illumio

GUIDE

How to Solve the Top 5 Cloud Security Problems

Securing applications and workloads in the cloud comes with challenges that are too often overlooked

INTRODUCTION

Cloud security has failed us

Cyberattacks are running rampant, and attacks on the cloud are growing at an alarming rate. In fact, **47 percent** of breaches in the last year started in the cloud, according to research by Vanson Bourne.

The security tools we're using in the cloud don't provide the visibility, confidence, efficiency, or resilience organizations need to scale. This leads to cloud deployments that are especially vulnerable to today's ever-evolving cyber threats, with **63 percent** of organizations saying their cloud security isn't prepared to mitigate these attacks.

Our current approach to cloud security is failing. But there's hope — Zero Trust Segmentation stops the spread of breaches across the entire attack surface so your organization can build resilience and ensure business continuity.

This guide examines the **five cloud application and workload security challenges** that are putting your organization at risk — and how Zero Trust Segmentation can help you solve them. With more awareness of what makes cloud security so complex and how to fix it, you'll make an important step toward improving your organization's cyber resilience.

47%

of breaches start in the cloud

93%

of security leaders say cloud security requires Zero Trust Segmentation

$4.1 MILLION

The average cost of a cloud breach

Why traditional cloud security tools aren’t working

The security tools that work well in on-premises data centers are struggling to adapt effectively to the cloud environment. This is primarily due to the fundamental differences between on-premises data centers and the cloud.

Traditional security practices are typically rooted in the concept of a network perimeter. In on-premises environments, this is often a well-defined boundary protected by firewalls, intrusion detection systems, and other security measures.

Cloud infrastructure is designed to be highly elastic to allow resources to scale up and down as needed. This makes the traditional fixed network perimeter much more fluid and effectively blurs or even erases the perimeter. This results in an ever-changing network footprint that makes it difficult to establish and maintain a fixed perimeter.

To combat this, many organizations have adopted vulnerability management approaches which scan systems and applications for known vulnerabilities and apply patches. However, these tools come with a few important challenges:

- They may miss vulnerabilities in transient resources or fail to keep pace with applications or workloads rapidly scaling up and down in the cloud.
- While proficient at scanning hosts and systems, they lack visibility into cloud environments’ complex traffic flows to help identify anomalies and potential vulnerabilities more effectively.
- They don’t offer holistic security because of a focus on identifying problems rather than fully addressing them.

ZTS secures dynamic cloud environments by constantly evaluating the context, including user and device identities, location, and behavior, to make access decisions. This modern approach to cloud security is best suited to the cloud’s ever-changing nature.

Zero Trust Segmentation (ZTS), also called microsegmentation, contains the spread of breaches and ransomware across the hybrid attack surface by continually visualizing how applications, workloads and devices are communicating, creating granular policies that only allow wanted and necessary communication, and automatically isolating breaches by restricting lateral movement proactively or during an active attack. ZTS is a foundational and strategic pillar of any Zero Trust architecture.

PROBLEM #1

Built-in security from cloud vendors only secures the infrastructure

Off-the-shelf security from cloud service providers isn’t enough to secure the cloud. It primarily addresses infrastructure-level security, leaving application, data, and configuration layers vulnerable. It also doesn’t account for individual organizations’ specific compliance, access control, and threat landscape needs.

That’s why cloud providers describe their security offering in terms of a Shared Responsibility Model. This means providers take on responsibility for securing the infrastructure and physical data centers, but in an “uneven handshake,” they expect customers to secure their cloud data, applications, and configurations.

Organizations must create a holistic, tailored cloud security strategy that accounts for both cloud providers’ security offerings and the specific needs of their environments.

PROBLEM #2

Cloud environments are complex and ever-changing

Traditional networks have a trusted internal system and a clearly defined external perimeter. But as organizations move to heterogeneous, hybrid cloud environments, these network boundaries get blurred. This means conventional tools that enforce security policies only at the network perimeter leave security gaps as workloads move within, between, and across environments.

To complicate things further, cloud environments are highly dynamic. Applications and workloads frequently scaling up and down, some for just a few hours at a time. Traditional security models built around static perimeters struggle to keep up with this fluidity, leading to gaps in protection and exposure to potential threats.

Traditional perimeter-based security doesn’t work in perimeter-less, fast-changing cloud environments. The cloud requires consistent security that is independent of the underlying network structure. This includes security policies that travel with workloads as they move across different environments.

PROBLEM #3

You can’t protect what you can’t see in the cloud

The cloud has become a favorite target for threat actors because it’s an easy place to breach and hide. Traditional network visibility leaves blind spots in the cloud. This makes it nearly impossible to proactively find and fix vulnerabilities or reactively detect and respond to breaches.

That’s why 95 percent of cybersecurity leaders say they need better visibility into their cloud connections.

While cloud providers typically offer some kind of built-in logging or monitoring, it’s never enough. Organizations need to understand how cloud services are interacting, what they’re accessing, and how they’re secured. This requires consistent, comprehensive application-focused visibility into traffic across all workloads, both on-premises and in the cloud.

Security teams can use this information to see, prioritize, and address risks that would otherwise be hidden.

PROBLEM #4

It’s easier for attackers to move in the cloud

Cybercriminals will inevitably breach your network, and their mission is to move laterally to the most important resources. Many organizations are now storing these high-value assets in the cloud.

But conventional cloud security is making this easy for them. Off-the-shelf cloud configurations, imperfect deployment processes, and the large number of workloads cause complexity and blind spots, leaving cloud environments more vulnerable than ever.

Unfortunately, even purpose-built cloud security tools only enforce policies between environments but cannot segment traffic between workloads or processes. These gaps make your hybrid network easy to breach and allow attackers to quickly move unhindered within the cloud, spreading from endpoints to servers, applications, and data.

PROBLEM #5

Teams are under pressure to adopt a shift-left strategy and speed up development

As security teams embrace DevOps best practices like continuous integration and continuous delivery (CI/CD), there's a growing need — and pressure — to shift-left security where defects or misconfigurations are identified earlier in the cloud application development cycle.

Conventional processes that place security later in the development cycle often result in significant vulnerabilities being discovered only after deployment or a breach.

At the same time, **96 percent** of security teams say they need to be more efficient. Overhauling and updating development processes mean more up-front work that many security teams just don't have. Organizations are looking for ways to update their cloud security processes while making their security teams as efficient as possible. This calls for a new way of securing the cloud.

How Zero Trust Segmentation solves cloud security problems

If your organization is in the cloud, it needs to be resilient against the next inevitable cyberattack. The best way to achieve cyber resilience is through adopting a Zero Trust security strategy based on a "never trust, always verify" mindset.

Zero Trust Segmentation (ZTS) is a key pillar of Zero Trust — you cannot achieve Zero Trust without it.

Unlike traditional prevention and detection technologies, ZTS provides a consistent approach to microsegmentation across the hybrid attack surface. This allows your organization to see risk, set granular security policy, and stop the spread of ransomware attacks and breaches across the cloud, endpoints, and on-premises data centers.

ZTS is easy and simple in comparison to attempting segmentation with static, legacy firewalls.

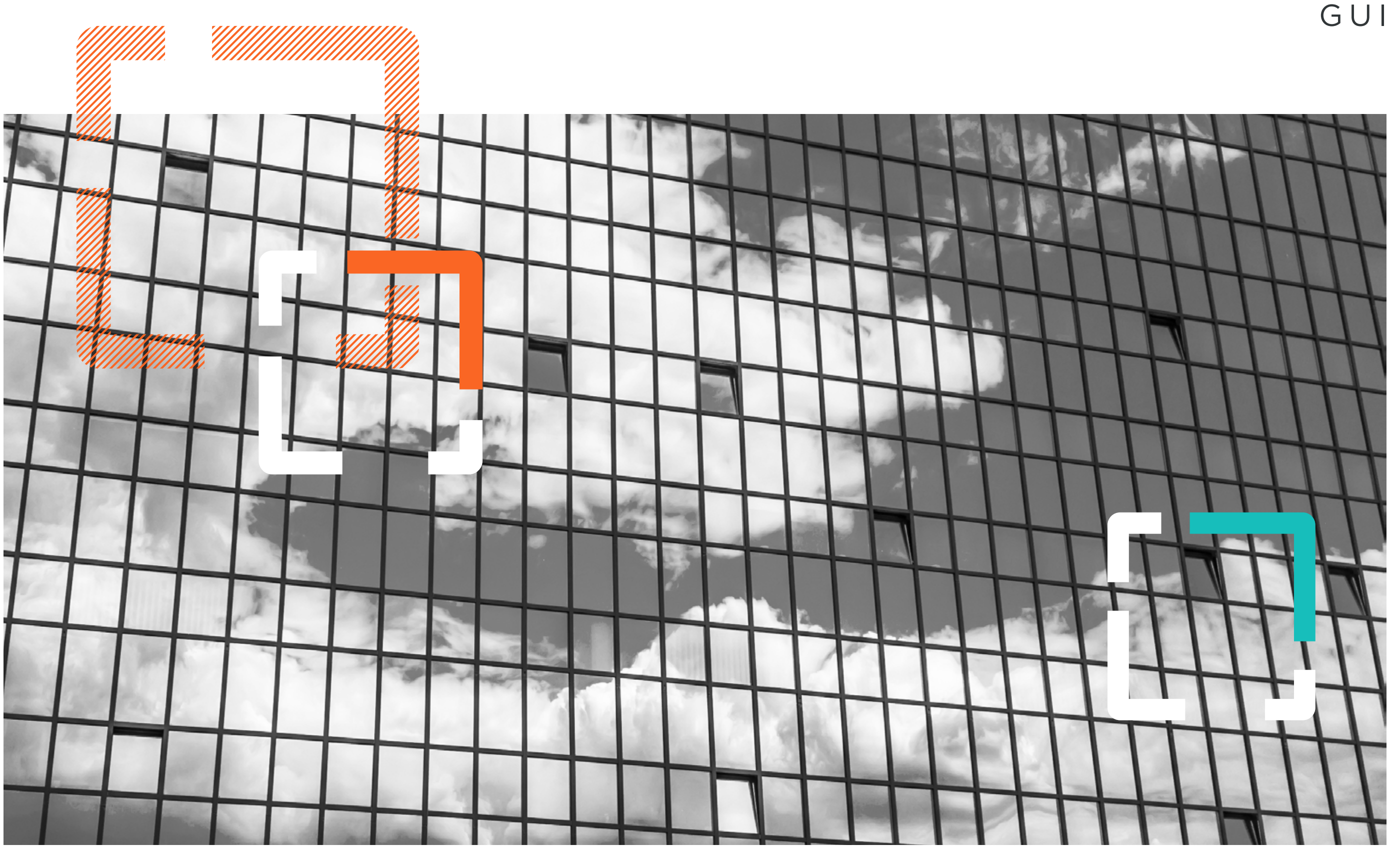
With Zero Trust Segmentation, you're empowered to:

- Stop and contain the spread of breaches and ransomware in cloud environments
- Eliminate security blind spots with a real-time view of your traffic flows across hybrid and multi-cloud environments
- Maintain a clear view of interactions and gain a full understanding of how applications are communicating
- Set granular, flexible security policies that protect applications and workloads to proactively prepare for inevitable breaches and reactively isolate breaches when they happen
- Limit exposure and maintain least-privilege access across data centers and public clouds

Why your existing security solutions need Zero Trust Segmentation

Platforms like CNAPPs, CSPM, CWPPs, and CIEM offer security specifically for the cloud — but they often lack the granularity, real-time adaptability, and comprehensive visibility that are required to fully secure cloud environments.

Pair Zero Trust Segmentation with your other cloud security tools to get consistent security and visibility across the entire network, not just in the cloud.



Illumio CloudSecure: Zero Trust Segmentation for the public cloud

Illumio CloudSecure extends Zero Trust Segmentation to the cloud. With Illumio CloudSecure, you can contain attacks on applications and workloads in public cloud environments, across servers, virtual machines, containers, and serverless computing by:

- **Visualize cloud workload connectivity:** Gather insights with an interactive of application deployments, resources, traffic flows, and metadata.
- **Proactively apply segmentation controls:** Create and deploy controls using labels and IP lists to build trusted communications between applications.
- **Contain cloud attacks:** Adapt segmentation policies even in dynamic, constantly changing environments.

Try Illumio CloudSecure free for 30 days

Start your free trial today
illumio.com/cloudsecure-free-trial