INVISINET
Where Zero Trust Begins

Solutions Brief: Micro-Segmentation

Micro-Segmentation and Zero Trust: Moving from Perimeter Defenses to Identity Aware Software Defined Perimeters

Due to the proliferation of programmatic scanning and attacks by AI, old modes of static network perimeter defense simply don't work. The reason for the basic three-network segmentation was to create a layered defense and multiple logins to protect the most secured assets on a network. This has become several orders of magnitude more important in modern networks with identity-driven micro-segmentation. On average it takes an attacker over 150 days to burn through layers of defense to get to the data they are trying to exfiltrate. They do this by carefully stealing credentials, exploiting known vulnerabilities of that layer of defense, and erasing their tracks. Unfortunately, the average dwell time before detection is 204 days. The purpose of micro-segmentation is to force a bad actor to move laterally between segments, because that is the best opportunity for your intrusion prevention system to flag an anomaly and detect them. If you can find and eliminate the bad actor by day 100, you can reduce the cost of mitigating the compromise by two-thirds, and with the average breach costing $4.9M, that is a lot of money. More importantly you probably have kept them out of the data you are trying to protect and avoid a reportable event to regulators.

Invisinet Micro-segmentation: Adaptive, Secure, Unmatched

Identity based Micro-segmentation is a cornerstone of Zero Trust architecture. The micro zones act as digital checkpoints, verifying that users and requests are legitimate, shrinking the attack surface for the bad actor and forcing them to do a lot more work to penetrate the security. Invisinet takes this two steps further by first embedding tokenized identity in the IP packets themselves as a hidden extra layer of credential check between segments and second blocking any unauthorized user frame scanning any segment of your network externally or internally. These combined features make if extremely difficult for attackers to get past the front door or remain undetected for long if they do. By taking away their ability to recon the network both externally and internally, you completely disrupt their attack.

Why Traditional Perimeters Fail

The outdated reliance on network perimeters has repeatedly failed against modern cyber threats. Organizations today face insider threats, sophisticated social engineering attacks, and vulnerabilities introduced by remote work and cloud adoption. A perimeter-only approach neglects these internal risks, making it easy for attackers with stolen credentials to move laterally, undetected, across the entire system.

Traditional enterprise networks were built on implicit trust, with minimal access controls and a focus on perimeter security. However, the rise of cloud computing, SaaS, IoT, and a mobile workforce has eroded the concept of a single, trusted perimeter. Attackers now exploit this by moving laterally within networks once inside. As a result, modern security demands a Zero Trust approach—where no device, user, or network segment is trusted by default, and continuous verification of identity and context is essential.

Why Invisinet Stands Above

- **Identity-Driven Security:** Unlike traditional methods that rely on static firewall rules or IP-based segmentation—which can be spoofed—Invisinet not only introduces multifactor authentication through Active Directory and X.509 certificates, but enforces miliary-grade access policies based on user identity, device context, and real-time risk assessment to impose real-time adaptive enforcement that blocks unauthorized access at the earliest possible moment via the patented **First Packet Authentication ™** technology.
- **Dynamic, Automated, Real-Time Protection:** Instead of static VLAN and firewall rules, Invisinet dynamically adapts segmentation based on user behavior, device location, and risk levels—blocking lateral movement in real-time.
- **Zero-Day Vulnerabilities Mitigation:** Invisinet detects anomalies instantly, proactively blocking suspicious activities and adapting security measures without requiring updates.
- **True Zero Trust:** Every communication between workloads, devices, and users is continuously verified, eliminating implicit trust and preventing attackers from moving laterally even if they breach one segment of the network.
- **Protection Against Credential Theft:** Invisinet continuously monitors behavior, enforcing role-based access, and blocking unauthorized logins or unusual activity like off-hour access attempts.
- **Moving Target Defense (MTD):** By dynamically shifting attack surfaces, Invisinet amplifies attacker workload, minimizes exploitable vulnerabilities, and enhances overall security resilience by making it exponentially harder for attackers to exploit vulnerabilities.
- **Regulatory Compliance:** Invisinet aligns with NIST 800-53, SP 800-207, and other Zero Trust frameworks, continuously adapting security to meet compliance requirements.
- **Fast, Cost-Effective Implementation:** Unlike traditional micro-segmentation solutions that rely on complex VLANs, ACLs, and static manual configurations, Invisinet automates much

of it through its dynamic approach. Using the Sigma-Cloud platform, Invisinet's Infrastructure-as-Code provides simple click implementation for not only multi-cloud networks but especially in legacy OT environments.

Invisinet and First Packet Authentication – A Lightweight Zero Trust SDP

Invisinet is taking micro-segmentation and Zero Trust to the next level. **First Packet Authentication (FPA)** technology – exclusively delivered by Invisinet -- operates as an identity aware **policy enforcement point** in the data plane. FPA inserts a cryptographically generated, single-use identity token into the very first packet of a connection attempt; if the token is not valid or the requester is not authorized, the packet is silently dropped, and the target asset does not respond. Because the enforcement happens before a TCP or TLS handshake is completed, FPA prevents reconnaissance scans from discovering services and stops unauthorized connections before they start. When the identity token is valid, FPA consults Invisinet's policy engine—which continuously evaluates user identity, device posture and contextual attributes—to decide whether to allow the connection. Approved flows are then permitted only to the specific port and application and for a limited time. This dynamic, per connection enforcement embodies the principles of software defined perimeter and micro-segmentation while maintaining performance and user transparency.

Unlike traditional VPNs and complex network segmentation projects, Invisinet's solution is designed to be lightweight and easy to deploy. It overlays existing networks without requiring changes to routing or IP addressing and integrates with identity providers to make policy decisions based on who the user is and what they are trying to access. By cloaking services and enforcing least privilege access on the first packet, Invisinet reduces the attack surface and removes the need for users to connect to a broad "trusted" network. Its micro-segmentation is therefore delivered as part of a full **Zero Trust Network Access** (ZTNA) platform that works across on premises, cloud and IoT environments.

About Invisinet

Invisinet Technologies (https://www.invisinet.com), a next-generation leader in Zero Trust identity and software defined perimeter, is a cybersecurity technology company specializing in innovative solutions that protect network infrastructure and critical assets from advanced threats. Invisinet's Zero Trust software enables cloaking of network assets and enforcement of identity-based access through First Packet Authentication ™, as well as granular identity-based micro-segmentation. Originally developed for the US Department of Defense and making its way to the approved product list in 2018, Invisinet is now available in the enterprise space. The platform supports IoT devices, legacy systems and modern cloud workloads alike, making it a fit for industries such as manufacturing, healthcare, energy and government where downtime and complexity are unacceptable. With more than 15 patents and FIPS 140-2 certification, Invisinet continues to develop solutions to address the evolving advancements of cyber-attacks

Request a Demo

If you are interested in seeing how Invisinet's First Packet Authentication and Software Defined Perimeter could simplify your journey to Zero Trust, we invite you to schedule a live demonstration. Our regional sales and engineering teams and partners are available to discuss your requirements; show the platform in action and help you plan a phased adoption of micro-segmentation. (info@invisinet.com)