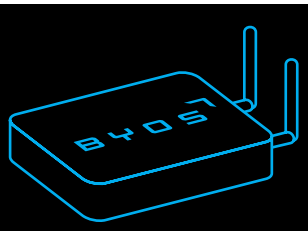
BYOS

Competitive Landscape for Byos Secure Gateway Edge



Why was the Byos Secure Gateway Edge created?

There is a renewed push towards modernizing Critical Infrastructure networks, to meet Industry 4.0 goals - increasing agility and data collection, reducing dependence on manual human labor, and ultimately increasing output. However, the threat of operational downtime from cyberattacks has never been higher.

There is a fundamental gap in protection between endpoints and the networks they connect to: endpoint and network security technologies fail to protect at the ingress/egress point of traffic to and from the endpoint, aka at the edge. This is especially true for IIoT/OT environments, where devices are often older, simpler, and running more brittle operating systems.

- Software-based endpoint protections can't typically be installed on networked production equipment and controllers/PLCs .
- Perimeter-based protections cannot protect individual endpoints on the network before an attacker gains a foothold and propagates.
- OT Network Scanning tools/products are detection-focused (ie. retroactive) and not prevention-focused.

Because of this, attackers leverage a number of tactics that many solutions are unable to protect against: Scanning/Enumerating/ Fingerprinting, Eavesdropping, Remote Access Exploits, Evil-Twin Wi-Fi, Lateral Network Infections, and DNS hijacking to name a few.

What is High Assurance Network Access?

High Assurance Network Access (HANA) asserts that the most critical or risky actions taken inside of a network should be managed using the strongest control mechanisms.

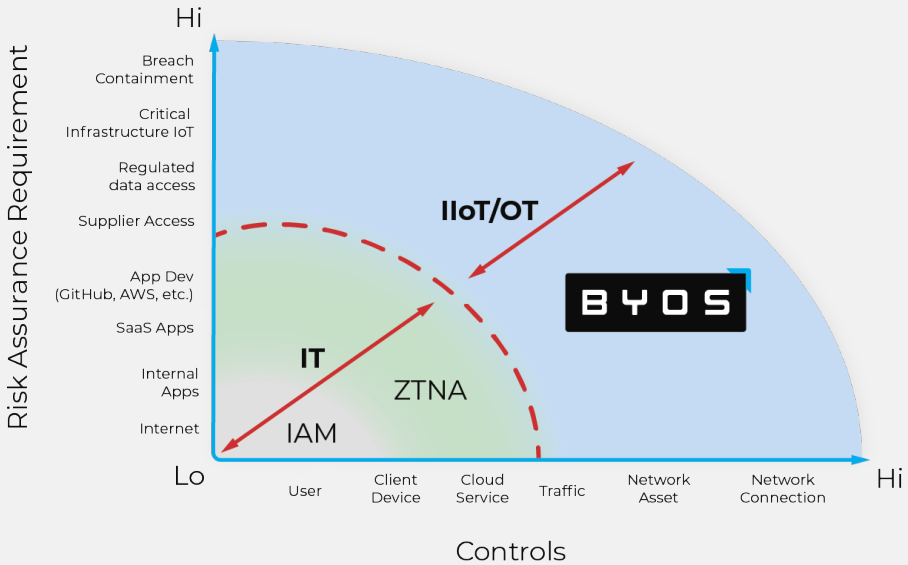
When evaluating a security posture, an administrator will first look at what controls they have available (x-axis); arranged from low control ("I cannot really control the user's behavior") to high control ("I can fully control their machine and their network connection").

They will then evaluate these controls against the different types of actions that are performed in their infrastructure (y-axis), graded from low risk assurance requirements ("The risk is low when my users are accessing google.com on the public internet") to high risk assurance requirements ("I need 100% certainty that access to my production networks is fully secure, end to end.").

When looking at what existing access solutions offer, HANA fills the gap in coverage by providing high assurance security and management of the networking assets and their network connections through edge microsegmentation.

1. Lower layer networking protection over the devices connecting from untrusted networks, and
2. Full "runtime visibility" into these devices connections and sessions.

Access Risk Management Solution Map



How does Byos fit into the stack?

Main Capabilities and Key Differentiators

Edge microsegmentation has a mix of both network and endpoint security capabilities including: segmentation, NAC, DNS + FW, policy administration, UTM, and malware protection.

Digging deeper, Byos has three unique differentiators:

1. Inbound protection from malicious networking attacks
   - » "First-hop" protection across OSI Layers 1-5 through Hardware-enforced Isolation
   - » Obfuscating the protected endpoint to become effectively invisible on the network
2. Outbound traffic protection and control
   - » Network Access Control (NAC)
   - » Route enforcement
   - » Traffic anonymization through layer 4+ data encapsulation and exit node enforcement
3. Secure Software-Defined Network (SDN) Overlay
   - » Secure remote access without endpoint exposure or packet leakage
   - » Policy-driven Layer 2, 3, and 4 access control per microsegment
   - » Invisible to both the Local Network and the Internet

What technologies does it replace?

- Traditional perimeter security and VPNs were the main technologies used for security of IIoT devices. These are the two most common technologies that organizations are now retiring in favor of more modern, perimeter-less technologies that conform with Zero Trust principles. With either of these traditional approaches, the underlying asset is still exposed to the internet and the local network - meaning it can be scanned, enumerated, fingerprinted, and ultimately exploited.
- DMZs, or VLANs, to provide traditional segmentation is not enough, since attackers will be able to easily navigate private segments once they bypass the perimeter protection.
- Likewise, IDS/IPS systems and cloud-based protections primarily focus on protecting the network perimeter, leaving the trusted assets inside vulnerable to malicious activities once connected.

What technologies does it complement?

Byos is complementary to OT Threat Detection and Vulnerability Management solutions.

- OT Threat detection and Vulnerability Management cover reconnaissance, and actions on objectives/exfiltration. Byos will cover intrusion, exploitation, privilege escalation, lateral movement, command and control

By focusing on preventing initial access all across OSI layers 1-5 and right at the edge, Byos adds true proactive security on top of active threat detection, and stops attacks before they even gain access. Combined with OT Threat Detection and Vulnerability Management solutions, gives a comprehensive multi-component shield that can both effectively prevent threats, as well as detect and isolate them to a degree that reduces the attackers ROI to meaningless levels.

Security Stack Component	Cloud/Server Segmentation Agents	Network-Based Segmentation Solutions	Byos Edge Microsegmentation
Where does it live? (or how is it deployed)	Agents installed on servers or within Instances/Containers	Network-based appliances (both physical and virtual) that sit at the perimeter of large network segments	Physical Edges deployed at the Assets to create small, protected Microsegments (Controllers, PLCs, Workstations, etc.)
Main capabilities	• Isolate and protect high-value cloud apps and databases, • Application behavior analytics • Discover application dependencies to reduce attack surface, secure critical applications, and ensure compliance • Container Security • Threat Detection and Response for Cloud and On-prem workloads • Visibility, third-party access control, and critical application ringfencing	• Network Perimeter Security (firewall, IDS/IPS) • Application Control • Threat Detection (AV, DLP, AntiSpam) • SD-WAN	Byos Secure Edge Technology • Physical Isolation • Route Enforcement • Inbound and Outbound local network protection Secure SDN Overlay • Controlled Asset Isolation • Granular Access Control • Secure Remote Management Cloud-Managed Control Plane • Policy-driven Internet Access • Tunnelized Exit Node • Byos-enforced IAM authorization
One-liner description	*"Segmentation and controls for cloud-native and on-prem workloads, to protect against cloud-based threats."*	*"Enables network traffic inspection using granular security policies, and Layer 7 inspection for network protocols and information passing through the firewall."*	*"Hardware-enforced segmentation that cloaks assets from the rest of the world, while still enabling centralized control and invisible overlay communications of distributed unmanaged assets on uncontrolled/decentralized networks."*
How are these solutions complementary?	Protection of Cloud Assets, while interacting with distributed physical assets.	Corporate network upper layer protections.	Layer 1-5 protection and control.

Why do customers choose Byos?

Byos is uniquely positioned to be the de facto standard for network security of industrial, unmanaged and IoT networks. Sitting at the edge provides many security and organizational advantages including:

- Cloaking and isolating legacy, unmanaged and industrial devices.
- Protecting and managing 3rd-party contractor devices that connect from unmanaged networks.
- Enabling secure remote management and troubleshooting of devices, and data collection from typically air-gapped devices.

Get Started

Contact us at engage@byos.io to schedule your demo today!