The common security threat concepts and corresponding remedy in the cloud.

While the cloud may offer significant benefits, organizations need to be aware of the security challenges when planning a cloud-first strategy. Some of those challenges involve not only protection and compliance but also operational considerations, such as the ability to integrate security solutions for on-premise and cloud workloads; to enforce consistent security policies across the hybrid cloud and to automate virtual machine (VM) discovery to ensure visibility and control over the dynamic infrastructure.

1: Balance protection and compliance

Striking a balance between protection and compliance is a huge challenge. Sometimes, it's all about discouraging threat actors by making them invest more time, energy, and resources than they first estimated into breaching the organization. Making attackers go through several layers of defenses means they could slip up at some point and trigger an alert before reaching the organization's crown jewels.

Recent data breaches should push leaders into thinking beyond compliance. Besides risking more fines, they risk their reputation as well. Compliance regulations tend to be addressed as base-minimum security options. However, thorough protection involves deploying multiple security layers designed to both help IT and security teams streamline operations, as well as increase visibility and accelerate detection of threats before a full-blown breach occurs.

2: Integrate security solutions for on-premise and cloud workloads

Finding the right security solution to seamlessly integrate with both on-premise and cloud workloads without impacting consolidation ratios, affecting performance, or creating manageability issues is also a challenge. Traditional security solutions can, at best, offer separate solutions for on-premise and cloud workloads; however, still, run the risk of creating visibility and management issues. At worst, the same traditional security solution is deployed on all workloads – cloud and local – creating serious performance issues for the latter. It's important for organizations to integrate a security solution that's built for automatically molding its security agent to the job at hand, based on whether the workload is on-premises or in the cloud, without impacting performance or compromising on security capabilities.

3: Deploy consistent security policies across the hybrid cloud

To address this challenge, organizations need to find security solutions that can adapt security agents to the type of environment they are deployed in. Cloud environment solutions must be agile enough to leverage all the benefits of the cloud without sacrificing security, while for traditional on-premise environments, versatile enough to enable productivity and mobility. Organizations must understand that deploying security policies

across hybrid infrastructures can be troublesome, especially without a centralized security console that can seamlessly relay those policies across all endpoints and workloads. It's important to automatically apply group security policies to newly spawned virtual machines, based on their role within the infrastructure. For instance, newly spawned virtual servers should immediately adhere to group-specific policies, as well as newly spawned VDIs the same, and so on. Otherwise, the consequences could be disastrous, in the sense that they would be left unprotected against threats and attackers for as long as they're operational.

4: Automate VM discovery

Automated VM discovery is the whole point of an integrated security platform, as security policies can automatically be applied based on the type of machine.

Organizations should consider adopting security solutions that can automate VM discovery and apply security policies accordingly, without forcing IT and security teams to push policies to newly instanced workloads manually.

Considering the hybrid cloud's flexibility in terms of endpoints (physical and virtual) and infrastructure (on-premise and in the cloud), it's important that the security solution embraces the same elasticity and enable organizations to fully embrace the benefits of these infrastructures without sacrificing performance, usability or security.

5: Maintain visibility and control over the dynamic infrastructure

In the context of adopting mobility- and cloud-first approach, it has become increasingly difficult for IT and security teams to view an organization's security posture, especially since traditional security solutions don't offer single-pane-of-glass visibility across all endpoints.

Integrating a complete security platform can help IT and security teams save time while offering security automation features that help speed up the ability to identify signs of a data breach accurately.

Addressing cloud security challenges is constant, ongoing work that requires IT and security teams to be vigilant while at the same time adopting the right security and automation tools to help take some of the operational burdens off their shoulders. Working together to find the right solutions ensures both teams get what they need. The collaboration of these two focused teams ensures the entire infrastructure is protected, regardless of on-premise or cloud workloads.

Source: https://www.quora.com/How-can-we-address-cloud-computing-security-issues