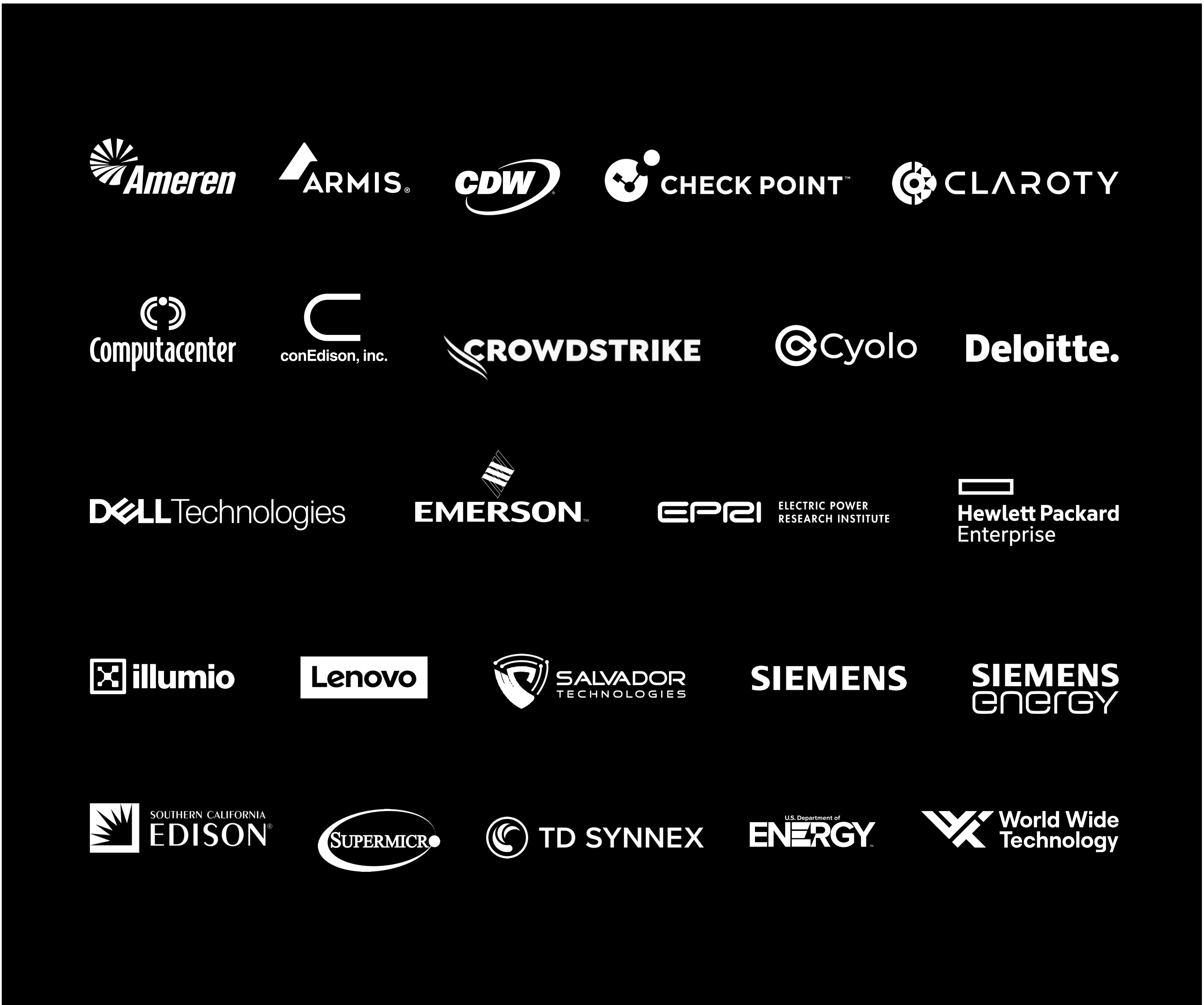
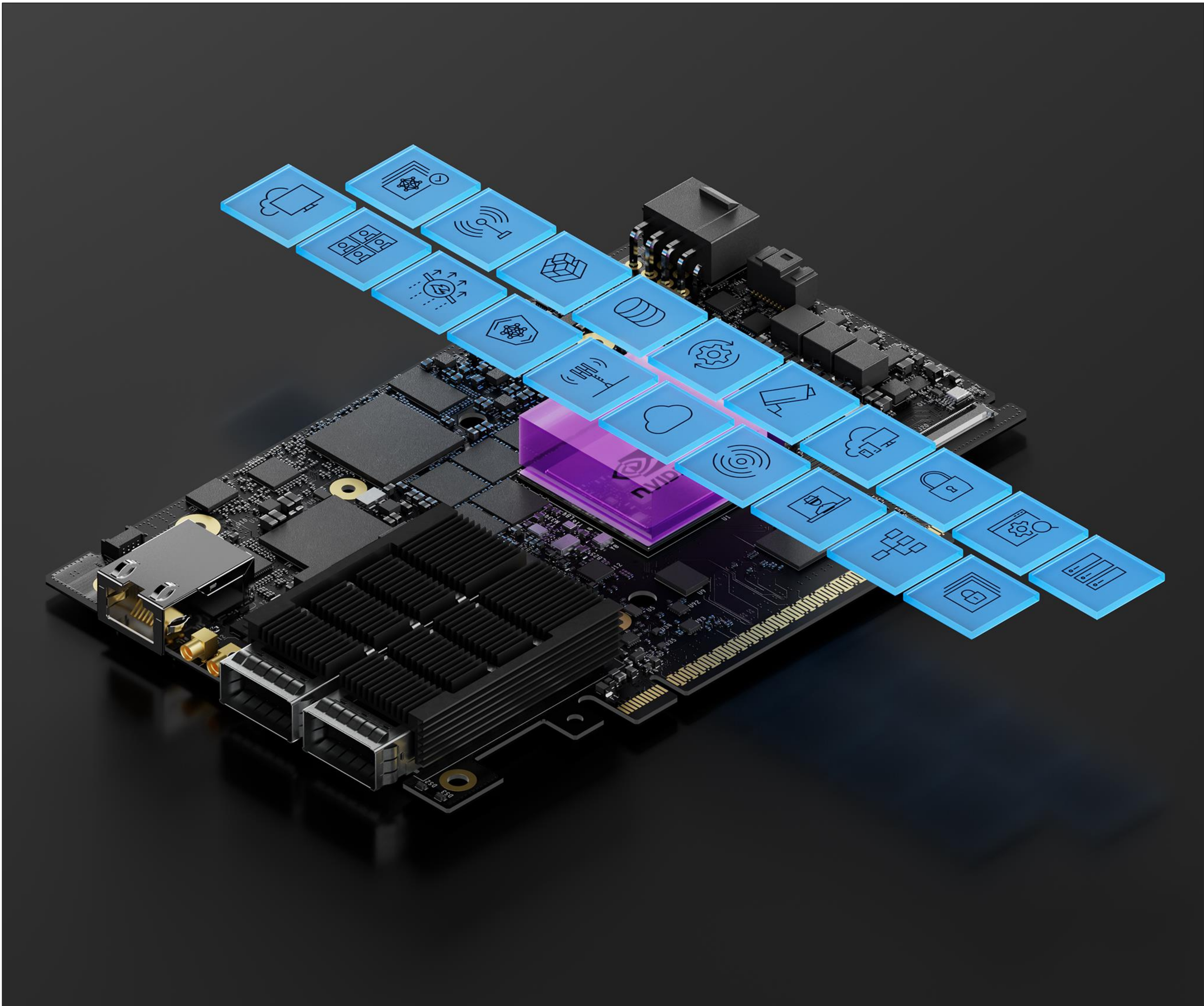
Secure Access Management

Powered by NVIDIA Cybersecurity AI



Enhance Critical Infrastructure with NVIDIA Cybersecurity AI

Driving cybersecurity innovations across a growing OT partner ecosystem



Enhance Critical Infrastructure with NVIDIA Cybersecurity AI

Key Features and Capabilities



Comprehensive 360° Visibility

Delivers real-time, granular insights into network, host, and application activity to enhance protection



Network Firewalling & Segmentation

Leverages software-defined, hardware engines to contain threats and prevent lateral movement



Command-Level Authorization

Authorizes the execution of every command issued, preventing certain commands from being executed



Secure Access Management

Implements zero trust by managing access, isolating OT from IT, and controlling third-party maintenance access



Real-Time Automated Response

Actively blocks suspected processes, terminates network connections, and isolates systems deemed compromised



AI-Powered Behavioral Analytics

Uses behavioral profiles, built per system and equipment type, to detect suspicious activity with AI

Enhance Critical Infrastructure with NVIDIA Cybersecurity AI

Transforming OT security for the age of AI



New Class of OT Security

Deliver cutting-edge, real-time protection with comprehensive 360° visibility into hosts, networks, and applications



Seamless Integration

Achieve robust security without disrupting existing OT networks or hosts, simplifying and streamlining operations



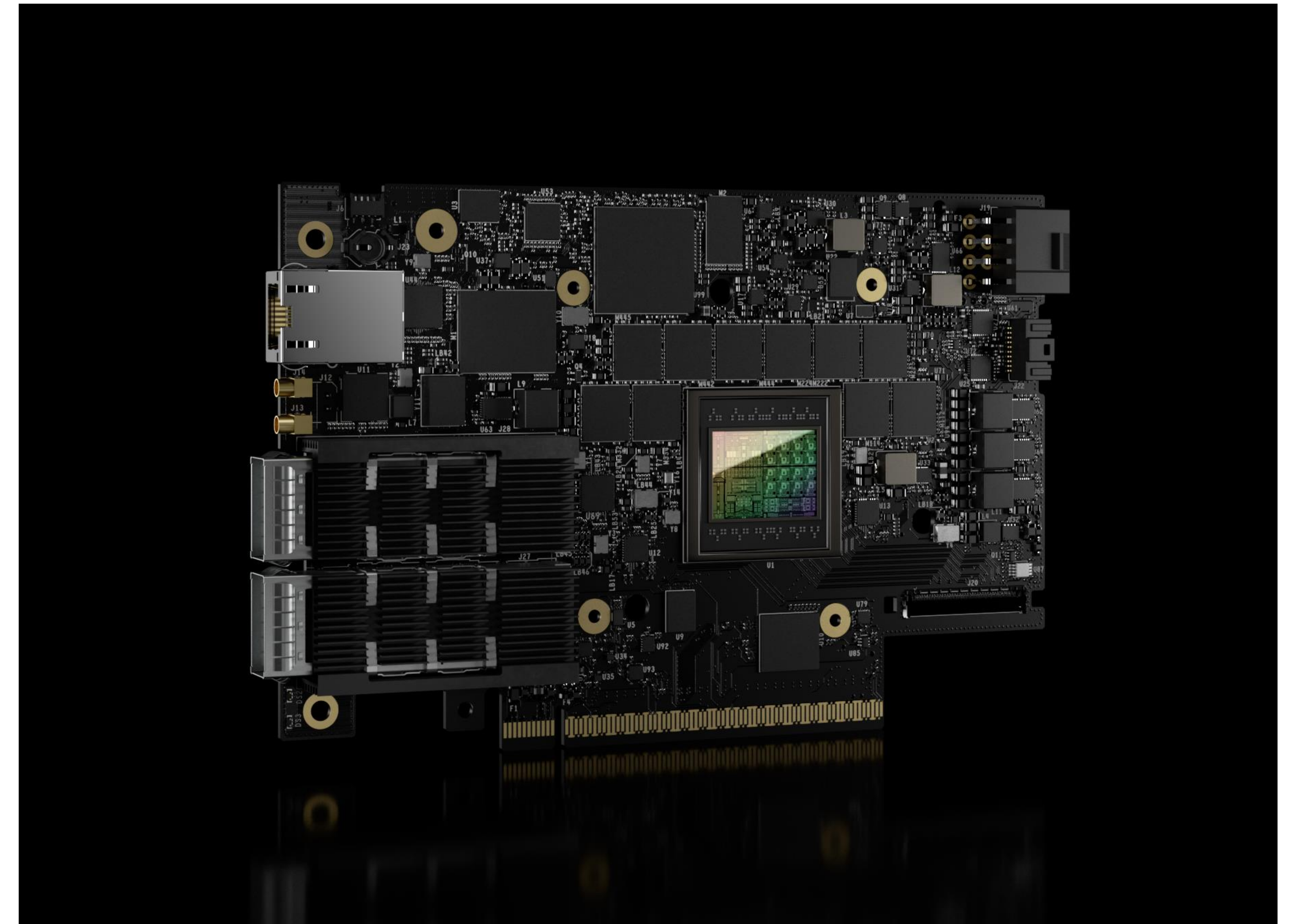
Built-in Security at the Edge

Push protection to every node with isolated, tamper-proof, out-of-band enforcement capabilities



AI-Powered Insights

Enhance security with AI-driven insights from NVIDIA Morpheus, enabling advanced threat detection and rapid response



NVIDIA BlueField-3 DPU

Accelerated computing platform for Cybersecurity AI

Enhance Critical Infrastructure with NVIDIA Cybersecurity AI

Key takeaways



- Securing critical infrastructure security is essential to saving lives
- Full-stack, accelerated computing platform for securing critical infrastructure assets
- Seamlessly integrates into existing network environments
- Enables real-time, AI-driven threat detection and response for OT systems
- Harnesses AI acceleration to optimize security data processing

