SOLUTION BRIEF

Intel® Data Center Blocks for Business–SGX Server Block

1U System Delivering Cryptographic Security

Content Delivery Networks, Cloud Service Providers, Communications Networks, and Financial Institutions

SGX Server Block from Intel

- **Industry-leading cryptographic isolation technology** eliminates expenses associated with crypto-processor based HSMs[1] while providing premium cryptographic security
- **Fully Validated Server Block** saves time and money,[1] freeing up resources to focus on value-add and competitive differentiation
- **Unbranded systems** enable resellers to customize and brand to meet end-user requirements
- **Intel Quality & Reliability** with world-class integration, validation, certification, and support
- **Standard Intel 3-year warranty,** with the option to extend parts of coverage to 5 years, ensures customer satisfaction

Safeguard Sensitive Information

In a highly competitive market, Content Delivery Networks (CDN), Cloud Service Providers (CSP), Communications Networks, and Financial Institutions (FI) need a cost-effective cryptographic security solution that delivers enterprise-grade performance, reliability and security in an easy-to-manage system. These businesses also seek competitive pricing for their server infrastructure. To address this demand, Intel offers the Data Center Blocks for Business - SGX Server Block, a fully-integrated server system that features Intel® Software Guard Extensions (Intel® SGX).

The SGX Server Block is designed for information security workloads and uses Intel's industry-leading cryptographic isolation technology. Intel® SGX provides CPU-hardened enclaves, or protected areas of execution in memory, that increase security for selected code and data on compromised platforms.

Making it Easier to Deliver Competitive Entry Server Solutions

To meet the needs of CDNs, CSPs, Communication Networks, and FIs, resellers design custom server solutions which is a costly and resource-intensive process. Intel helps reduce the complexity of this process with its Intel® Data Center Blocks, fully validated, unbranded server systems that include Intel's latest data center technology. By taking advantage of Intel's engineering and validation resources, resellers can reduce both capital and operational expenses with integrated server systems, like the SGX Server Block. This approach gives partners more flexibility and choice about where to invest R&D funds to ensure they remain competitive and drive differentiation in the market.

Intel-Built for Quality, Reliability and Value

The SGX Server Block is powered by the latest Intel technology, and includes the Intel® Server Board S1200SPOR4 that can scale as customers grow via SATA and PCIe* expansion options for increased storage functionality for faster networking speed. The SGX Server Block features a 1U rack optimized system configuration that is quiet and well-suited for a small datacenter environment. To make server management easier, this product supports Intel® Node Manager and includes a dedicated management port with support for advanced management features to enable secure, anywhere-access from any device, and provide ongoing monitoring and troubleshooting.

Smart Boards Ensure System Stability and Increased Uptime

Intel® Server Boards have more than 100 sensors built in that monitor all critical functions and use management capabilities to automatically flag problems before

they impact business operations. Event logs and light- guided diagnostics also assist in rapid identification and remediation of issues.

Business-Class Performance with Intel® Xeon® processor E3 Family

These pre-configured server blocks feature the Intel® Xeon® processor E3 family that delivers high memory, I/O and storage capacity, fast application loading and performance, and the capacity to support multiple users. This latest processor from Intel delivers increased productivity with Intel® Turbo Boost Technology, Intel® Hyper-Threading Technology, and more performance than previous generations.[2] It also delivers hardware- based security features like Intel® Data Protection Technology and Intel® Platform Protection technology for better protection of data.[3]

To allow the system to scale as your business grows, the configuration is upgradable with up to 4x 2.5" SSD drives and Intel® RAID Modules for increased storage capacity, as well as having additional Intel® I/O Expansion Module options.

Intel Warranty Delivers Value and Confidence

The SGX Server Block comes with a standard three-year warranty with the option to extend parts of coverage to five years. Warranties come with Intel's 24/7 technical support and commitment to replace, repair or refund any components that fail. Additionally, since all components are purchased in a single SKU, there is a single source for all support needs.

Engage with Intel Today

Intel continuously delivers leading- edge technologies to help you innovate and differentiate in the market. This is true with the SGX Server Block, designed to help you accelerate time to market with innovative server solutions that feature premium cyrptographic security.

Contact your Intel sales representative or Intel authorized distributor for any inquiries.

More information on the SGX Server Block can be found online at **http://www.intel.com/content/www/us/en/data-center-blocks/business/business-blocks.html**

Premium Security with reduced TCO

Intel® SGX enables customers to protect their intellectual property using hardened key management, preventing malicious denial of service attacks, while reducing expenses associated with cypto-processor based HSMs.

Intel® SGX

- Protects TLS keystore using trusted memory enclaves
- Isolates enclaves from malware and privileged software attacks
- Processor controls access, prevents intrusion, encrypts transported and stored data

IT Benefit

- Reduces attack surfaces
- Supports hardware-based attestation and TLS keystore

Developer Benefit

- Familiar development environment
- Familiar application deployment model.

Targeted Workloads

- Content Delivery Networks can protect trade secrets and intellectual property.
- CSPs & Communications Networks can deploy the SGX Server Block to protect end-user information.
- Financial Institutions can prevent data breaches and identity theft, and more easily comply with industry regulations.

1U Server Block	Components Included in the system	
	Component	Description
Order Code: LR1304SPCFSGX1 **MM#: 953556**	Chassis	Intel 1U chassis with hot-swappable 4x3.5" (2.5" SSD ready) drive trays, dual 450W redundant PSUs (R1304SPOSHORR)
	Board	Intel® Server Board S1200SPOR4
	CPU	Intel® Xeon® Processor E3-1270 v6 (8M Cache, 3.40 GHz)
	Memory	64GB (4 x16GB), 2133MHZ, DDR4, UDIMM
	Storage	Two Intel® SSD DC S3520 Series (1.2TB, 2.5in SATA 6Gb/s, 16nm, MLC)
	Adv. Remote Management	Intel® Remote Management Module 4 Lite 2 (AXXRMM4LITE2)
	Security	TPM 2.0 Module

Server Specifications	Intel® Server System R1304SPOSHORR
Form Factor	1U
Chassis Dimensions	1.7 in (43.18 mm) x 17.26 in (438.5mm) x 21.06 in (548.9 mm)(Height x Width x Depth)
Server Board	Intel® Server Board S1200SPOR[4]
Server Board Form Factor	microATX 9.6" x 9.6"
Storage	4 x 3.5" (2.5" SSD Ready) hot-swap drive bays 1 x optical drive bay
Cooling	Three managed 40mm single rotor system fans One fan for each installed power supply module
System Power	Two 450 Watt, Gold, hot swap modules, redundant
Processor Support	Single Intel® Xeon® processor – E3-1270 v6, up to 80W TDP
Processor Socket	Socket-H4 LGA1151
Chipset	Intel® C236 chipset
Memory Support	4 DIMMs, 64GB maximum total DDR4 UDIMM ECC at 2133MT/s maximum
On Board LAN Support	Dual 1GbE – Intel® Ethernet Controller i210
Front Control Panel	Control Buttons–Power/Sleep, System ID, System Reset, NMI LEDs – Power, System Status, System ID, NIC Activity, Drive Activity

External I/O Connectors	
USB	Back Panel – 2x USB 2.0 + 2x USB 2.0/3.0 Front Panel – 2x USB 2.0/3.0
Network Interface	Dual 1GBase-T (RJ45)
Management Port	Single 1GBase-T dedicated server management port (RJ45)
Video	VGA graphics via BMC (Front and Back DB-15 VGA connectors)
Internal I/O Connectors	
USB	One Type A USB 2.0 connector
Serial Port	One DH-10 Serial Port 'A' connector
SATA	Eight SATA3 via 7-pin SATA connectors One M.2 SATA SSD 2242 connector Embedded Software SATA RAID Options – Intel® Rapid Storage Technology enterprise (Intel® RSTe) and Intel® Embedded Server RAID Technology 2
SATADOM Support	Yes - Apacer* SATADOM options
TPM Support	One TPM 2.0 connector
Expansion Options	
I/O Module Support	One proprietary connector for Intel® I/O Expansion Module options One proprietary connector for Intel® Integrated SAS RAID Module option –Mounting Support for one Intel® RAID Maintenance Free Backup Unit
PCIe Add-in Card Slot via 1U Riser Card	One PCIe 3.0 x16 slot (x8 electrical)

For product specifications visit: **ark.intel.com**

For more information on Intel® Server Products and Solutions visit: **intel.com/serverproducts**

For more information on Intel® Data Center Blocks visit: **intel.com/dcb**

1. Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.
2. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to http://www.intel.com/performance
3. Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.
4. Intel® Server Board S1200SP family firmware does not support monotonic counters and trusted time features. Therefore, some SGX use models such as distributed ledger with Proof of Elapsed Time (PoET) consensus algorithm can't be supported.