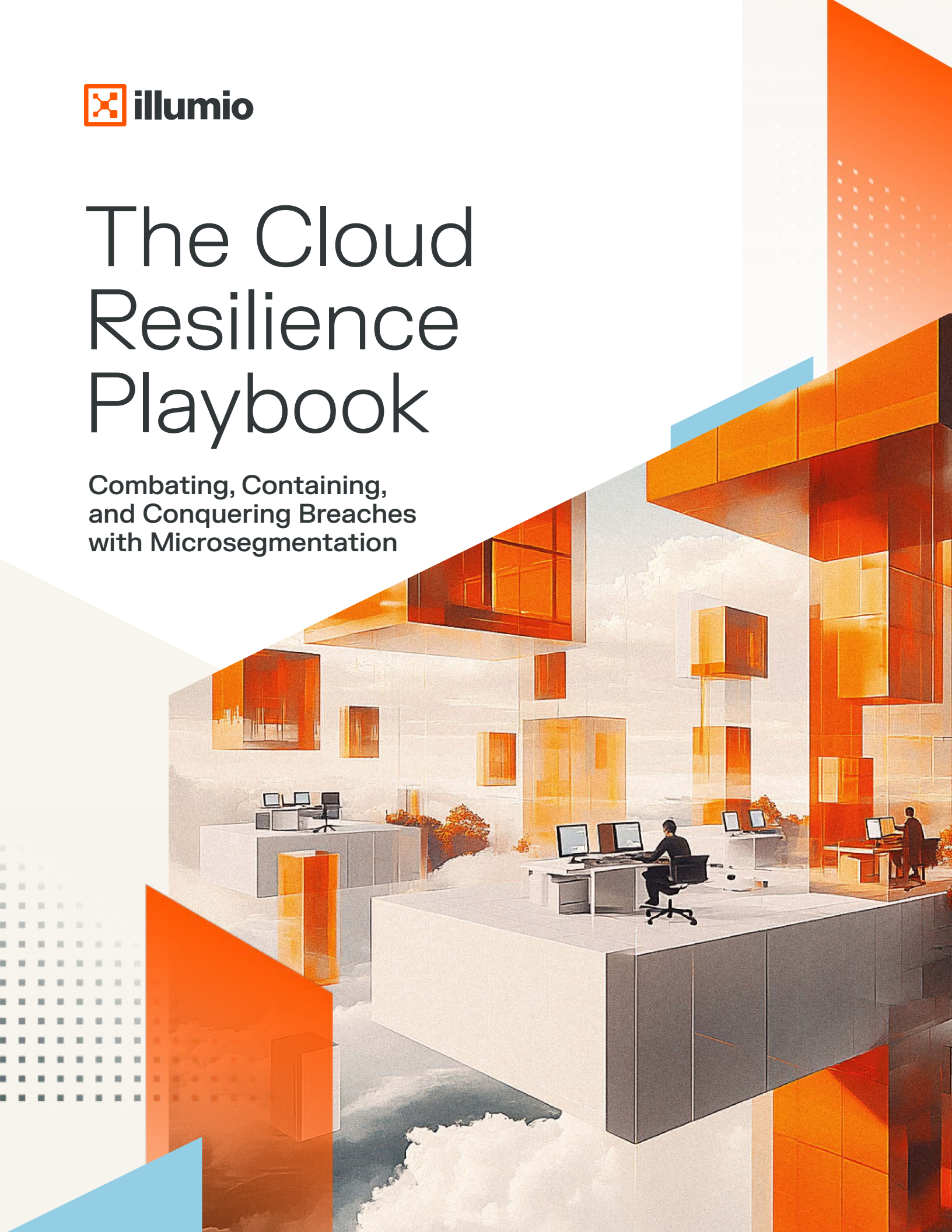
illumio

The Cloud Resilience Playbook

Combating, Containing, and Conquering Breaches with Microsegmentation



Contents

Cloud security has failed us

One of the largest breaches in history started in the cloud. The Clop ransomware group's May 2023 attack on MOVEit, a managed file transfer software, hit nearly 3,000 organizations and exposed the sensitive data of over 93 million people.[1]

This was not an isolated incident. **Nearly half of all data breaches now originate in the cloud.**[2] Let that sink in — *half*.

These kinds of large, sophisticated cloud attacks highlight a stark reality: Cloud environments are increasingly becoming a playground for cybercriminals. And the tools most organizations rely on for cloud security? They're simply not cutting it.

This isn't a hypothetical problem. According to recent surveys, 63% of organizations openly admit their cloud security is not ready to face the current threat landscape.[3] That means their data, and potentially yours, is exposed. Today's advanced cyber threats, including ransomware and AI-generated attacks, can cripple operations faster than many realize.

The current approach to cloud security is failing, and the stakes couldn't be higher. But there's a solution: microsegmentation. With 93% of security leaders agreeing that it's essential, microsegmentation stops breaches from spreading like wildfire across your hybrid multi-cloud.[4] This helps keep your operations running smoothly, even when an attack gets through.

In this ebook, we'll dive deep into why cloud security is so challenging and how microsegmentation is the key to making it better. You'll learn practical steps to shield your organization from becoming another breach statistic.

47%

of breaches start in the cloud

63%

of organizations' cloud infrastructure isn't prepared for the next breach

$4.1M

the average cost of cloud breaches

Source: Cloud Security Index 2023

[1] Cybersecurity Drive, Progress Software's MOVEit meltdown: uncovering the fallout
[2] Cloud Security Index 2023
Ibid.
Ibid.

What makes the cloud so challenging to secure?

The cloud is fundamentally different from your on-premises data center. That means securing it requires a fundamentally different, modern approach. Many organizations are still trying to fit traditional data center security approaches into their cloud environment — and it's not working.

Here are the five biggest security challenges today's security and IT teams face.

PROBLEM #1

Your cloud vendor secures the infrastructure, not your data

As more businesses move to the cloud, they need to consider that their cloud providers' security services might not be enough. Cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) often promote their security under the Shared Responsibility Model. This model explains how security duties are shared between the cloud provider and the customer.

While the model clearly divides the tasks, it can create a false sense of security. In fact, many security experts call the model an "uneven handshake." It's easy to think that the cloud provider's strong infrastructure security is enough to protect all your organization's assets in the cloud.

But relying only on the cloud's built-in security can leave big gaps and blind spots. Security teams must get better visibility and control to keep your apps and data safe. Handing over your cloud's security entirely to the cloud vendor puts you at risk of attacks, data loss, and noncompliance.

Cloud providers offer many security features to help protect the resources you use. But it's ultimately up to you, not your provider, to make sure your cloud security aligns with your level of risk and compliance needs.

The "uneven handshake"

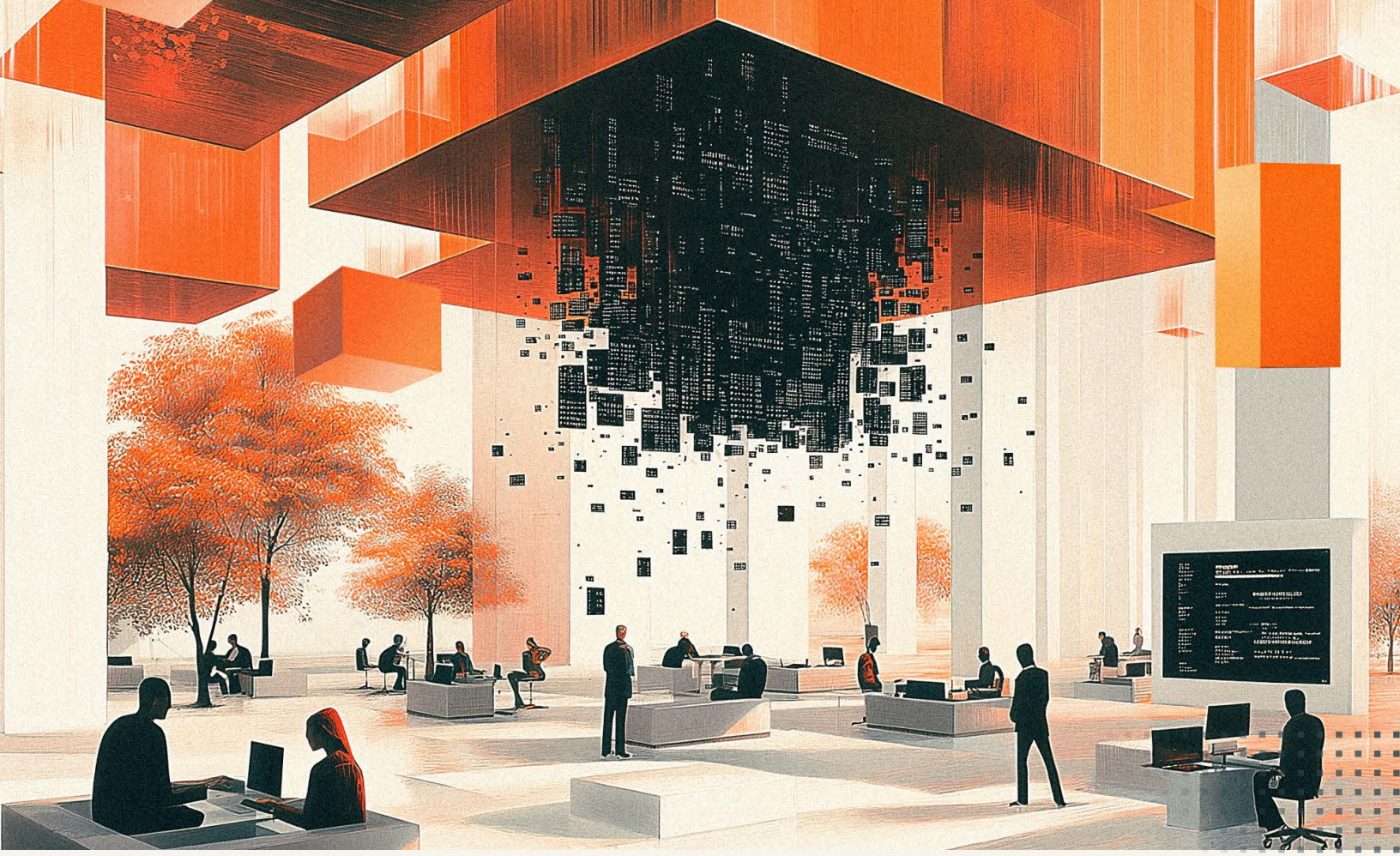
Here's how the Shared Responsibility Model divides security roles between cloud platforms and the organizations that use them.

Provider responsibility

- Secure the cloud infrastructure, including physical data centers, hardware, and basic software
- Monitor and respond to security threats related to the cloud itself and its underlying infrastructure
- Offer some additional security if the service is offered as IaaS, PaaS, or SaaS

Customer organization responsibility

- Secure the data and applications stored in the cloud.
- Configure cloud security settings
- Set up secure access controls
- Manage user accounts and credentials
- Encrypt data in transit and at rest
- Devices



PROBLEM #2

The cloud is complex and ever-changing

Traditional security tools are designed to protect a fixed perimeter, often only from known threats. They assume, incorrectly, that everything inside the perimeter is safe and everything outside is a potential danger.

When networks had a clearly defined perimeter, it might've made sense to focus on preventing attacks. Security teams put tools such as firewalls, intrusion detection systems, and antivirus software at the network perimeter to keep threats out.

Whether this model ever worked is debatable. What's beyond question is that it's not working now.

The cloud brings a new set of challenges:

- **The cloud creates perimeter-less networks:** A cloud environment has no clear boundaries. People can access company resources from anywhere. And even in hybrid, multi-cloud networks, perimeter boundaries are blurred. Data and applications move within, between, and across environments constantly.
- **The cloud is always changing:** Cloud instances like virtual machines (VMs) can spin up and down based on demand. This can happen in minutes. In fact, it's the reason why the cloud offers so many benefits for companies. But the cloud's dynamic also makes it difficult to keep up with security.

We must adapt our security thinking to meet the realities of the cloud. Conventional tools that enforce security policies only at the network perimeter leave cloud security gaps.

Modern cloud environments need security that is separate from the network architecture. This means security policies should be in sync with workloads as they spin up and down and move across environments. It also means being aware of the possibility that breaches will happen in the cloud and proactively preparing to contain them.

PROBLEM #3

You can't protect what you can't see

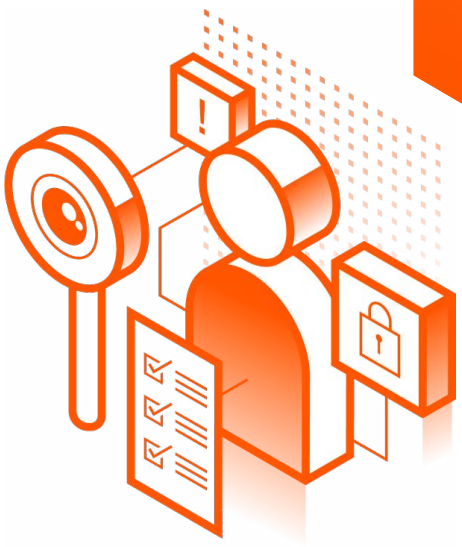
The cloud is complex. It runs virtual machines, containers, and microservices — all with changes that can last a matter of minutes. But without a clear view of how everything connects and interacts, cloud security risk skyrockets.

Security teams know the risk. More than 95% of security leaders say their organization needs better visibility into cloud connections.[5] But why aren't legacy visibility approaches working? Here's a few key reasons:

- **A fixed view of the network.** Traditional on-premises networks are static and change slowly. In this environment, security teams needed only a snapshot of the infrastructure at a specific time. So that's what legacy security tools provided. But in today's fast-changing cloud environments, the static approach doesn't show the real-time changes in workload connections.
- **Network visibility rather than application-level communication.** Modern apps are made up of microservices and containers that communicate across different layers. This means network-focused visibility alone can't capture the complex relationships and dependencies between applications in the cloud.
- **Lots of data but little context.** Legacy tools can produce an overwhelming amount of data without meaningful insights into how workloads are connected. This means you'll likely have a hard time telling the difference between legitimate traffic and potential threats, leading to false positives — or worse, false negatives.

Worse still, attackers know that less visibility means it's easier to breach a network and hide in the shadows. They can steal data, stop operations, and demand a ransom, all before you even notice an anomaly.

Security teams must have complete, granular visibility to see, prioritize, and fix vulnerabilities. Seeing what's happening in the cloud is not just a nice-to-have. It's a must.



Is hidden cloud connectivity costing you?

The cloud has transformed modern business, giving IT teams flexibility and scalability they could scarcely imagine just a few years ago. But the shift has also complicated their jobs, especially when it comes to security. And in some cases, cost savings — one of the cloud's main selling points — comes with a big caveat.

The cloud's pay-as-you-go model can lead to budget overruns. The biggest contributor is unknowingly overspending on unnecessary cloud connectivity and exposing your organization to cloud security risk in the process.

Without complete visibility into applications and workloads, you can't see if they have unnecessary or inefficient communication. This can lead to using more resources than needed, higher data transfer costs, and wasted processing power.

[5] Cloud Security Index 2023

PROBLEM #4

It's easier for attackers to move in the cloud

When cybercriminals breach your network, their mission is to move as quickly as possible to your critical data and assets. Many businesses are making it easier for attackers in the cloud by using:

- Conventional cloud security approaches
- Off-the-shelf or incorrect cloud configurations
- Flawed deployment processes
- Large, complex networks without completely visibility

Unfortunately, even purpose-built cloud security tools aren't enough to stop attackers from moving laterally through your environment. These platforms may enforce security policies between environments, but they can't segment traffic between workloads or processes.

The gaps leave your hybrid network easy to breach. Attackers can quickly move unhindered within the cloud, spreading from endpoints to servers, applications, and data.

Why is the cloud a prime target for cyber criminals?

98%
of organizations store sensitive data in the cloud

89%
of organizations are running their highest-value applications in the cloud

89%
of organizations run most or all of their services in the cloud

38%
of organizations are fully cloud native

Source: Cloud Security Index 2023

PROBLEM #5

Pressure to shift-left security and speed up development

Many DevOps teams are striving to use best practices like continuous integration and continuous delivery (CI/CD). This puts them under pressure to take a shift-left approach. This tactic can help identify security issues earlier in the cloud application development cycle rather than at the end.

But shift-left testing can come with its own issues. Time pressures can cause teams to overlook runtime and post-deployment security concerns. It also does little to address new threats, such as zero-day attacks, that weren't present at the beginning of the development cycle.

At the same time, many teams are also worried about increasing efficiency. In fact, 96% say they need to be more efficient to keep up with the needs of their growing business.[6] Overhauling and updating development processes mean more up-front work, taking time that many security teams just don't have.

While the rise of artificial intelligence (AI) and machine learning (ML) can help teams speed up manual processes, it's not enough. There's strategic planning, cross-functional collaboration, and ongoing board-level communication involved in cybersecurity success that AI can't do.

Are these security gaps leaving your cloud exposed?

If your team is feeling stretched thin, it's easy to miss vulnerabilities. But attackers are always on the prowl. You can expect them to find and exploit these five common security gaps if you aren't prepared.

1. **Application security**
   Cloud providers make sure the infrastructure is secure, but customers need to handle security for their applications.

2. **Data security**
   Cloud vendors encrypt data at rest, but customers need to secure data both at rest and in transit.

3. **Misconfigured cloud settings**
   It's the customer's job to use and manage these tools properly.

4. **Lack of visibility**
   Because the cloud changes so often, it's hard to see everything happening across entire hybrid multi-cloud environments. Poor visibility means security teams often don't know what is running in their clouds.

5. **Compliance issues**
   Cloud vendors have compliance certifications, but it's up to users to make sure they're meeting compliance requirements in the cloud.

[6] Cloud Security Index 2023

Cloud security tools that aren't working

Even if you're aware of cloud security risks, you might be choosing the wrong tools to combat them. Is your organization using any of these approaches? If so, think twice — they aren't enough to prevent and contain cloud attacks. Here's why.

Traditional on-premises data center security tools

These tools were built for another era. They protected applications and workloads within a well-defined network perimeter that rarely changed.

In today's ever-changing cloud environments, this kind of boundary simply doesn't exist. Cloud resources can be accessed anywhere, blurring the network perimeter entirely.

On-premises security measures weren't designed to follow apps and workloads to the cloud. Relying on these traditional tools creates blind spots and leaves your critical assets vulnerable.

Vulnerability management tools

Vulnerability management tools, which scan systems and applications for known vulnerabilities and apply patches, fall short in today's complex cloud environments.

Because the cloud is always changing, and sometimes only for minutes at a time, these tools often miss vulnerabilities in temporary resources and lack visibility into cloud traffic flows. They focus on identifying problems rather than fully solving them, leading to incomplete security.

The reality is that not all organizations are born in the cloud. They have on-premises, multi-cloud, and hybrid environments. Cloud security solutions should provide consistent visibility and control over the entire hybrid multi-cloud.

Cloud-native security platforms

Cloud-native security platforms, including CNAPPs, CSPMs, CWPPs, and CIEM, offer security tailored specifically for cloud environments. But they fall short in several critical areas:

- They lack granularity, real-time adaptability, and comprehensive visibility necessary to fully secure cloud environments. This means they can't stop attackers from spreading through your network.
- While they provide valuable telemetry data, they often can't enforce security policy. This leaves gaps in security coverage.

Why they all fall short

These tools must be paired with security solutions that extend consistent security and visibility across the entire network. This includes on-premises, multi-cloud, and hybrid environments. Without this comprehensive approach, cloud-native platforms alone can't meet the security needs of today's networks.

Why microsegmentation is the solution to modern cloud security challenges

Your organization needs to be prepared for the next breach. The best way to achieve this resilience is through a Zero Trust security strategy based on a “never trust, always verify” mindset.

Microsegmentation, also called network segmentation, is foundational to Zero Trust. You can’t achieve Zero Trust without it.

Modern segmentation solutions give you end-to-end visibility across your cloud, endpoint, and on-premises environments. With this information, you can build granular segmentation policies that stop the spread of ransomware attacks and breaches.

Microsegmentation is crucial for cloud security because it means security travels with the workload wherever it goes. This means security isn’t siloed to one environment and there aren’t security gaps as workloads move around your network.

In today’s complex networks, microsegmentation is easy and simple compared to segmentation with static, legacy firewalls.

With microsegmentation, 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.
- **See and understand** how applications are communicating and where high-risk ports are open.
- **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.

Next steps

Traditional cloud security is failing to meet the demands of modern hybrid and multi-cloud environments. With more breaches than ever originating in the cloud and attackers moving faster than ever, relying on these legacy tools is no longer an option.

Microsegmentation offers a powerful, Zero Trust approach that can contain the spread of breaches, get rid of security blind spots, and give you the granular control you need to safeguard critical assets.

Learn how Illumio stops the spread of breaches and ransomware attacks across your hybrid multi-cloud.

Breaches will happen.
Disasters are optional with Illumio.

Visit illumio.com/illumio-segmentation

About Illumio

Illumio is the leader in breach and ransomware containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by the Illumio AI Security Graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters. Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.

illumio