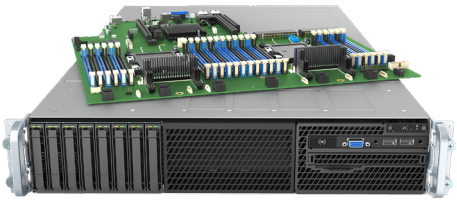
SOLUTION BRIEF

Critical Infrastructure, Government, Financial Institutions

Intel® Data Center Block with Firmware Resilience

Making it easier to deliver competitive and secure servers for critical infrastructure, government, and financial industries



Intel® Data Center Block with Firmware Resilience

- **Protects, detects, and corrects against attacks** on critical components below the operating system
- **Fully validated server block** saves time and money, 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 and 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

As the intensity, sophistication, and disruptive impact of security attacks continue to escalate, security IT officers are driving for a holistic approach to protect their critical infrastructure. This includes protecting the server all the way down to the firmware at the lowest layers of the platform, where threats are most difficult to detect. While technologies exist to protect the higher layers of the infrastructure stack, system IT users increasingly need assurance that the underlying platform launching these security technologies can be trusted.

To address this, Intel has developed the Intel® Data Center Block with Firmware Resilience (Intel® DCB with Firmware Resilience). Featuring Intel® Platform Firmware Resilience (Intel® PFR) technology, these systems enable platform security starting at the factory floor and maintained through power-on, system boot, OS load, and beyond.[1] With this offering, customers can protect firmware from being intercepted, detect firmware corruption, and restore a system to a known good state if malware is detected. This capability to mitigate firmware corruption is an important industry innovation, and provides an optimal solution for security-sensitive organizations including government, financial institutions, and those responsible for critical infrastructures.

Intel is simplifying adoption of this technology through fully validated systems featuring Intel® Xeon® Scalable processors, Intel® Server Boards, Intel® Server Chassis, third-party memory, and multiple upgrade options to provide a solution that customers can deploy quickly and with confidence.

Intel-Built for Quality, Reliability, and Value

Designed for government, financial, and critical infrastructure needs

The Intel DCB with Firmware Resilience is designed with security-sensitive users in mind, featuring a 1U or 2U rack optimized system configuration combined with hardware-enhanced security features for critical infrastructure, government, and financial customers. To make server management easier and more efficient, this product includes utilities to simplify the provisioning of security features and to securely[1] update firmware components remotely across an entire rack. The system also includes a dedicated management port to enable secure[1], anywhere-access from any device.

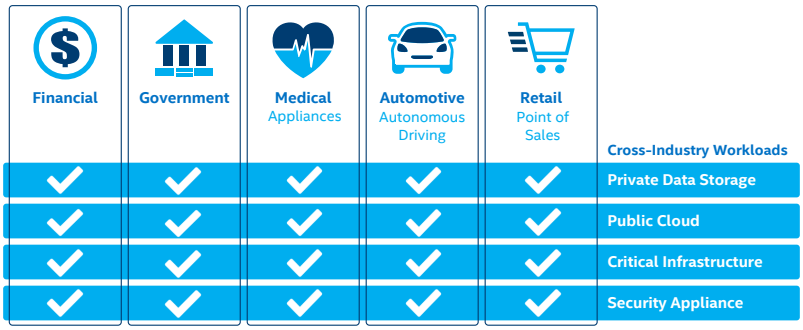


Figure 1. Designed for security-sensitive industries and cross-industry workloads.

Intel® DCB with Firmware Resilience—Providing a Trusted Foundation

Fully integrated and validated 1U or 2U rack server block featuring the latest Intel data center technology and optimized for security-sensitive customers.

Features:

- **Intel® Platform Firmware Resilience (Intel® PFR)** protects critical firmware during boot and runtime attacks. If malware is detected, Intel PFR will perform a recovery to a gold image.
- **Protect-in-transit feature of Intel® PFR** allows customers to lock and unlock systems while in transit, protecting firmware from changes during shipment (optional feature).
- **Intel® Transparent Supply Chain with Platform Certificate** creates transparency in the supply chain to prevent counterfeit components from being used.
- **Intel® Trusted Execution Technology with TPM** enables attestation of the authenticity of the UEFI Firmware and its operating system.
- **Deployment Flexibility:** Choose from one of three security-optimized processors and multiple upgrade options to design a system that meets your unique needs.

Upgrade Options:

- Intel® Integrated RAID Module options
- Intel® I/O Expansion Module options
- Intel® SSD drives
- Memory

Optimized for security with Intel® Xeon® Scalable processors

The Intel DCB with Firmware Resilience supports three Intel Xeon Scalable processors enhanced to support Intel PFR. These processors anchor the root of trust at the lowest levels of the platform. Together with a security-specific ASIC and authenticated code modules, Intel PFR guards the platform through a processor-directed secure boot mechanism to authenticate firmware and, if necessary, restore firmware images.

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.

Intel warranty delivers value and confidence

The Intel Data Center Block with Firmware Resilience comes with a standard three-year warranty that includes the option to extend coverage to five years. Warranties come with Intel's trusted technical support and commitment to replace or refund any product that fails. 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 Intel Data Center Block with Firmware Resilience, designed to help you realize an easier path to reliable and secure[1] server solutions.

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

More information can be found at https://www.intel.com/content/www/us/en/products/servers/data-center-blocks/dcb-business.html.

Intel® Data Center Blocks with Firmware Resilience

MM#	PRODUCT CODE	CPU	CHASSIS FORM FACTOR	STORAGE	NUMBER OF POWER SUPPLIES	MEMORY MODULES (2X)
974985	LFRB1208WFTF801	Intel® Xeon® Platinum 8160H	1U	Up to 8 x 2.5"	1¥	16GB, RDIMM, DDR4, 2666 MT/s
974987	LFRB2208WFTF801	Intel® Xeon® Platinum 8160H	2U	Up to 8 x 2.5"	2	16GB, RDIMM, DDR4, 2666 MT/s
974989	LFRB2312WFTF801	Intel® Xeon® Platinum 8160H	2U	Up to 12 x 3.5"	2	16GB, RDIMM, DDR4, 2666 MT/s
974986	LFRB1208WFTF601	Intel® Xeon® Gold 6130H	1U	Up to 8 x 2.5"	1¥	16GB, RDIMM, DDR4, 2666 MT/s
974988	LFRB2208WFTF601	Intel® Xeon® Gold 6130H	2U	Up to 8 x 2.5"	2	16GB, RDIMM, DDR4, 2666 MT/s
974990	LFRB2312WFTF601	Intel® Xeon® Gold 6130H	2U	Up to 12 x 3.5"	2	16GB, RDIMM, DDR4, 2666 MT/s
974992	LFRB1208WFTF401	Intel® Xeon® Silver 4106H	1U	Up to 8 x 2.5"	1¥	16GB, RDIMM, DDR4, 2666 MT/s
974993	LFRB2208WFTF401	Intel® Xeon® Silver 4106H	2U	Up to 8 x 2.5"	2	16GB, RDIMM, DDR4, 2666 MT/s
974991	LFRB2312WFTF401	Intel® Xeon® Silver 4106H	2U	Up to 12 x 3.5"	2	16GB, RDIMM, DDR4, 2666 MT/s

¥Power supply can be 1100W or 1300W.

SERVER SYSTEM SPECIFICATIONS	
2U Chassis Dimensions	16.93" W x 27.95" L x 3.44" H
1U Chassis Dimensions	16.93" W x 27.95" L x 1.72" H
Server Board	Intel® Server Board S2600WFTF
Server Board Form Factor	Custom 16.7" x 17"
Processor Support	Dual select PFR enabled Intel® Xeon® Scalable processor
Processor Socket	Socket-P
Chipset	Intel® C624 chipset
Max DIMM Slots	24 DIMMs Total – 6 channels per processor, 2 DIMMs per channel
On Board LAN Support	Dual 10GbE
Front Control Panel	Control Buttons – Power/Sleep, System ID, System Reset, NMI LEDs – Power, System Status, System ID, NIC Activity, Drive Activity, and RFID antenna

INPUT/OUTPUT	DETAILS
USB	Three external USB 3.0 ports One internal Type-A USB 2.0 port One internal 20-pin connector for optional 2x USB 3.0 port Front Panel support One internal 10-pin connector for optional 2x USB 2.0 port Front Panel support
Serial	One external RJ45 Serial Port A connector One internal DH-10 Serial-B port header for optional rear serial port support
Video	One DB-15 external connector One 14-pin internal connector for optional Front Panel Video support
Storage	Two single port 7-pin SATA Gbps connectors Two 4-port SATA Mini-SAS HD connectors Two 80mm M.2 connectors – (x2 and x4 PCIe and SATA) PCIe OCuLink connectors for direct attach NVMe* 2.5" SSDs
Network	Two Integrated 10GbE Ports

EXPANSION OPTIONS	DETAILS
PCIe Add-in Card Support	Three Riser card slots supporting up to 8 PCIe 3.0 add-in cards
OCP Module Support	Support for one of several available PCIe x2 OCP KR-based mezzanine module options – 1GbE Cu, 10GbE Cu/SFP+
SAS Raid Support	Support for one of several available 12 GB/s Intel® Integrated RAID Module options

For product specifications visit: ark.intel.com

[1] 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.

Printed in USA 0818/KK/MIM/PDF Please Recycle 336075-002