DATA SHEET

ZSCALER WORKLOAD SEGMENTATION

1-Click Zero Trust

Automated Microsegmentation For Public Clouds And Datacenters

Microsegmentation that's impossibly simple

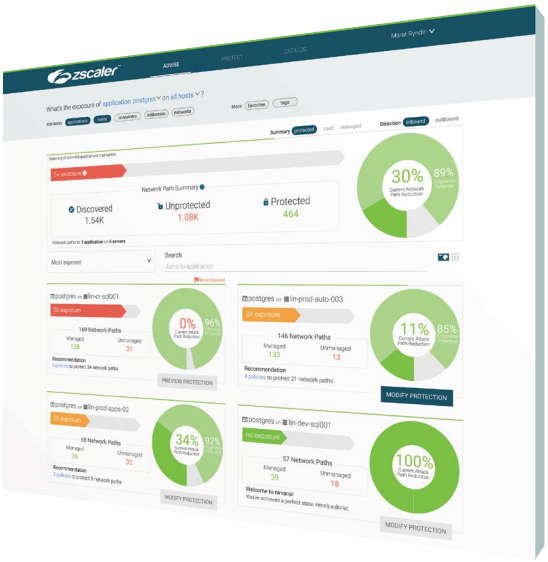
Cyber threats need attack paths to reach vulnerable targets. The most effective way to reduce the network attack surface is segmentation. Experts agree that microsegmentation is a core protection strategy for workloads, however, the time required, complexity, and cost of implementing segmentation has 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."
>
> goulston&storrs

Benefits of Application-Aware Control

Cloud and data center networks are full of data that's attractive to cyber criminals. Despite the strength of your perimeter controls, cyber criminals 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 also 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.

This new methodology means that security control adapts to any environment—with fewer policies to manage. Zscaler Workload Segmentation zero trust auto-segmentation provides stronger, simpler, scalable protection for hybrid clouds with six differentiating attributes:

Policies built automatically

Risk is reduced through policy compression

Security outcomes are provable

Software identity verified through cryptographic attributes

Segments adapt to accommodate application updates and changes

Security monitoring tools are enriched with app data

Zero Trust Identity

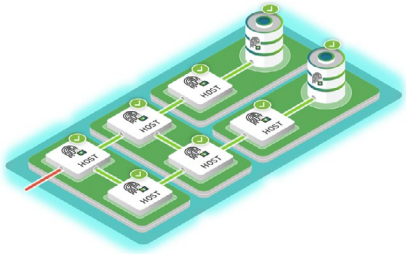
The technology that drives Zscaler's Workload Segmentation automated microsegmentation is based on zero trust identity (ZTID). Identity attributes that comprise a workload's identity include the SHA256 hash, fuzzy hash, executable signing, PE header values, UID, CPU serial numbers, provisioned host name, and more. Each unique identity informs the machine learning that builds recommended policies and is used for access control decisions. Because Zscaler Workload Segmentation policies are zero trust, only software that can be verified by its ZTID is allowed to communicate on your networks, creating a more secure yet operationally efficient network.

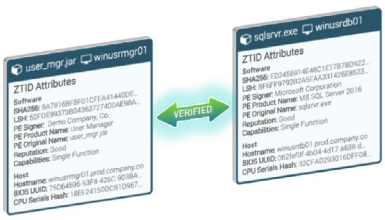
Simpler for operations

Instantly microsegment your environment—with one click. Your business applications are automatically protected and operational. No network changes required. No need to manually build or update a single policy. And lengthy deployment schedules are history.

Stronger for security

Define microsegmentation boundaries based on interdependencies of communicating software—not IP address. Prevent malware propagation and abuse of admin tools by verifying software identity to authorize communications in your cloud and data center, and ensure that only valid business applications communicate.





Scalable for DevOps

As your workloads are deployed, guarantee they always have the required access for smooth business operations. As your environment auto-scales, Zscaler Workload Segmentation policies adapt automatically across VMs and Kubernetes containers, on premises, or in the public cloud.

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 1-click auto-segmentation.

Linux Windows Windows Server kubernetes docker Amazon ECS

Azure Google Cloud Platform aws vmware

Zscaler Workload Segmentation Zero Trust Segmentation Use Cases

ZERO TRUST FOR CLOUD WORKLOAD PROTECTION
Protect your business-critical applications across cloud environments from one central platform.

ZERO TRUST MICROSEGMENTATION FOR COMPLIANCE
Segment applications into "secure zones" to see and stop compliance violations before they happen.

DATA FLOW MAPPING FOR VISIBILITY
Visualize your application topology and see when changes occur.

CONTAINER SECURITY
Protect applications in ephemeral production environments without disrupting the CI/CD workflow.

EVENT CORRELATION AND SECURITY MONITORING
Feed application communication logs into your SIEM, enabling remediation prioritization.

> Zscaler's Workload Segmentation platform lets us establish zero trust security across our entire hybrid cloud environment. They've made it so amazingly simple that we were astonished at how quickly Zscaler Workload Segmentation was able to visualize and microsegment our workloads. There really is nothing out there like it.

Steve Strout, Global Head of Technical Operations

Vonage

About Zscaler
Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

zscaler

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com