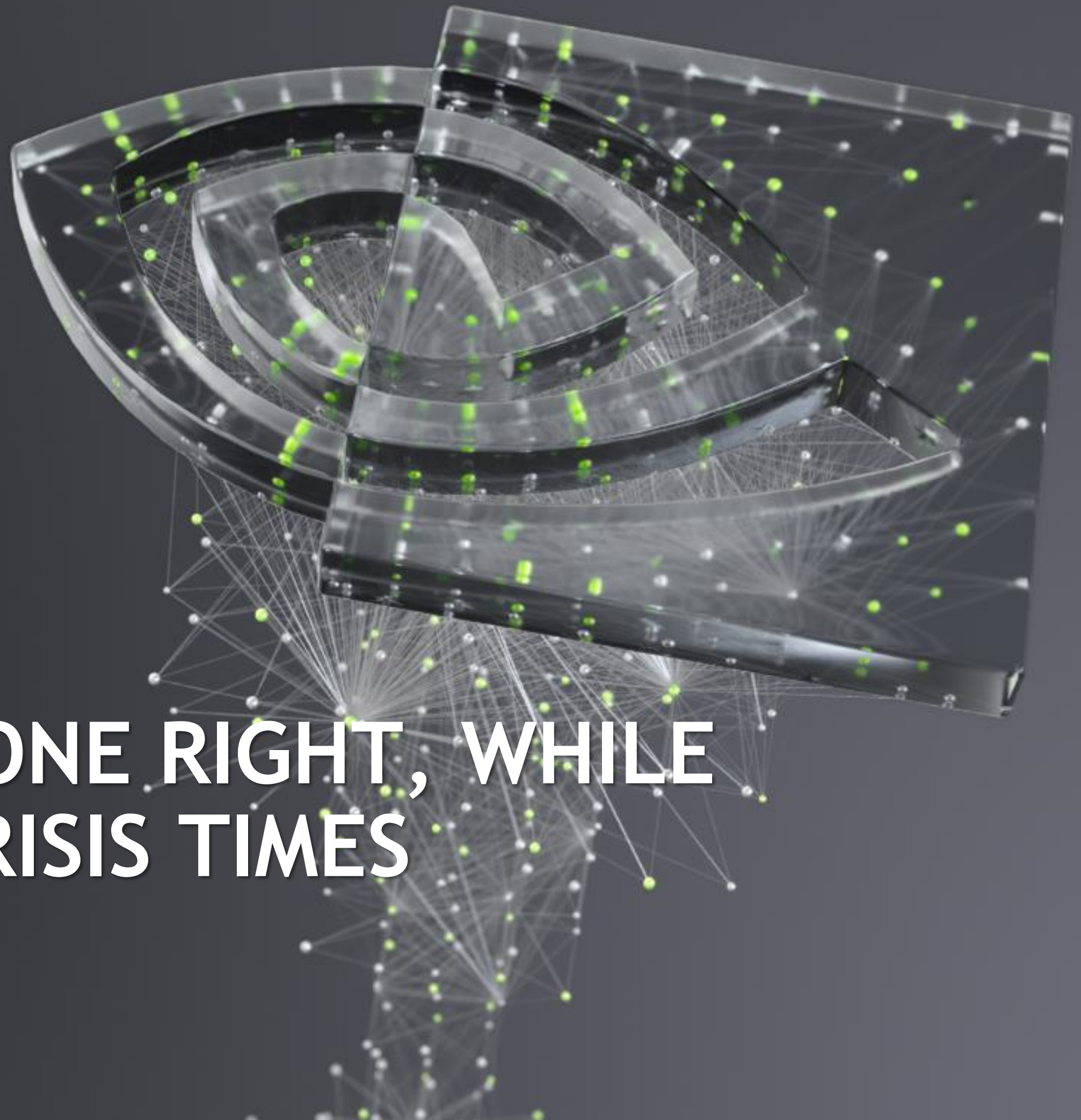




CLOUD SECURITY DONE RIGHT, WHILE TELEWORKING IN CRISIS TIMES

Ariel Levanon, Mellanox VP Cyber Security

June 2020





AGENDA

Nvidia Mellanox Cloud & Edge Cyber Security

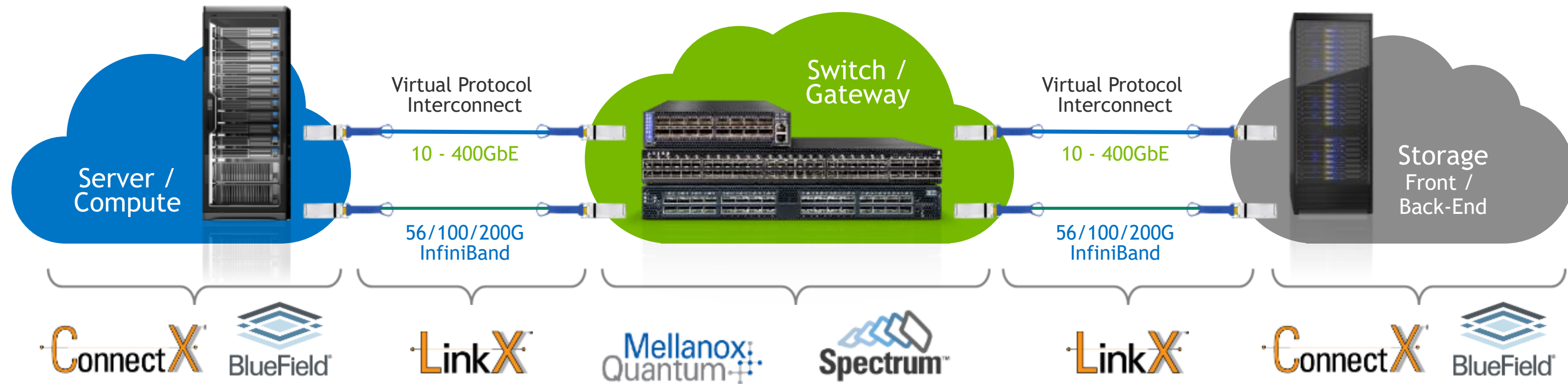
Micro-Segmentation: Best Practice for reducing the attack surface

Enabling Cyber Predictive Analytics with Elastic NVMe

Q&A

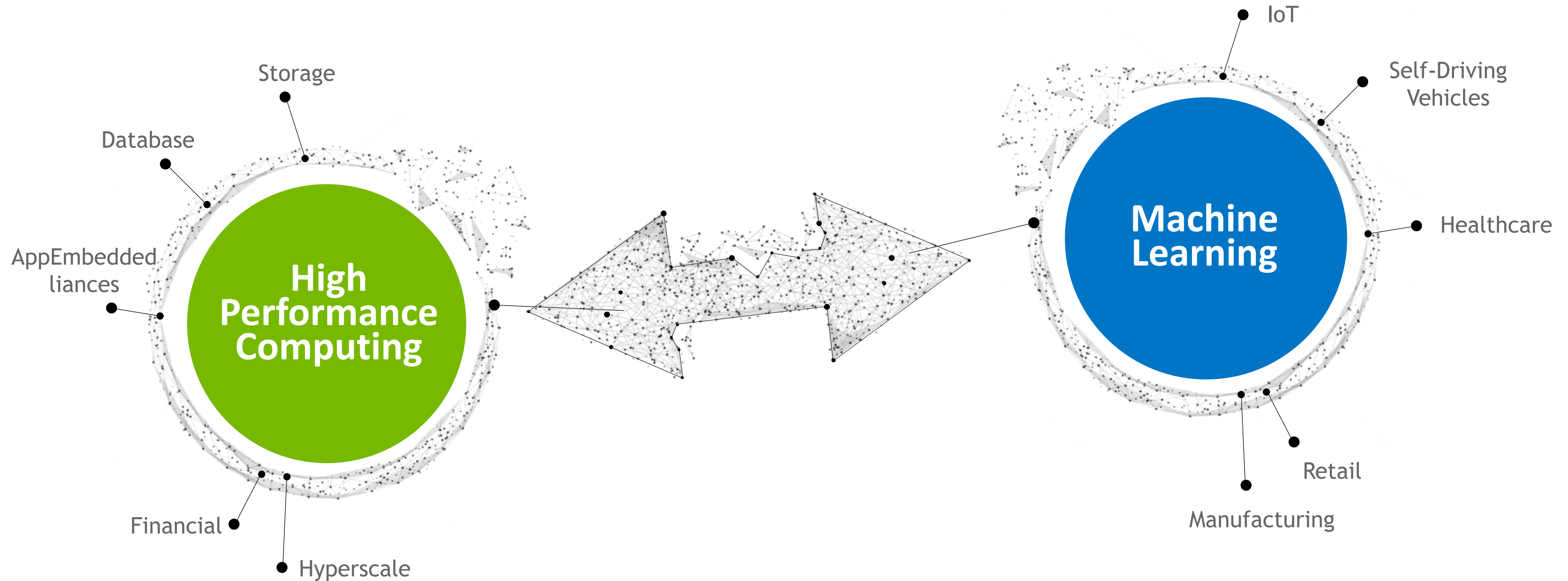
LEADING SUPPLIER OF INFINIBAND AND ETHERNET END-TO-END INTERCONNECT SOLUTIONS

The Smart Choice for Intelligent Compute and Storage Platforms



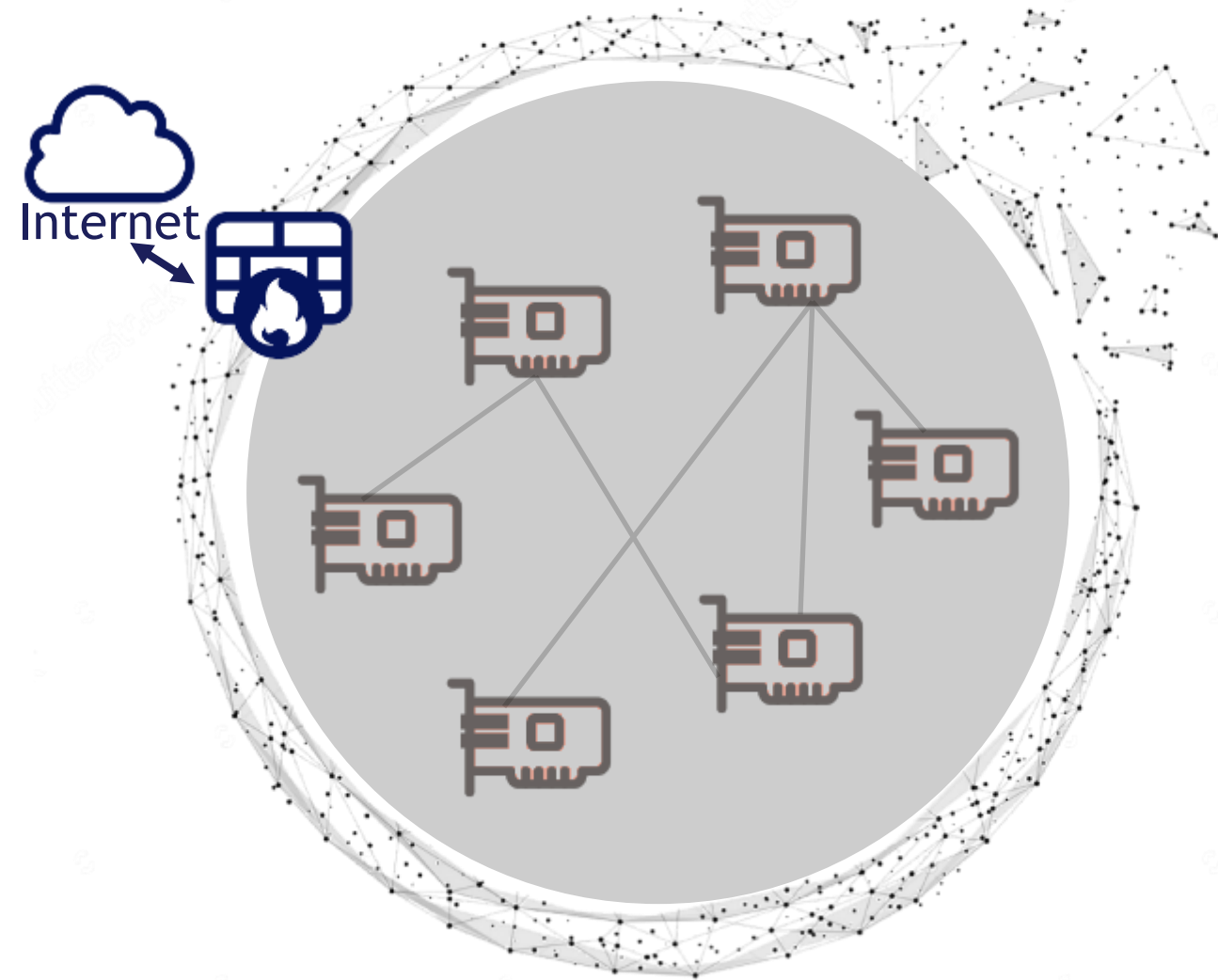
ENABLING THE FUTURE OF MACHINE LEARNING

HPC and Machine Learning Share Same Interconnect Needs



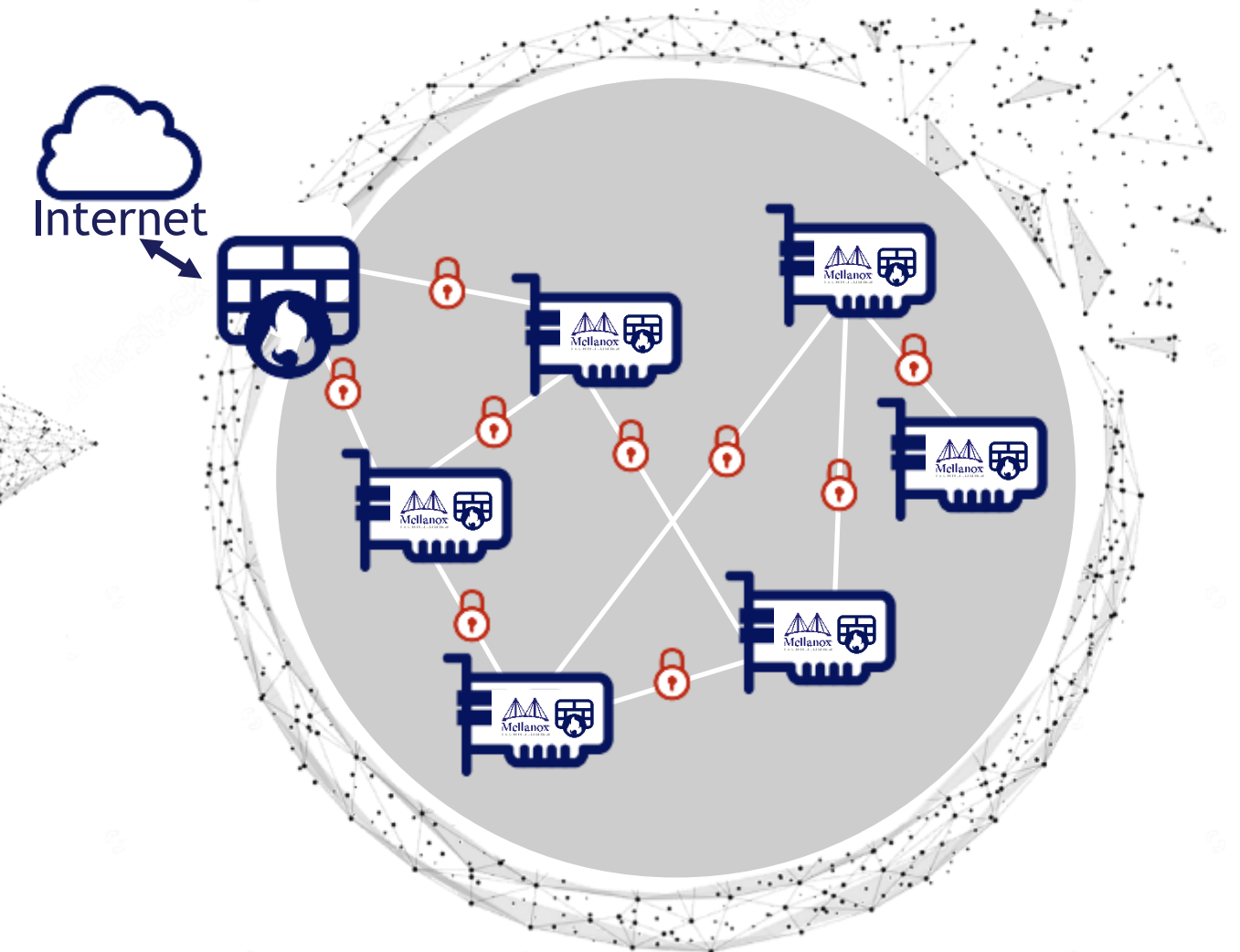
NVIDIA MELLANOX SMARTNICs MAKE THE SECURE CLOUD POSSIBLE

Foundational NICs - Perimeter Security Only



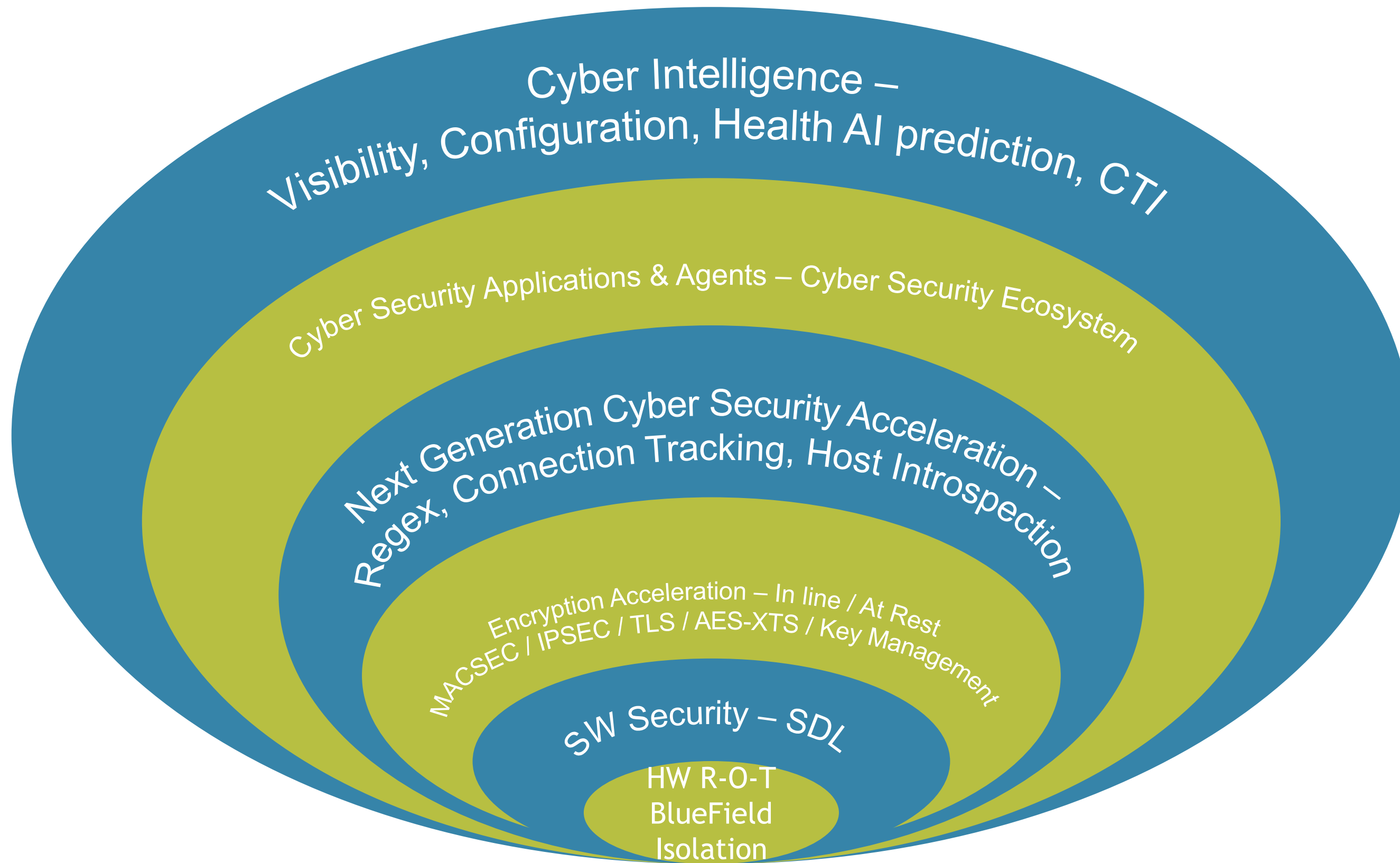
Traditional Security Model

NVIDIA Networking SmartNICs - Secure Cloud



Security Everywhere

NVIDIA MELLANOX CYBER SECURITY SPHERES



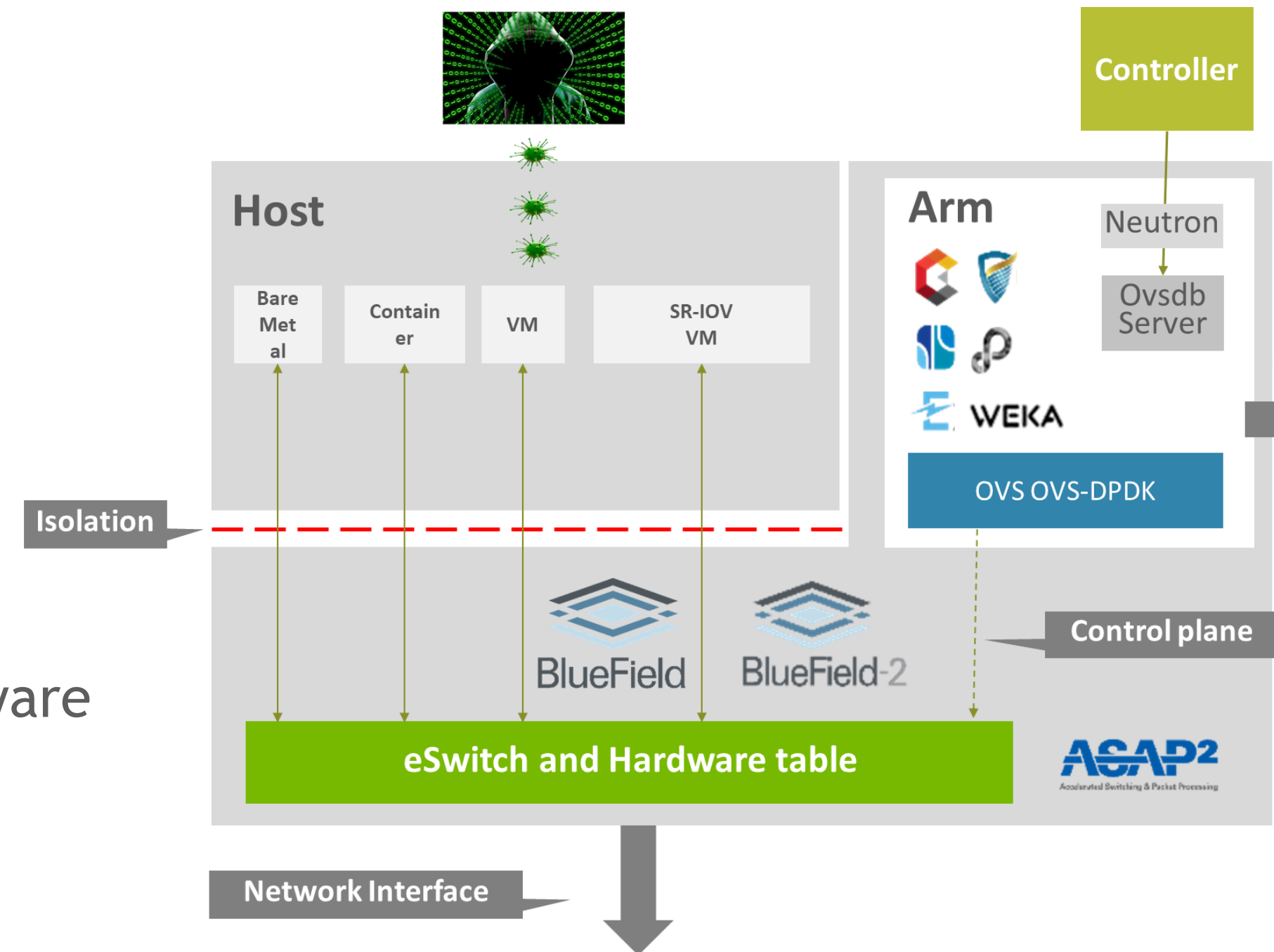
BLUEFIELD FUNCTIONAL ISOLATION

A Computer in front of a computer

Infrastructure functions fully isolated in SmartNIC

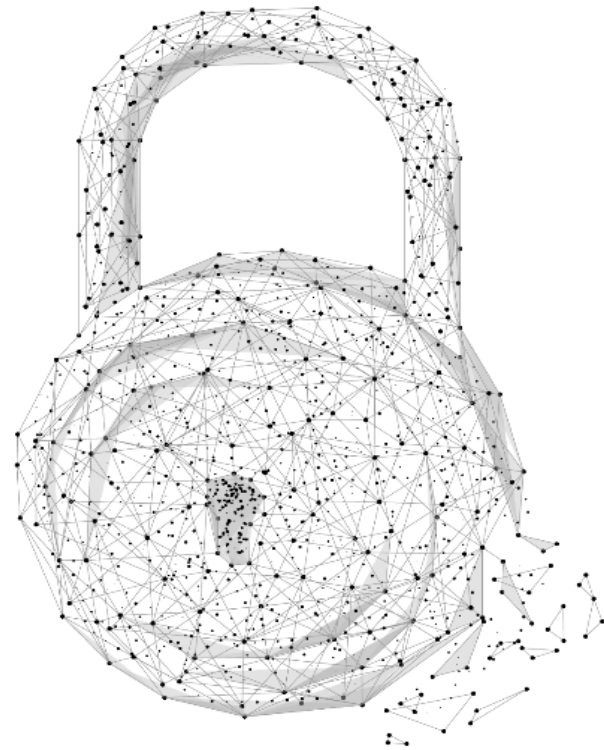
Functionality runs secure in separate trust domain

- Enforces policies on compromised host
- Host access to SmartNIC can be blocked by hardware



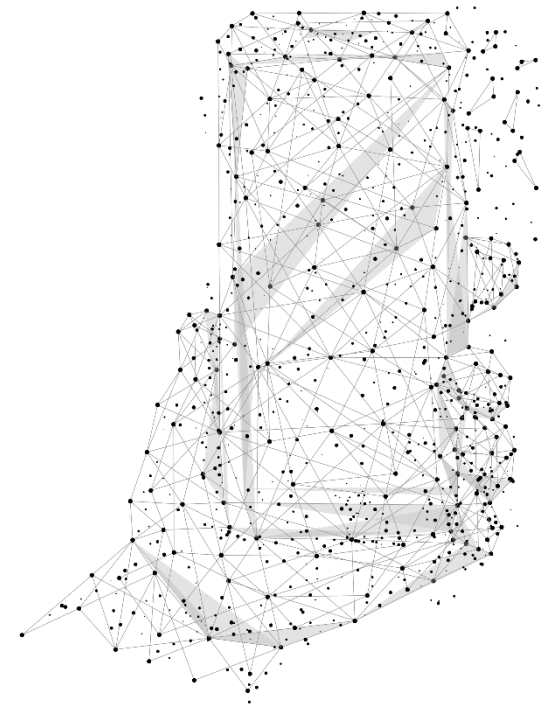
BLUEFIELD DPU SECURITY PACKAGE

Security in All Levels



Secured Hardware (RoT)

- Secure firmware upgrade
- Secure boot
- Arm Trust Zone



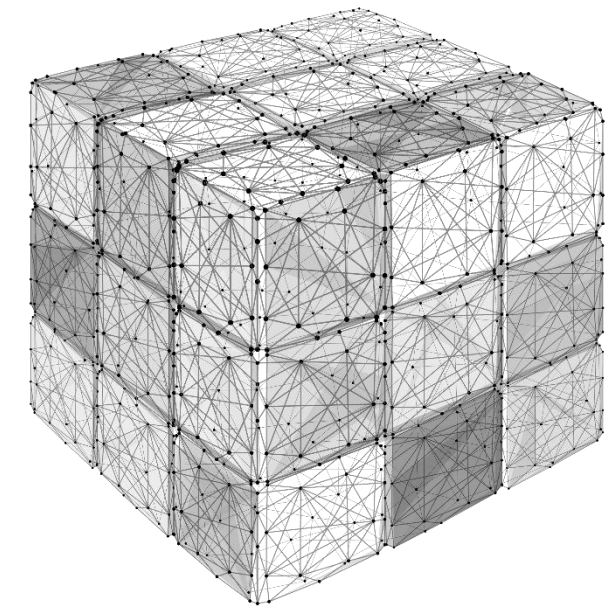
Advanced L4-L7 Security

- NG Stateful firewall
- Deep Packet Inspection
- Host Introspection



Crypto Accelerations

- Inline encryption: IPsec \ TLS
- Storage encryption: AES-XTS
- Hardware public key acceleration



Programmability & Isolation

- Functional isolation
- Security ecosystem
- Ability to run privacy & authentication algorithms

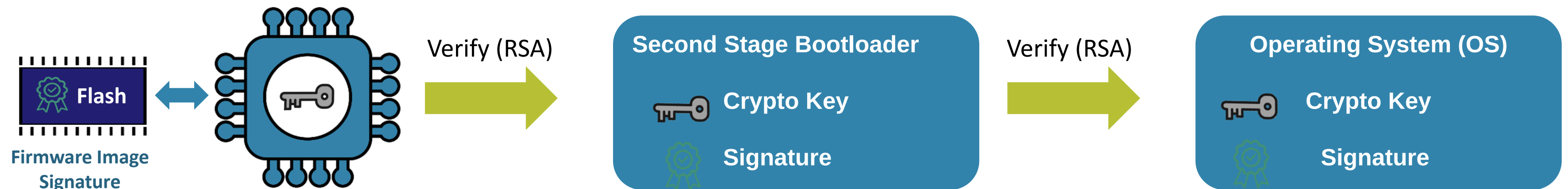
BLUEFIELD-2 HARDWARE ROOT OF TRUST

Protect from supply chain and firmware attacks

Assure the authenticity and integrity of the off-chip storage

Root-of-Trust is an on-chip ROM code and OTP (One Time Programmable)

- RSA based with SHA2-512 (of 4K public keys) burned in EFUSE (2 keys for NIC and Arm subsystem in BlueField-2)
- Follows NIST spec SP 800-147 “BIOS Protection Guidelines”
- Hardware roll-back protection information is included in the device-specific digest calculation



BLUEFIELD-2 INLINE ENCRYPTION- IPSEC/TLS

Lower CPU utilization with significant higher performance

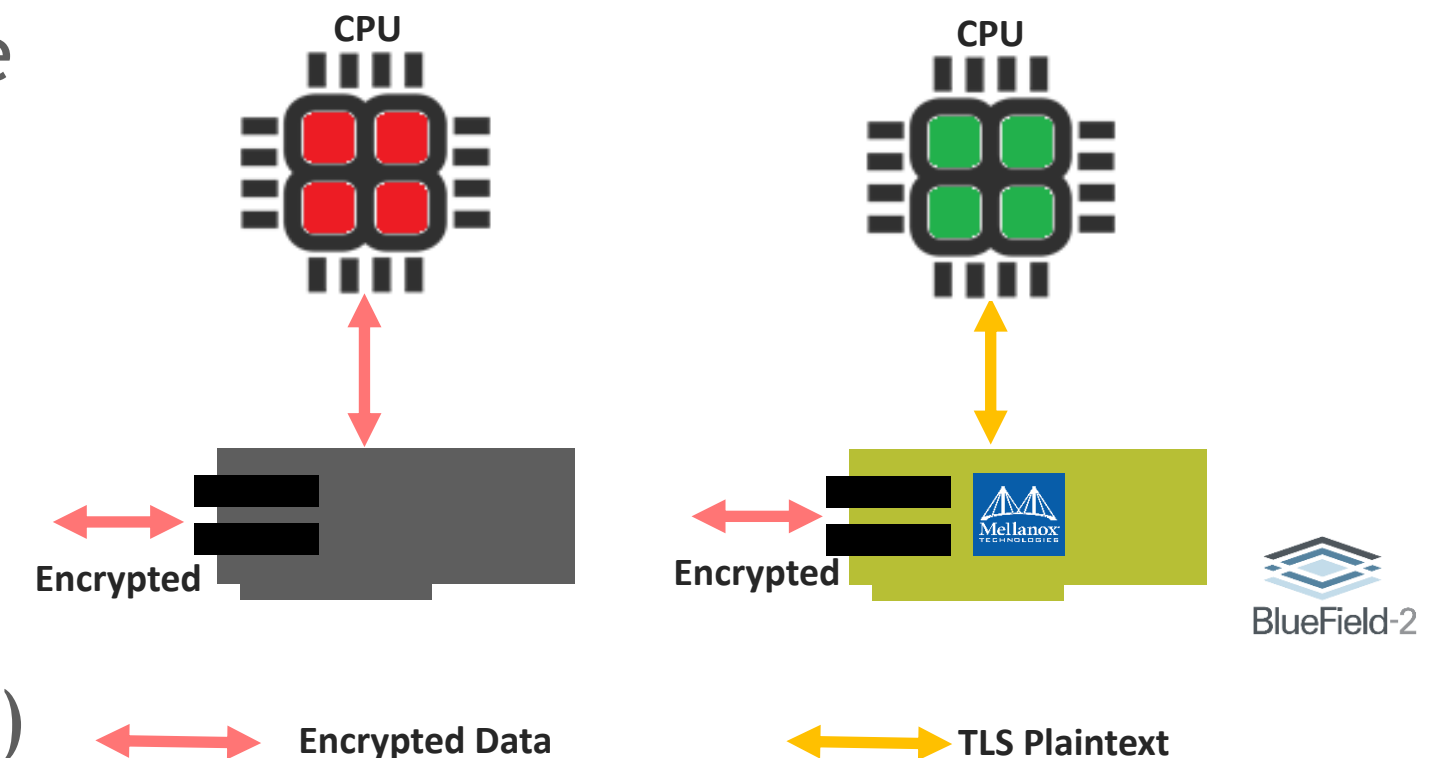
- Encryption/decryption at 100G (IPsec) or 200G (TLS)

Inline offload at the Application level

- Removes software overhead of invoking accelerator
- Inline with other offloads (tunneling, IPsec, SR-IOV etc.)
- Independent of Host interference

Cipher: AES-GCM 128/256bit keys

Supports TLS1.2 and TLS1.3



BLUEFIELD-2 IPSEC INLINE ENCRYPTION - DATA-IN-MOTION

IPSec encapsulation and data plane offloads (aware/un-aware modes)

Lower CPU utilization with significant higher performance

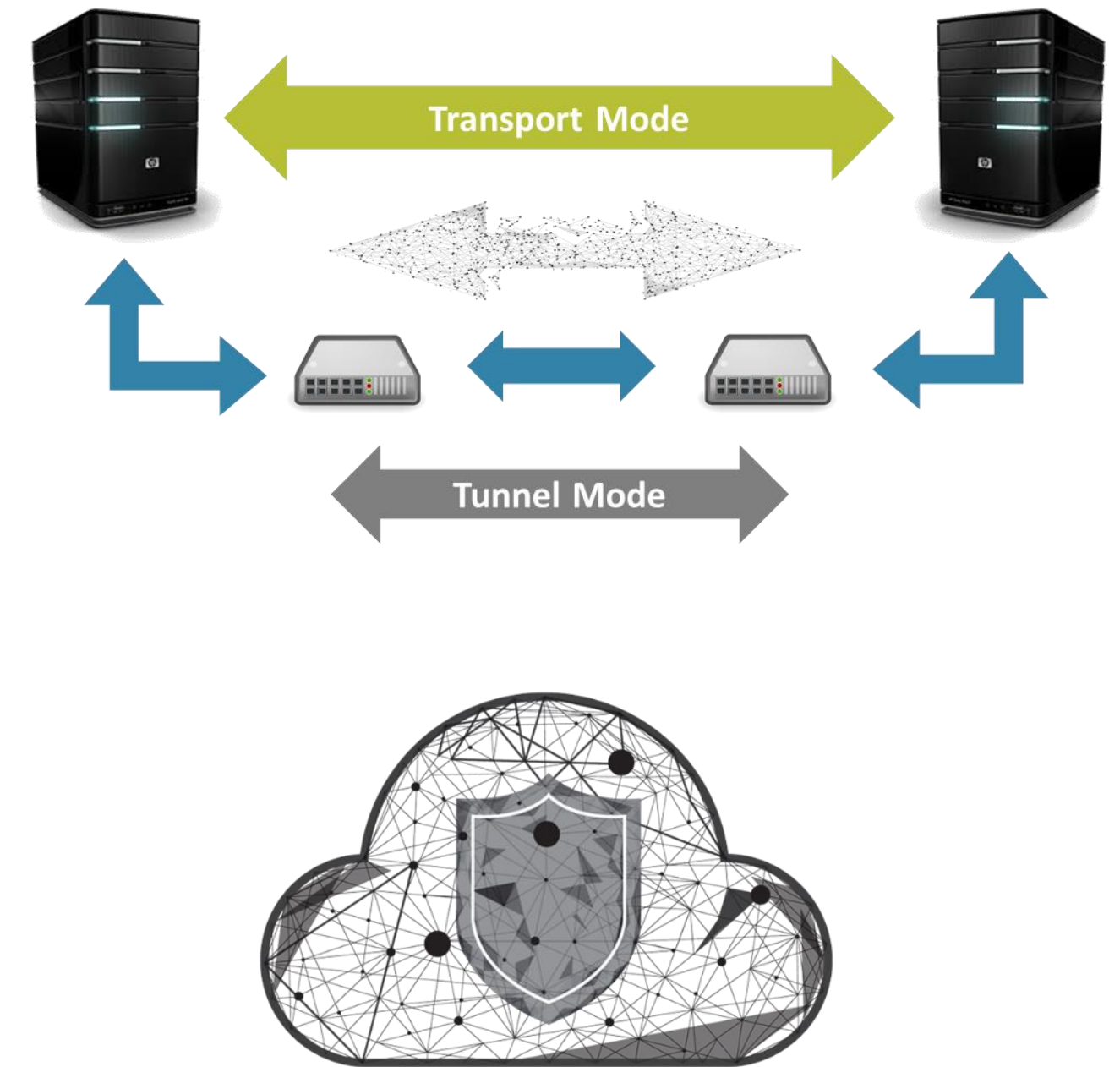
Inline offload with other offloads (tunneling, TLS, OVS, SR-IOV etc.)

IPsec key management in software

Supports Transport mode and Tunnel mode

Use-cases

- East-west data center encryption
- Transparent IPsec (BlueField-2 and Hypervisor)
- Encrypted bare metal cloud (BlueField-2)

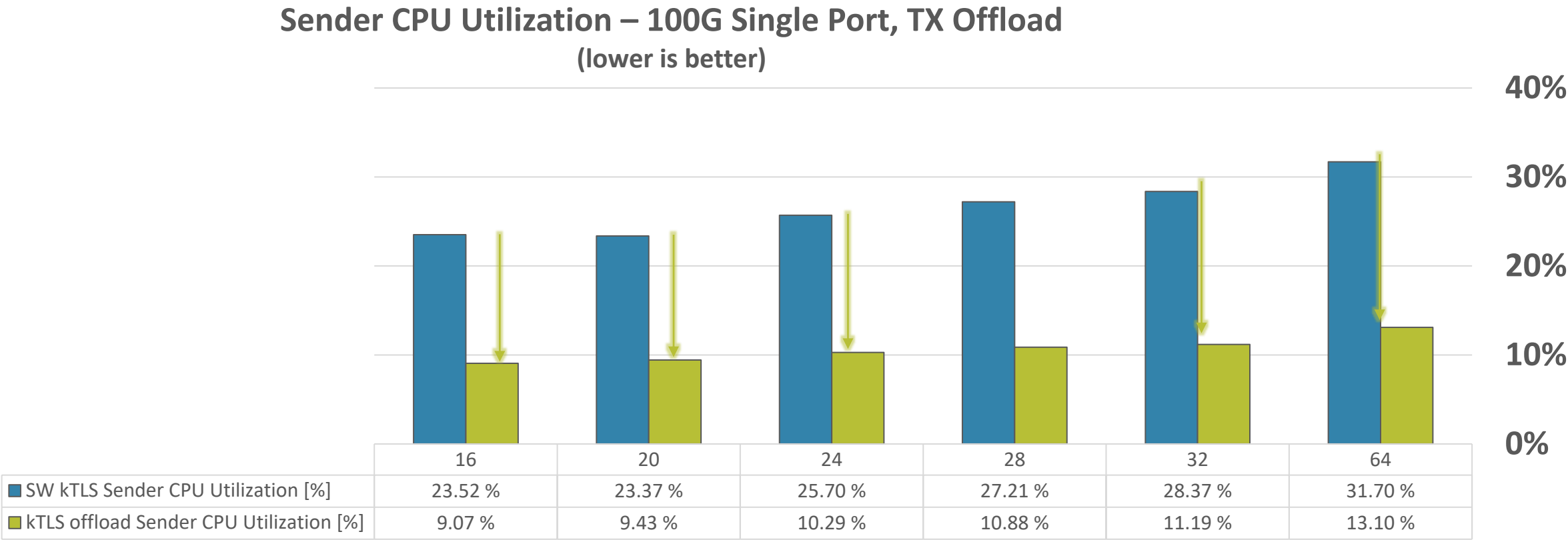


BLUEFIELD-2 KTLS OFFLOAD PERFORMANCE

Up to 66% Improvement in CPU Utilization with transmit offload

Offload recovers and improves TLS’s CPU overhead

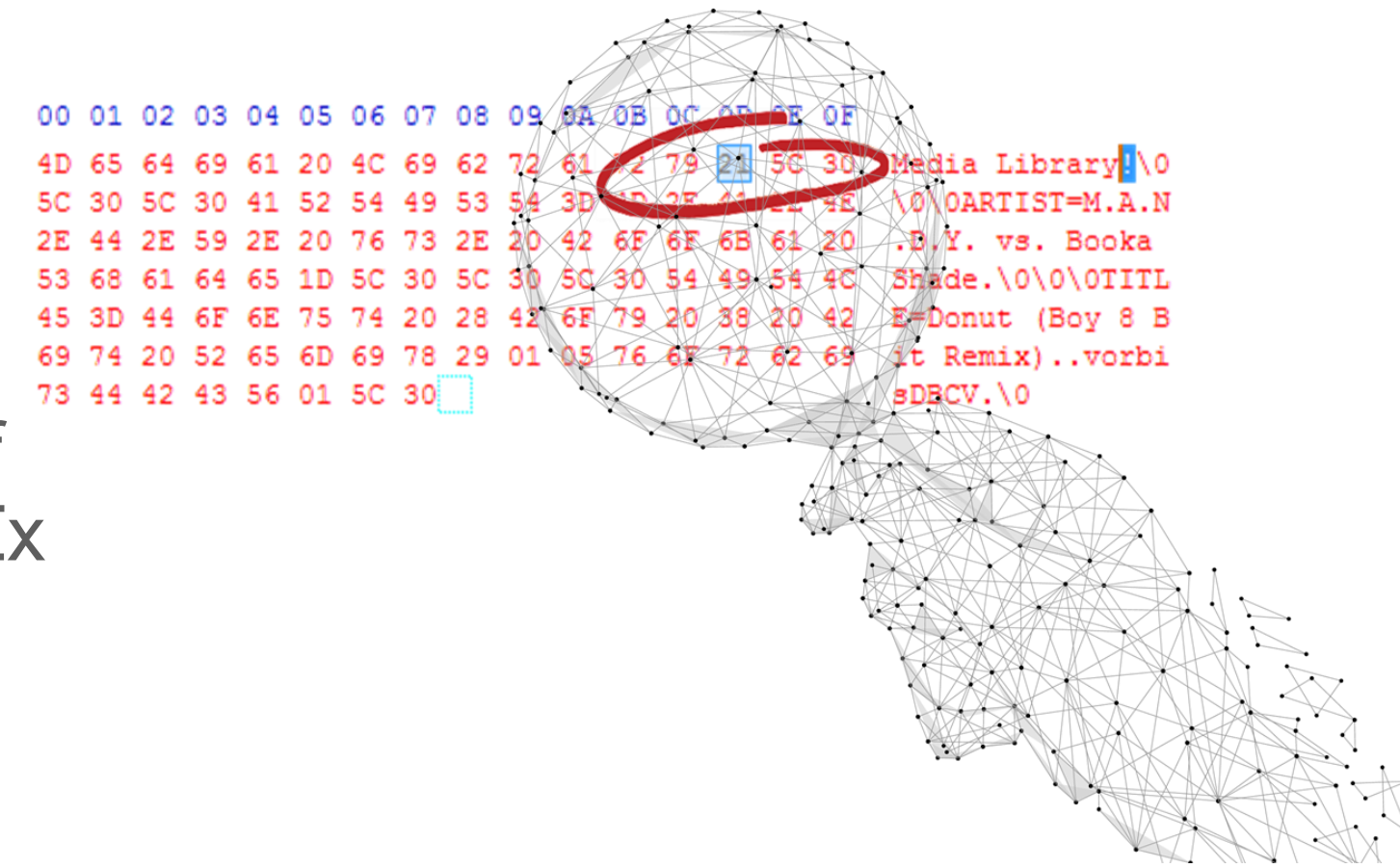
Significant CPU Savings - more than 3 Xeon E5 cores can be saved



BLUEFIELD-2 REGULAR EXPRESSION ACCELERATION

RXP SECURITY ACCELERATION

- ▶ Enables search & analysis of IP traffic for detection of malicious or unwanted content at high speed
- ▶ Searches data for threats and patterns, defined by sets of rules and signatures based on Regular Expressions or RegEx
- ▶ Uses either:
 - ▶ pre-defined signature database rulesets
 - ▶ or user-defined rules and signatures



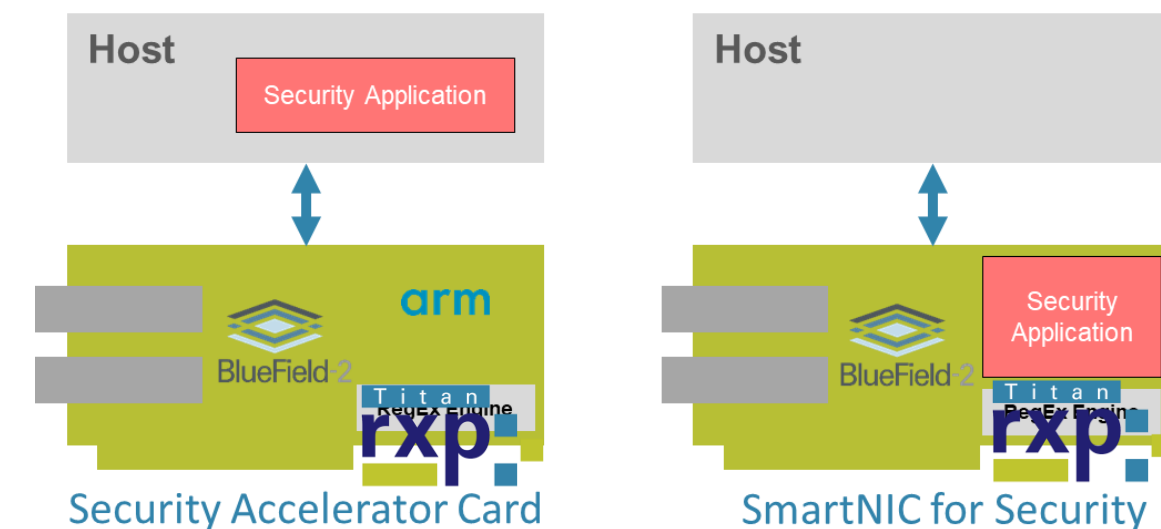
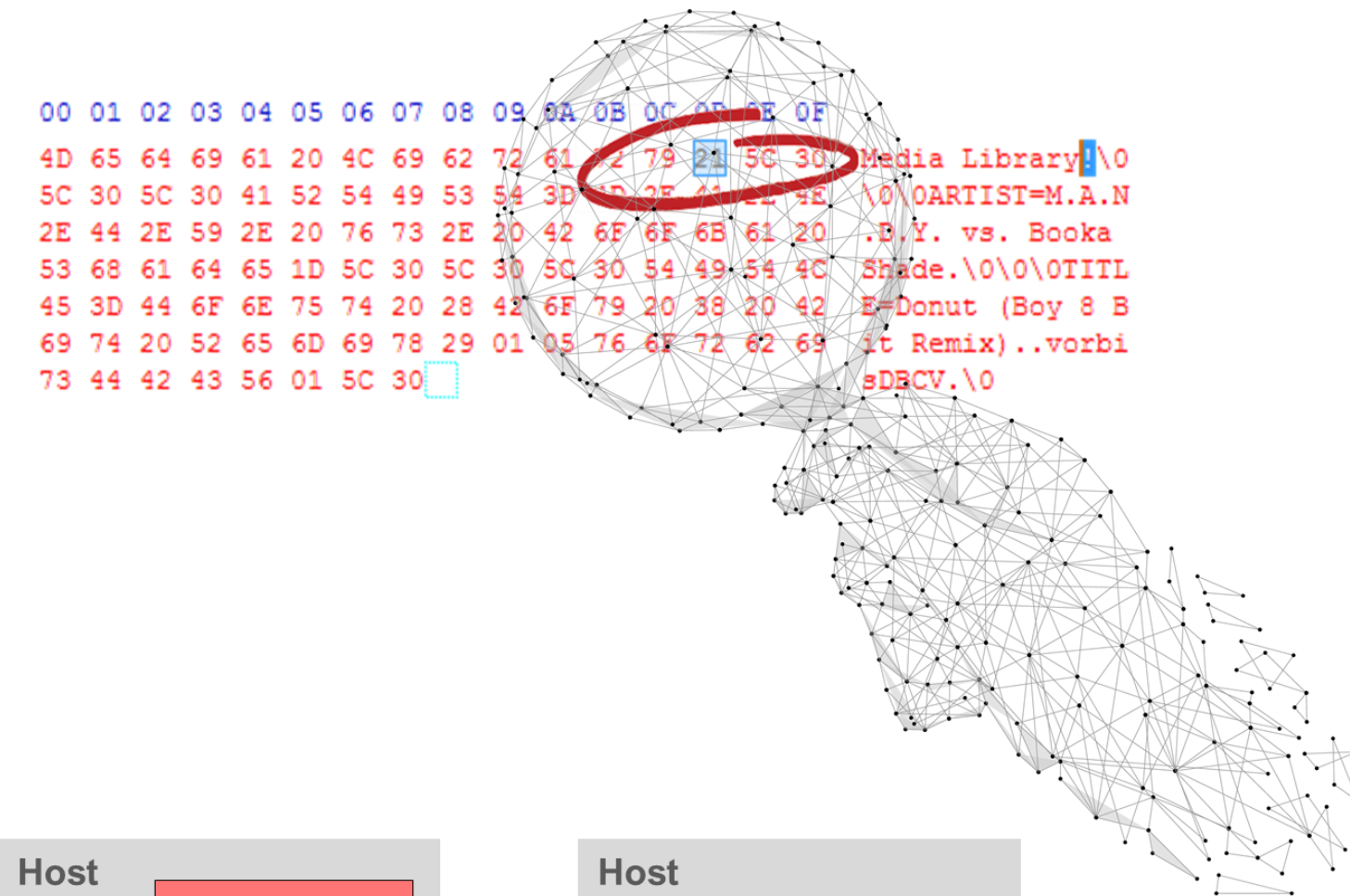
BLUEFIELD-2 REGULAR EXPRESSION ACCELERATION

Analyze network flows, memory, files

- ▶ Detect malicious content
- ▶ Deep Packet Inspection (DPI)

Regular Expression (Regex) processing is widely used by

- Next generation Firewalls (NGFW)
- Network based Application Recognition
- Cyber security applications
- IDS/IPS tools (Snort, Suricata)
- Host Introspection
- Security Information and Event Management (SIEM)



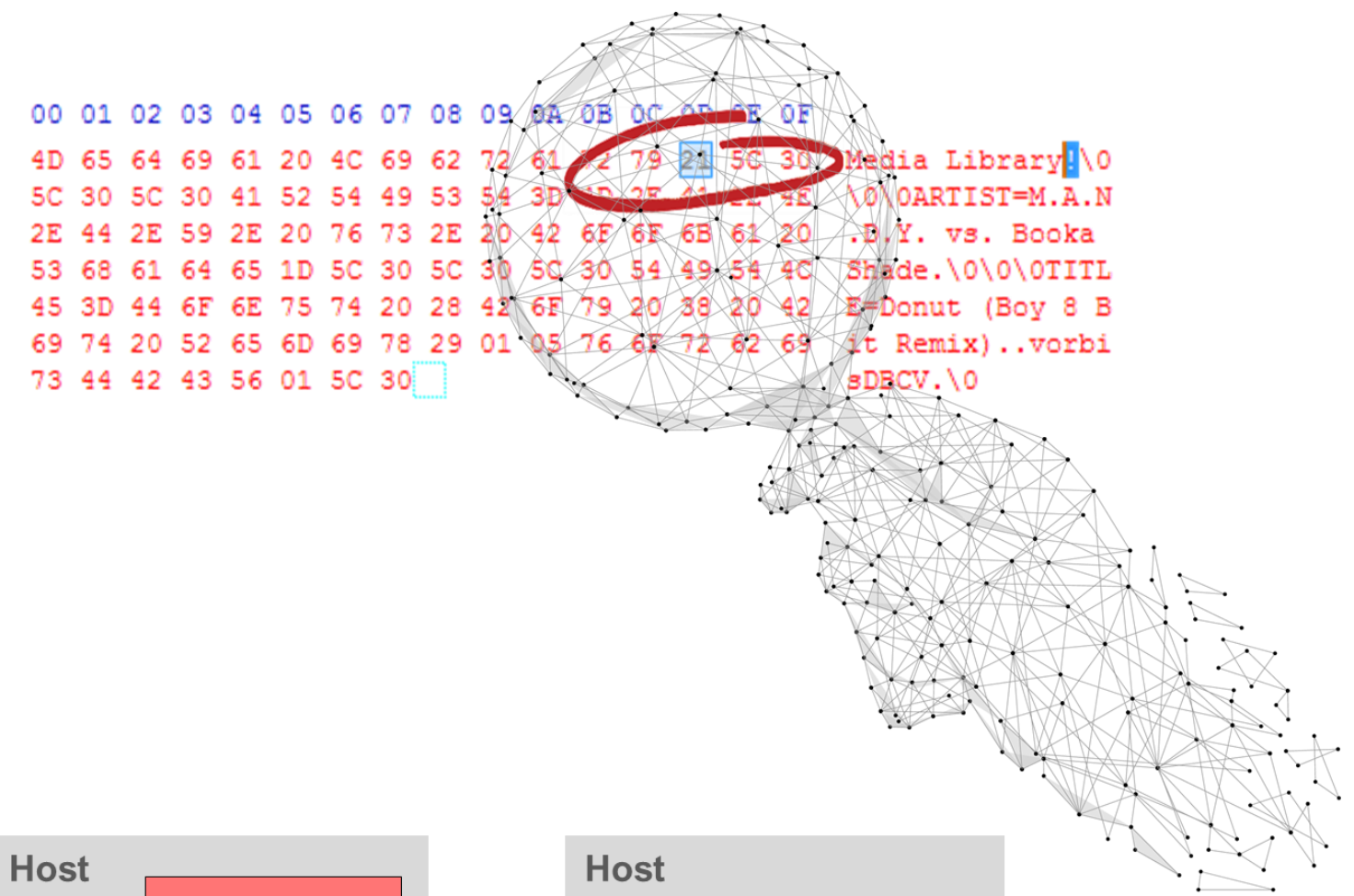
BLUEFIELD-2 REGULAR EXPRESSION ACCELERATION

BlueField-2 50Gbs RegEx engine enables

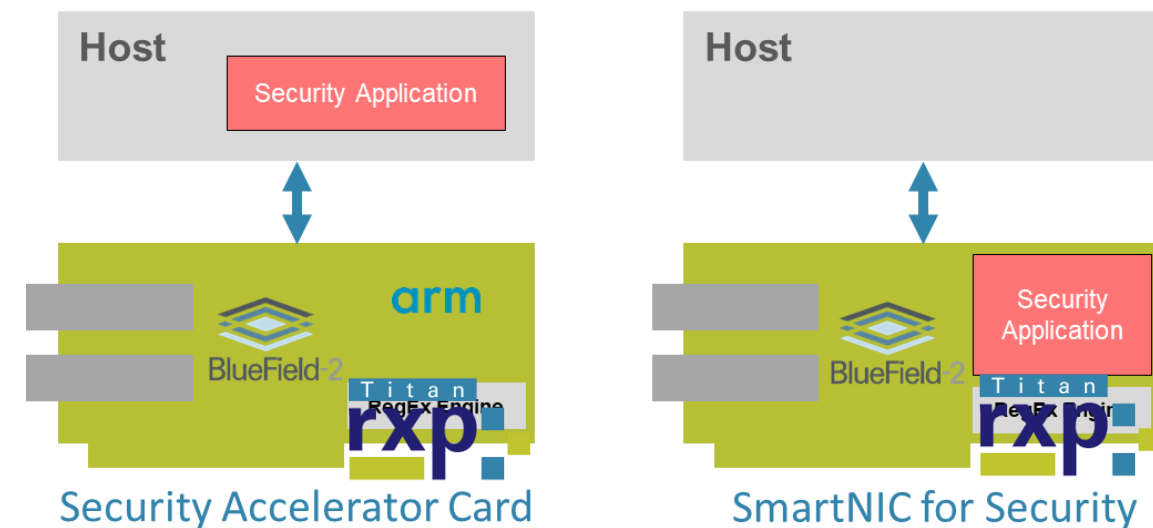
- Application recognition at real time
- Situation awareness (Network)
- Log parsing and analysis
- Anomaly detection

Modes of Operation

- Accelerator card for security applications
- SmartNIC for endpoint security
- Security appliance (bump-in-wire)



```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
4D 65 64 69 61 20 4C 69 62 72 61 22 79 21 5C 30 Media Library\0
5C 30 5C 30 41 52 54 49 53 54 3D 4D 2F 41 2E 4E \0\0ARTIST=M.A.N
2E 44 2E 59 2E 20 76 73 2E 20 42 6F 6F 6B 61 20 .E.Y. vs. Booka
53 68 61 64 65 1D 5C 30 5C 30 5C 30 54 49 54 4C Shade.\0\0\0ITIL
45 3D 44 6F 6E 75 74 20 28 42 6F 79 20 38 20 42 E=Donut (Boy 8 B
69 74 20 52 65 6D 69 78 29 01 05 76 6F 72 62 69 it Remix)..vorbi
73 44 42 43 56 01 5C 30 sDCV.\0
```



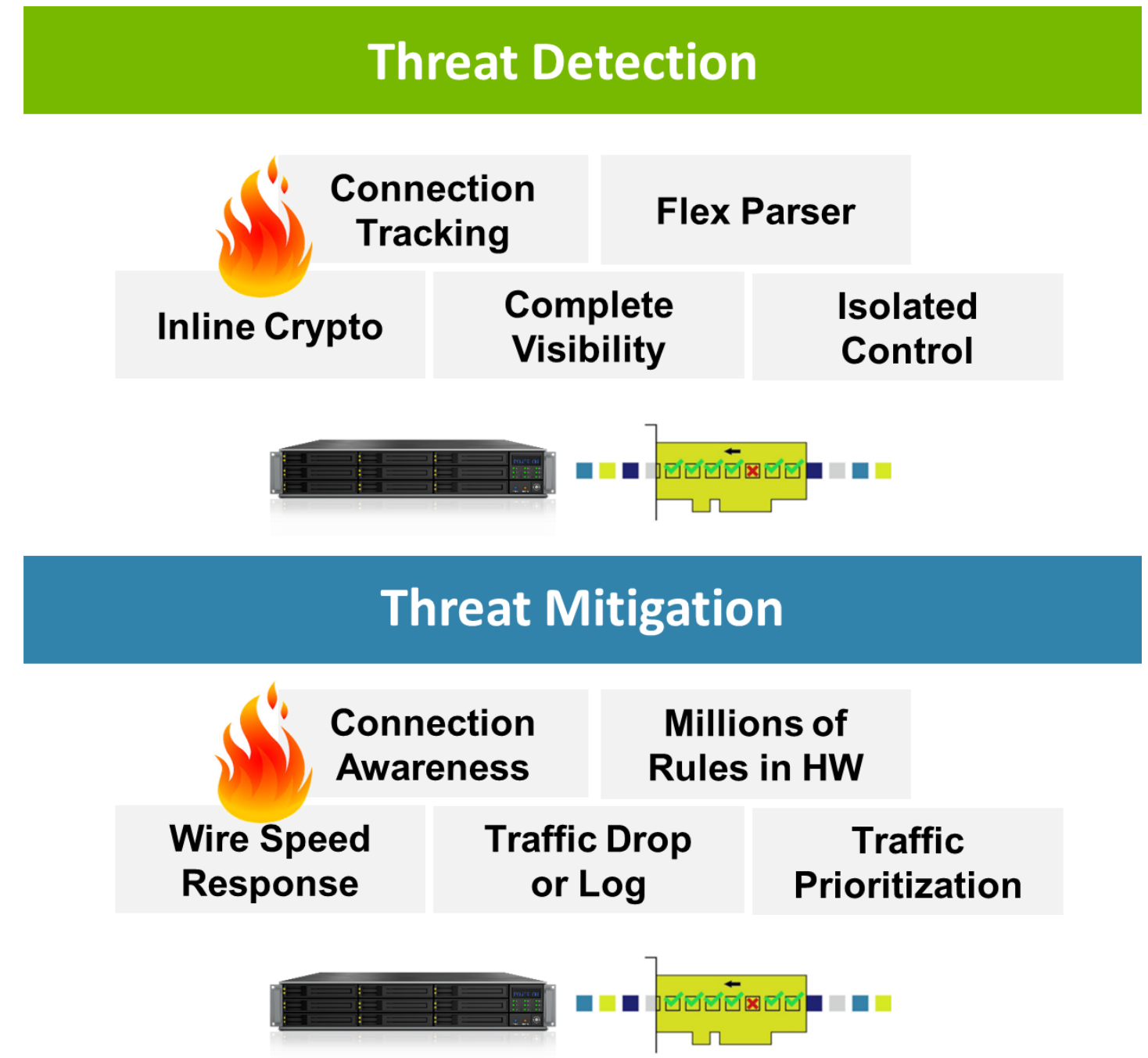
BLUEFIELD-2 NG STATEFUL FIREWALL

Static Firewall rules at wire speed programmed using OVS

Accelerated through Connection Tracking

Mellanox ASAP² enables seamless offload of filtering and steering

Next-generation Firewall agents can run on Arm cores



USE CASES - ECOSYSTEM OPPORTUNITY



Cyber Security



NGFW/DDoS/WAF/M-S



IDS / IPS



Visibility & Analytics



Encryption / Key Mgmt.

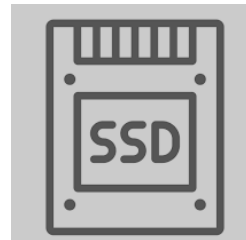
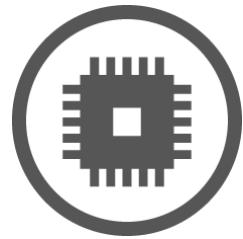
SPECTRUM 3 - SHIELDING BACKDOORS

Software



Standards

Hardware



HARDWARE

Secured boot, root-of-trust capable CPU and TPM provide the ability to authenticate the SW (Boot, BIOS, NOS)

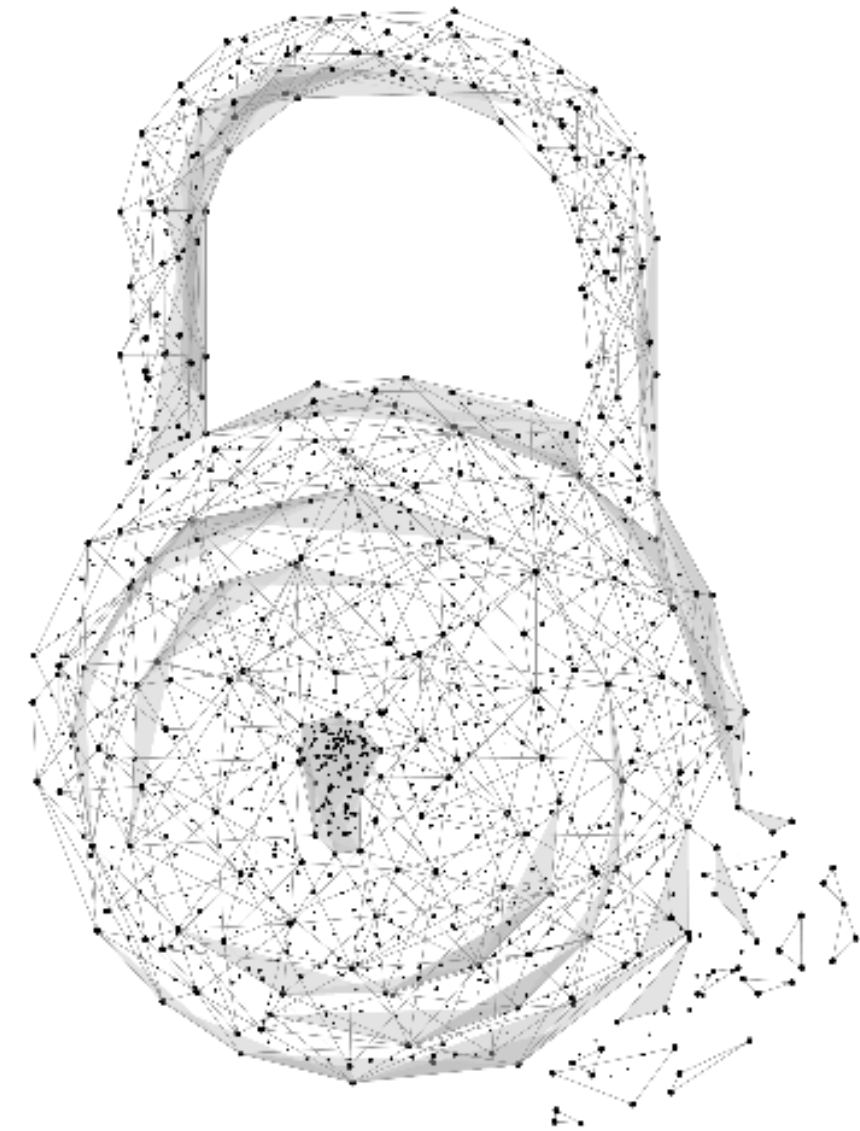
Secured CPLD permits only authorized and signed logic to run on top of the programmable component

Secured JTAG and burning buses

Secured Storage, encryption of the stored information in the switch (Filesystem, images, configuration, logged data)

MACSec(*)

(*) Roadmap



SECURED NOS

Maximum security for the SW and FW

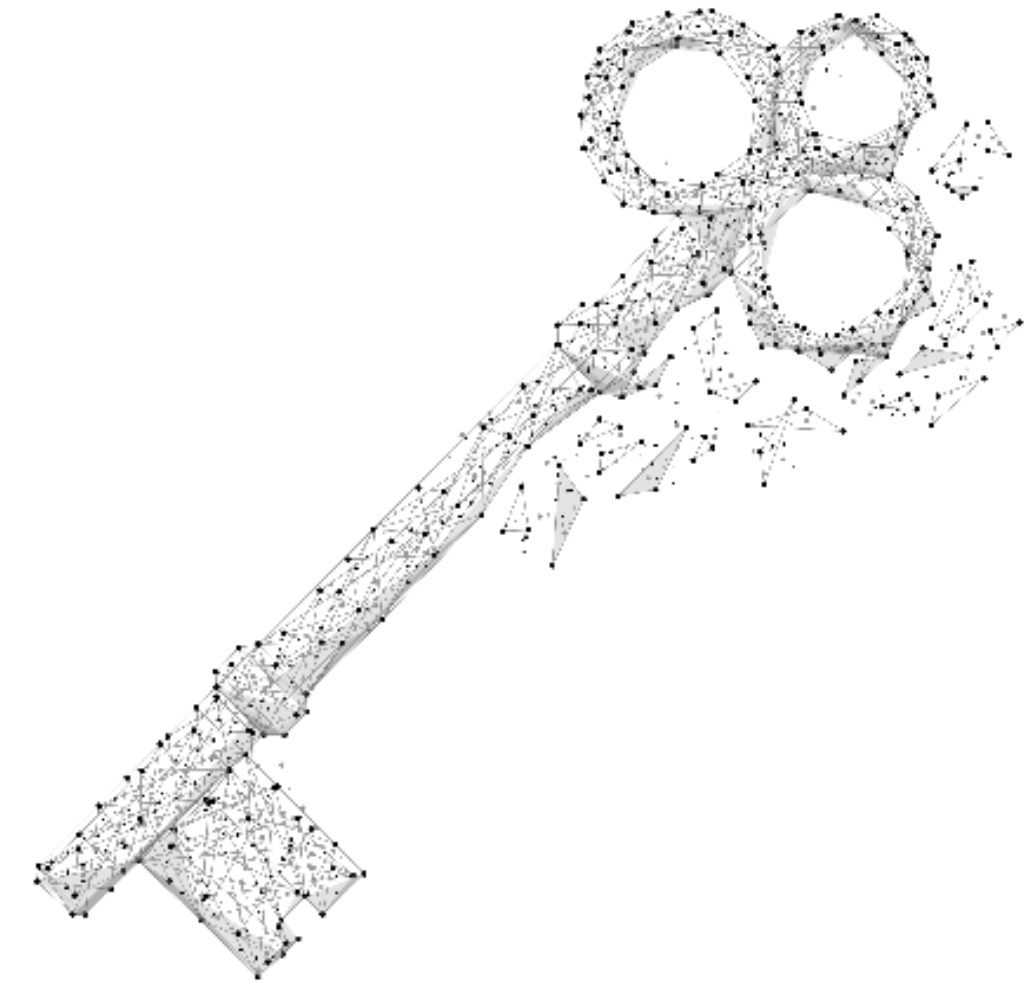
The pre-signed NOS image is using cyphered keys burnt into the switch for authentication

Based on root-of-trust, each component authenticates the next

In case of failure in the authentication chain, the switch deemed unusable

Planned for support in Onyx, SONiC, Cumulus and DENT

On-going NOS threat Analysis and regular updates



SECURED ETHERNET SWITCHES PORTFOLIO

Edge Router



SN3930R: 30x100G

Spine Switches



SN3700-C: 32x100G



SN3700-V: 32x200G

Super Spine Switches



SN4700: 32x400G



SN4600-V: 64x200G



SN4600-C: 64x100G



SN4800: 128x100G



PureLinkX product line for Secured Cables and Transceivers

- 800GbE and InfiniBand NDR



Supported security features

- Authentication: electronically identifies cable hardware is Mellanox genuine
- Secured Firmware Update: blocks installation of malicious firmware
- Secured boot: post reset hardware authenticates firmware image

Implementation

- Upgrade hardware and firmware to support security features
- Optics: Add u-Controller and an Authentication & Brand Protection Secure solution
- Copper: add a mini u-Controller to support security features



REVOLUTIONIZING SUPERCOMPUTING

InfiniBand Data Center Cyber Intelligence and Analytics Powered by Artificial Intelligence

Scalable supercomputers host many application users and variety of research and simulations jobs

Based on ITIC 2020 global server hardware survey*, 88% of firms say hourly downtime costs exceed \$300k

Users may leverage data center access to run prohibited applications, resulting in increase of operation costs and misused of compute resources

The new NVIDIA Mellanox UFM Cyber-AI platform combines enhanced and real-time network telemetry with AI-powered cyber Intelligence and analytics, to discover operations anomalies and predict network failures for preventive maintenance

*<https://www.ibm.com/downloads/cas/DV0XZV6R>

“Supercomputers Hacked Across Europe to Mine Cryptocurrency”

ZDNet
May 2020

“Cost of Hourly Downtime Increases: 88% of Firms Say Hourly Downtime Costs Exceed \$300k”

ITIC, Information Technology Intelligence Consulting
March/April 2020



UFM PLATFORMS OPTIMIZE SUPERCOMPUTING OPEX

InfiniBand Data Center Cyber Intelligence and Analytics Powered by Artificial Intelligence

Build a rich database with real-time network telemetry information, workload usage, system configuration and more

Provide enhanced network monitoring and management, workload optimizations and periodical configuration checks

Learn the system's normal operation, condition, and usage

Detect overtime performance degradations or change in conditions

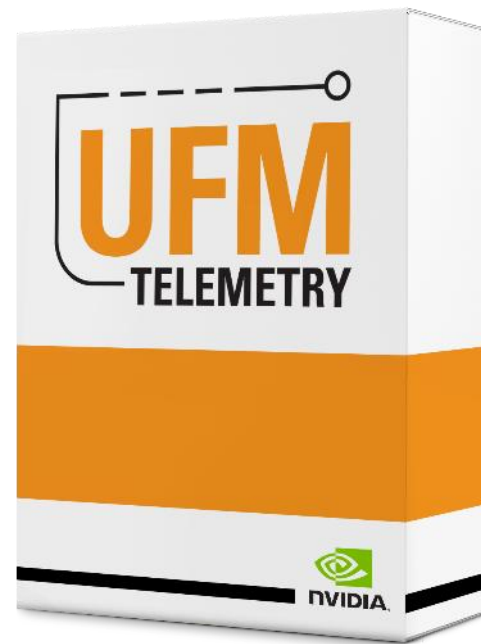
Provide predictive analytics, alerts of abnormal system and application behavior, and potential system failures

System administrators can quickly detect and respond to potential security threats, and address future failures more efficiently, saving OPEX and maintaining end-user SLAs

Predictability is optimized over time as system data is collected



UFM PLATFORMS PORTFOLIO



UFM Telemetry
Real-Time Monitoring



UFM Enterprise
Management, Monitoring & Orchestration
(UFM Enterprise includes UFM Telemetry)



UFM Cyber-AI
Cyber Intelligence and Analytics
(UFM Cyber-AI includes UFM Enterprise)

UFM CYBER-AI PLATFORM

Cyber Intelligence and Analytics

Includes all UFM Enterprise services

Learns system heartbeat, operation mode, condition, usage, workload network signatures

Builds enhanced databased of telemetry information and discovers correlations

Detects performance degradations, usage and profile changes over time

Provides alerts of abnormal system and application behavior, and potential system failures

System administrators can quickly detect and respond to potential security threats

System administrators can efficiently plan and address future failures

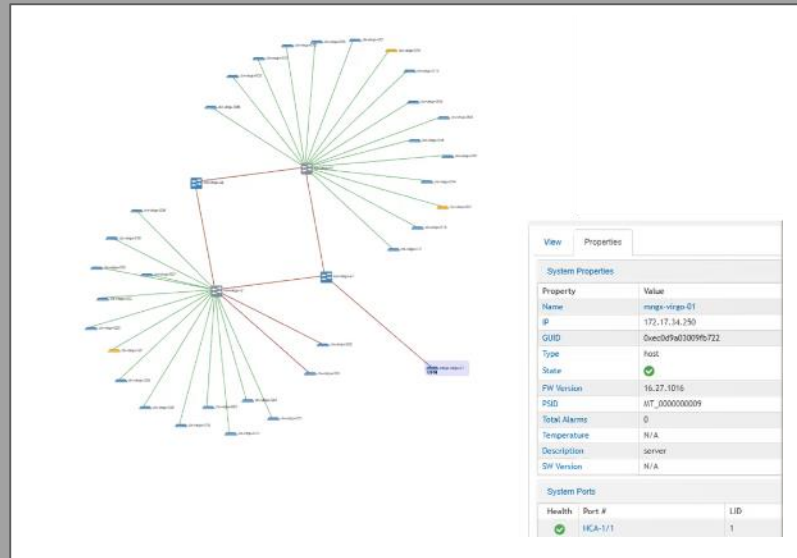
Predictability is optimized over time as system data is collected

Performs corrective actions

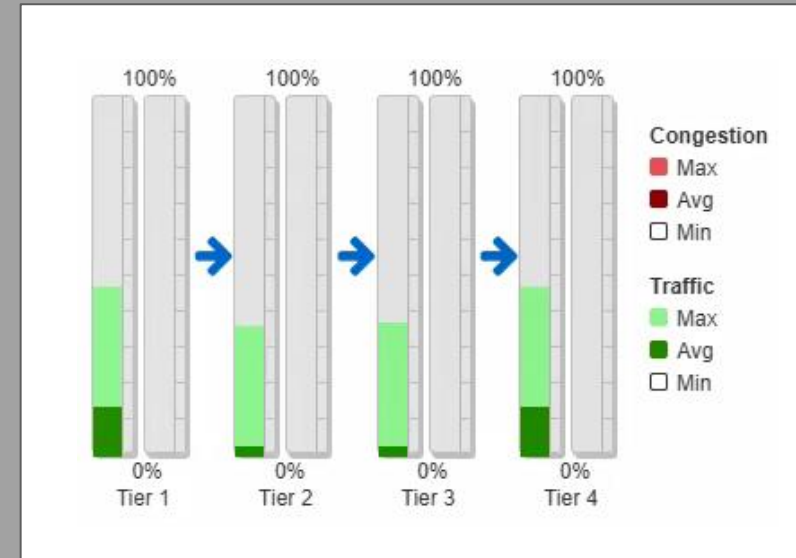
Platform: UFM Cyber-AI appliance



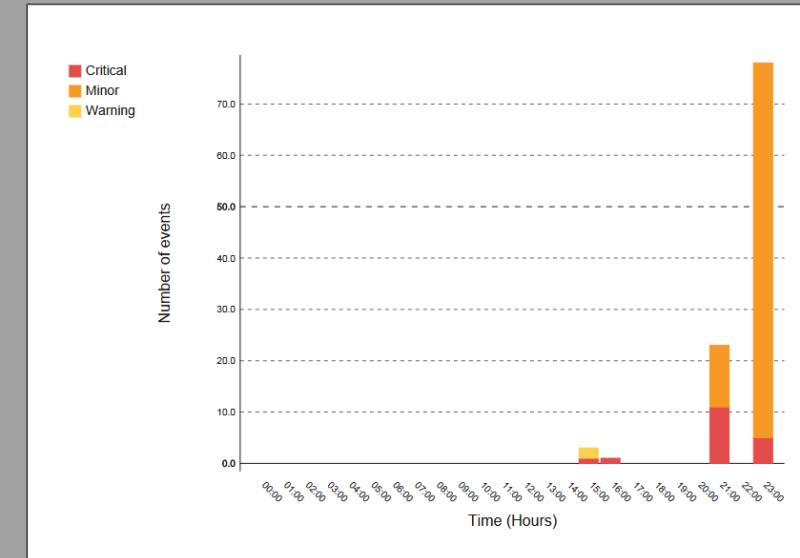
UFM CYBER-AI DASHBOARD



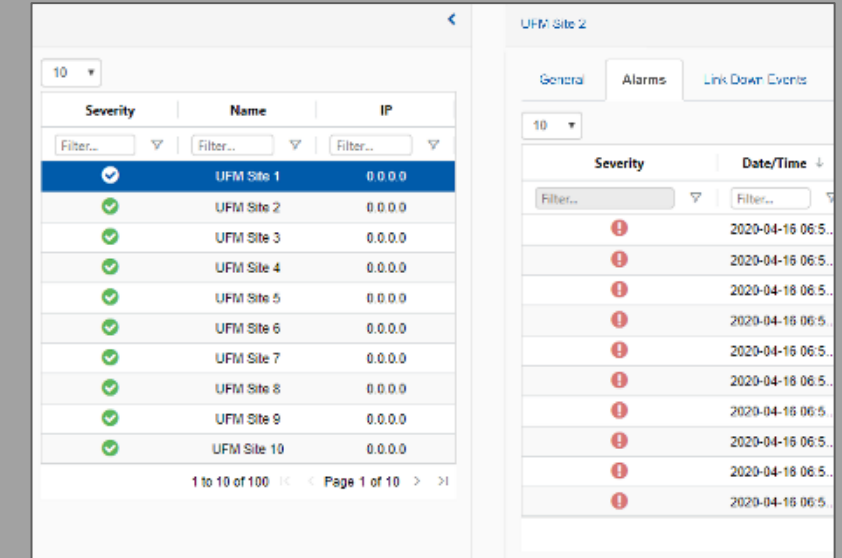
Network Validation



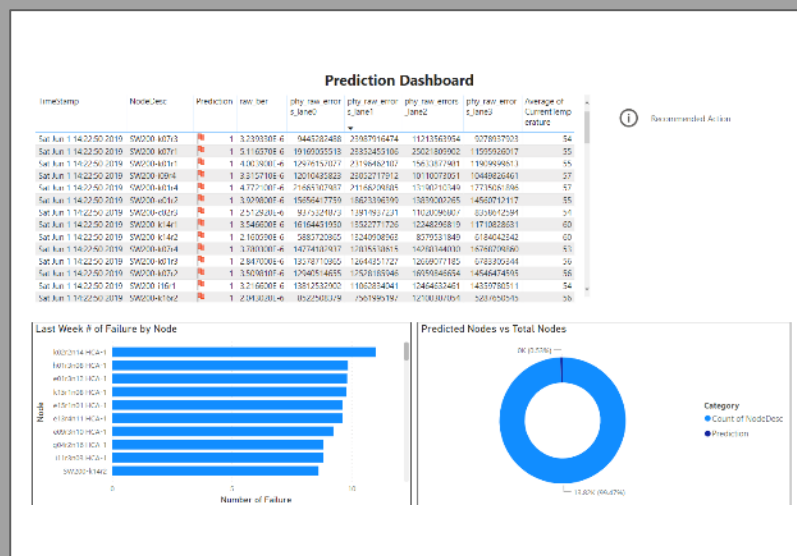
Congestion Mapping



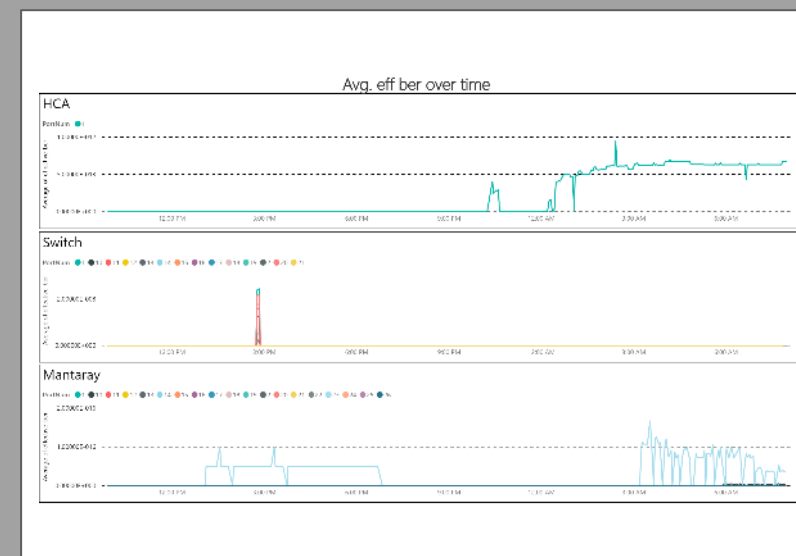
Health Reports



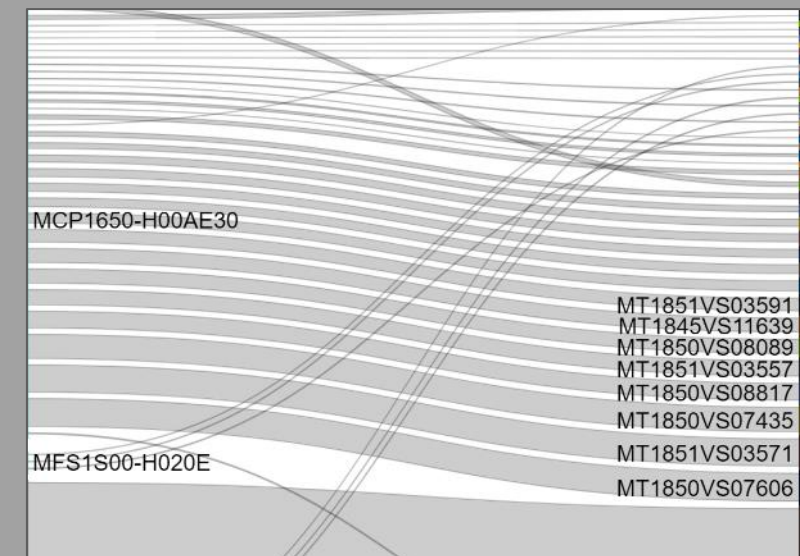
Inventory Mapping



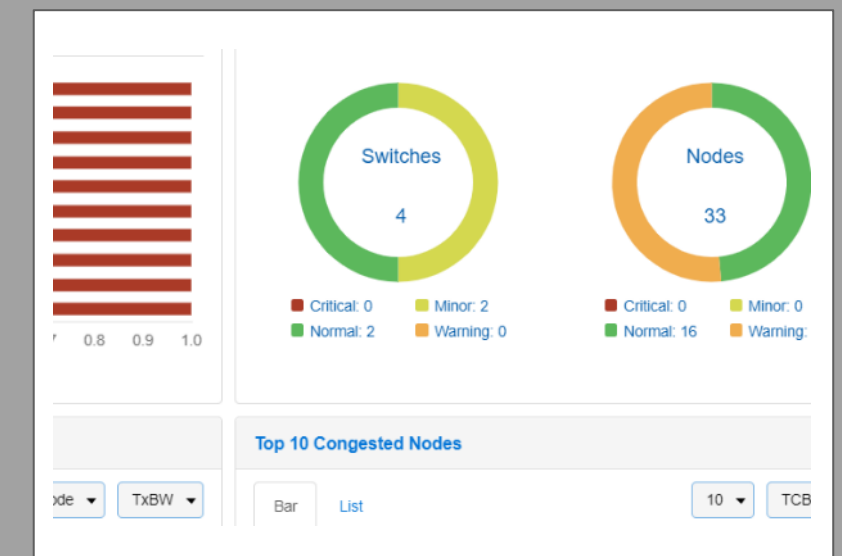
Prediction Dashboard



Real-Time Analysis



Performance Monitoring



Secure Cable Management

