CHEAT SHEET:

Building Cyber Resilience with a Closed-by-Default Architecture:

5 Best Practices to Reduce Attack Surface and Shrink Blast Radius

As attackers leverage AI-accelerated techniques to achieve impossibly fast breakout times and weaponize the emerging agentic attack surface to subvert traditional security strategies, the only reliable advantage for defenders is proactive resilience: **reducing the attack surface and limiting how far adversaries can move when breaches inevitably occur.**

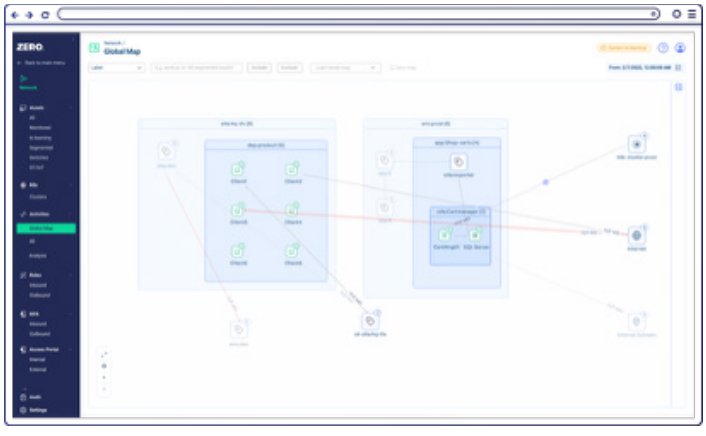
Rather than investing in more faithful detection or faster response, security teams can ensure breaches stay isolated before the first alert fires by focusing on five interconnected priorities.

1. Gain Comprehensive Network Visibility
2. Remove Unnecessary Access Paths and Close Unused Ports
3. Implement Identity-Based Microsegmentation
4. Enforce Just-in-Time MFA for Privileged Access
5. Dynamically Adapt Policies with Deterministic Automation

01. Gain Comprehensive Network Visibility to Identify Risk Exposure

Before controls can meaningfully reduce risk exposure, security teams need a complete, real-time view of what's happening in the network – every asset, identity, and active communication path. This goes beyond asset inventories and firewall logs; the goal is to uncover previously hidden vulnerabilities, like service account sprawl, shadow AI, overly permissive third-party access, or risky protocols that remain statically open.

By observing actual traffic flows across the environment, security teams gain an up-to-date picture of the organization's overall attack surface and where internal reachability exceeds operational need, enabling proactive risk reduction and providing a baseline for measuring improvement.



02. Remove Unnecessary Access Paths and Close Unused Ports to Reduce Attack Surface

Most networks carry significant trust and reachability that exist for historical, operational, or convenience reasons, not because of an active, defined business purpose. In turn, the fastest path to reducing attack surface and shrinking blast radius is simply closing what doesn't need to be open.

By leveraging network behavior insights gained from comprehensive visibility and learning, security teams can confidently pursue a closed-by-default architecture – systematically closing unnecessary communication pathways and open ports without impacting legitimate traffic.

03. Implement Identity-Based Microsegmentation to Structurally Constrain Blast Radius

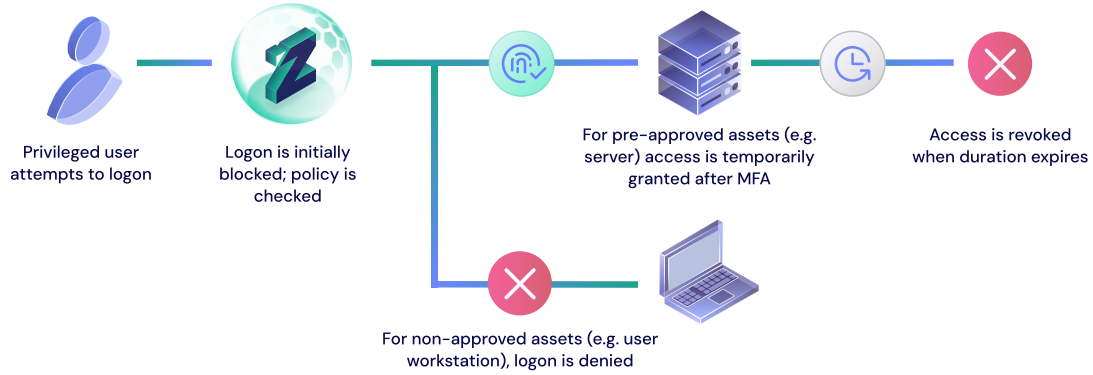
The vehicle for enforcing a closed-by-default architecture is comprehensive microsegmentation where identity governs reachability at the network layer. Access policies follow the identity (of users, devices, or applications) through the network, meaning there are no hidden gaps where an attacker with stolen credentials can slip through.

In practice, this means every connection is verified and intentional, lateral movement paths are closed by default, and infrastructure is effectively invisible to unauthorized users. By tightly coupling identity and network enforcement, security teams effectively harden against the most common attack vectors, proactively limiting the potential scope of a breach.

04. Enforce Just-in-Time MFA for Privileged Access

Always-on privileged access is a significant blast radius amplifier. If admin credentials provide 24/7 privileged access without additional verification, they provide a frictionless path to the highest value targets in the environment. Elevated permissions should be the exception – not the rule.

By enforcing just-in-time (JIT) MFA verification for all privileged activity, security teams limit privileged access to a defined window; once that window expires, enhanced permissions are automatically revoked, but operational friction remains minimal. Critically, applying MFA at the network layer allows organizations to secure risky ports and protocols, OT/IoT devices, databases, legacy apps, and other non-SaaS assets that remain uncovered by traditional application-layer MFA.



05. Dynamically Adapt Policies with Deterministic, Human-on-the-Loop Automation

Over time, networks change and exceptions accumulate; when policy maintenance is handled manually, privilege creep and policy drift are almost inevitable, creating a gap between documented access controls and real-world permissions. Deterministic automation closes the gap.

Rather than relying on security teams to manually update policies as environments evolve, a deterministic automation engine that maintains persistent visibility into network behavior can maintain up-to-date knowledge on what access is legitimate, propose policy updates, simulate enforcement before it goes live, and apply changes with minimal effort or oversight, but while keeping a human on the loop.

Contain the Blast and Strengthen Cyber Resilience with Zero Networks

Zero Networks proactively minimizes the impact of any cyberattack with automated, identity-based microsegmentation.

How It Works

Zero delivers always-current network visibility to map and control your organization's attack surface, powering deterministic enforcement to minimize blast radius in real time – without adding operational complexity.

Granular identity-based access controls and segmentation boundaries limit internal reachability to least privilege, while JIT network-layer MFA ensures connections are verified before privileged access is temporarily granted.

The result is a containment-first architecture designed to keep critical operations running, even when cyber incidents occur.

See how Zero Networks unlocks a proactive security posture, making threat containment a built-in feature for cyber resilient orgs.

Request a Demo→

ZERO. Networks