How Can Organizations Improve Threat Detection and Response in Hybrid Cloud Environments?

Key Takeaways

- Best practices for threat detection in hybrid cloud environments focus on visibility across both cloud and on-premise systems.
- Hybrid cloud monitoring helps security teams identify suspicious behavior across distributed workloads.
- Detection and response strategies must connect identity, network, and workload activity.
- Automating incident response in a hybrid cloud environment improves containment and investigation speed.

Hybrid cloud environments rarely start as a carefully planned architecture. Most organizations reach that point gradually.

A few workloads move to the cloud first. Then development teams adopt additional cloud services. Meanwhile, critical systems continue running on-premise because they cannot easily migrate.

Over time, the result is an enterprise hybrid cloud environment that spans multiple infrastructure layers.

From a business perspective, this flexibility is useful. Teams can scale applications quickly, deploy services across regions, and maintain legacy infrastructure where necessary.

From a security perspective, it introduces a different challenge.

Threat detection becomes harder when infrastructure lives in multiple places.

Some telemetry comes from cloud platforms. Other signals originate from on-premises systems. Network traffic flows between them constantly. Attackers understand this complexity, and they often take advantage of it.

Once attackers gain access to part of a hybrid environment, they rarely stay in one location. They move between workloads, cloud services, and internal systems looking for opportunities to expand access.

That’s why threat detection in hybrid environments requires a different approach.

It’s not just about monitoring one platform. It’s about understanding how activity across environments connects.

Let’s break down how that works in practice.

What makes threat detection in hybrid cloud environments challenging?

Hybrid environments are really complicated. That makes it hard for traditional security monitoring to do its job. The infrastructure is over the place and workloads are moving from one platform to another.

This means that it is easy to lose track of what's going on and visibility becomes fragmented. Now think about what attackers do when they find themselves in this kind of environment.

They try to figure out how systems work. They check to see what they are allowed to do with identity permissions.

They look for spots where the monitoring might not be very good. That is usually where hybrid cloud security threats start to show up in hybrid cloud security threats and cause problems, for hybrid cloud security.

Reason 1: Visibility gaps between cloud and on-premise systems

Security people have to use tools to keep an eye on the cloud and the systems in our office. The cloud has its way of tracking what is going on and our old systems have their own way of keeping logs.

The problem is that these systems do not always talk to each other in a way that makes sense. Let us say someone bad gets into our cloud system by using someone Login information.

This might look weird in the cloud logs. If that person starts looking around our internal systems it might not be clear that these two things are connected. Without a way to monitor everything together the people who are trying to keep us safe might only see parts of what's happening rather than the whole thing.

Cloud and on-premise systems are like two things and it is hard to see what is going on when we look at them separately. They can move from one system to another without being seen.

Reason 2: Identity and access complexity across environments

Identity plays a crucial role in a hybrid cloud environment. Cloud-based workloads make use of service accounts and identity roles.

Similarly, on-premise workloads could make use of traditional directory services.

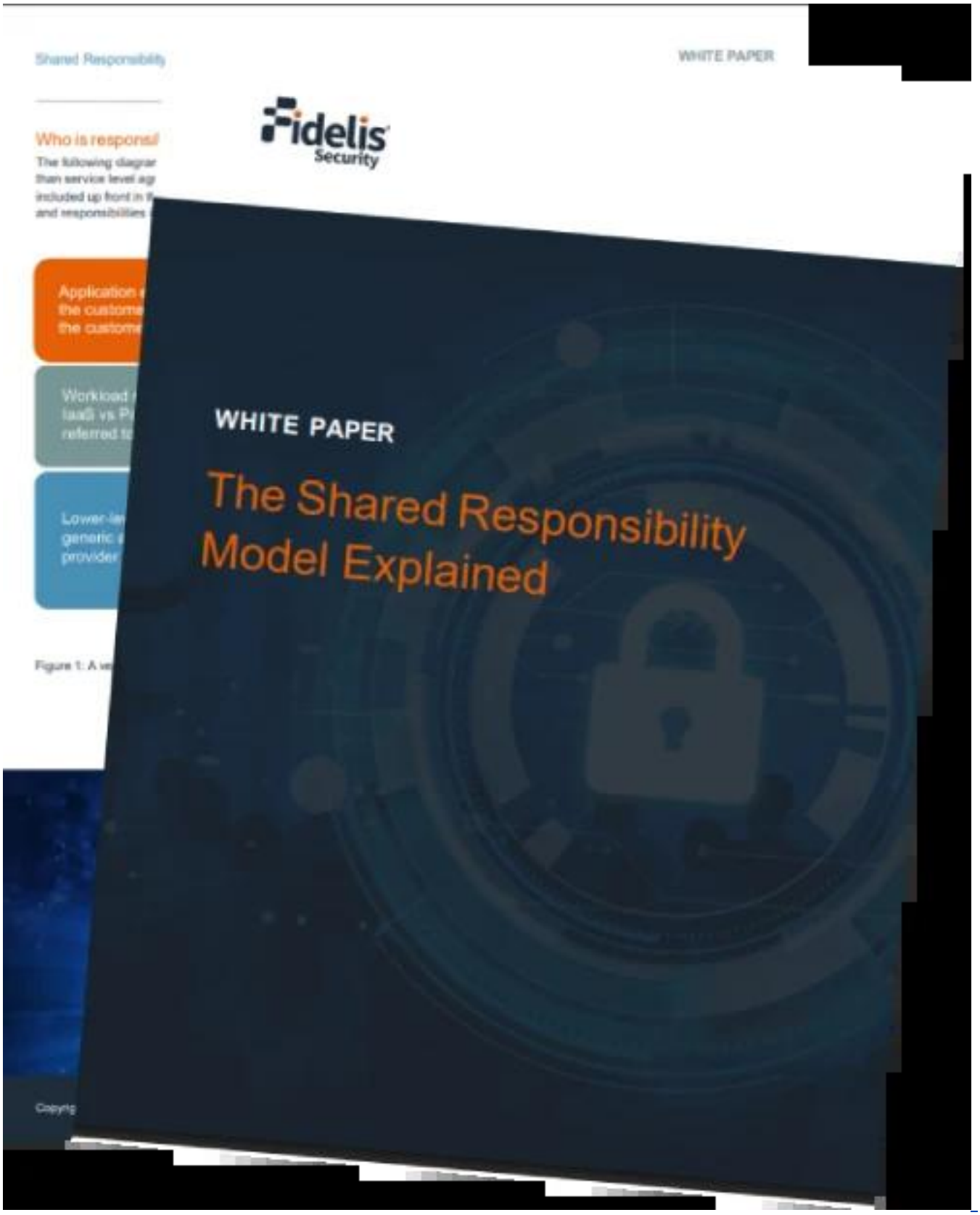
Threat actors often target these relationships. For instance, after gaining access to a cloud-based identity role, a threat actor could attempt to access internal services that have trust relationships with this role.

However, this could be normal behavior, especially if monitoring tools have not been able to correlate this behavior. As a result, detection solutions in a hybrid cloud environment often place emphasis on identity monitoring.

Shared Responsibility Automation—It's Not Optional

- Shared Responsibility Basics
- The Shared Responsibility Model in Practice
- Key Attributes of a Security Automation

Download the Whitepaper Now!



Reason 3: Workload behavior across distributed infrastructure

When we have applications that are used in an environment they usually do not work alone.

For example a workload might have some parts in the cloud. It might have databases that are actually located on the premises of the company and it might have APIs that are out on the internet.

So people who are in charge of security need to keep an eye on what the workload's doing in all of these different places.

The people who are trying to cause trouble often try to change what the workload is doing after they have gotten into the system.

For example after they have gotten into a workload these troublemakers might try to figure out what the rest of the infrastructure looks like.

Then they might try to do things like run commands in the cloud look for passwords, on the company premises and see if they can connect to the networks of the company.

What are the best practices for threat detection in hybrid cloud environments?

Threat detection in hybrid environments requires more than simply adding new monitoring tools. It requires building visibility across infrastructure layers. The goal is not just collecting more telemetry. It's understanding how activity connects across environments.

Step #1 : Establish unified hybrid cloud monitoring

One of the most important best practices for threat detection in hybrid cloud environments is unified monitoring.

Instead of relying on separate monitoring systems for each platform, organizations benefit from aggregating telemetry across cloud and on-premise infrastructure.

This unified view helps analysts answer questions such as:

- Which workloads are communicating across environments?
- Which identities are accessing resources across cloud and internal systems?
- Which systems show signs of unusual activity?

When monitoring remains fragmented, analysts may miss these relationships.

Hybrid cloud monitoring helps bring those connections into view.

Step #2 : Monitor workload activity rather than infrastructure alone

Infrastructure configuration is important, but many attacks unfold after infrastructure access occurs.

Now think about how attackers behave after initial compromise.

They interact with workloads. They search for credentials. They test connections to other systems.

Monitoring workload behavior helps detect these actions earlier.

For example, if a container suddenly begins executing unfamiliar commands or accessing sensitive files, those signals may reveal malicious activity.

Hybrid cloud security strategies often combine infrastructure visibility with workload monitoring to detect these patterns.

Step #3 : Correlate network, identity, and workload signals

Hybrid environments generate large volumes of security data.

Cloud logs capture API activity. Network monitoring systems observe traffic flows. Identity platforms record authentication events.

Individually, these signals may not reveal much. But when analysts correlate them, patterns begin to appear.

For instance, a suspicious login event may not seem urgent on its own. But if the same identity begins accessing multiple cloud services and internal resources shortly afterward, the behavior becomes more concerning.

Detection and response strategies that correlate signals across infrastructure layers help reveal these connections.

How can organizations implement effective threat detection in hybrid cloud environments?

Implementing detection strategies in hybrid environments requires practical operational changes.

Organizations must adapt their monitoring and response processes to account for distributed infrastructure.

Step 1: Make sure monitoring strategies are the same in all environments

One problem in big companies with hybrid cloud environments is that monitoring is not done in the same way everywhere.

The cloud can create a lot of logs. Older systems do not give us as much information.

Companies do better when they make sure their monitoring strategies are the same on all platforms. This means that the people who watch the systems can see what is happening in the way all the time. To do this we need to connect our monitoring tools to a place where we can look at all the information from different sources.

When we can see everything in the way it is easier for the people who watch the systems to find patterns that do not look right. This is very important for workloads and legacy systems. Monitoring strategies are very important, for companies.

You need to make sure our monitoring strategies are the same.

Step 2: Strengthen incident response workflows

Detection alone is not enough.

Security teams must respond quickly once suspicious activity appears. Hybrid environments

make incident response more complicated because activity may span multiple platforms.

For example, an investigation might involve reviewing cloud API activity, analyzing network traffic, and examining workload behavior simultaneously.

An incident response tool for hybrid cloud environments helps security teams coordinate these investigations across infrastructure layers.

This ensures analysts can follow attacker behavior across systems rather than treating each event in isolation.

Step 3: Automating incident response within the hybrid cloud

The hybrid cloud is really big and it gets even bigger. So automation is very important. When someone tries to break in it can take a while to notice.

The bad guys can move really fast once they get in. Automating incident response within the cloud can really help us respond faster when something goes wrong.

The incident response automation does not do the job of the security analyst. The incident response automation can help the security analyst do their job better when there are threats to the hybrid cloud. Automating incident response within the cloud is a good thing because it helps the security analyst respond to threats, to the hybrid cloud.

How does Fidelis Security help strengthen hybrid cloud threat detection?

Hybrid environments require visibility across networks, workloads, and infrastructure layers. Fidelis Security focuses on helping organizations observe activity across these environments rather than treating each platform separately.

In hybrid cloud environments, suspicious activity rarely stays confined to a single system. Attackers move between workloads, networks, and cloud services as they explore the environment.

Fidelis helps security teams follow that activity.

- **Expanded visibility across hybrid environments**
  Fidelis solutions help analysts monitor activity across cloud infrastructure, on-premise systems, and hybrid workloads. This helps security teams maintain awareness of how activity flows between environments.
- **Connecting detection signals across infrastructure layers**
  By analyzing network, workload, and identity signals together, Fidelis helps reveal patterns that may indicate attacker movement.
- **Improving investigation context**
  When suspicious behavior appears, Fidelis helps analysts understand how that activity relates to surrounding infrastructure. This context helps security teams respond more effectively during investigations.
- **Complementing hybrid cloud security solutions**
  Fidelis capabilities are designed to work alongside existing hybrid cloud security solutions by providing deeper visibility into attacker behavior.

In complex environments, that additional perspective can make detection much clearer.

To learn how expanded visibility can strengthen detection and response across your hybrid infrastructure, consider connecting with the Fidelis team for deeper insight.