BYOS

Competitive Landscape for Byos Secure Endpoint Edge

Why was the Byos USB µGateway created?

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, a.k.a. at the edge:

- Software-based endpoint protections installed on the OS can be bypassed/evaded.
- Perimeter-based protections cannot protect individual endpoints on the network before an attacker gains a foothold and propagates.
- Getting centralized runtime visibility into the active sessions of distributed endpoints is cumbersome with current tools.

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 Movement, and DNS hijacking to name a few.

Byos is a new layer of protection in the security stack called **Edge Microsegmentation**; it protects against these network attacks and contains lateral movement while allowing administrators to manage and control remote endpoints. This type of solution falls in a new category called **High Assurance Network Access (HANA)**.

What is High Assurance Network Access?

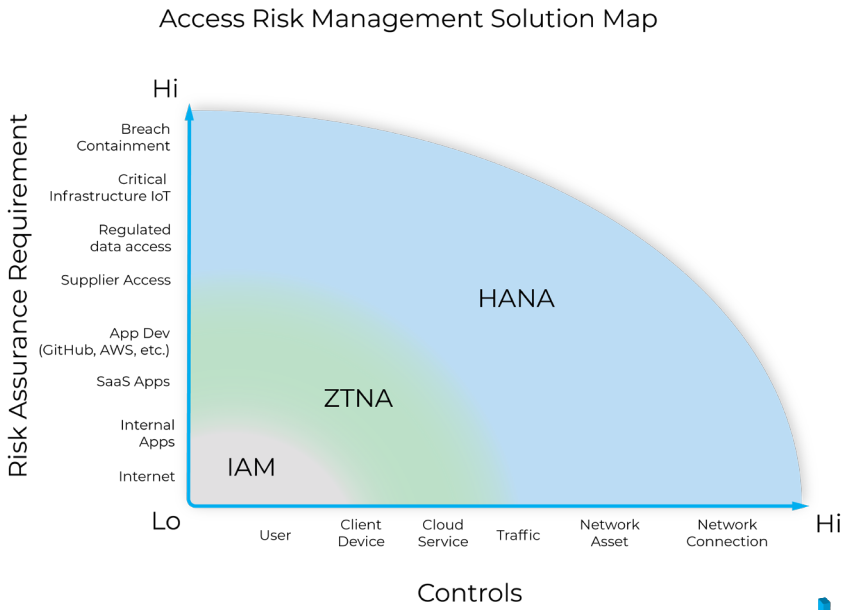
High Assurance Network Access (HANA) asserts that the most critical or risky actions taken inside of a network should be managed using the strongest control mechanisms.

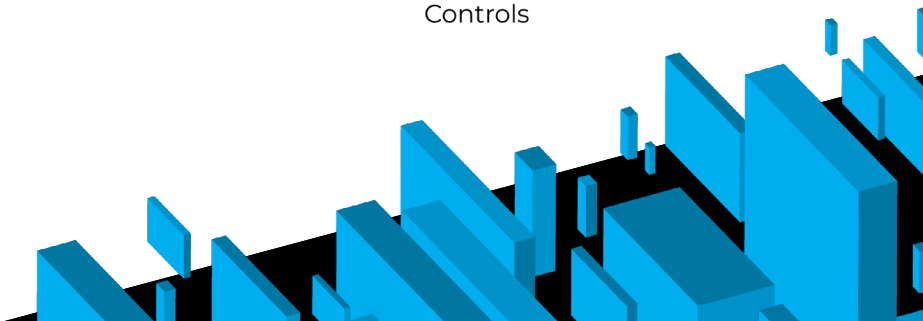
When evaluating a security posture, an administrator will first look at what controls they have available (x-axis); arranged from **low control** (*"I cannot really control the user's behaviour"*) to **high control** (*"I can fully control their machine and their network connection"*).

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:

- Lower layer networking protection over the devices connecting from untrusted networks, and
- Full "runtime visibility" into these device's connections and sessions.





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.

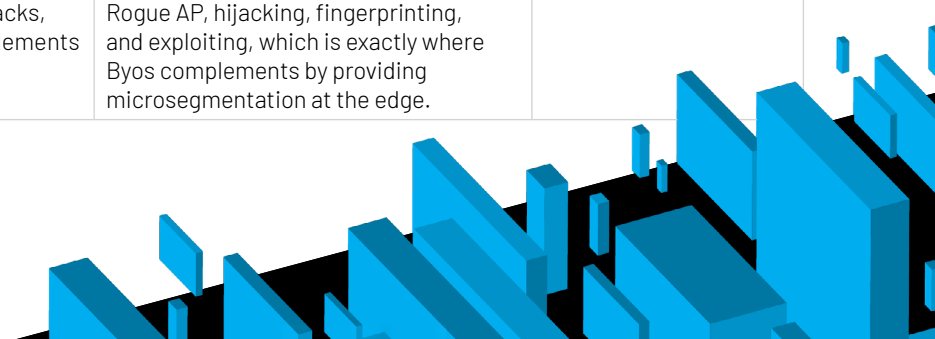
Digging deeper, Byos has three unique differentiators:

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. **Centralized Management:**
   - Policy-driven access control per microsegment
   - Byos-enforced IAM Conditional Authorization
   - Secure remote access without endpoint exposure

What technologies does Byos complement?

For a distributed, modern organization, the ideal security stack is one that combines EDR, ZTNA, SASE, and HANA technologies to deliver a full Zero Trust security architecture.

Security Stack Component	EDR	SASE/ZTNA	Byos (HANA)
Where does it live?	Installed on the Endpoint	In the cloud	At the edge of the endpoint
Main capabilities	Endpoint visibility and behavioral protections against attacks at Layers 5-7 (in the user space).	CASB, SWG, DLP, UTM, IAM, PAM, etc.	Agentless, lower layer network protection (OSI Layers 1-5) providing endpoint isolation
One-liner description	*"Protection above the OS, for security-related events such as process creation, driver loading, registry modifications, disk access, memory access, etc."*	*"Is the user allowed and able to access this resource, at this time?" and "Classic perimeter + network security, but in the cloud."*	*"Network security at the edge of the endpoint, below the OS, for protection against lateral movement."*
How are these solutions complementary?	Because EDRs are agent-based, they offer OS-layer protections like: • Anti-malware • DLP • Anti-phishing However, EDRs cannot stop attacks from reaching the endpoint, and are susceptible to bypass/evasion attacks, which is exactly where Byos complements with hardware-enforced isolation.	SASE and ZTNA provide layer 7 security processing like: • Traffic inspection • Data protection • URL filtering However, SASE and ZTNA cannot protect against local network attacks, such as Rogue AP, hijacking, fingerprinting, and exploiting, which is exactly where Byos complements by providing microsegmentation at the edge.	N/A



What technologies does Byos replace?

Enterprise security stacks are evolving because of two main drivers: the ubiquity of remote work and the widespread impacts of ransomware and large security incidents.

In the old world, traditional perimeter security and VPNs were the main technologies used for security of remote workers. These are the two most common technologies that organizations are retiring in favor of more modern, perimeter-less technologies that conform with Zero Trust principles.

What technologies does Byos integrate with?

- IAM

Byos-leveraged IAM for Conditional Authorization - The Byos µGateway becomes the authoritative signal for whether or not Identity and Access Management (IAM) solutions, like Okta, will grant permission to the user to access the desired resource - *eg. "Is John Doe using his Byos µGateway to connect to the Wi-Fi? If yes, he can access Github; if not - access is denied."*

- SIEM

All threat intelligence and relevant telemetry data can be sent to the SIEM for aggregation. Byos provides administrators with runtime visibility of active sessions for their entire fleet of devices.

Why do customers choose Byos?

Byos is uniquely positioned to be the de facto standard for network security of distributed organizations. Sitting at the edge provides many strategic security and organizational advantages including:

- Isolating employee laptops from home and public Wi-Fi networks.
- Protecting and managing 3rd-party contractor devices that connect from unmanaged networks.
- Ensuring all traffic and data originating from endpoints on unmanaged networks flows through controlled exit nodes.

Get Started

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