How Can Organizations Perform Hybrid Infrastructure Risk Assessment Effectively?

Key Takeaways

- Hybrid Infrastructure Risk Assessment helps organizations identify security gaps across cloud and on-premise environments.
- Hybrid cloud risk assessment requires visibility across workloads, networks, and identities.
- A strong risk assessment framework for hybrid infrastructure connects infrastructure risk with real operational behavior.
- Mitigating risks of non-human identities in hybrid and multi-cloud environments

Most organizations didn’t design their infrastructure to become hybrid. It happened gradually.

A few workloads moved to the cloud first. Development teams adopted new services. Meanwhile, some systems stayed exactly where they were — inside internal data centers — because moving them wasn’t practical.

Over time the environment expanded.

Now many organizations run applications across cloud platforms, private infrastructure, and on-premise systems at the same time.

From an operational perspective, that flexibility is useful.

From a security perspective, it creates a different challenge.

Infrastructure risk no longer exists in one location. It appears across systems that interact with each other constantly. A cloud service might rely on an internal database. An internal application might authenticate through a cloud identity service.

Attackers understand these relationships.

Once they gain access to part of a hybrid environment, they rarely stay in one place. They explore connections between systems, searching for opportunities to move deeper.

That’s why Hybrid Infrastructure Risk Assessment has become essential.

Instead of evaluating systems individually, organizations need to understand how infrastructure components connect — and where those connections introduce risk.

Let’s break down how that works.

What makes hybrid infrastructure risk assessment different from traditional assessments?

Traditional IT environments were easier to evaluate. Most systems existed inside a single network boundary. Identity systems were centralized. Infrastructure followed predictable

patterns.

Hybrid environments are different.

Now think about how systems interact in a hybrid environment. A cloud application may access internal data. Internal workloads may authenticate through cloud identity providers. Automation scripts may create resources across several platforms at once.

Each of these interactions introduces potential risk. That’s where hybrid security risks begin to emerge.

1. Infrastructure visibility becomes fragmented

One of the first challenges in hybrid infrastructure security is visibility.

Cloud platforms provide their own monitoring dashboards. On-premise systems rely on traditional monitoring tools. Security teams often have to check multiple systems just to understand what infrastructure exists.

Now imagine an attacker entering that environment.

They may compromise a cloud workload first. From there they start exploring connections to other systems. If monitoring remains fragmented, analysts may only see part of that activity.

Hybrid cloud risk assessment helps close those gaps by mapping infrastructure relationships across environments.

Without that mapping, important exposure paths can remain hidden.

2. Identity relationships create cross-environment exposure

Identity systems often connect cloud platforms with internal infrastructure.

Service accounts, automation identities, and API credentials frequently operate across environments. These identities allow applications to communicate automatically.

Attackers often target these identities first.

Now think about how an attacker behaves after gaining access to a service account.

They begin testing what the identity can access. They attempt connections to other systems. They look for privileged roles or administrative permissions.

If those identities operate across environments, the attacker may gain access far beyond the original entry point.

That’s why mitigating risks of non-human identities in hybrid and multi-cloud environments has become a critical part of hybrid risk assessment.

Hybrid Infrastructure, Hidden Risk: The Visibility Problem CISOs Must Address

- Establish a Unified Visibility
- Support Incident Response
- Operational Efficiency for Security Teams

Get the eBook Now

3. Infrastructure relationships reveal hidden attack paths

Applications rarely operate independently in hybrid environments.

A single application might involve:

- cloud workloads
- internal APIs
- external identity services
- internal databases

Each of these connections creates a potential path for attackers.

Now imagine an attacker exploring a compromised workload. They begin checking configuration files. They test connections to other systems. They search for credentials stored inside the environment.

Hybrid IT systems risk assessment helps security teams identify these connections before attackers discover them.

Understanding how systems depend on each other is one of the most important steps in assessing hybrid infrastructure security.

How should organizations conduct a hybrid infrastructure risk assessment?

Conducting a meaningful risk assessment requires more than running vulnerability scans.

Organizations need to evaluate how infrastructure behaves as a connected system.

Step 1 – Establish a risk assessment framework for hybrid infrastructure

A structured approach helps security teams evaluate infrastructure consistently across environments.

A risk assessment framework for hybrid infrastructure usually focuses on several areas:

- infrastructure configuration exposure
- identity permissions and trust relationships
- workload behavior patterns
- network connectivity between systems

Each of these factors can introduce risk.

For example, a cloud service may appear properly configured on its own. But if identity permissions allow internal systems to access it broadly, the exposure becomes larger than expected.

Framework-based hybrid risk assessment helps analysts evaluate these relationships systematically.

Step 2- Identify high-risk infrastructure components

Not every system carries the same level of risk.

Risk assessments usually begin by identifying infrastructure components that support critical operations or store sensitive data.

These systems often include:

- identity platforms
- cloud storage services
- application gateways
- orchestration platforms

Now think about how attackers behave once they identify these systems.

They focus on them.

Attackers frequently target high-value systems because compromising them provides access to larger parts of the environment.

Hybrid cloud risk assessment helps organizations identify where these systems exist and how they interact with other infrastructure.

Step 3- Evaluate automation and machine identity risks

Modern infrastructure relies heavily on automation.

Deployment pipelines, cloud services, and orchestration platforms often rely on machine identities to access infrastructure resources.

These identities typically operate without direct human oversight.

Now imagine an attacker obtaining those credentials.

Instead of compromising individual systems, the attacker may gain access to automated processes that interact with multiple environments.

Evaluating machine identities has therefore become one of the most important steps in hybrid infrastructure risk assessment.

Security teams must understand:

- where these identities exist
- what permissions they hold
- which systems trust them

Without that visibility, hybrid infrastructure risks may go unnoticed.

How do organizations reduce hybrid infrastructure security risks?

Risk assessment is only valuable if it leads to meaningful improvements.

Once risks are identified, organizations must reduce exposure across infrastructure layers.

Step 1- Strengthen hybrid network security monitoring

Network activity often reveals how systems interact.

Hybrid network security monitoring helps analysts observe communication patterns across environments. Suspicious connections between workloads may reveal early attacker activity.

Now imagine a workload suddenly communicating with internal infrastructure it normally does not access.

That change may indicate compromise.

Monitoring these patterns helps security teams detect hybrid security risks earlier.

Step 2 – Improve hybrid cloud data protection controls

Data often moves between cloud services and internal systems.

Without strong controls, sensitive information may become exposed during these transfers.

Hybrid cloud data protection strategies typically focus on encryption, access control policies, and monitoring of data movement.

These controls help ensure that sensitive information remains protected even when it moves across infrastructure boundaries.

Step 3- Use IT risk management tools for hybrid infrastructures

Large hybrid environments generate complex infrastructure relationships.

Managing these relationships manually becomes difficult as environments grow.

IT risk management tools for hybrid infrastructures help security teams evaluate infrastructure exposure more efficiently. These tools often provide visibility into configuration posture, identity permissions, and workload behavior.

Over time, they help organizations maintain stronger hybrid infrastructure security.

How does Fidelis Security help organizations assess hybrid infrastructure risk?

Hybrid environments require visibility across multiple infrastructure layers.

Fidelis Security focuses on helping organizations observe activity across networks, workloads, and hybrid infrastructure simultaneously.

In complex environments, risk signals often appear in different places.

Some signals originate from network activity. Others appear inside workloads or infrastructure telemetry. Without correlation, these signals may appear unrelated.

Fidelis helps security teams connect those signals.

- **Expanded visibility across hybrid environments**
  Fidelis solutions help analysts monitor activity across cloud infrastructure, internal systems, and hybrid workloads.
- **Connecting risk signals across infrastructure layers**
  By analyzing network activity, workload behavior, and infrastructure telemetry together, Fidelis helps reveal patterns that may indicate emerging security risks.
- **Supporting investigation of hybrid security risks**
  When suspicious activity appears, Fidelis helps analysts understand how activity moves across infrastructure layers during an investigation.
- **Complementing hybrid infrastructure security solutions**
  Fidelis capabilities work alongside existing hybrid security solutions by providing deeper operational visibility across environments.

Download the Datasheet

In complex hybrid environments, that additional context helps analysts identify infrastructure risks more clearly.

Final Thoughts

Hybrid environments introduce flexibility, but they also introduce new security challenges.

Hybrid Infrastructure Risk Assessment helps organizations identify where infrastructure relationships create exposure before attackers exploit them.

Fidelis helps security teams gain deeper visibility across hybrid environments so suspicious activity becomes easier to detect and investigate.

To learn how expanded visibility can strengthen your hybrid infrastructure security strategy, consider connecting with the Fidelis team for deeper insight.