SOLUTION SHOWCASE

**NVIDIA BlueField-2 DPUs and Guardicore Centra Security Platform enable high-performance, agentless zero-trust security from cloud to core to edge**

## Industry

- Finance
- Banking
- Insurance
- Retail
- Telecommunications

## Challenge

- Traditional network segmentation technologies fail to deliver the necessary protection against east-west attacks
- The ability to deploy security agents for application workloads isn't always possible, rendering network islands vulnerable to security risks

## Products Used

- NVIDIA BlueField-2 data processing units (DPU)
- Guardicore Centra Security Platform

# UNLEASHING THE POWER OF AGENTLESS AND HIGH PERFORMANCE MICRO-SEGMENTATION SECURITY

## Challenges

With the speed at which enterprises are migrating to the cloud, traditional security approaches no longer provide adequate cyber threat protection. Modern security architectures extending from the perimeter are distributed to every host. The question arises as to how organizations can protect computing environments, like bare-metal clouds, high-frequency trading (HFT) and more, especially where deploying security agents is neither feasible nor desirable?

Micro-segmentation is an emerging data center and cloud security best practice that enables fine-grained security policies in data center networks. As a core pillar of the zero-trust security model, micro-segmentation bolsters individual workload isolation and protection, reducing risks, and when combined with the software-defined approach, also simplifies security management. These advantages are essential as a growing number of enterprises adopt hybrid cloud services and new deployment models, such as containers.

Data collection and policy enforcement as key tenets of micro-segmentation, and are achievable through various agent and network-based techniques. Collecting data and enforcing policies on a data-processing unit (DPU) offers a unique value proposition:

- No need to install agents on servers.
- Improves server performance by offloading the security enforcement to the DPU
- Fully isolates segmentation enforcement from the workload.

## Results

- High-performance, agentless and, zero-trust security
- View and map all communications using a single pane of glass
- Manage policies across all environments – legacy, cloud, and more

## Key Use Cases

- Bare-metal clouds
- Containerized workloads
- High-frequency trading
- Mainframe environments
- Network-attached storage

## Key Benefits

- Reduces the data center's attack surface—with zero impact on performance
- Agentless and high-performance, low latency micro-segmentation
- Enables fine-grained data center network security
- Provides visibility into all application workloads
- Enforces in-hardware security
- Streamlines enterprise DevOps automation

**Gartner has described micro-segmentation as being well suited for thwarting "the spread of data center attacks in both on-premises and cloud environments."**

## NVIDIA BlueField-2 DPUs

The NVIDIA® BlueField®-2 data processing unit (DPU) delivers a broad range of accelerated software-defined networking, storage, security, and management services. BlueField-2 offers purpose-built, hardware-acceleration engines with full software programmability by combining the industry-leading NVIDIA ConnectX®-6 Dx network adapter with an array of Arm® cores. Installed on every server, BlueField-2 can handle critical infrastructure, storage, and security tasks, increasing data center efficiency and improving the organization's security posture.

## Why BlueField-2 DPU for Micro-Segmentation?

A BlueField-2 DPU is a computer that runs a fully-functioning operating-system and applications, like any other computer in the data-center. Due to its unique form factor and features, BlueField-2 enables applications to run on its Arm cores, fully isolated from the host's CPU and operating-system. This isolation enables software agents to run on the DPU, making BlueField-2 work best in micro-segmentation solutions.

BlueField-2 also has high-speed network interfaces, which deliver superior performance for a range of network security applications. Deploying BlueField-2 DPUs in the datacenter, specifically those comprising bare-metal and containerized workloads, gives security teams enhanced visibility across cloud domains and enforces a consistent micro-segmentation policy in the enterprise, while offering unmatched performance.

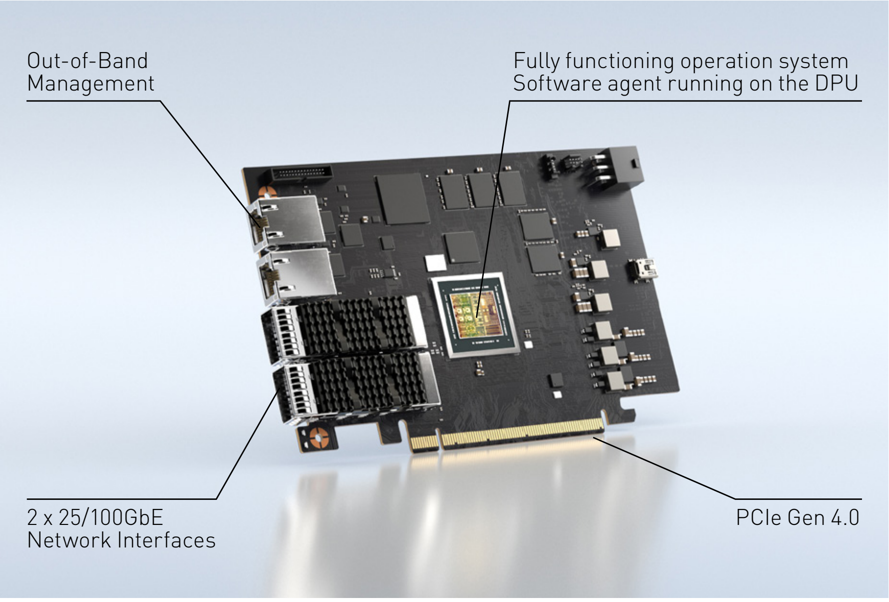

Out-of-Band Management
Fully functioning operation system Software agent running on the DPU
2 x 25/100GbE Network Interfaces
PCIe Gen 4.0

*Figure 1 illustrates an NVIDIA BlueField-2 DPU running a software agent.*

## Guardicore Centra Security Platform

The Guardicore Centra™ Security Platform is a comprehensive data center and cloud security solution that delivers the simplest and most intuitive way to apply micro-segmentation controls to reduce the attack surface and detect and control breaches within east-west traffic.

It provides deep visibility into application dependencies and flows and enforcement of network and individual process-level policies to isolate and segment critical applications and infrastructure. The platform also protects workloads in hybrid cloud environments that span on-premises workloads, legacy systems, VMs, containers and deployments in public cloud IaaS including Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud and others.

Guardicore Centra enables enterprises to successfully deploy micro-segmentation in three easy steps:

- **Reveal:** Guardicore Centra features best-in-class visibility that automatically discovers and visualizes all applications, workloads and communication flows with process-level context. This visualization, coupled with automatic importation of orchestration metadata, enables security teams to easily label and group all assets and applications and streamline policy development.
- **Build:** Centra simplifies micro-segmentation policy development and management A single click on a communication flow generates automated rule suggestions based on historical observations and quickly builds a strong policy. An intuitive workflow and a flexible policy engine support continuous policy refinement and reduce costly errors.
- **Enforce:** With the ability to enforce communication policy at the network and process level on both Windows and Linux systems, Centra maintains security regardless of operating system enforcement limitations. Integrated breach detection and response capabilities enable you to see policy violations in the context of an active breach and identify the method of attack.

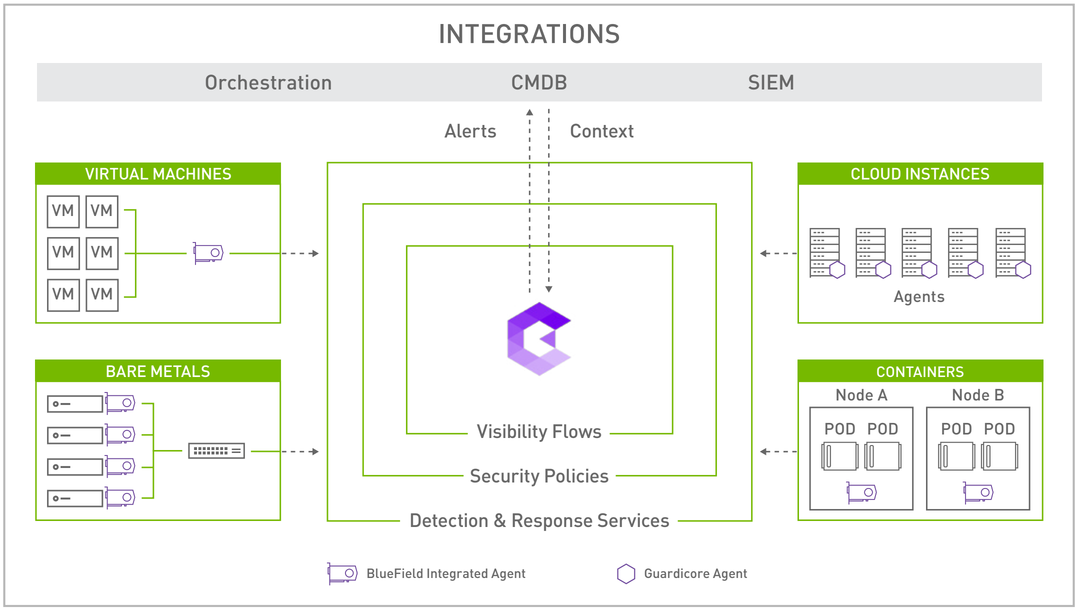
## Guardicore Centra on NVIDIA BlueField-2 DPUs

Guardicore and NVIDIA have partnered to deliver an agentless and high-performance micro-segmentation solution that leverages the advanced Guardicore Centra security platform and BlueField-2 DPUs.

The joint solution addresses the challenges faced by enterprises seeking to gain visibility and to protect application workloads as they deploy and operate agents across their infrastructures. The solution provides the functionality of the software agents on BlueField-2 DPUs rather than installing directly on the computing instances, where deploying agents is not feasible or not desirable. As a BlueField-2 DPU is a fully isolated computer on its own, deploying the agent on BlueField-2 compromises neither the host nor the compliance regulations in any way. Additionally, running the Guardicore agent on the BlueField-2 DPU delivers incredible enforcement performance—allowing/blocking traffic at wire-speed level. It also frees up CPU resources that would otherwise be used for security control and enforcement. The solution gives enterprises the freedom to apply micro-segmentation on every workload in any environment and at any scale, from cloud to core data-center to edge, while catering to the following deployment options:

- Agentless with BlueField-2 DPU—the agent runs on the DPU, fully isolated from the host
- Hybrid—this option includes agents running both on the compute node and on the BlueField-2 DPU
- Native—the agent runs directly on the compute node on the host operating-system or in a guest VM/container, which is the traditional type of deployment for micro-segmentation.

The choice of deployment options varies based on the IT environment, type of workloads, etc., for every enterprise. BlueField-2 is ideal for bare-metal and Kubernetes deployments; running agents on the DPU removes the need to deploy and maintain agents in these environments, enabling enterprise DevOps automation. BlueField-2 also enhances the out-of-box experience for enterprises as they roll-out microservices across their infrastructures, delivering improved agility, resiliency and business continuity.



## Conclusion

Micro-segmentation is a priority for enterprise security teams; it is the most cost-effective way to reduce risk and has been proven to be highly effective in heterogeneous environments. The combined Guardicore Centra and BlueField-2 DPU solution enables enhanced visibility and policy enforcement without applying agents on compute nodes. BlueField-2 provides high-speed networking with unmatched performance that enforces micro-segmentation policies in 100Gb/s networks at-line-speed. Providing the most innovative micro-segmentation solution in the industry, Guardicore and NVIDIA enable ease of deployment and operations in an hybrid cloud environment.

## About Guardicore www.guardicore.com/company

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint.

LEARN MORE

Contact us: **NVIDIA Networking Store**

Learn more: **www.nvidia.com/dpu**