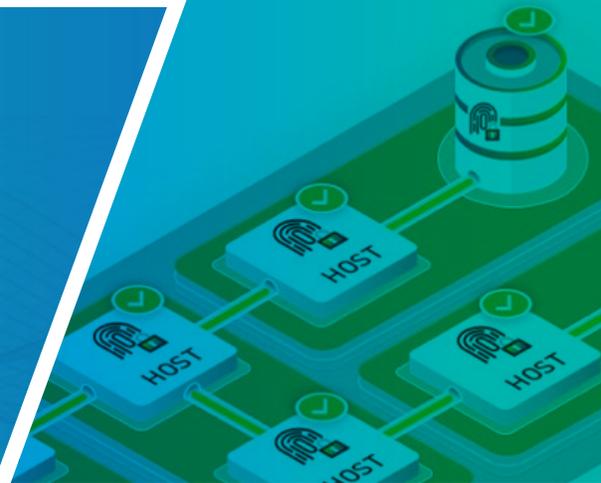


ZSCALER™ WORKLOAD SEGMENTATION

One-Click Zero Trust

Automated Microsegmentation for Public Clouds and Data Centers



Microsegmentation that's impossibly simple

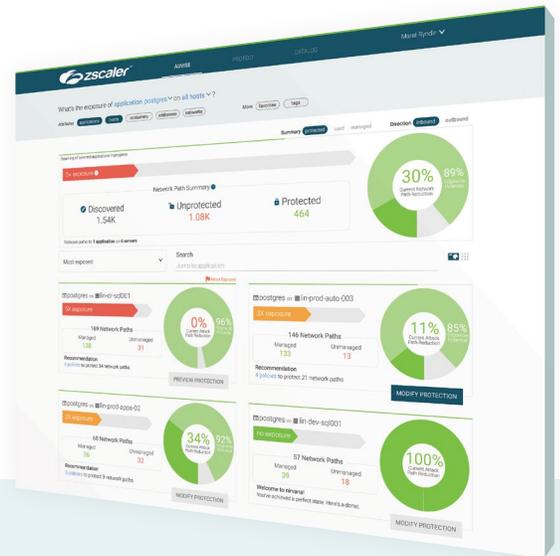
Cyberthreats need attack paths to reach vulnerable targets. The most effective way to reduce the network attack surface is segmentation, and experts agree that microsegmentation is a core protection strategy for workloads. However, the time required, complexity, and cost of implementing segmentation has historically outweighed the security benefit.

Not anymore.

Zscaler Workload Segmentation is a new way to microsegment your environment. It's impossibly simple and all it takes is one click. Reduce risk and erase operational effort by allowing Zscaler Workload Segmentation to reveal risk and apply identity-based protection to your workloads, without any architectural changes to your networks, and no reboots. Zscaler's Workload Segmentation software identity-based model provides gap-free protection with policies that automatically adapt to the environment in which they're running. Eliminating your network attack surface has never been simpler.

Zscaler Workload Segmentation Value

- Provides full visibility into east-west network communications
- Patented identity-based policies that adapt to your dynamic environment
- Agent-based protection for maximum security and performance
- Effortlessly optimizes policies for risk reduction and operational ease
- Provable return on your security investment

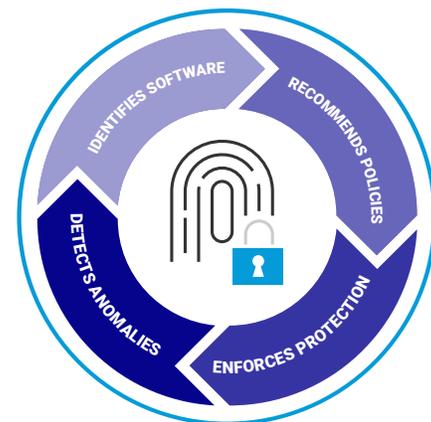


“...at some point, Zscaler Workload Segmentation could be deployed in every company in the world.”

Benefits of Application-Aware Control

Cloud and data center networks are full of data that's attractive to cybercriminals. Despite the strength of your perimeter controls, cybercriminals can access your network through phishing or some other form of social engineering. With a traditional network-based security strategy, once an attacker has stolen credentials or exploited a vulnerability to gain access to the network, they can "feed off the land" — introduce malware and move laterally inside trusted network communication paths to gain unauthorized access to critical applications. Network compromise can be highly disruptive, causing far-reaching financial, reputational, and operational damage. To prevent unauthorized east-west communications, organizations need security controls to center on the *verified identity of approved applications*.

Zscaler Workload Segmentation allows businesses to become application aware and to protect any network from application compromise with zero trust security controls based on the cryptographic identity of communicating software.



Embrace a Zero Trust Approach

Zscaler's Workload Segmentation zero trust, workload identity-based approach abandons the traditional security model of allowing application communication based on trusted IP addresses, ports, and protocols. Our zero trust model treats internal communications like the internet: potentially hostile and filled with threats. Only applications and services verified by their cryptographic identity are allowed to send and receive communication—resulting in stronger security that works wherever your applications do.

Patented Identity-Based Auto-Segmentation

Legacy microsegmentation involves multiple steps that can take months. Zscaler Workload Segmentation microsegmentation happens in mere minutes—with just one click. From asset inventory to mapping data flows to deploying policies for enforcement, our microsegmentation is quick and simple.

Zscaler Workload Segmentation protects critical data and applications in the hybrid cloud through a fundamentally new control plane: software identity. All software in an Zscaler Workload Segmentation-managed environment is fingerprinted using a combination of cryptographic identity attributes. Software identity is the basis for every access control decision. Per our zero trust model, if software can't be verified, it can't communicate, regardless of previous permissions. This ensures the strongest level of protection for your workloads, independent of network changes.

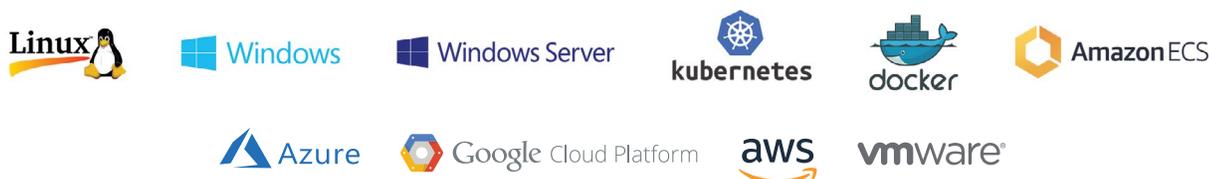
Protecting Newly Introduced Applications with Auto Re-Segmentation

While Auto-Segmentation is ideal for speeding up initial deployment of microsegmentation, it is equally important to ensure newly introduced applications are also protected. These new applications may have entirely new communication pathways and could also have interactions with existing application services—all of which needs to be protected. Zscaler Workload Segmentation makes protecting these new applications impossibly simple with Auto Re-Segmentation, achieved with one click. Zscaler Workload Segmentation builds on your existing segmentation and recommends new or modified policies to cover the new application communications, all achieved with one click. Together, Auto-Segmentation and Auto Re-Segmentation ensure that your dynamic environment is always secured.

Centralized Management for Your Multi-Cloud, Hybrid Cloud Environments

Zscaler Workload Segmentation provides the broadest support across all environments, whether it is bare metal on premises, virtualized private cloud, the public cloud, or any combination thereof. Environments can be static or highly dynamic. Zscaler Workload Segmentation supports 10 distributions of Linux (with over 800 patch levels dating back to 2.6), Windows 7 onwards, and any Windows Server operating systems. Supported container environments supported include Kubernetes, Docker, and AWS Elastic Container Service (ECS).

Zscaler’s Workload Segmentation continuously adaptive platform and products are API-driven. Zscaler Workload Segmentation can integrate with existing security tools and DevOps processes, enabling one-click auto-segmentation.



Zscaler Workload Segmentation Use Cases

 <p>ZERO TRUST FOR CLOUD WORKLOAD PROTECTION</p> <p>Protect your business-critical applications across cloud environments from one central platform.</p>	 <p>ZERO TRUST MICROSEGMENTATION FOR COMPLIANCE</p> <p>Segment applications into “secure zones” to see and stop compliance violations before they happen.</p>	 <p>DATA FLOW MAPPING FOR VISIBILITY</p> <p>Visualize your application topology and see when changes occur.</p>	 <p>CONTAINER SECURITY</p> <p>Protect applications in ephemeral production environments without disrupting the CI/CD workflow.</p>	 <p>EVENT CORRELATION AND SECURITY MONITORING</p> <p>Feed application communication logs into your SIEM, enabling remediation prioritization.</p>
---	--	--	--	--

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.

