Guardicore and Mellanox Deliver Agentless and High-Performance Micro-Segmentation in Hybrid Cloud

TECHNICAL PARTNERSHIP SOLUTION BRIEF

Unleashing the Full Potential of Micro-Segmentation

Micro-segmentation is an emerging data-center and cloud security best practice that enables fine-grained security policies in data center networks. Providing several advantages over more established approaches like network segmentation and application segmentation, Microsegmentation bolsters individual workload isolation and protection, reducing risks and simplifying security management. These advantages are essential at a time when a growing number of enterprises are adopting cloud services and new deployment options, such as containers.

Data collection and policy enforcement are the most common applications of micro-segmentation, and is achievable through a variety of agent- and network-based techniques. Collecting data and enforcing policies on a SmartNIC offers a unique value proposition:

- No need to install agents on servers. This is of special value when the installation of an agent is either not feasible or not desirable

- No impact on server performance

- Full isolation of segmentation enforcement from workload

Mellanox BlueField® SmartNIC

BlueField is the best SmartNIC solution for addressing performance and cyber-security concerns of the modern data-center. Integrating the world-leading Mellanox ConnectX® network adapter with a set of Arm processors makes BlueField SmartNIC deliver powerful functionality, including bare metal provisioning, stateful L4 firewall and more. Combining hardware acceleration engines with embedded software and fully integrated advanced network capabilities helps turn BlueField into the ideal platform for developing custom security applications.

BlueField enhances data-center security by enabling prevention, detection and responses to potential threats in real time. BlueField's design offers built-in functional isolation that protects each individual workload, and provides flexible control and visibility at the server level, reducing risk and increasing efficiency.

Why BlueField SmartNIC for Micro-Segmentation?

BlueField SmartNIC combines a NIC and CPU integrated onto the same device; in fact, BlueField 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 SmartNIC acts as a "computer-in-front-of-a-computer," enabling applications to run on its CPU, fully isolated from the host's CPU and operating-system. This isolation enables software agents to run on the SmartNIC when they cannot run on the host system, making BlueField work best in micro-segmentation solutions.

BlueField is also a high-speed network adapter, which when coupled with the right software stack, delivers superior performance for a range of network security applications. Deploying BlueField SmartNICs 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. Figure 1 shows an illustration of a BlueField SmartNIC running a software agent.
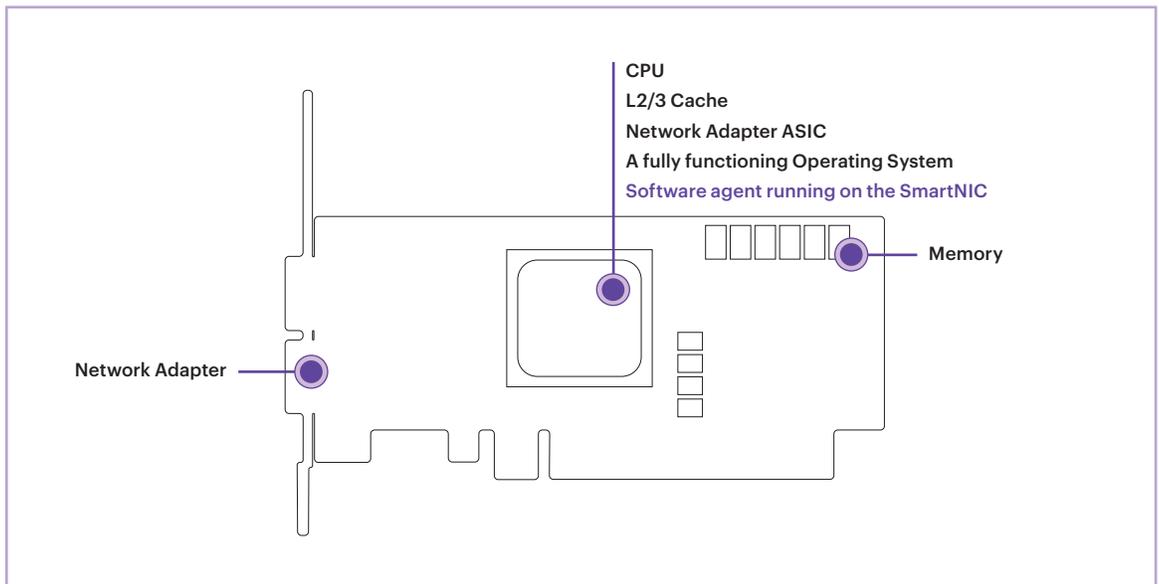

CPU
L2/3 Cache
Network Adapter ASIC
A fully functioning Operating System
Software agent running on the SmartNIC

Memory

Network Adapter

Figure 1: *Illusration of a SmartNIC 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 and Google Cloud Platform.

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 reduces 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 Mellanox BlueField

Guardicore and Mellanox have partnered to deliver the first agentless and high-performant micro-segmentation solution in the industry, which leverages the advanced Guardicore Centra security platform and Mellanox BlueField SmartNIC solutions.

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 runs the software agents on the Mellanox BlueField SmartNIC rather than directly on the computing infrastructure workloads, where deploying agents is not feasible or not desirable. As a BlueField SmartNIC is a computer on its own, deploying the agent on BlueField compromises neither the host nor the compliance regulations in any way. Additionally, running the Guardicore agent on the BlueField high-speed SmartNIC delivers unmatched enforcement performance - allowing/blocking traffic at wire-speed level and without any impact on the server performance.

Guardicore

The solution gives enterprises the freedom to deploy software agents on every workload in any environment and at any scale, including private, public and hybrid cloud instances, while catering to the following deployment options:

- Agentless with BlueField SmartNIC – the agent runs on the SmartNIC, fully isolated from the host

- Hybrid – this option includes agents running both on the compute node and on the BlueField SmartNIC

- 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 microservices.

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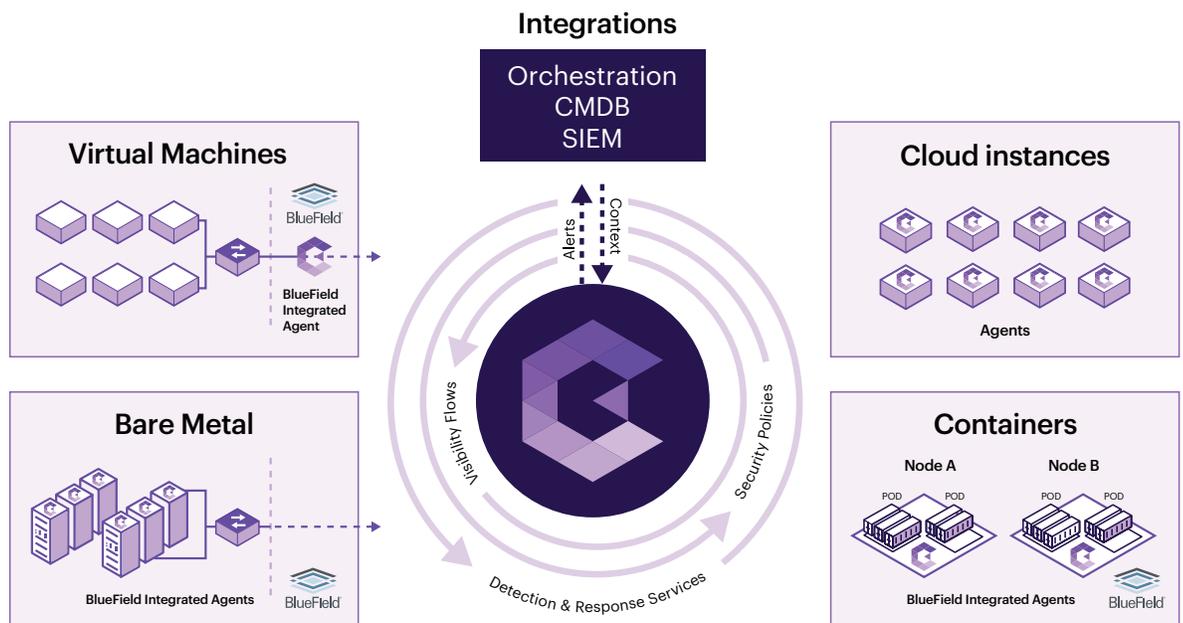

Figure 2: *The Integrated Solution*

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 Mellanox BlueField SmartNIC solution enables enhanced visibility and policy enforcement without applying agents on compute nodes. Agents are integrated into the BlueField SmartNIC in a manner fully isolated from the application workload, while also complying with strict regulations and embracing DevOps automation. As a high-speed network adapter, BlueField delivers unmatched performance that enforces micro-segmentation policies in 100Gb/s networks at full wire speed.

The first agentless and high-performant micro-segmentation solution in the industry, Guardicore and BlueField enable ease of deployment and operations in both new and existing environments.

Guardicore

About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security - for any application, in any IT environment.

www.guardicore.com

Guardicore

About Mellanox Technologies

Mellanox Technologies (NASDAQ: MLNX) is a leading supplier of end-to-end Ethernet and InfiniBand smart interconnect solutions and services for servers and storage. Mellanox interconnect solutions increase data center efficiency by providing the highest throughput and lowest latency, delivering data faster to applications, unlocking system performance and improving data security. Mellanox offers a choice of fast interconnect products: adapters, switches, software and silicon that accelerate application performance and maximize business results for a wide range of markets including cloud and hyperscale, high performance computing, artificial intelligence, enterprise data centers, cyber security, storage, financial services and more. More information is available at: **www.mellanox.com**