BYOS

Layering Additional Security onto SASE Networks

At first glance, Byos and SASE solutions might look like overlapping/competitive solutions however they are complementary, providing different layers of security.

Byos Edge Microsegmentation Technology

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*:

- Software-based protections installed on the OS are commonly bypassed/evaded, since the malware can deactivate or modify their software processes
- Network-based protections are unable to protect individual endpoints on the network *before* an attacker gains a foothold and propagates

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

Byos provides a new layer of protection in the security stack called "Edge Microsegmentation", helping to protect and eliminate lateral movement while allowing administrators to manage, and control remote endpoints.

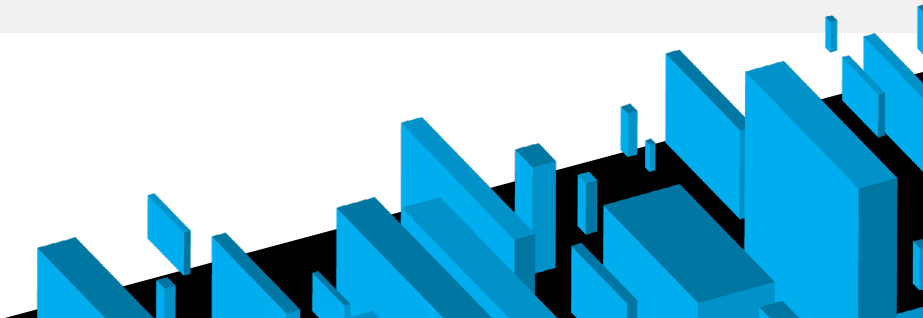
How Byos Capabilities Extend SASE Security

SASE is an improvement upon classical centralized perimeter networking and security capabilities to meet the demands of global organizations. It combines:

- Networking as a service layer to secure the data in transit
- Security as a service performing traffic inspection and access control

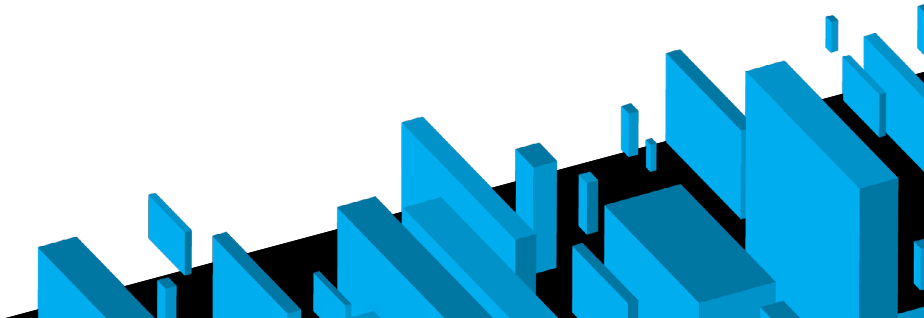
Byos adds three significant enhancements to a mature SASE deployment:

1. Byos makes all endpoints invisible to the rest of the network as well as from the internet.
   - » Devices cannot "see" the Byos-protected endpoint unless their hardware credentials plus other security authentications place it into the cloaked network. Devices cannot be discovered from the internet because the devices respond only to other microsegmented endpoints inside the Byos-protected network.
   - » Inside the Byos-protected network, Layer 3 role-based access control means that only those devices with the appropriate policy set can communicate with each other, and are permitted to know that its peer device in another microsegment even exists. And each device only responds to other devices it knows are permitted to communicate.
2. Security processing performed by the µGateway happens locally, independent of the cloud and the end user's OS. Because of this agentless and isolated approach, the protection mechanisms are unable to be modified, evaded or disabled by an attacker living within the endpoint.
3. Policy driven access controls are the mechanism that determine what communication is permitted between two devices. Byos policies enable microsegmentation in a way that enforces policies so that the absolute minimum of permissions are allowed. Because both peer devices are enforcing and adhering to the permitted policies, the communications cannot be hijacked, impersonated nor bypassed.
   - » Remote access is secured without exposing the endpoint nor a single packet to the internet.



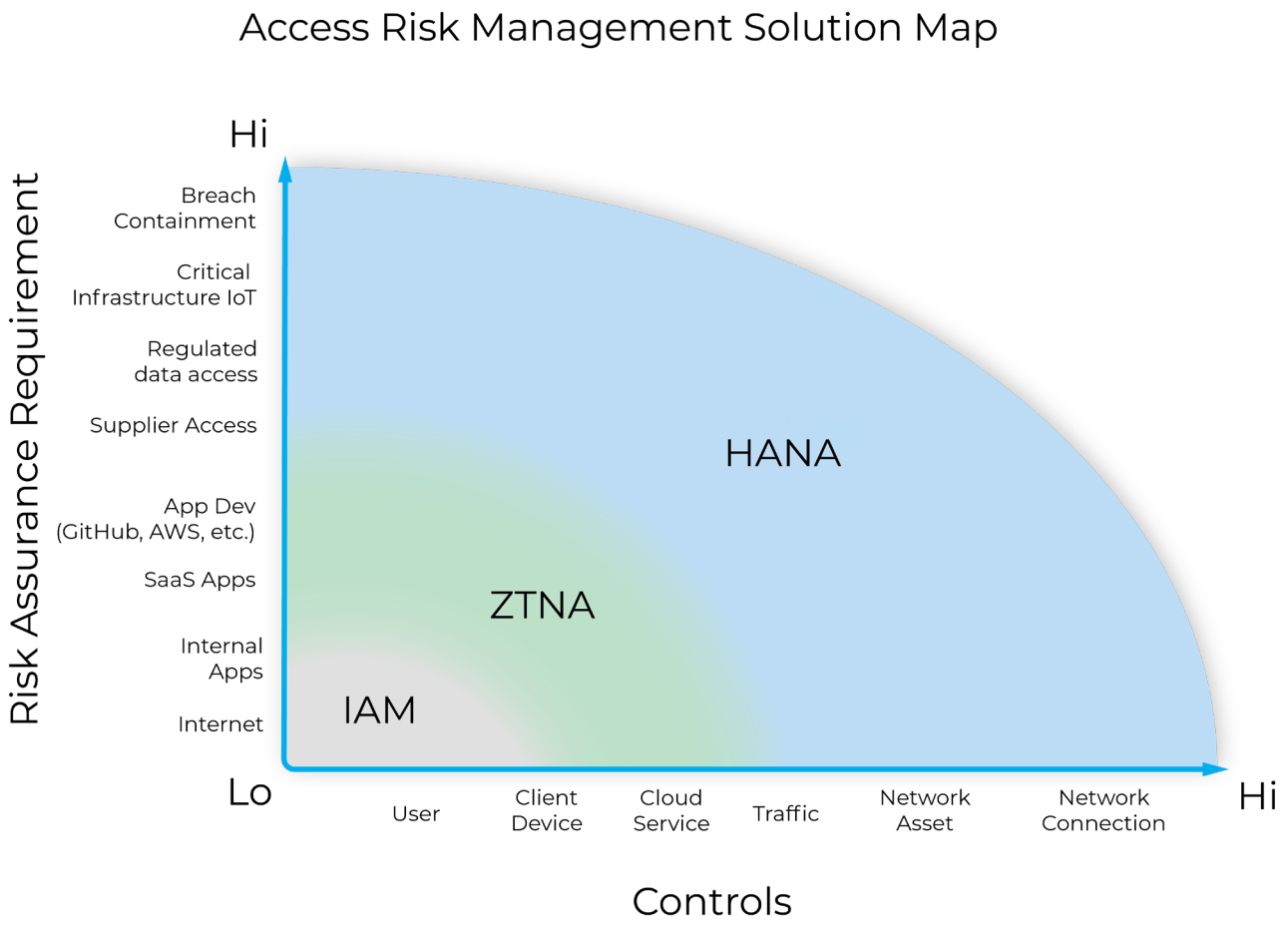
Comparison Matrix

Technology	SASE	Byos
One liner description	*"Cloud-based perimeter + network + endpoint security"*	*"Network security on the endpoint, independent of the OS"*
Where does it live?	• Security processing + management - cloud & on-prem • SASE client apps installed on the endpoints	• Security Processing - Edge of the endpoint • Management Control Plane - cloud or on-prem
Main Security Capabilities	Upper Layer Data Protection and Traffic Inspection (Layers 5-7) • Traffic is routed from the endpoint's agent to the SASE cloud, where the security is processed » DNS Security » Secure Web Gateway » Firewall • Access Control happens at Layer 7 • Cloud Access Security Broker works securing access to SaaS, PaaS, and IaaS resources • Threat Prevention • Data Loss Prevention	Lower Layer Networking Protection (Layers 1-5) • Security processing is decentralized at each edge » DNS Security » Secure Gateway Edge » Firewall • Endpoint Route Enforcement • Access Control happens at Layer 3 • Cloud Access Security Broker works securing access to SaaS, PaaS, and IaaS resources, as well as any Byos microsegment, whether on-prem or in unmanaged networks (endpoints don't need internet access) • Inbound protection from malicious networking attacks » Rogue AP Protection » ARP Poisoning Protection » Route Alteration Prevention » Gateway Identity Alterations
Summary	SASE requires internet access and secures to the entry point of the HQ/Data center/SaaS/Public Cloud, and Byos complements it by taking protection and access control a step further to the microsegment. Endpoints do not have to be exposed to the internet, but are still able to communicate with said resources, regardless of the network posture or hostility. Byos devices do not have to ask the cloud for permission to protect the endpoint; they act before the fact (inbound and outbound), and have no internet dependency. Byos applies access controls at Layer 3 (instead of at Layer 7, like SASE) providing true quarantine, isolation, and block capabilities. When Byos blocks access, the endpoint literally does not know how to communicate to the outside world. And an outsider attacker simply does not have a valid network route to get to the endpoint. In other words, SASE will get you securely to the front door of the house, and Byos will take you to the specific room in that house that you're allowed to be in.	



What is High Assurance Network Access?

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



Basic access operations within today's networks are sufficiently secured by existing IAM and ZTNA technologies. As an example, managing access to a cloud-based SaaS app (action) using a cloud service (control mechanism) is one covered by existing ZTNA solutions.

However, when you have actions like containing a breach (quarantining endpoints) or accessing critical infrastructure IoT devices remotely, and legacy and unmanaged BYOD devices, ZTNA doesn't provide enough coverage over the control mechanisms. This is where HANA fills the gap - Providing high assurance security and management of the networking assets and their network connections through edge microsegmentation.