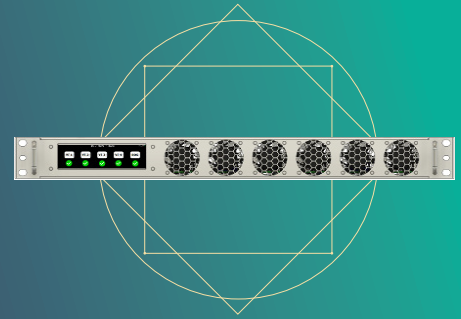


High Speed Verifier 2 Platform



Key Benefits

- › Assured protocol break in hardware logic
- › Assured data break in hardware logic
- › Data break with semantic verification
- › Concurrent verification of multiple data streams
- › Over-the-wire firmware updates
- › Delivered through a trusted supply chain
- › Built in line with best practice guidance

High Speed Verifier 2 (HSV2) is Forcepoint's second-generation data verifier. The HSV can be used as part of an Information eXchange (iX) Appliance for general-purpose cross domain applications. Or it can be used standalone to embed a high-assurance protocol and data break into custom cross domain applications.

Hardware Logic Protocol Break

Data passes into and out of HSV2 using TCP, handled by protocol proxies running on network processors associated with each network interface. The proxies communicate with the logic verifier using a simple protocol across raw Ethernet, thus, no TCP or IP protocols pass across the verifier giving a protocol break. As the protocol is simple enough to be implemented in logic, this implementation is fully independent of the software implementation in the proxies, assuring the function of the protocol break.

- Protocol break enforced by hardware logic
- Protocol breaks enforced between all three networks – two data and one management

Hardware Logic Data Break

All data exchanged between networks is transformed into a simple, strongly typed, data format with semantic constraints, designed to be verified in hardware logic. Complex data formats are transformed into the simple format using software, the simple data is verified in logic, then it is transformed back into the complex format using software. Data received is never delivered, as all the data delivered is built from verified simple data, giving an assured data break. The data break is built on top of the protocol break, assuring that the verification cannot be bypassed.

- Semantic verification in hardware logic
- Byte stream operation at line speed for low-latency verification
- Data break enforced between all three networks – two data and one management

Device Management

Each HSV2 has a digital identity, used to allow the administrator to authenticate the device. The identity is managed by a dedicated micro-controller and is linked to the secure boot of the device. Administrators authenticate to the device using SSH.

- Software and firmware authenticity checked on every boot
- Monitoring through SNMP, syslog and StatsD
- Chassis tamper detection



Front View



Rear View

Physical

The HSV2 is a 1U chassis suitable for running in an air-conditioned server room environment in a 19" rack. Up to 4 independent logic verifiers can be installed in a single chassis giving a small footprint. The chassis' LCD touch panel display can be used to identify and review the status of an installed device.

- Compact deployments, with 4 verifiers in 1U
- Dual redundant hot-swappable power supply
- SFP network interfaces

SDK

To embed an HSV2 into custom cross domain applications, the HSV2 Software Development Kit (SDK) is used by application developers to prepare data for passing through the verifier. The SDK provides or creates an interface that allows the application to serialise / de-serialise the data structures that are to be exchanged. The data is passed through the HSV using standard networking protocols.

- Boolean, integer, float and binary coded decimal types
- Unicode character string and binary string types
- Arrays, lists and choice structures
- Constrained number ranges, and string, array and list lengths

Note: A separate SDK is provided for transforming complex file formats into verifiable data structures, supporting common file formats such as internet imagery and Microsoft Office.

Operating Environment (System)

OPERATING ENVIRONMENT	
Operating Temperature Range	10 - 40°C (50° to 104°F)
Non-Operating Temperature Range	-20 - 70°C (04° to 158°F)
Humidity Range	40 - 60% non-condensing
Non-Operating/ Humidity Range	30 - 70% non-condensing

Technical Specification

CHASSIS	
Unit Size	Height: 4.4cm (1.7in.) x Width: 48.2cm (19.0in.) x Depth: 36.9cm (14.5in.)
Unit Weight	Up to 11.1kg (24.5 lbs)
System Cooling	6 x 40mm, 2,900 - 15,600 RPM axial fan, front to back air flow
Fan MTBF	70,000 hours (@ +40°C)
Finish	Smooth finish powder coat in white and silver

POWER (DUAL POWER SUPPLIES)	
AC Voltage	Minimum 90, Nominal 100-240, Maximum 264 VAC
Power	Up to 11.1kg (24.5 lbs)

PROCESSORS AND MEMORY (PER VERIFIER)	
Number of Processors	3 (one for each network interface)
Processor Cores	4
Processor	NXP QorIQ LS1043A
Processor MTBF	N/A
Memory	3 x 4 Gbyte DDR4

STORAGE (PER VERIFIER)	
Type	Serial NOR Flash (for system images)
Number of Disks	N/A
RAID	N/A
Hot-Swappable	N/A
Memory	3 x 128 Mbyte
Disk MTBF	N/A

INTERFACES (PER VERIFIER)	
Networking	3 x 1000BASE-T copper Ethernet, or 3 x 1000BASE-SX multi-mode fiber, LC connector, 850nm
DVD-RW	N/A
USB Ports	N/A
Serial	N/A
IPMI	N/A

DISPLAYS (PER CHASSIS)	
Front panel LCD	Touchscreen
VGA	N/A

DEPLOYMENT	
Indicators	Tamper detection Verifier status, fault indicator, fan speeds on LCD
Warranty	1-year warranty
Accessibility	N/A
Power Supplies	2 (redundant, hot-swappable)
Power Supplies MTBF	100,000 hours
Connectivity	HSV002 connects into standard network infrastructure.

VERIFIER STATE MACHINE (PER VERIFIER)	
Maximum States (2B)	65535
Maximum Choices	16384
Maximum Number of Ranges	4096
Concurrent Channels	1024
State Stack	16
Counter Stack	16