Byos Secure Cluster Edge™

SOLUTION OVERVIEW

Solution Overview

The Byos Secure Cluster Edge™ brings hardware-enforced microsegmentation security to the datacenter. Deployed inside of a server rack, it allows for administrators to add Byos Secure Edge™ microsegmentation to existing server infrastructure. Bring isolation, control, and granular access to your data centers without any complicated installation.

Key Features & Benefits

Internet Isolated Access

Access resources on the server without having to expose the server to the internet.

Server Rack Mountable

Deploy directly in existing datacenter infrastructure.

Plug and Play

Nothing to change or install on the network or server, fully compatible with brownfield installations

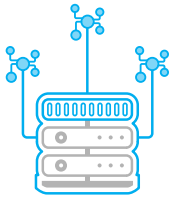
Product Specifications

- 10 Dedicated Microsegments
  (Each with a 1GbE port)
- 10 Individual 1GbE Uplink Ports
- 2U Rack-Mountable Design
- Dimensions: 8.0" L x 16.6" W x 3.5" H
- Redundant AC and DC inputs.
  - 2 AC Inputs, 85-264V~50/60Hz
  - 2 DC Inputs, 24V⎓20A
- Manufactured in the USA
- Certified Secure Supply Chain Components
- FIPS 140-2 Validated Software

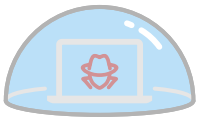
Use Cases

Secure Multi-Tenant Environments Without Physical Separation

- **Context**: A datacenter hosts multiple clients (eg. in colocation or cloud setups) and needs to ensure each tenant's data and applications are isolated from others, even within shared infrastructure.
- **Pain Point**: Traditional VLANs or physical separation are either insufficiently secure (VLAN hopping risks) or costly (dedicated hardware per tenant).
- **Use Case**: Byos Secure Cluster Edge enables microsegmentation within a single server rack, creating isolated zones for each tenant's workloads. This allows a colocation provider to offer secure, cost-effective multi-tenancy without overhauling their physical layout or relying solely on software-based firewalls.
- **Outcome**: Tenants get robust security assurances (eg. compliance with regulations like PCI DSS), and the provider maximizes rack space efficiency while reducing hardware costs.



Contain Lateral Movement During a Security Breach



- **Context**: A datacenter operator needs to limit the damage of a breach (eg. ransomware or insider threats) where an attacker gains initial access to one server.
- **Pain Point**: In a flat network, attackers can move laterally across servers, exploiting weak points. Adding firewalls or network appliances per rack is complex and expensive.
- **Use Case**: Byos Secure Cluster Edge microsegments the rack into zones (eg. by application, department, or sensitivity level). If one segment is compromised, the attacker can't easily pivot to others, as each zone has its own access controls enforced at the hardware level.
- **Outcome**: Faster containment reduces breach impact, downtime, and recovery costs, giving security teams a practical way to enforce zero-trust principles within a single rack.

Simplify Compliance for Regulated Workloads

- **Context**: An enterprise datacenter runs workloads subject to strict regulations (eg. HIPAA for healthcare, GDPR for EU data), requiring clear separation of sensitive data from other operations.
- **Pain Point**: Proving compliance often involves complex audits of network configurations, and software-defined segmentation can be hard to validate physically.
- **Use Case**: Byos Secure Cluster Edge creates microsegments tailored to compliance needs—eg. isolating patient data servers from administrative systems within the same rack. The hardware-based segmentation provides a tangible, auditable boundary that's easier to demonstrate to regulators.
- **Outcome**: Compliance audits become less burdensome, and the business avoids fines or delays while maintaining operational flexibility.

BYOS

Optimize Resource Allocation for Hybrid Workloads

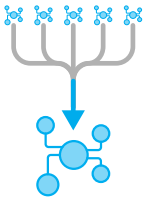
- **Context**: A datacenter supports a mix of high-performance computing (HPC), virtualized apps, and legacy systems, all sharing rack space, with varying network and security demands.
- **Pain Point**: Mixed workloads can lead to resource contention or security gaps, and reconfiguring networks dynamically is slow and error-prone.
- **Use Case**: Byos Secure Cluster Edge microsegments the rack to allocate resources efficiently—eg. dedicating a segment to HPC with high bandwidth and minimal latency, while another segment isolates legacy apps with stricter access controls. Adjustments can be made on the fly without rewiring.
- **Outcome**: IT teams improve performance, reduce conflicts, and adapt quickly to changing workload demands, all within a single rack footprint.

Enable Secure Testing and Development Environments

- **Context**: A datacenter supports DevOps teams needing to test new applications or updates alongside production systems without risking interference or exposure.
- **Pain Point**: Spinning up separate physical or virtual environments is resource-intensive, and shared racks increase the chance of test traffic affecting production.
- **Use Case**: Byos Secure Cluster Edge carves out microsegments within the rack—one for production, another for testing—ensuring test workloads can't leak into or disrupt live systems. Developers can simulate real conditions securely.
- **Outcome**: Faster development cycles, reduced risk of outages, and lower costs by avoiding dedicated test racks or external cloud resources.

Reduce Network Complexity in Edge Data Centers

- **Context**: An edge datacenter (eg. in retail, manufacturing, or telecom) needs to process local data quickly while maintaining security, but space and staff are limited.
- **Pain Point**: Traditional networking gear (switches, firewalls) adds complexity, cost, and management overhead in small-scale deployments.
- **Use Case**: Byos Secure Cluster Edge integrates microsegmentation into the rack itself, creating secure zones for IoT devices, local apps, or customer data. It simplifies the network stack by handling segmentation at the appliance level.
- **Outcome**: Edge operators deploy faster, cut equipment costs, and manage security with less expertise, making edge computing viable in constrained environments.



If you'd like to learn more about Byos, visit us at byos.io

or connect with us at engage@byos.io