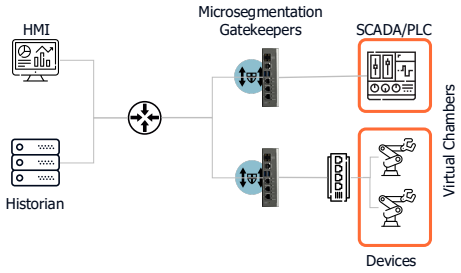
Microsegmentation Gatekeeper

Inline Security Appliance for Industrial Zero Trust Segmentation and Access Control

The Zentera Systems® Microsegmentation Gatekeeper (MSG) provides advanced Zero Trust Segmentation and ZTNA-based access control that protects critical OT assets. Deploying inline with the asset as a "bump in the wire," the MSG enforces access policies that model the business' expected operational usage and filters unauthorized network traffic.

The zCenter Orchestrator provides a centralized single pane of glass for observing existing traffic, managing identities of users, devices, and software, and configuring security policies for enforcement by distributed MSGs throughout the operational environment, dramatically streamlining operations and reducing security management overhead.

MSG-IL-2BPI
Microsegmentation
Gatekeeper
Industrial Rated



High-Security

- Inline network appliance that secures connectivity and filters application traffic for OT devices
- Rugged design for industrial applications

Zero Trust Segmentation

- Instantly create a Zero Trust DMZ to segment individual devices, inhibiting lateral propagation of attacks
- Learn function exposes existing traffic flows with ML-assisted policy development

Protects on-premises traffic

- Overlay optionally allows on-premises traffic to be secured inside TLS 1.3 tunnels to prevent snooping

Compatible with Existing Network Infrastructure

- OSI Layer 2 implementation, transparent to Layer 3
- No need to change asset IP addresses and no impact to switch/routing architecture

Integrated Zero Trust Network Access

- Enable users and machines to securely access protected assets subject to security checks (authorized user, device, software)

Simple to Deploy and Manage

- Centralized policy management through the zCenter Orchestrator for single pane of glass control
- Automated security policy enforcement streamlines operations with high scalability

Bypass Ensures Load Availability

- 3rd generation hardware bypass fails open, ensuring the availability of the asset under failure conditions

 © 2025 Zentera Systems, Inc. All Rights Reserved.

The Microsegmentation Gatekeeper deploys in an inline mode to insert security functions "on the wire" in front of a protected device.

Security functions include advanced Zero Trust Network Access (ZTNA) to authenticate machine-to-machine and user-to-machine accesses, application-aware stateful firewalling, and microsegmentation on each of its independent ports.

Firewall and segmentation policies are defined on the zCenter Orchestrator, which manages pushing policies to each MSG. Centralized end-to-end policies are easy to understand and manage, regardless of the various network domains that application traffic transits through.

All traffic between pairs of MSGs and other CoIP components (e.g. servers running the zLink agent) can leverage CoIP tunnels using advanced TLS 1.3 encryption, dynamically set up by zCenter on demand.

Each MSG is fully managed by the zCenter, which handles pushing software updates and patches to the MSGs. The zCenter supports a powerful RESTful API, enabling security policies to be defined as code and pushed to the system.

High availability and redundancy are supported at multiple levels: at the MSG level, advanced 3rd generation bypass is supported on Ethernet ports to enable a wire "pass through" in the event of software or hardware failure. Additionally, the associated zCenter Orchestrator supports high availability deployment and disaster recovery options.

Functional Specifications

Zero Trust Specifications	
Zero Trust Network Access	✓
Trust establishment	User, endpoint, and application identity
Advanced application control	✓

Security Capabilities	
Firewall capabilities	L4 stateful
L4 firewall throughput (IMIX, min)	2Gbps
Firewall policies (max)	4,096
Concurrent TCP sessions	1M (per port-pair)
Intranet-only operation	✓
Microsegmentation	✓
Real time policy updates	✓

Networking and Connection Security	
Layer 3 Protocols	IPv4, IPv6-ready
QoS rate limiting	By port-pair
CoIP Access transport security	TLS 1.3
Ciphersuites	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256 TLS_AES_128_CCM_8_SHA256 TLS_AES_128_CCM_SHA256

Management and Monitoring	
Central policy controller	zCenter Orchestrator
API support	✓
Supported admin authentication	SAML 2.0, RADIUS, TACACS+, local database
Upgrade and patch management	Managed by zCenter
SNMP versions	v1, v2, v3
SNMP traps and polling	✓
LLDP support	✓
Syslog	✓
Configurable log export	✓

Resiliency and High Availabilty	
Network bypass	✓ (Gen 3)
Supported Network Redundancy	HSR, PRP

 © 2025 Zentera Systems, Inc. All Rights Reserved.

Physical Specifications

Hardware Specifications	MSG-IL-2BPI
CPU	Single Intel® Atom X (Apollo Lake-I)
GE RJ45 Interfaces	2 (1 pair) auto-sensing 10/100/1000 Mbps
Console	1x GE RJ45, 1x RS-485
Local Storage	32GB (SATA 3.0 DOM)
Onboard Memory	8GB
Hardware Bypass	1 (Gen 3)
Power over Ethernet	Not Supported
USB Interfaces	2 x USB 3.0
Digital I/O	1x DI, 1x DO

Security Specifications	MSG-IL-2BPI
Secured Devices	Up to 2

Physical Specifications	MSG-IL-2BPI
Form Factor	DIN-rail
Cooling	Fanless
Chassis Dimensions (W x D x H)	140mm x 110mm x 40mm
Weight	0.91kg (2.0 lbs)

Electrical Specifications	MSG-IL-2BPI
Power	DC 12-48V
Max TDP	6.5W
Power Inputs	2 (Redundant)

Environmental and Certifications	MSG-IL-2BPI
Operating Temperature	-40°C - 70°C
Storage Temperature	-40°C - 85°C
Relative Humidity	0% - 95%, non-condensing
Certifications	CE/FCC Class A, UL, IEC 61850-3, IEEE 1613

Ordering Part Numbers

Product	SKU	Description
MSG-IL-2BPI	SE200-121A	Microsegmentation Gatekeeper, Industrial, 2x GE RJ45 Bypass, 1x GE Management

Copyright© 2025 Zentera Systems, Inc. All rights reserved. Zentera®, Zentera CoIP®, CoIP®, Cloud over IP®, and certain other marks are registered trademarks of Zentera Systems, Inc., in the U.S. and other jurisdictions, and other Zentera names herein may also be registered and/or common law trademarks of Zentera. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Zentera, and Zentera disclaims all warranties, whether express or implied, except to the extent Zentera enters a binding written contract with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Zentera. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Zentera's internal lab tests. In no event does Zentera make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Zentera disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Zentera reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

DS-MSG-IND-PA-R1.0