WHITE PAPER

Cloudy or Clear?

CURRENT VISIBILITY CONDITIONS—PARTICULARLY AS THEY PERTAIN TO SECURITY—HAMPER ENTERPRISE ADOPTION OF CLOUD SERVICES

Market Pulse

Research Indicates Information Security Visibility Chasm with Cloud Services

Enterprises polled in a recent survey expressed significant interest in improving their visibility into the cloud services they are using or evaluating. Security was the biggest driver behind the desire for better visibility: companies want to be able to see and act on unauthorized and unwanted activity. This makes sense, as companies are more concerned about information security now than ever before.

And well they should be: governance, risk and compliance (GRC) initiatives have expanded and are a higher priority for companies around the world. Enterprises once primarily worried about warding off mischievous teenage hackers are now battling serious and costly attacks carried out by organized cybercriminals. At the same time, the economic attraction of public cloud services is fierce. Cloud services are gaining attention because they allow cash-strapped companies to push hefty capital expenditures (capex) into usage-based, pay-as-you-go operational expenditures (opex). This model makes IT expense budgets more manageable and predictable.

Many IT departments, however, perceive that being able to reap the cost advantages of cloud services while also being comfortable with service and security visibility is beyond their reach. IDG Research Services recently surveyed 132 senior IT professionals involved in information security and/or cloud deployments and learned there is a significant chasm between the level of cloud service visibility that is available and what is desired. According to the survey data, this gap is holding back public cloud service deployments, and better visibility into the cloud would spur enterprise acceptance and accelerate the adoption of cloud services.

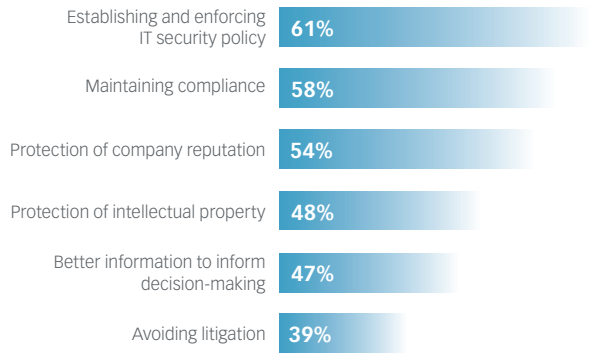
Key Findings

IDG Research Services' survey of information security and cloud professionals revealed the following:

- Only a small percentage of respondents were "extremely confident" in the adequacy of cloud network traffic visibility.
- A significant gap exists between the level of importance respondents placed on what visibility capabilities are desired and what is commercially available.
- Security is the biggest driver behind enterprises' desire for better cloud visibility.
- Most organizations have deployed multiple point solutions for cloud visibility and lack a comprehensive view of network activity.
- The majority of respondents are making it a strategic priority to get better cloud visibility during the next 12 months.

Figure 1:

Enterprise Goals with Cloud Visibility



SOURCE: IDG RESEARCH SERVICES, AUGUST 2012

CSO Custom Solutions Group

RSA

verizon terremark

Cloud Visibility Drivers, Requirements and Availability

"Visibility" is a relative term that describes the degree to which an enterprise is able to see, in a meaningful and actionable way, the activity taking place across its IT infrastructure and applications. There is a full spectrum of visibility levels. At one extreme is capturing and analyzing every packet that traverses the network, reconstructing sessions and alerting for unauthorized or unwanted network activity. The other extreme may involve simply conducting an after-the-fact audit using usage reports compiled from data collected during a given time period, such as each month or each year.

In between are such activities as viewing user logs of who accessed which applications either in real time or after the fact at varying frequencies, scanning for malware, and determining traffic pattern peaks and valleys across coarse or granular time periods. Where a given enterprise falls on the spectrum depends on what tools they invest in and what views a service provider is able and willing to provide. Visibility can happen at any or all layers of the traditional open systems interconnect (OSI) model, in real time or at preset frequencies. The visibility can be enabled using tools in which the enterprise invests, as a part of the service from the cloud provider or a mix of both.

The higher up the OSI stack an enterprise goes with cloud services, the more control it relinquishes. Relinquishing control—and responsibility—for many mundane functions is often desirable and the point of using such services. Using cloud services at the OS level, for example, means the cloud provider becomes responsible for updating and patching the OS, something the IT department no longer must worry about every day. However, the enterprise also gives up the ability to add new OS users themselves, which might or might not fit the organization's business processes and requirements.

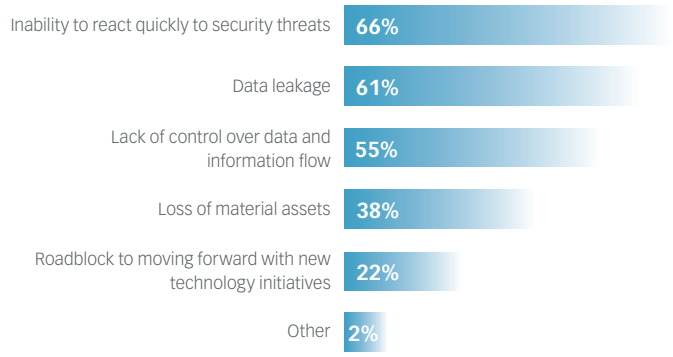
The best way for enterprises to determine the level of visibility they require is to assume that the same network monitoring data available to them in their private data centers will continue to be available using a cloud service.

Security Concerns Prevail

An enterprise will strive to attain a level of visibility that matches both its needs and comfort level. According to the IDG survey, the biggest drivers for wanting better visibility are related to security issues (Figure 1).

Security issues also drive respondents' biggest concerns over not having enough visibility into a cloud service infrastructure and their organization's network traffic behavior (Figure 2). Many respondents indicated, for example, that an inability to react quickly to security threats and possible data leakages were their biggest worries about limitations with cloud network visibility.

Figure 2:
Lack of Visibility Concerns



SOURCE: IDG RESEARCH SERVICES, AUGUST 2012

It's clear from these findings that security threats to confidential data and compliance violations top enterprise IT departments' lists of visibility issues. Whether reality or perception, respondents feel that moving resources into a third party's data center shared by other cloud customers is a risk, but one that would be mitigated by improved access and visibility into their own traffic flows.

Gaining deep visibility into a third party's network (the provider's) has always been tricky. Traditional service providers have monitored their own networks and offered traffic usage reports to business customers for years; however, for reasons related to integrity, performance, security and process, providers stopped short of granting customers unrestrained access and visibility into their networks. It's up to the carrier, not the business customer, to traffic-engineer optimal network infrastructures and manage traffic performance on its own public, shared-customer network.

The purpose of visibility before the era of cloud services was primarily for helping enterprises see their own usage volume trends and plan capacity accordingly. Today, enterprises want many of the control benefits of having a private network, particularly as they pertain to intrusions, malware and data leakage. But

they are also attracted to the cost and simplification benefits of paying for infrastructure and application services by the drink, and many appear uneasy at this time that the cloud can be secured as tightly as the traditional enterprise data center.

In terms of importance, survey respondents ranked the following resources as the most critical data types requiring visibility: employee/personnel files (89 percent), financial records (86 percent) and personally identifiable information (84 percent).

Where Are the Gaps?

Organizations surveyed indicated that they do not have the desired level of visibility into network traffic related to their cloud-hosted data. This is shown by how survey respondents rated the importance of various types of visibility compared with the availability of that visibility. A gap of 30 or more points between what respondents wanted and what they understood was commercially available to them was common in these findings (Figure 3).

At least in part because of these network visibility gaps, only 8 percent of respondents said they felt "extremely confident" about the adequacy of visibility into cloud data traffic. More than a quarter (26 percent) said they were "not very confident" or "not at all confident," while another 36 percent expressed a touch more optimism by describing themselves as "somewhat confident."

Visibility Impact on Cloud Adoption

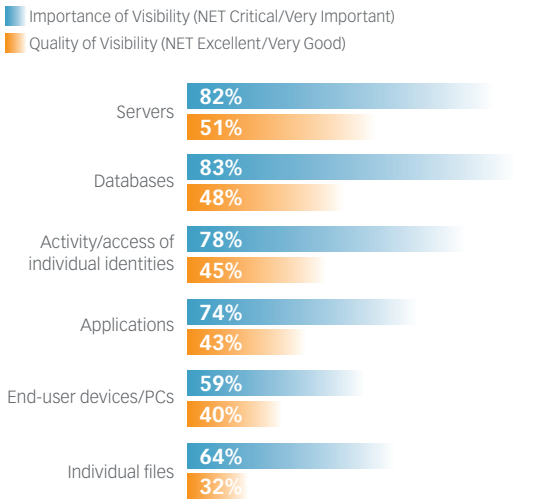
Survey takers were asked point blank if there was a relationship between the state of cloud service visibility and their willingness to deploy cloud services. Respondents indicated that there was. About two thirds said that they see visibility limitations as a cloud adoption roadblock, and about the same percentage said improvement in cloud visibility would increase their comfort with using the services (Figure 4).

Some of the hesitation may be real, perceived, or confused with having a third party handle a function that traditionally has been fulfilled in-house. The terms "cloud" and "public" may imply something less than secure, even if the provider is able to 1) give the enterprise customer the level of direct visibility to suit the organization's comfort level or 2) assume responsibility for security services on behalf of the customer.

In other words, there are varying models that undoubtedly carry different acceptance levels depending on the security posture of each enterprise. Depending on the size of the company and industry, organizations might turn to cloud services for different reasons. Small companies that care deeply about security might actually feel more secure in the cloud. Other companies that don't necessarily believe the cloud is more secure might have some resources with moderate risk levels for which the cloud savings outweigh risk.

Figure 3:

Importance of Visibility vs. Actual Quality Available



SOURCE: IDG RESEARCH SERVICES, AUGUST 2012

Sample Scenarios

Consider a small business that feels the expertise and staff size of the third-party cloud provider trumps what it can afford to hire and retain in-house. This organization might feel confident that if it procures security services for malware scanning/intrusion filtering, GRC management and application white listing, it will get a better result than if it attempted to handle the functions itself.

Similarly, as noted, a large enterprise with a moderate risk profile might be more concerned with offloading capex into opex using the cloud provider than with control and feel justified moving less sensitive resources into the cloud. Meanwhile, though, another large enterprise in a highly regulated industry might have a different view. The organization must decide whether security services available from cloud providers are likely to put it at more or less risk or whether the situation is a draw. Highly regulated companies using cloud services will likely

demand a level of visibility into network behavior that is at least on par with what they can get by running their own data centers and network monitoring tools and, if they can't get it, forego cloud services altogether.

There are also differences in cloud deployment models to consider as they pertain to security visibility. For example, who is responsible for running down alerts when they occur? Answers to such questions depend on what's spelled out in the service contract. If the cloud service provider has been retained for a set of services that include security, for example, then it's the provider's job to actively monitor traffic, filter anomalous connections and packet signatures off of the network and to white list/filter applications.

If, on the other hand, the enterprise contracts for a "pure visibility" service and keeps security functions in-house, the provider's responsibility is to collect and provide the needed information to the customer only. It's then up to the enterprise to follow through on the incident response functions itself.

Fragmented Capabilities

In addition to needing certain levels of network visibility, how enterprises get that visibility seems also at issue. Based on the rankings provided by respondents, the norm for being able to see unauthorized network activity generated in the cloud requires multiple point solutions and tools, which can be complex, costly and sometimes ineffective. In some cases, respondents felt they had little to no visibility into network activity on a day-to-day basis. Some views were available in real time, but not others.

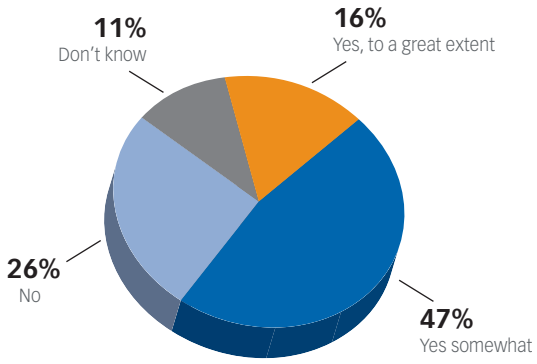
These inconsistencies need resolving. Resolution could take the form of cloud security services from providers or visibility services from providers combined with on-premises tools that give enterprises a comprehensive view of what's happening in real time. Enterprises, or an entity on the enterprise's behalf, must remain able to react to security threats quickly and use historic monitoring information to ensure compliance with security access controls and policy.

Conclusions

In these early days of cloud services, the industry is fragmented in terms of the availability of visibility into business customers' network activity. Different cloud providers and cloud technology vendors offer different levels of visibility, which does not necessarily suit organizations of all sizes, industries and security

Figure 4:

Visibility Limitations as a Cloud Adoption Roadblock



SOURCE: IDG RESEARCH SERVICES, AUGUST 2012

postures. Most organizations are primarily concerned with giving up network visibility because of security worries, particularly as attacks become more sophisticated and formalized, GRC programs grow tighter and companies stand to lose more if a breach should occur.

That's why a large majority of organizations—79 percent of the IDG survey respondents—are making the improvement of cloud network visibility at least a moderate strategic priority over the next 12 months. They are motivated by fears about their responsiveness to threats, data leakage, loss of business and reputation damage. Given the importance respondents place on the proper levels of visibility and the ability to mitigate bad behavior, enterprises are advised to make sure that the level of visibility available with a cloud service offering they are considering matches the company's comfort level and risk tolerance.

For more information on Verizon's security products and services, visit **http://www.verizonbusiness.com/us/Products/security/**

For more insights and features on security from RSA, visit **http://www.emc.com/ emc-plus/rsa-thought-leadership/index.htm**

CSO Custom Solutions Group

RSA

verizon terremark