WHITE PAPER

CISOs' Guide to Enabling a Cloud Security Strategy: Focus on SaaS

Sponsored by: IBM Security

Pete Lindstrom
October 2015

Introduction

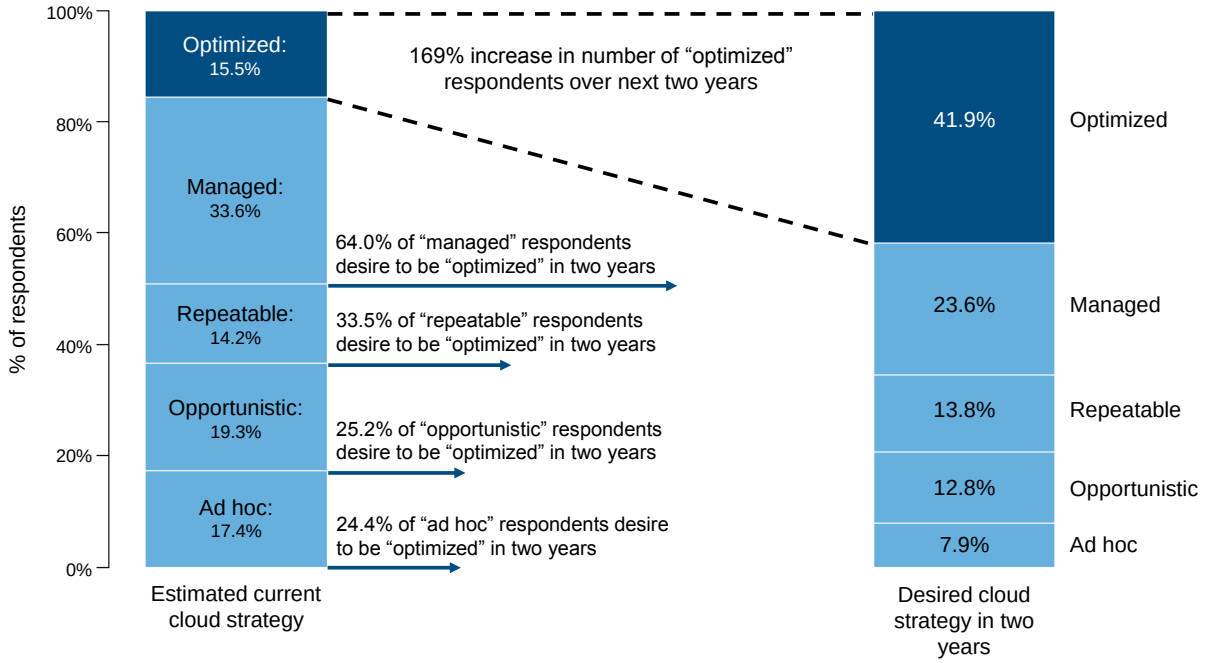
For years, enterprises and the security community have debated whether the cloud is more secure or less secure than the datacenter. Always a strawman argument, now that debate becomes moot. The cloud is here to stay. And the job now is to operationalize security across the datacenter and into the cloud architecture, fully covering evolving use cases and hybrid architectures along the way.

We are moving towards IT architecture models that integrate all sorts of topologies from datacenter to cloud and everything in-between. IDC surveys reveal that more and more enterprises are maturing their cloud strategies toward optimization over the next two years. (See Figure 1). A cloud security model must be flexible enough to align with these highly distributed architectures across many service providers. In particular, a model should address software-as-a-service (SaaS) architectures which are the most prevalent and architecturally distinct new entrants into an IT architecture model.

October 2015, IDC #259429

FIGURE 1

Self-Rated and Desired Cloud Maturity



n = 3,463 worldwide IT and LOB respondents

Source: IDC's *CloudView Survey,* December 2014

The forward-thinking enterprise is already fully engaged in various cloud projects and applying controls in an ad hoc way. More importantly, even the most conservative organizations are likely to have unsanctioned cloud apps in use by their employees. As these projects are moved from one-off proof-of-concept status to full integration into the enterprise architecture, the piecemeal cloud security solutions being put in place must be re-evaluated within the context of a broader security model to rationalize the individual components both among themselves and also within the scope of the existing security solutions inside the enterprise.

Protect your SaaS

The most immediate need for securing the cloud is protecting SaaS cloud applications. These applications are in abundant use by enterprise employees for purposes ranging from traditional customer relationship management to addressing ad hoc file sharing needs.

The sheer volume of adoption and usage justifies the focus, but more importantly these applications also vary significantly in their security profiles. Enterprises rarely have any ability to employ their own technical controls at the traditional network and host layers of an architecture, and each application has its own scheme for the type of protection available at the application layer.

Objectives for SaaS Security

In order to build their cloud security model, enterprises must first determine their security objectives.

While architectures are constantly changing, the principles of security remain the same. Organizations are always looking for elements of confidentiality, integrity, and availability for their data while factoring in needs for propriety (appropriate use) and productivity of their systems.

The various SaaS security options that address these needs include the following:

Discovery of SaaS application usage

At a high level, enterprises categorize two different types of SaaS applications: sanctioned or approved applications, and unsanctioned applications that must be assessed to determine whether the use should be sanctioned or denied. Due to their nature, these unsanctioned applications must usually be identified online.

Completeness of control coverage

Perhaps the biggest challenge in securing cloud applications is ensuring that all activity from the mobile workforce is being evaluated. A cloud security architecture must be designed to address all pathways from an enterprise's user base through to the cloud resources. This coverage may be gained by using some combination of endpoint agent, inline network proxy, and active API monitor. In addition, traditional edge solutions and the cloud resources themselves should be configured appropriately to direct traffic along the correct path.

Identity and access awareness

Users that access sanctioned cloud applications should be properly authenticated. Identity insight provides an opportunity for adding policies that apply to individual users across a number of cloud resources. Ideally, enterprises will continue to build out single sign-on architectures with federated resources, More importantly, the model should account for ongoing identity awareness to allow for policy decisions within sessions.

Activity and content monitoring

With solutions in the right places and providing identity awareness, a model can provide activity and event monitoring capabilities that capture logs for compliance as well as look for threats. Basic activity such as access requests and data submissions evolve into more complex ones, as applications and resources continue to build out APIs and other mechanisms for remote procedures.

Centralized security management

While enterprises operationalize cloud resources in an ad hoc manner based on projects and business units, the security professional must think more strategically. A centralized solution typically provides a lower TCO than one-off capabilities simply due to reduced training needs. In addition, the ability to provide protection through policies that apply to multiple applications from different providers and aggregate the activity and log information is enhanced and leads to better risk management. A central solution that is separate from individual cloud applications can often provide insight that the cloud solution providers are unable or unwilling to share.

Integration with existing security solutions

Of course, the same principles described above have applicability to existing on-premises architectures and security models. Enterprises should look for ways to integrate the processes and applications that currently exist with those being built out for cloud-based resources. This scenario may indicate a need for phasing out solutions or creating a more distributed model, for example, or it may point towards selectively using gateways and brokers to assist.

Discovering Cloud Applications in Use

Organizations often face the challenge of employees and business units taking their computing needs into their own hands. The reality of "shadow IT" has gotten a whole new life with the ease of connecting to cloud applications. Nowadays, these unsanctioned apps are prevalent across most enterprises.

The first step to operationalizing cloud security is through discovery of the cloud resources being used today. This identification can be accomplished in many ways. Collecting data like connection attempts and Web requests at network egress points provides key insight into the variety and volume of cloud applications being accessed by the endpoints inside the enterprise. From here, a rationalization can begin that evaluates the applications for functionality and use cases to determine which applications are – or should be – sanctioned, and which ones are unsanctioned and should be blocked or further justified.

It is worth recognizing that most unsanctioned applications have some value to the end user. They may fill some previously unidentified gap in services within the enterprise. Therefore, a progressive security group will continue to build out its understanding of enterprise requirements and develop strategies for turning unsanctioned apps into sanctioned ones.

Assessing Existing Security Solutions

Large enterprises already have huge investments in their security architecture. In the move to the cloud, they must determine which solutions are likely to provide some benefit and which will not. In addition, as architecture and models are assessed, a similar set of capabilities must be built out that are tailored to address cloud applications.

Some of the common solutions with capabilities that must be ported to the cloud are:

- **Secure Web gateways** can capture and assess the requests from endpoints to determine whether access is allowed. Having pioneered this capability with inappropriate Web sites, the solutions often provide information useful for a more thorough review of cloud application usage.
- **Identity management solutions** provide mature processes to provision, monitor, and deprovision users and accounts across many applications inside the datacenter. As cloud applications become more prominent, the need to provide a similar capability for the new applications increases in importance as well.
- **Threat management solutions** provide intrusion detection/prevention and security event management capabilities for identifying attacks against an organization's resources.
- **Mobile device management solutions** provide management capabilities for provisioning and deprovisioning mobile devices. Mobile-to-cloud connectivity creates a new path for security solutions to address.

Each of the solutions should be evaluated for their ability to address cloud applications. Some will likely be deficient in their visibility, for example, or their ability to integrate with cloud solutions.

Architecting the Cloud Application Security Model

With the strategic planning done, enterprises can follow their standard policies and practices to identify one or more appropriate solutions to evaluate that may suit their needs. Often, the alternatives revolve around suitability to task and ability to integrate with existing capabilities. The process can and should be iterative – many enterprises will already have piecemeal solutions in place to support small projects and proof-of-concept use cases.

At a broader procedural level, the enterprise should follow these steps:

- Identify the users, data, and applications within the scope of the project
- Map how the users, data, and applications interact with each other
- Instrument the paths among the elements with a solution for monitoring and policy enforcement
- Employ a solution that consolidates security management functions from disparate cloud applications into a single management console

Understanding IBM's Cloud Security Enforcer

IBM's Cloud Security Enforcer is a new solution the vendor is adding to its portfolio to address the challenges around cloud security models. The product fills in gaps that have developed between traditional security solutions and those needed for cloud security. It consists of a cloud-based proxy architecture with optional mobile app to integrate into the cloud security architecture.

Cloud Security Enforcer provides a host of capabilities as described below.

Discovery and Visibility

Cloud Security Enforcer leverages technology from its Qradar Security Intelligence Platform to analyze logs, events and network flows via manual push or automated collection. The product resolves source IP addresses to users – complete with account details – and destination IPs get checked with risk data provided by IBM X-Force, which tracks thousands of cloud applications with dynamic reputational analysis.

Identity and Access Control

Cloud Security Enforcer provides federated cloud single sign-on capability that leverages integrated connectors to popular cloud applications to provide simple access to add a new app. The product will provide risk-based access control and also integrates its reporting function with the same technology used in QRadar and applied to the cloud environment.

Threat Intelligence and Prevention

Application-layer traffic can be inspected for threats using the same technology as IBM's XGS IPS tailored to address cloud-based needs and to work with a cloud proxy architecture. At the operational level this provides threat signatures and protocol analysis, and uses a real-time threat intelligence feed from X-Force to provide more strategic capabilities.

Cloud Event Correlation

With active monitoring of user activity, Cloud Security Enforcer aggregates and correlates events across multiple resources to compare with active policies.

Policy Enforcement

Cloud Security Enforcer proxies mobile or off network traffic that does not travel through a corporate firewall. The product can enforce policies that are designed for custom and anomalous situations, and can redirect mobile traffic and/or coach users about policies.

Challenges

IBM's Cloud Security Enforcer provides identity-as-a-service functionality along with threat protection for cloud-based resources. This area is fast moving and many solutions have sprung up to fill the gaps. IBM must continue to innovate in this area with additional capabilities for complex policies and perhaps machine learning techniques. As an enterprise security provider, IBM must demonstrate that it can operate with flexibility and leverage its integration opportunities to provide a path for a strategic cohesive security model.

Conclusion

There is no doubt that cloud applications are a mainstay in today's enterprise IT architectures. Security professionals should embrace the move to the cloud and look for ways to align their security models with this new reality. Enterprises should look for ways to build in security controls that enable the move to the cloud and make the organization more efficient and effective, all while managing the associated risks.

SaaS applications are clearly the most important area that must be addressed. Enterprises must look for ways to maintain a level of control over their users, data, and applications all while conceding some control over the resources. The way to do this is with cloud security gateway solutions that can apply appropriate controls in appropriate ways throughout the new cloud application architectures.

At a broader level, the new IT enterprise is expanding its IT architecture to incorporate private and public cloud capabilities. The moves continue to drive security "up the stack" away from traditional network and host security to securing those fundamental elements – users, data, and applications. Enterprises are well-served by solutions that are built with integration among more traditional solutions and new cloud solutions.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com