HYBRID CLOUD SECURITY: 5 QUESTIONS SKEPTICS WILL ASK

BY KEVIN CASEY

You say hybrid cloud security, the skeptics say wait a minute. Here's expert advice on addressing the biggest concerns.

Here's one thing you can bank on with any significant IT trend: The skeptics will soon follow. Take cloud: Security concerns, often misunderstood or overstated, have long been cited as one of the top cloud barriers. While many of those concerns have been addressed or debunked, growing hybrid cloud adoption will likely bring in another wave of security-related skepticism.

IT teams should be concerned about security. But there's certainly a difference between a culture of security and a culture of organizational stasis, especially when most IT leaders are tasked with catalyzing their company's overall digital transformation strategies. Bottlenecks simply won't do.

We identified five questions skeptics are likely to ask—and how to respond in a manner that helps you to get people to buy into your architectural vision and build a strong hybrid cloud security posture.

1. Doesn't hybrid cloud mean we give up visibility and control?

Do blind spots in your environments increase security risks? Sure. Are gaps in visibility and control more likely in hybrid cloud environments? Only if you allow that to happen.

Conceding a lack of visibility and control is really just a cop-out. One emerging lesson of hybrid cloud security is that "shadow IT" might just be a fancy way of saying that a company has failed to put in place the processes and policies necessary for governing how its people use cloud services.

"Organizations that are doing it right have taken stock of all the environments they are running in, so they have a full inventory of what needs protection," Tim Prendergast, CEO and co-founder of Evident.io, told us recently.

That kind of 360-visibility enables another hybrid cloud security fundamental: Ownership. "A key tenet in IT security is having an owner identified for every asset, and having the owner responsible for least privilege and segregation of duties over the asset," says J. Wolfgang Goerlich, VP of strategic programs at CBI.

2. Isn't hybrid cloud security more complex?

Hybrid cloud does come with new considerations for security. Your threat landscape is now distributed, for example, and perimeter-focused security strategies will no longer suffice on their own.

But the notion that hybrid cloud makes security "too complex" is inherently flawed. Among other reasons: it suggests IT security has been easy in the past. The never-ending list of threats of emerging threats and breaches IT pros must contend with would indicate otherwise. Your skeptics should be very familiar with that list of threats.

3. Our security playbook is working—why mess with it?

Your skeptics are very fond of their existing security processes and tools. Here's the deal: You shouldn't throw out your entire security playbook, but you do need to revisit and revise it.

Red Hat technology evangelist Gordon Haff points to the increased need for unified management and resource pooling across a variety of infrastructures, for example. "It's about providing delegated administration and self-service for users while maintaining granular policy control for IT," he says.

In addition to bringing your hybrid cloud resources under a unified management tool, security experts point to the growing need to shift from perimeter-centric defenses to identity-oriented strategies.

"Perhaps most useful [security strategy] in the adoption of a hybrid cloud at enterprise scale is the re-definition of perimeter to include identity," says David Emerson, VP and deputy CISO at Cyxtera.

4. Doesn't this boil down to a technology problem?

> “
> Leaving a customer list unencrypted in a public cloud bucket? That's almost certainly the result of human error, not a technology failure.

Modern tools and processes are key, but the fundamental security risks haven't changed all that much. Leaving a customer list unencrypted in a public cloud bucket? That's almost certainly the result of human error, not a technology failure.

Those companies that "get it right" realize that security is as much about people as it is about any particular tool or process.

"They are building out a culture of security across the whole organization and putting an emphasis on protecting data, no matter where it lives," Prendergast explains.

5. Will our cloud vendors have ultimate responsibility for our security?

Strong cloud providers make significant, ongoing investments in security and related areas. That doesn't absolve you of ultimate responsibility for security, though.

As Red Hat's Haff notes, people tend to worry too much about security process at public cloud providers. "The nature of public clouds is that they approach security using specialized staff, automated processes, and discipline (which is not to say that enterprises don't, but it's by no means a given)," he says.

However, you should beware the "move and forget" mindset when it comes to hybrid cloud architectures. For example, appropriate identity and authorization controls remain on you, Haff says.

> You should beware the 'move and forget' mindset when it comes to hybrid cloud architectures.

"Many practices, especially at the operating system level and above, shouldn't change in a public cloud—for example, obtaining software from known, trusted sources, using certified software images, and maintaining those images throughout their lifecycle," he says. This is why you want to use public cloud providers with back-end services that provide and install timely updates to relevant software patches. Linux containers and Kubernetes can further strengthen this security model.

SAS CISO Brian Wilson offers related advice: "Be diligent about keeping your providers accountable for their controls." That's true at the initial evaluation stage: If you can't federate with SAML, you're not getting through the door to Wilson's office, for example. But don't limit security to vendor selection. It should be a part of a process of ongoing review and evaluation.

Read more at EnterprisersProject.com