Xage Delivers Unified Zero Trust for AI with NVIDIA BlueField

Xage Zero Trust Platform Integrates with NVIDIA BlueField Acceleration to Secure AI Deployments

AI factories and critical infrastructure are becoming the backbone of modern life and innovation — from advanced AI data centers hosting agentic AI workloads to the energy grids needed to keep both digital and physical infrastructure running.

These environments face unprecedented cybersecurity challenges:

- Billions of data flows and millions of assets, both digital and cyber-physical, spread across data center and critical infrastructure environments.
- Experimental AI components and legacy critical infrastructure systems, either of which may have limited built-in security.
- Zero-trust-specific risks, including rogue agents, compromised models, supply chain threats, and privilege escalation in complex entitlement environments.
- Regulatory and compliance pressures such as NIST, NERC CIP, EU NIS2, and U.S. DoD Zero Trust mandates.

To stop advanced adversaries and prevent disruptions, organizations must enforce identity-driven security and access controls in the moment directly where decisions and actions occur.

The Solution: Xage Fabric Platform and NVIDIA BlueField DPUs

Xage delivers a hardware-accelerated Zero Trust solution, powered by NVIDIA BlueField, that provides real-time, line-speed enforcement for the most demanding AI and critical infrastructure environments. The integration represents a breakthrough in securing modern innovation by combining the Xage Fabric Platform with NVIDIA BlueField DPUs, enabling organizations to achieve unmatched performance, resilience, and security for AI factories and the cyber-physical systems that power our world.

Key Benefits

- **Hardware-Accelerated Enforcement:** Real-time security at line speed, with zero impact on host performance.
- **Identity-based Segmentation:** Prevent lateral movement between systems, workloads, models, AI agents, etc.
- **Resilience for Critical Infrastructure Environments:** Secure legacy systems and distributed deployments without downtime or rip-and-replace disruption.
- **Jailbreak-proof Protection for AI Factories:** Govern data flows between agents and models in real time, line-speed protection for AI factories.
- **Regulatory Compliance Support:** Built-in controls to meet NIST, NERC CIP, EU NIS2, and DoD mandates.

Key Components and Architecture Overview

Xage enables a closed-loop security architecture that prevents, detects, and blocks or contains threats before they spread.

Xage Fabric Platform for Dynamic Access Control and Segmentation

- Applies least-privilege policies to every interaction between humans, systems, AI models, and autonomous agents.
- Governs who or what can access which data, pipelines, or models, the exact actions allowed, and for how long.
- Provides visibility and interaction data for traceability, regulatory, and compliance
- Xage Fabric platform includes Xage Fabric Nodes, Xage Extended Protection (XEP), and centralized policy management components.
- XEP leverages BlueField-3 DPUs to enforce secure real-time segmentation of workloads to prevent lateral movement and isolate threats.

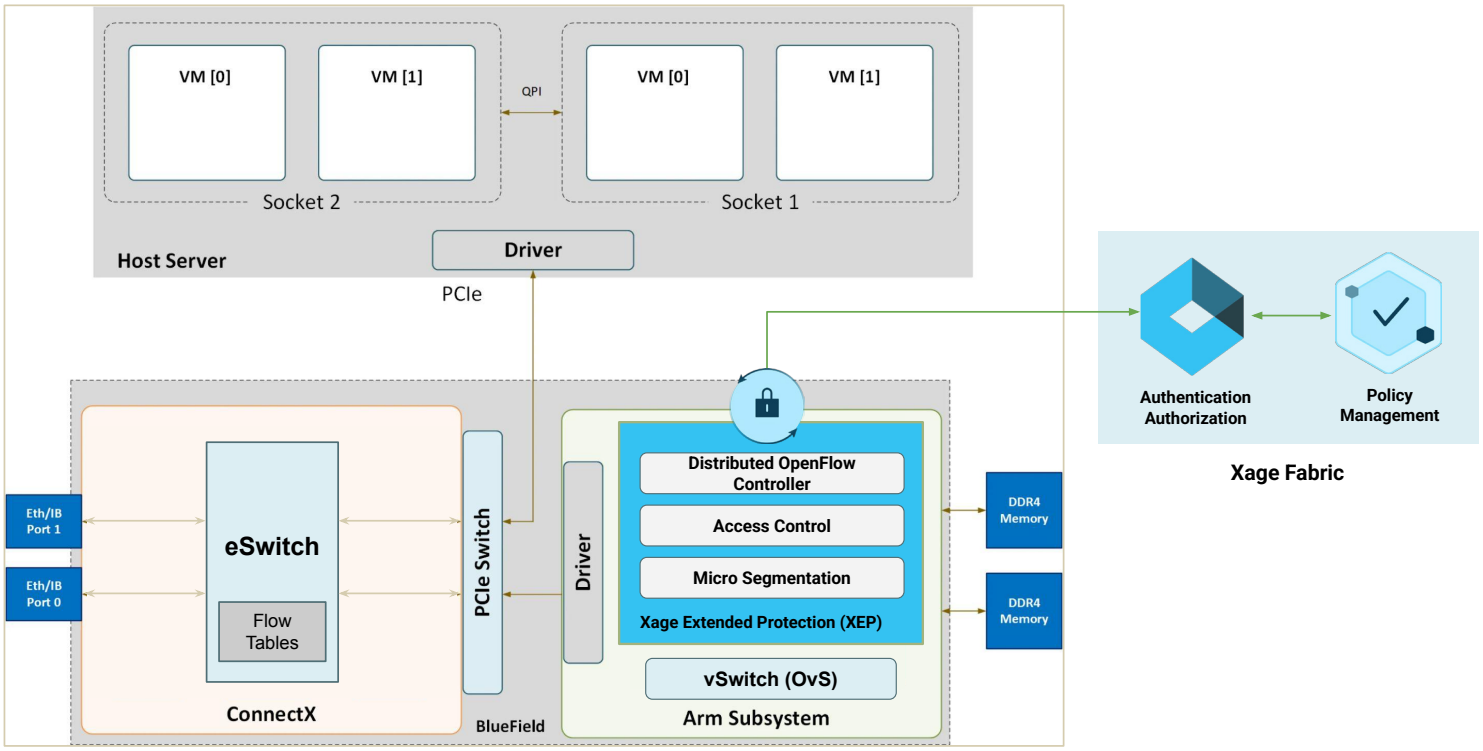
NVIDIA BlueField-3 DPU Hardware Acceleration

- Processes security functions directly on the BlueField processor for low-latency, high-performance operations.
- Provides the foundation for controlling billions of data flows without impacting system performance.

As shown in the architecture overview diagram, XEP software executes natively on the NVIDIA BlueField, operating as a core enforcement and telemetry component within the Xage Fabric architecture. Upon initialization, XEP registers with the Xage Fabric, which then keeps XEP up-to-date with the access control and network segmentation policies required to maintain security. Acting as an OpenFlow controller, Xage programs the Open vSwitch (OvS) instance running on BlueField, ensuring that network and workload isolation rules are dynamically enforced at the virtualization layer.

Inbound and outbound traffic traversing the BlueField passes through OvS, where policy evaluation determines whether the flow (including directionality of the flow) is permitted or denied. Approved flows are offloaded to the embedded eSwitch for line-rate packet forwarding, enabling hardware-accelerated data paths between workloads or network endpoints. Using the policy architecture, admins can configure segmentation between AI workloads, Agents, and models and also identity-based access control between humans, workloads, LLMs, agents, and data.

Architecture Overview: Xage Fabric Integration with NVIDIA BlueField



XEP performs continuous traffic telemetry, capturing communication patterns between all local workloads and external peers. These interactions are exported as event logs to the Xage Fabric for contextual enrichment, visualization, and policy optimization. XEP enforces traffic control at OSI Layer 2, Layer 3 and above.

By utilizing the cryptography offloading capabilities of BlueField, XEP can also enable IPSEC tunneling between the workloads across multiple BlueField running Xage software. All policy changes, user-to-workload access events, and flow control operations are logged for traceability and compliance. Audit logs are compatible with external SIEM and observability platforms through standard export mechanisms such as Syslog or REST APIs, allowing seamless integration into enterprise security monitoring workflows.

Conclusion: Governing Agentic AI and Complex Critical Workloads

The Xage solution represents a breakthrough in securing modern innovation. By combining Xage's Zero Trust Fabric with NVIDIA BlueField acceleration, organizations can achieve accelerated performance, resilience, and security — from AI factories to cyber-physical infrastructure.

Agentic AI systems rely on autonomous agents and LLMs interacting with each other and external APIs, and this complexity introduces new attack vectors such as data leakage between models or tenants, rogue agents taking unauthorized actions, and jailbreaks aimed at bypassing AI guardrails.

Xage and NVIDIA Integration:

- Governs and enforces data flows between agents and models in real time, directly at the BlueField DPU layer.
- Provides role-based segmentation to prevent privilege escalation or risky actions.
- Delivers jailbreak-proof controls that remain effective even as systems self-modify or engage in non-deterministic behavior.
- Maintains performance for large scale, containerized workloads, including multi-tenant, without slowing operations.
- Orchestrates and enforces protection for systems that may have limited native security capability, whether those systems are experimental AI agents or legacy OT components.
- Realtime visibility and interaction data for traceability, regulatory, and compliance.
- Ensures resilience with continuous policy enforcement, even for environments experiencing disrupted or intermittent connectivity.

> ***"As AI factories emerge as the foundational infrastructure accelerating AI innovation, safeguarding them has become a critical priority. Together, NVIDIA BlueField and Xage's zero-trust security enable organizations to modernize their protection strategies across AI factories and infrastructure —driving secure, scalable innovation forward."***
>
> **Ofir Arkin, Sr. Distinguished Architect, Cybersecurity Team at NVIDIA**

About Xage Security

Xage Security is a global leader in Zero Trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere while preventing advanced adversaries and insider threats at every stage of the attack chain. Visit xage.com to learn more.