Revolutionizing Cloud Workload Security

Why Zero Trust–based architecture that can inspect traffic and data egressing workloads in hybrid-cloud deployments is the future.

The Legacy Model Does Not Work Anymore

NGFW/VPN-based solutions are complex to manage, do not prevent lateral movement of threats, and leak sensitive data.

How Organizations are Securing their Cloud Workloads

Cloud Native Security Solutions

Azure aws

Google Cloud

Third-Party Tools

Firewalls
VPN
TLS/SSL Inspection
Data Loss Prevention

On-premises Infrastructure

Backhaul traffic to on-premises

Risks and Challenges of Legacy Security for Cloud

TLS Visibility Gaps

Managing distributed certificates or applying exclusions to pinned workloads creates operational challenges and increased costs.

Increased Threats of Lateral Movement

A network-based model where workloads are discoverable facilitates threat propagation.

Complexity & Poor Performance

Virtual firewalls, proxies and more often requires virtual appliances for each security function, creating latency.

Elevated Cost

Point products lead to expensive staffing costs and overprovisioning of network security infrastructure.

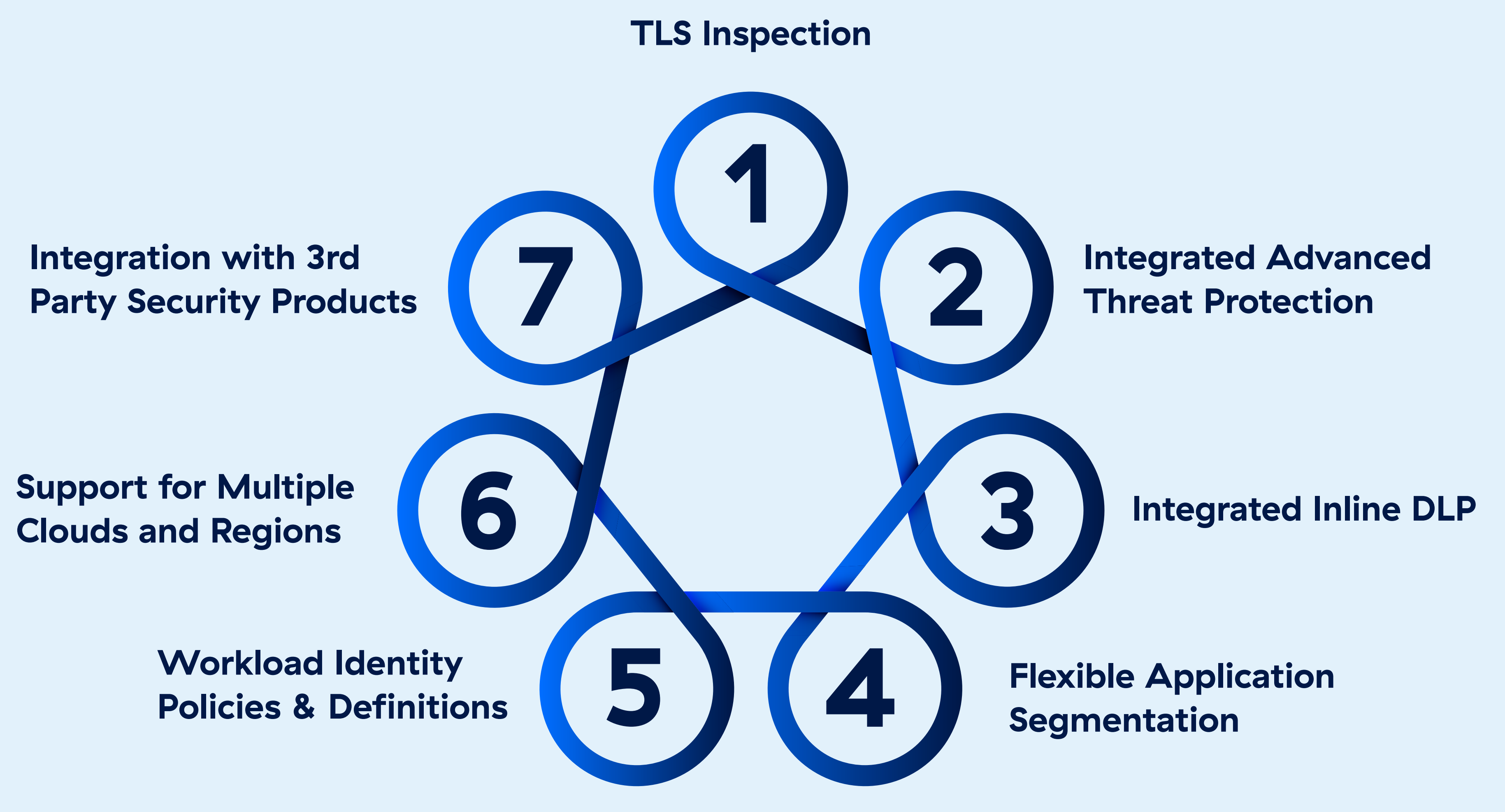
Logging & Event Management Challenges

Accessing logs from different cloud environments and storing them in a central SIEM infrastructure is complex and expensive.

What a Comprehensive Workload Security Model Can Do For You

- ✓ **Prevent/Detect External Threats**
  High-scale TLS inspection.
- ✓ **Prevent/Detect Insider Threats**
  Least-privilege access with zero trust.
- ✓ **Stop Lateral Movement**
  Granular workload-specific security policies.
- ✓ **Unify Security Across Multi-Cloud**
  Cloud-delivered solution for multi-cloud connectivity and monitoring.
- ✓ **Simplify & Streamline Tools for Developers**
  Security delivered as code.
- ✓ **Meet Risk & Compliance Requirements**
  Detailed workload monitoring and traffic controls.

7 Critical Capabilities to Secure Workloads Deployed in Hybrid Cloud



1 TLS Inspection

2 Integrated Advanced Threat Protection

3 Integrated Inline DLP

4 Flexible Application Segmentation

5 Workload Identity Policies & Definitions

6 Support for Multiple Clouds and Regions

7 Integration with 3rd Party Security Products

Secure Workload Egress Traffic at Scale

Security and engineering teams will need to decide how they want to track data and network traffic leaving workloads across large-scale hybrid deployments. To help guide these decisions, Zscaler partnered with SANS to create a buyer's guide to securing egress traffic from workloads in the public cloud.

+ DOWNLOAD NOW

zscaler™ | Experience your world, secured.™

© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

*All figures represent estimated USD annual savings
**Estimates based on third-party costs

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