DATA SHEET

Zscaler Microsegmentation

Challenges with legacy microsegmentation

Many enterprises rely on legacy segmentation architectures to secure their workloads. These architectures are inadequate—they are complex to deploy, increase the attack surface, amplify lateral movement, and increase operational cost.

- Getting an accurate asset inventory is a challenge, specifically for resources in the cloud, where they are brought up and torn down dynamically.
- Solutions such as firewalls extend the network to workloads and servers, amplifying lateral movement risks.
- Patchworks of virtual appliances, operational tools, and nonstandard policies introduce known and unknown gaps in security coverage, increasing risk.
- Custom third-party segmentation tools are complex to deploy, and enforcement of corporate security policies is inconsistent.

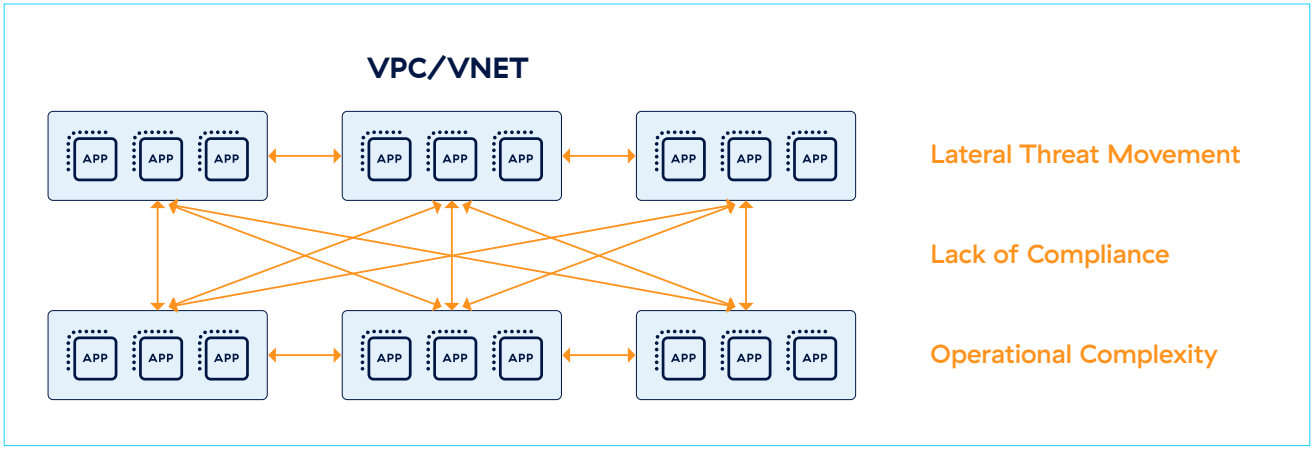

Figure 1: Legacy workload protection architectures are inadequate to stop lateral threat movement

Extend zero trust architecture to segment workloads in public clouds and on-premises data centers

Host-based microsegmentation addresses these challenges by breaking down the network into smaller, more controllable segments. It enforces security rules on each segment, granting only essential access. This way, if one segment is breached, the rest of the network stays secure. With cyberthreats growing more advanced, it's evident that basic perimeter defenses can't stop these clever attacks anymore.

Zscaler Microsegmentation provides:

Real-time asset discovery and visibility: Get inventory of assets across your infrastructure.

- Discover assets in near-real time. Get an inventory of assets based on user-defined tags, cloud attributes (VPC/VNET), or networking objects (IP/subnet).
- Get visibility into resources across multiple public clouds, data centers, and co-locations in one console.

Automated policy recommendation: Ensure all assets are covered by a security policy.

- Get policy recommendations to segment workflows based on traffic flow analysis.
- Receive proactive policy suggestions to cover resources that are not segmented.

Granular policy enforcement: Stop lateral threat movement.

- Enforce controls at the host level to limit access.
- Achieve consistent security policy across resources in data centers and public cloud.

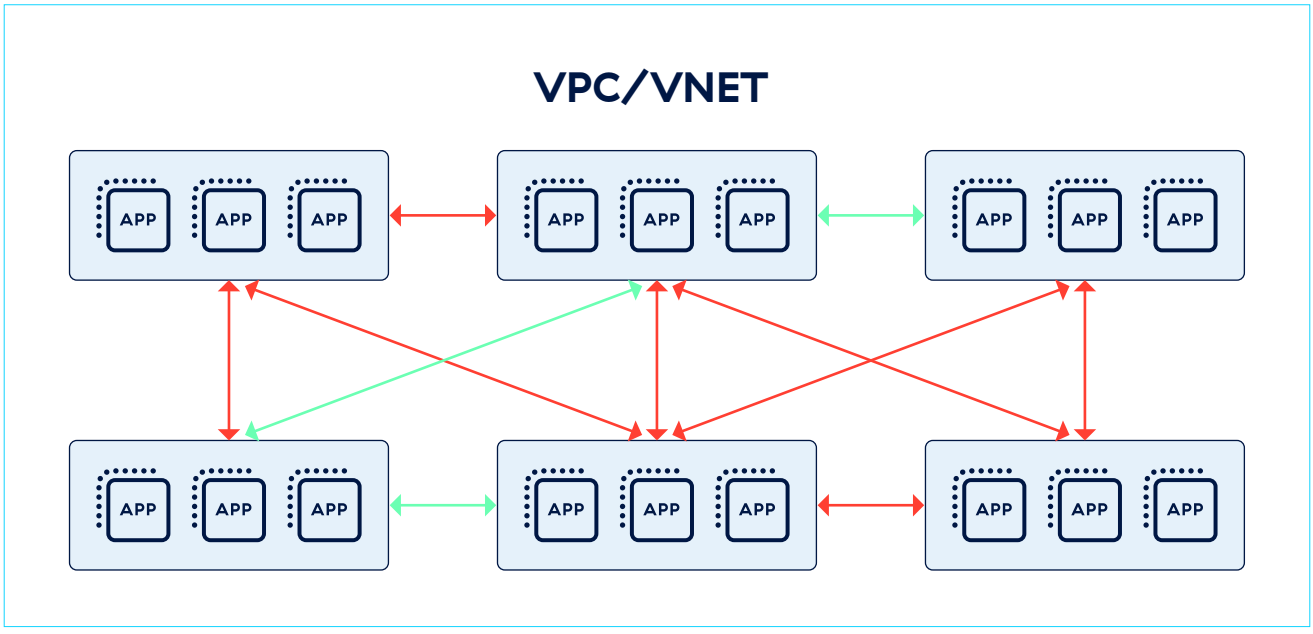

Figure 2: Zscaler Microsegmentation delivers zero trust-based, host-based segmentation

Zscaler Microsegmentation Capabilities

FEATURE	DETAILS
Public Cloud and On-Premises Coverage	Secure workloads in AWS, Microsoft Azure, with additional support for on-premises data center servers.
Host Inventory	Gain visibility into your cloud workloads, including host details, cloud environment, and user-defined tags.
Flow Inventory	Gain granular visibility of flows, including 5-tuple details, application name, and application path.
Application Map	Get an interactive map of matched flows between application resources in the environment.
Resource Policies	Create and enforce policies between your application resources.
Application Zones	Control span of the policy rules based on Application Zones or Environments.
Simplified Agent Upgrades	Upgrade Zscaler Microsegmentation agents by groups using version profiles.
Analytics Dashboard	Analytics dashboards including Top N resources as Initiators, Receivers, Flows to Internet based on observed flow logs.
Broad Platform Support	Lightweight agents can be installed on common operating systems, including Windows and Linux.
Log Streaming	Consolidate logs from all workloads and servers, globally, into a central repository determined by your organization, with Zscaler Log Streaming Service. Administrators can view and mine traffic log data from workloads in real time.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com