Intel® Software Guard Extensions (Intel® SGX) Memory Encryption:

Keeping Your Data Safe In Cloud And Across CDN

Vsevolod Vayner, G-Core Labs
John Yanagi, Supermicro

G-Core Labs Cloud

with Intel® SGX Memory Encryption

G·CORE LABS

Vsevolod Vayner

Head of G-Core Labs Cloud Platform Department

Intro to G-Core Labs

G·CORE LABS

Who We Are

G-Core Labs is an international provider of cloud and edge solutions with 140+ points of presence. The company has built its own global infrastructure on all continents.

Average CDN response time is 30ms.

Our services:

- Powerful Cloud
- DDoS Protection
- Content Delivery Network (CDN)
- Hosting
- Advanced Streaming Platform
- Object Storage, etc.

G-Core Labs and Intel

G-Core Labs is a member of Intel Partner Alliance (IPA).

We have been working with Intel for 5+ years.

Security Breaches Are An Increasing Issue

G·CORE LABS

SUPERMICRO

Problem Statement

- Business moved to the cloud due to the pandemic
- Clouds suffer from massive DDoS attacks
- Sensitive data needs extra protection

Security Statistics

✓ Revenue Loss – According to a 2021 report from IBM and the Ponemon Institute, the average cost of a data breach among companies surveyed reached $4.24 million per incident in 2021[1]

✓ The number of data breaches through September 30, 2021 has exceeded the total number of events in full-year 2020 by 17 percent (1,291 breaches in 2021 compared to 1,108 breaches in 2020)

Critical industries

 Retail

 Finance

 E-commerce

Gaming

Technologies that solve the problem

✓ Safe and performative **G-Core Labs Cloud** with Intel® Software Guard Extensions (Intel® SGX) memory encryption

✓ **Supermicro Bare Metal** with Intel® SGX memory encryption

1 https://www.govtech.com/blogs/lohrmann-on-cybersecurity/data-breach-numbers-costs-and-impacts-all-rise-in-2021

G-Core Labs Public Cloud

G·CORE LABS

SUPERMICRO

1. Performative & User-Friendly Cloud

The Public Cloud consists of several levels of services:

Infrastructure as a Service

Platform as a service

Management

You can easily spawn a new instance through self-service port, REST API or Terraform provider.

2. Data Protected by Intel® Software Guard Extensions (Intel® SGX)

Intel® Software Guard Extensions is a hardware-based encryption.
It isolates specific application code and data in memory.
Neither the cloud service provider nor an outsider can get to the encrypted area and access the data stored in these enclaves – even if the servers were hacked.

Result: Industry Problem Solved

We help our customers to:

- ✓ Migrate to the cloud safely
- ✓ Grow in the cloud
- ✓ Make sure that their data is safe

G-Core Labs Public Cloud: technical details

G·CORE LABS

SUPERMICRO

Intel components in the Cloud infrastructure:

✓ 3rd Gen Intel® Xeon® Scalable processors

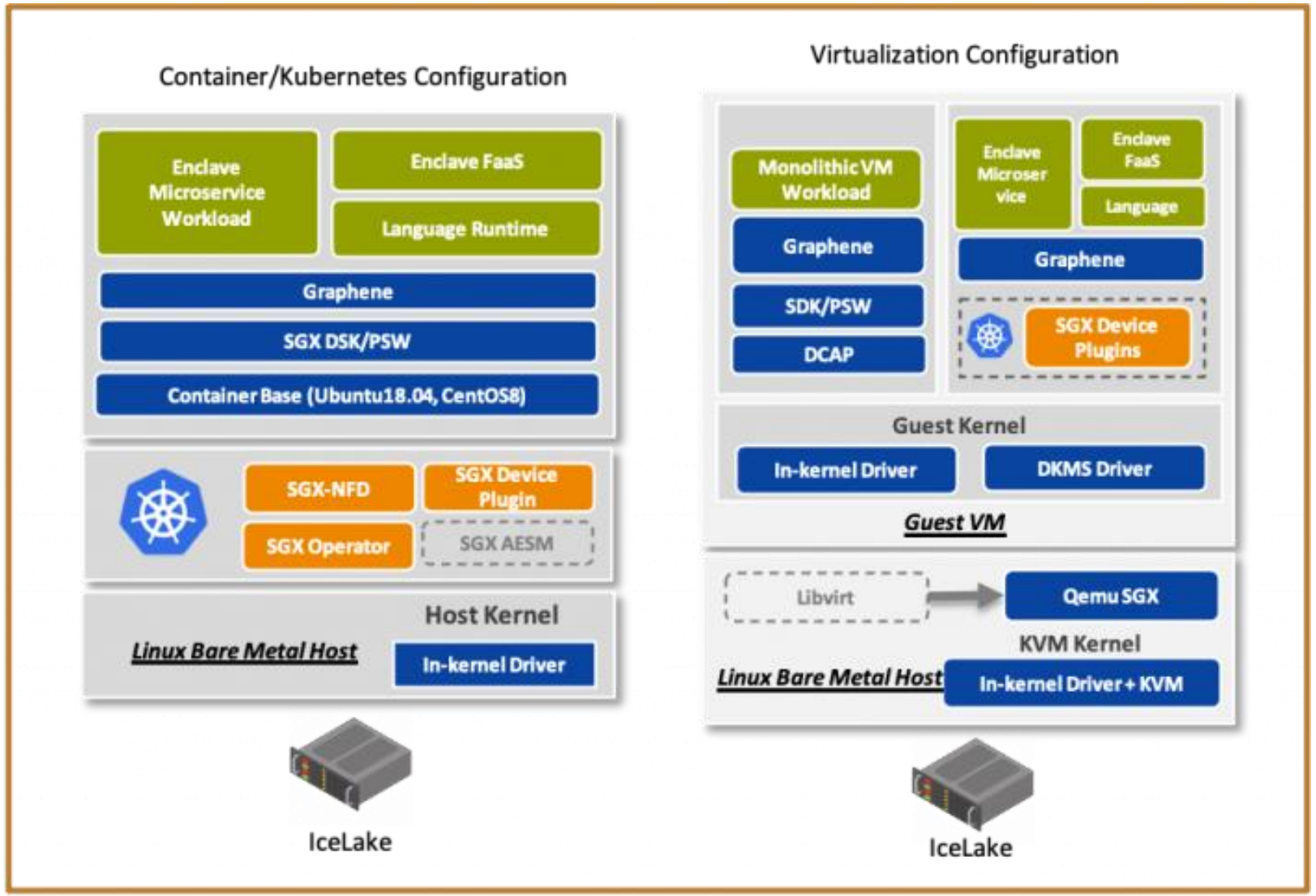
✓ Updated flavors / configurations of Virtual Machines.

SGX- 1	SGX- 2	SGX- 4	SGX- 8	SGX- 16
vCPU: 1 RAM: 2GB EPC Size: 1GB	vCPU: 2 RAM: 4GB EPC Size: 2GB	vCPU: 4 RAM: 8GB EPC Size: 4GB	vCPU: 8 RAM: 16GB EPC Size: 8GB	vCPU: 16 RAM: 32GB EPC Size: 16GB

How our solution work

G·CORE LABS

SUPERMICRO



Supermicro Bare Metal

with Intel® SGX Memory Encryption

John Yanagi

Senior Solutions Architect
Supermicro

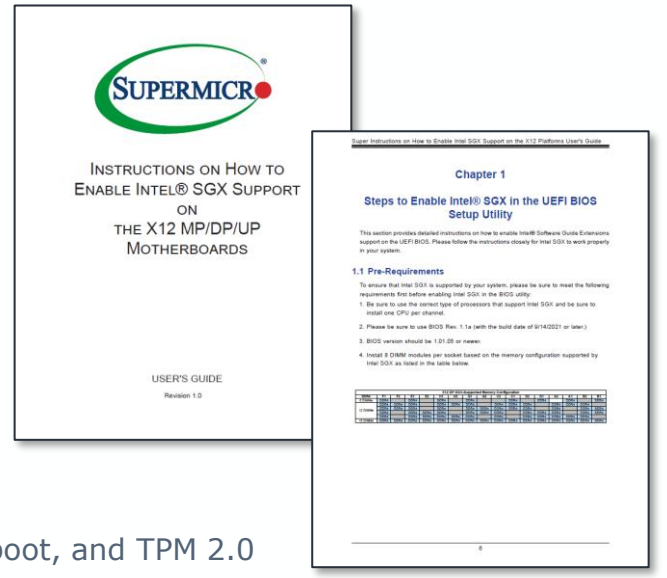
Enhanced Security with Supermicro and Intel

To accelerate websites and applications, developers are turning to CDN solutions to deliver content closer to users across global edge networks. Using a CDN without a proper mitigation strategy can create security vulnerabilities. Fortunately, attacks on CDN services are well-understood by companies like Supermicro and G-Core Labs who have taken security measures to help reduce cyber exposure for their customers.

With Supermicro Twin systems, we offer industry leading computing power and throughput, while physically isolating traffic on each compute node. After deploying our systems to G-Core Labs, we've worked together to configure and validate Intel® Software Guard Extensions (Intel® SGX). With larger SGX enclaves, the X12 BigTwin® can provide additional safeguards for developers to rapidly build and deploy applications with higher confidence.

Supermicro Value Added Services:

- ✓ Global manufacturing sites
- ✓ Engineering services to validate, optimize, and scale out infrastructure
- ✓ Orchestrate & streamline system configurations with SGX support
- ✓ Store and archive signed SW/FW with tight source code revision control
- ✓ Secure supply chain management
- ✓ Platform security supporting silicon root of trust, secure boot, and TPM 2.0



Why Supermicro BigTwin?

2U 4-Node BigTwin

Compute & Highest Storage Density

SYS-220BT-H Series:

6 NVMe/SAS/SATA (per node)

Per Node:

- ✓ Dual 3rd Gen Intel® Xeon® Scalable processors
- ✓ DDR4-3200 DIMMs (1DPC)
- ✓ Intel® Optane™ SSD DC P4800X Series
- ✓ Intel® SSD D3-S4510
- ✓ Dual 10GbE AIOM (Based on Intel® Ethernet Converged Network Adapter X710 Series)
- ✓ Dual 25GbE LP NIC (Based on 100GbE Intel® Ethernet Network Adapter E810)

No-compromise Computing

Double Compute density vs 1U servers and up to 20% more power efficiency

Optimized IO Performance

Double the IO bandwidth with PCI-E 4.0 for NVMe storage and high-performance networks

Field Serviceability

Hot-swappable compute nodes and tool-less support for ease of deployment

Why Supermicro BigTwin?

SUPERMICRO

G·CORE LABS

Memory

16 DIMM slots,
up to 2TB
Up to 1TB SGX
Enclave

Drives

24 Hot-swap 2.5”
Hybrid drive bays
and internal M.2
support
(optional RAID)

Input/Output

1 AIOM + 2x
PCI-E 4.0 x16

Power

Redundant
2600W/2200W
Titanium Level
(96%); Optional
3000W

How To Learn More

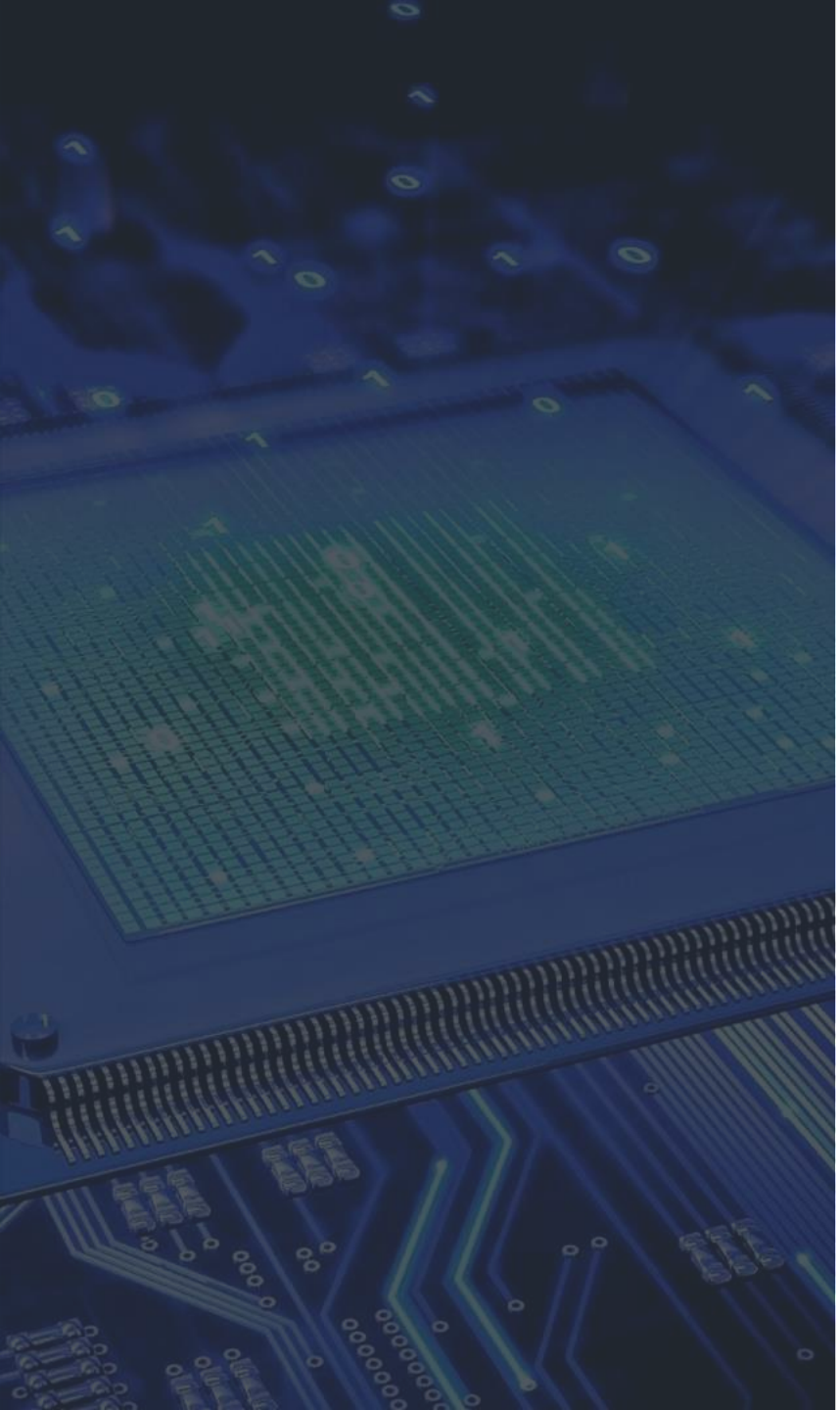
To know more about G-Core Labs Cloud solutions, kindly visit gcorelabs.com or write directly to Vsevolod Vayner: v_vayner@gcore.lu

To learn more about Supermicro, the BigTwin product suite, and our collaboration with G-Core Labs and Intel, please

contact your sales representative or email:

sales@supermicro.com

cloudnativesys@supermicro.com



Intel Legal Notice and Disclaimer

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

No product or component can be absolutely secure.

Your costs and results may vary.