Highlights from a recent webcast on Hybrid Cloud Security

A SEISMIC SHIFT: WHY IT'S TIME TO RETHINK HYBRID CLOUD SECURITY

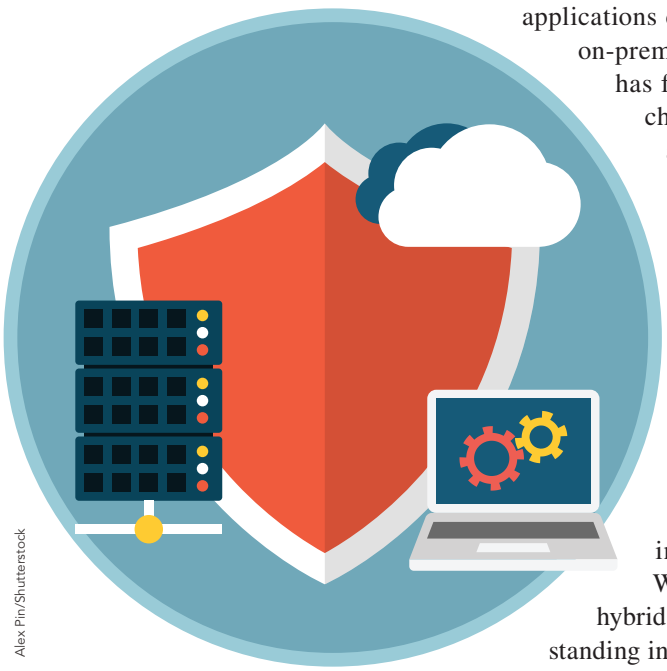
Securing the edge of the network doesn't meet the challenges of managing a hybrid cloud. It's time for a new security model, the application-based architecture.

Enterprises are deploying hybrid cloud environments to take advantage of cost-savings and faster deployment. However, the move to hybrid cloud poses three major challenges: security, agility, and manageability.

Security: Why the Network Perimeter Fails

The security piece might seem simple, but it isn't. A cloud provider's responsibility to secure its infrastructure doesn't prevent malware or other malicious applications from entering a company's computing environment. While the old method of simply setting up a perimeter firewall around the datacenter does provide some level of security, it doesn't offer a comprehensive solution in the hybrid-cloud architecture. And it's difficult to scale and nearly impossible to manage.

The perimeter-security method dates to a time when companies simply needed to control inflow and outflow of information from their environments to the Internet and back.



Alex Pin/Shutterstock

But the nature of how applications connect to the on-premises environment has fundamentally changed. Prior to the advent of the hybrid cloud, networking and security applications managed a layer 3 or 4 network connection, meaning they regulated information flow going to and from a company's infrastructure.

With the rise of the hybrid cloud and applications standing in a public infrastructure, such as Amazon Web Services or Microsoft Azure, apps now have layer 7 connections back into the enterprise. In the old perimeter model, there is no control over or monitoring of those connections, and companies cannot apply security policies to them.

This has created a seismic shift: the concept of a network perimeter no longer exists.

Application-Based Security

A single app has footprints in several locations, including the on-premises data center, a SaaS platform, or the public cloud—and that traffic is encrypted. Further, apps are connected with multiple other apps running in multiple environments, but they all need to behave like a single, tightly-integrated app. With increasing frequency, layer 7 gateways connect apps to each other in the hybrid environment.

Now that apps are distributed, companies have to change the way they apply security to those apps. Instead of addressing these security concerns with firewalls controlling layer 3 unencrypted traffic, enterprises must apply the controls to the applications themselves, app by app.

Addressing Agility and Manageability

One of the great advantages of

the cloud is the ease with which companies can spin up and deploy applications. Both on-premises and in the cloud, getting an app up and running usually takes a day or two at most and sometimes only a few minutes. That's great for app-hungry users, but it can be a real headache for IT—and it can slow the delivery of apps to users.

After all, each new app requires some adjustment of security policy. But that's easier said than done in a typical enterprise environment, which has many thousands of lines of security configuration at its edge. Plus, getting an app up and running often involves many teams deploying their own code or working to get commercial apps operational within a SaaS or IaaS environment. With one small IT team trying to control many business-driven, application-specific teams, chaos can easily ensue.

> It's no longer sufficient, then, just to draw a security firewall around a datacenter and consider it secure.

In order to scale the hybrid cloud, the process of getting an app up and running must be a self-service process, just as it is in the public cloud. Beyond that, IT needs to control that process. Here is where manageability becomes an issue: IT needs to be able to deliver an architecture that will let business-driven teams set up applications transparently for users but leave IT in control of managing security.

Hybrid Cloud Edge Security and the Skyport Solution

The only way to tackle all of these challenges is to fundamentally rethink edge security. Securing the network perimeter doesn't work anymore. The way forward is to secure applications themselves, with a security gateway in the datacenter for each individual application, no matter whether it runs on-premises, in the cloud, or both.

App-based gateways eliminate the major hassle of changing network security policy for each new application by making policies application-specific. Companies can change policy for one app and not touch—or risk breaking— those of other apps. The app-based method also enables self-service deployments while keeping IT firmly in control of the overall security structure.

That's the security architecture Skyport Systems enables. Business units often act as "shadow IT" and spin up apps without IT having to make changes to security policy. But IT still controls the overall security environment. Perhaps more critically, Skyport protects the multiple connections applications have to each other and to the overall IT environment. It moves protection from layers 3 and 4 of the network to layer 7, with encryption, where the most important connections exist in the hybrid cloud environment.

The hybrid cloud is by far the most common architecture for enterprises, and it requires a fundamental change in the way companies approach security. Merely securing the network perimeter is no longer sufficient. In order to ensure security without sacrificing agility or manageability in the hybrid cloud, companies need to abandon the notion of focusing on edge security and instead adopt the kind of application-based gateways Skyport makes possible.

REAL WORLD EXAMPLE

The concept of a perimeter that all network security is based on doesn't exist anymore. Now that apps are distributed, companies have to change the way they apply security to those apps. For instance, a CRM app could run in a vendor's cloud, but it will also have gateways and connectors that bring functions back to the enterprise to access on-premises ERP and other enterprise applications.