Solution Brief

Symantec
A Division of Broadcom

Six Key Security Considerations for Responsible Cloud Migration

To help illuminate the best practices associated with responsible migration, let's take a deeper look at six important issues to consider when moving enterprise data and applications to the cloud.

1. Navigate the Complex with Smart Policies

Most of us are familiar by now with the core advantages of cloud computing: greater accessibility, the ability to customize and scale application resources as needed, and lower infrastructure and maintenance costs. Yet organizations must recognize the challenges that come with cloud migration, particularly in the context of security.

For most organizations, cloud computing isn't an all-or-nothing proposition. Some companies dive into the cloud, head first; others implement a measured approach adopting cloud solutions in specific areas where it makes sense. This hybrid approach can work well, but it should be built on a solid foundation of security and compliance policies and protocols that remain consistent regardless of the delivery platform.

When attempting to safely negotiate the cloud migration process, it's important to grasp the complexity that arises as a result of the many different roles, functions, and capabilities associated with a hybrid approach and how this affects rules, regulations and compliance. For example, people in the marketing department may have to access their cloud applications from many different locations and may need to give access to data in these applications to business partners in other companies. Salespeople typically need to access applications from remote locations using mobile devices, and sensitive client data can frequently be included in the customer records. Accounting, on the other hand, may have policies that severely limit access to certain applications and allow such access only through corporate devices via an onsite network. Finally, there are some external web or cloud properties that company policy may dictate should not be used by any employees, regardless of whether they are connecting from inside the corporation or direct-to-net from a car using a personal device while on-the-go.

Because most companies now have a mix of on-premises applications, such as those used for finance, accounting, and supply chain, as well as applications in the cloud, such as those used for customer relationship management, marketing, storage, and IT help desks, controlling the access and compliance of these apps can be a challenge. Routing all employee traffic from mobile devices and remote offices back through the corporate data center to force consistent security and compliance often proves impractical. But opening the door to different paths to access and use applications creates serious security and compliance holes.

How do we tame this complexity? We must implement a unified method for pushing policies out to govern access and control, regardless of whether the security gateways and services being used to govern application access control and protect information are located onsite or in the cloud. This is an absolutely critical step that must be a high priority for those who recognize the threat that outdated, misaligned, or ineffectual policies have in the context of security breaches and compliance. Universal policy enforcement, wherein policy is set once and then pushed out to gateways and security applications, whether onsite or in the cloud, is a critical solution for those looking to migrate responsibly to the cloud.

2. Make Flexibility Imperative

We've seen the importance of managing complexity, yet there's another attribute that holds similar importance: flexibility.

We live in the era of the omnipresent network; because our users and applications are everywhere—and by extension, so is our data—our networks are also everywhere. Moving some functions to the cloud—while maintaining many tried-and-true applications onsite for a variety of legitimate business reasons—represents the kind of flexibility that's necessary for most enterprises considering serious cloud migrations.

Businesses are looking at detailed data flows as they consider security and compliance issues. Data must flow not only among various applications and users but also into different security components. This raises several important questions:

Where is the data sitting, where is it getting processed, and who has access to it at different times? Consider a single cloud application; the data may be encrypted at rest, but it may get pulled into the clear when it is being processed and flowing around in the cloud. At the same time, it might get pinged back and forth to other cloud apps as part of a service function.

Some organizations may find this acceptable whereas others may not. Either way, it's important to understand—from a security and compliance perspective—that data is flowing to these locations. Control of data going to cloud environments may require flexibility in security form factors (physical and virtual appliances/cloud-based services) if enterprises want to give their employees the ability to access these sorts of applications directly over the Internet. Decisions on who should be able to access what data in which applications from what locations and devices need to be thought through for specific use cases and the unique business requirements of each enterprise.

High-performance security technologies such as secure web gateways (SWGs) can be deployed onsite— as either physical or virtual appliances—an approach that is especially useful in corporate locations with many employees. SWGs delivered via the cloud are also ideal for remote offices and distributed sites as well as situations where remote workers need direct access to cloud applications such as Office 365 or Salesforce.com. The same sort of flexibility is available with security applications for malware prevention and advanced threat protection. Look for vendors that give you the flexibility to deploy security layers where you need them, whether in the cloud or onsite, based upon your enterprise's evolving requirements.

3. Apply the Data-Centric Principles of Zero Trust

Hybrid operating environments can create some unique challenges in the area of information protection and compliance. Adopting a "never trust, always verify" mindset is the best way to overcome these challenges and minimize risk exposure. First, be ensure access is managed with Zero Trust Network Access technology, applying precise controls over what resources are available and how they're used. Then make sure you have a data loss prevention (DLP) solution that can protect your data while your employees are increasingly going to the web and cloud, regardless of where they are when trying to access the cloud. An enterprise's SWGs, whether they are onsite or cloud-based, need to provide robust DLP to enforce data protection policies on web traffic. If you already have tuned DLP solution in place, your SWG should be able to integrate with it to make sure your policies are likewise enacted for cloud traffic. Interestingly, we are seeing situations where enterprises are using a mix of centrally managed SWGs, both cloud-based and onsite, that all integrate with their existing onsite DLP systems. Very few enterprise-class offerings have this capability, but this is just the sort of thing that is critical to enable a responsible move to the cloud for security-conscious organizations.

In terms of DLP, we typically see two varieties of policies within organizations: those crafted from an external compliance perspective, to comply with Health Insurance Portability and Accountability Act regulations, for example, and those designed to meet internal company-specific requirements. Savvy organizations understand the value of maintaining control of their own internal data, including intellectual property, source code, and any other sensitive data that would benefit from the existence of policies designed to restrict access or block over-sharing.

For those evaluating whether to put parts of their business in the cloud, there are a few key issues to consider from a DLP perspective. First, it's important to understand that there are two ways information can get into the cloud: via an internal system where DLP policies can be enforced in-line, and via outer-band mechanisms, where no in-line inspection is available. Advanced DLP solutions can cover both means of entry; ones that do not do so leave a huge blind spot that enterprises must recognize and address.

Regardless of where your DLP is located, consistent policy enforcement is essential to maintain an enterprise's information protection framework. When making the decision to migrate applications or security infrastructure to the cloud, organizations should avoid starting from scratch and recreating all the DLP policies that they have painstakingly developed over time.

Instead, a provider should be able to take existing onsite DLP solutions. If you want to move DLP to the cloud, look for solutions that will allow you to easily export policies to cloud-based DLP services. Let's face it: Once data protection policies are in place, few people want to replace them, considering the significant time it takes to deal with all the related security and compliance issues. Starting over could open a serious can of worms, so organizations are generally loathe replacing their established policies.

4. Assess the Benefits of Cloud-Access Security Broker Solutions

We've outlined how organizations need to have controls in place to ensure sensitive information does not inadvertently leak into cloud applications such as Salesforce.com or Box. Adding a cloud-access security broker (CASB) solution to your SWG with DLP capabilities can cover additional cloud security requirements—even the DLP blind spot of out-of-band access mentioned earlier.

Leading CASBs can help in a number of other important cloud control areas, too. By having a proxy interact with a security broker, a CASB is able to take log information about which end-users are going to which endpoints and display it to compliance, security, and network operations staff. This allows them to see the cloud destinations end-users are accessing and what is occurring at those destinations. Some of the clouds may be unsanctioned, and security professionals can set policies in their SWG to control access to those clouds, helping to manage and control shadow IT.

CASBs can also help an organization address threats unique to cloud environments. For example, user behavior analytics and machine learning technologies can help spot behavior that may be indicative of compromised user credentials, such as user IDs and passwords. If an employee account's risk score becomes elevated due to risky behavior—downloading a massive amount of documents, for example—account access can be suspended and IT and security professionals can be notified to investigate further.

5. Assess Your Global Threat Intelligence Database

Unfortunately, it is becoming increasingly common to see news of high-profile security breaches in the headlines. SWGs can play a key role in mitigating against these threats by performing a few vital tasks.

The first is to look for threats as traffic is coming in. To do so, an SWG must be able to analyze content, even encrypted content, to ensure nothing problematic is being downloaded behind the scenes. An SWG must also be able to stay on top of sites and locations that have been known to cause trouble for enterprises of a similar nature. Speed is essential when identifying risky sites and communicating about them, as many new and dangerous URLs intent on delivering threats and malware pop up daily.

This is why a global intelligence network fed by real-time risk information, tens of thousands of network-deployed proxies, and the telemetry and threat data from millions and millions of endpoint devices is so critical. These devices are constantly pinging websites, encountering unsafe locations, and defeating advanced malware. When an enterprise's device spots a new threat, the rest of the network is immediately informed through its updated threat intelligence data feed. By sharing this information, an organization's existing policies can react to catch new URLs and cloud locations that are now properly classified as risky.

Relying solely on a single enterprise's security professionals to handle the voluminous number of threats isn't realistic; it's a giant game of whack-a-mole. But working with a provider able to build a massive global database of security information offers a strength in numbers that profoundly changes the equation.

6. Protect From Advanced Threats and Malware

We've discussed the value of global intelligence, which leads to critical protection in advanced threat defense—also called "the sandbox"—a mechanism for performing advanced inspection and quarantining files and programs, so they can be evaluated without the risk of wider harm.

Sandboxing is a critical component to a multi-tiered security infrastructure because of its unique ability to combat sophisticated attacks. Only by placing risky files and programs in a sandbox and exposing them to rigorous inspection can experts determine the malicious intent of certain files. But because attackers are becoming so sophisticated in their approaches, the security architecture of some sandbox platforms has become overwhelmed and has grown too expensive to maintain at a larger scale.

Some sandboxing approaches are losing their efficacy because of the sheer volume of activity; people have essentially been conditioned to toss everything into the box.

There's an answer for this problem. Employing an SWG with threat and malware intelligence in front of a sandbox will significantly cut down on the volume of files that truly need sandbox-level analysis. This allows the sandbox to return to its original purpose: focusing solely on the truly troublesome items. By augmenting sandbox capability, organizations do not have to make greater and greater investments as traffic increases.

In short, introducing an advanced SWG to the mix delivers a superior advanced threat protection sandbox architecture by dramatically lowering the load on the enterprise's sandboxes. More malware is captured up front, which means organizations can lower costs by right-sizing their sandbox architecture. As an added bonus, this may shorten incident response queues by up to 50%.

Takeaways

Responsible cloud migration can be achieved by a diligent approach to a few core security considerations. These include the following:

- An understanding of the risks and complexity generated by increased web and cloud use and the importance of smart and consistent policies to address it
- Flexibility in terms of form factors
- The ability to address data leakage
- The unique benefits of cloud-access security broker (CASB) solutions
- The critical threat prevention benefit of a global intelligence network
- The ability to relieve pressure on sandboxes by incorporating upfront malware protection

By choosing an SWG with the ability to deliver these advanced capabilities, organizations will find themselves in a great position to proactively address these issues and ensure a safe and compliant move to the cloud.

Cloud-Migration-Security-SB100 November 30, 2021