Securing Your Enterprise in the Cloud

IT executives must be ready to move to the cloud safely

Symantec

The technology pendulum is always swinging. And chief information security officers must be prepared to swing with it—or get clocked.

A look at recent history illustrates the oscillating nature of technology. In the 1980s, IBM mainframes dominated the landscape. In the ’90s, client-server computing came on the scene and data was distributed on personal computers. When the Web assumed predominance, the pendulum started to swing back to a centralized server. Then, just as quickly, mobile took the lead, with apps downloaded to workers’ devices—the new client server.

Now, as mobile devices continue to populate the enterprise at a rapid rate, the IT model is changing again—to the provisioning of information on a just-what’s-needed, just-in-time basis from centralized servers consolidated in the cloud. The pendulum continues to swing and IT workloads are moving to the cloud en masse.

IT executives must wrap their arms around the cloud

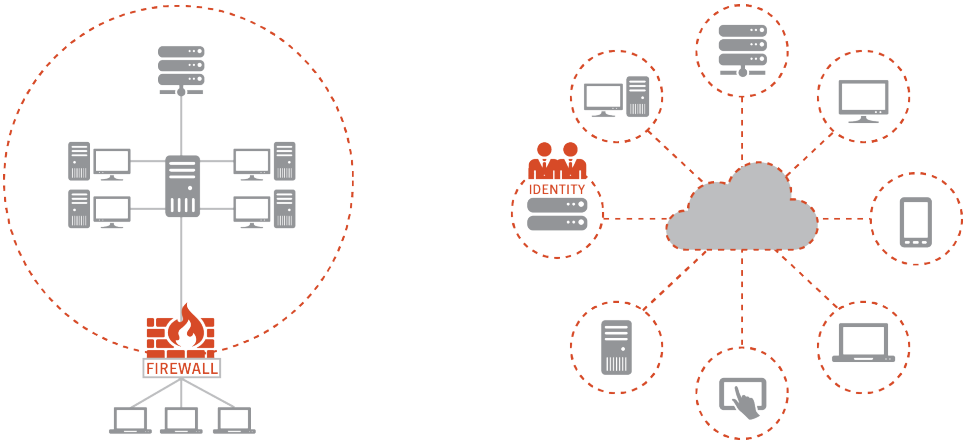
IT executives, such as chief information security officers, need to move quickly to take advantage of their organizations’ accelerating adoption of the cloud—and to do so they must adjust their approach.

Yes, the new model may resemble the old client-server environment. But in many ways it is a very different world, involving technologies linked to the cloud as well as the cloud itself. IT research firm Gartner calls it the “Nexus of Forces”: cloud, mobile, social, and information. Market research company IDC calls it the “3rd Platform.” Whatever tag is applied, most analysts agree that the convergence of mobile computing, social networking, cloud services, and big data analytics has fundamentally altered the way we do business and live our lives.

This is not a completely new concept. What is new is the pace with which organizations are embracing the cloud as the platform of choice—and accepting new realities as they do so. They are acknowledging that they no longer own or manage most of their applications because apps such as Salesforce, Box, and Office 365 now do it in the cloud. IT organizations are also beginning to contract out management of their infrastructures because, to stay competitive, they need to take advantage of the benefits provided by cloud vendors such as Amazon and Rackspace. Companies don’t even own all their mobile endpoints anymore because employees are bringing their own devices to work.

Perhaps most important of all—from a security perspective—the organization is losing its perimeter defense because work happens everywhere, not only within the four walls of the organization. Offices are virtual, and collaboration takes place all over the Internet.

So what are smart business leaders focusing on? When there is no perimeter, data is at its most vulnerable, so smart leaders are securing the aspects of the cloud they can control to protect their intellectual property. These are identity and information.



To protect their intellectual property, smart leaders are securing identity and information—the aspects of the cloud they can control.

IT executives can safeguard their organizations by securing and authenticating the identity of the people who access corporate apps and information. They can also implement solutions and policies to govern the movement of sensitive information to prevent its relocation to insecure places where it can be leaked or stolen.

Yes, the cloud is quickly transforming the way business gets done. And, yes, security controls for this new world are still in short supply. But business leaders do have solutions to achieve information protection in the cloud. Following is a framework IT executives can use to keep their enterprises secure.

Cloud security relies on three keys

The foundational concept behind a successful data security strategy is not significantly different whether it is the enterprise or the cloud that is being secured. In both cases, the strategy should seamlessly combine three key components: identity protection, information management, and a correlation engine to trigger actionable automated responses. However, the cloud does pose unique challenges when it is necessary to secure employees outside the corporate network who are using their personal devices under a “bring your own everything” policy. Let’s take a look at each component separately.

1. Identity protection

ID protection is the lock on the cloud’s front door. It keeps attackers out and ensures that workers have access to the cloud apps they need. Done properly, it also improves the user experience by enabling a transparent login process. The ideal is one password-free login—from any device, anywhere, anytime—to gain access to necessary data and apps.

The user experience is vital here because the user is typically the weakest link in the security chain. If the process behind security is easy and effective, you can limit the risk posed by users. You can implement security that is strong yet simple and provide access that is not so cumbersome that it spurs some users to resort to circumvention.

Let us look at the way identity protection works in a breach scenario when an information protection solution is in place. It enables you to pinpoint the party responsible for the suspicious or risky action and assess what data is being touched from what device. Identifying who (user/device) is the perpetrator of the attack, what is being targeted, and how to take immediate laser-focused action is the key.

Identity protection also gives you the ability to correlate different incidents and relate them to a particular user or device, which is critical because attacks are often not one activity but many small, seemingly innocuous actions that, viewed as a whole, add up to a serious threat.

2. Information management

Identity protection alone is not enough. Data is what must be protected—and it is everywhere. Therefore, a comprehensive information management solution must discover, monitor, and protect data across cloud, mobile, and enterprise environments. You may have already investigated a solution that addresses data in the enterprise; so now is the time to extend that concept to include cloud-friendly information management.

Information management ensures that data is not insecurely stored or moved to places within the enterprise, and especially the cloud, where it is easily accessible to would-be attackers. A flexible information management solution supports granular content-aware policies that allow you to choose how to deal with particular types of data. Can the data safely be moved to the cloud with a simple reminder that the move makes the data more vulnerable; or is the move too risky to be allowed.

3. Correlation engine

A correlation engine enables detailed tracking and correlation of activities by users. Your correlation engine should not only consolidate alerts that are identity-centric and data-centric but should add context or intelligence.

Near real-time correlation requires context to make sense of what is happening. Growing your identity and data intelligence with context increases the speed of detection, which can trigger actions to quickly begin remediation. After all, it is only through rapid detection and remediation that damage to your organization can be contained. Putting the jigsaw puzzle together by hand across multiple systems, even an hour after the fact, is risky business.

Cloud security won't thrive in a vacuum

Ideally, your information protection solution will not have to work in a vacuum. A truly resilient organization, especially one that has adopted a hybrid cloud model, will also have a solution that quickly detects advanced threats, so that even if a user or device has been compromised, the organization can pinpoint when the threat entered the network.

In a best-case scenario, information protection (monitoring access attempts and tracking data governance) is part of a larger strategy that identifies external threats and observes activity on endpoints, in addition to regularly evaluating processes for improvement and continually educating employees to update their security IQs.

The new security ecosystem: Protecting your enterprise in the cloud demands a number of interrelated measures.

Real-world example shows how cloud security works

Imagine that your information protection solution notices an engineer named Jane who has a flurry of failed login attempts before she successfully gains access to the network. This is out of the ordinary, though not necessarily alarming. But then Jane tries to access a file she is not authorized to access. Access is denied and her attempt is logged.

Not long after this, Jane accesses a file containing information on the roadmap for a new product. It is not a file she is blocked from accessing, but it is not integral to her job either. Jane is now flagged as a higher-risk user by the correlation engine. Then she issues a command to copy that new-product file to an unsanctioned cloud app. Now action is automatically taken.

The file is removed from the cloud app and quarantined, and Jane is issued an authentication challenge. If she fails, she will be locked out until IT staff can determine whether she is a malicious insider or her credentials have been compromised. As it happens, there was an incident logged earlier in the week regarding a suspicious email message but the message did not appear to be part of a targeted attack. However, when Jane's identity is correlated with all the recipients of the message, IT staff begin to suspect Jane is a victim. Using the data collected regarding the suspicious email, team members are able to identify other possible victims of what may be an advanced persistent threat.

Symantec™ solutions are clear choice for cloud security

The cloud is enhancing the way enterprises do business, creating new ways to compete and increasing employee productivity. Employees are embracing these new opportunities, moving ahead even if the IT organization is not on board, using their personal devices to access data in unsanctioned cloud applications. It is the leadership who is ultimately responsible for protecting the organization and its data, and that means finding a cloud security solution that limits risk—and does so without impacting productivity in an increasingly complex cloud environment.

Symantec™ Identity: Access Manager is an industry-leading access-control platform that provides the foundation to meet your information protection needs. Access Manager tightly integrates with two Symantec authentication solutions, Symantec Validation and ID Protection Service and Symantec Managed PKI Service, to add two-factor authentication to all your cloud-based apps.

And to help discover and monitor all your critical data, at rest and in motion, look no further than the market-leading Symantec Data Loss Prevention solution. Symantec identity protection and information management working together provides a formidable layer of security to protect your sensitive data in the enterprise or in the cloud.

And protect you, the business leader, when the pendulum suddenly swings.

To find out more about how Symantec can help your organization, visit go.symantec.com/sam and go.symantec.com/dlp.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com