

NETWORK SEGMENTATION & MICROSEGMENTATION.



A flat network lets one compromised device reach everything else — **microsegmentation contains the blast radius so a breach cannot spread into the next zone.**

- VLAN SEGMENTATION
- MICROSEGMENTATION
- ZERO TRUST ZONING
- LATERAL MOVEMENT CONTAINMENT

01 THE MECHANISM

VLAN Segmentation
Dividing a network into isolated broadcast domains using **switch-level VLAN tagging**.

Microsegmentation
Applying granular, **workload-level policies** that control traffic between individual assets.

Zero Trust Zoning
Requiring every east-west connection to be **explicitly authorized, not just perimeter-trusted**.

02 THE FLOW

The Segmented Network CONTAINED

1

A workload in one zone attempts to reach another, **triggering a policy check first**.

2

The policy evaluates identity, workload role, and destination **before allowing east-west traffic**.

3

An attacker who compromises one zone **cannot reach adjacent zones without a new, authorized path**.

The Flat Network EXPOSED

1

Every device on the network can reach **every other device by default**.

2

An attacker who compromises one endpoint **immediately gains network-level access to everything else**.

3

Lateral movement continues unchecked **until the entire environment is compromised**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
VLAN Segmentation	Separates broadcast domains at the switch layer to reduce network-wide exposure.
Microsegmentation	Enforces workload-to-workload policy at the host or hypervisor layer, independent of topology.
Zero Trust Zoning	Treats every zone boundary as untrusted, requiring authentication and authorization at each hop.
Lateral Movement Containment	Limits how far an attacker can travel across the network after an initial compromise.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Flat, Single Broadcast Domain	No	Any compromised device can reach every other system on the network.
VLANs Without Access Control Lists	No	Separates traffic visually but still allows unrestricted routing between segments.
Perimeter Firewall Only	No	Controls north-south traffic but ignores east-west movement inside the network.
Segmentation Without Identity Context	No	Blocks by IP or subnet but cannot distinguish a legitimate workload from a compromised one.
Microsegmentation + Zero Trust + Identity Policy	Yes	Enforces least-privilege access between every workload, regardless of network location.

NETWORK SEGMENTATION.

ZONE · DENY · CONTAIN

05 PROGRAM OPERATIONS

Flat networks turn one compromise into a full breach. Without segmentation, an attacker who lands anywhere can reach everywhere.

Microsegmentation moves the control point to the workload. Policy travels with the asset instead of depending on network location.

VLANs alone do not stop lateral movement. Without enforced access control lists, VLAN boundaries are cosmetic, not protective.

Segmentation policy must be tested, not just deployed. Untested rules either block legitimate traffic or leave gaps attackers can find.

06 CONTROL MAPPING

NIST SP 800-207

Zero trust architecture guidance for eliminating implicit trust between network zones.

PCI DSS

Network segmentation requirements for isolating cardholder data environments.

CIS CONTROLS V8

Network infrastructure management safeguards for east-west traffic control.

NIST SP 800-41

Firewall and boundary protection guidance for zone-based access control.

07 WHAT THIS DOES NOT SOLVE

Overly Permissive Policy Rules

A microsegmentation rule left too broad still allows the exact lateral movement it was built to stop.

Unmanaged or Shadow Devices

Devices outside policy enforcement bypass segmentation entirely, whether known to IT or not.

Compromised Identity Within a Zone

Valid credentials inside an authorized zone still grant access the policy was designed to allow.

Segmentation Rule Sprawl

Thousands of granular rules become impossible to audit or verify are still correct.

08 MYTHS VS. REALITY

MYTH	REALITY
"VLANs are the same thing as microsegmentation."	VLANs separate broadcast domains; microsegmentation enforces policy at the individual workload.
MYTH	REALITY
"A strong perimeter firewall makes internal segmentation optional."	Perimeter defenses do nothing once an attacker is already inside the network.
MYTH	REALITY
"Segmenting the network once is a completed project."	New workloads and cloud migrations constantly shift what needs to be re-segmented.
MYTH	REALITY
"More segments always means better security."	Overly granular segmentation without governance creates unauditable rule sprawl.
MYTH	REALITY
"Microsegmentation only applies to data centers."	Cloud workloads, containers, and remote endpoints all need the same workload-level policy.

09 SPEAK THE PROGRAM — KEY TERMS

MICROSEGMENTATION

Granular, **workload-level policy enforcement** independent of network topology or subnet.

EAST-WEST TRAFFIC

Network traffic **moving laterally between internal systems**, rather than in or out of the perimeter.

ZERO TRUST ARCHITECTURE

A model requiring **verification of every connection** regardless of network location.

BLAST RADIUS

The extent of systems an attacker can **reach after an initial compromise**.

VLAN

A virtual LAN that **logically separates broadcast domains** on shared physical switching hardware.

LATERAL MOVEMENT

An attacker's **progression from an initial foothold** to other systems on the network.

SOURCES: NIST 800-207 · PCI DSS · CIS · NIST 800-41

NETWORK SEGMENTATION & MICROSEGMENTATION · FIELD REFERENCE