

Network Box: Guide to Cloud Security – What is (and what isn't) suitable for the cloud

To paraphrase President Clinton – 'it's the cloud stupid'. While there are a lot of exciting applications being ported into the cloud and the debate around how secure some cloud services continues, this guide addresses the separate issue of delivering security via the cloud: what can and what can't be done.

There has been considerable publicity around security services in the cloud being the next big thing and, as with many new IT trends, the predicted numbers are impressive. Infonetics Research recorded growth of [70% in 2009](#) totalling \$9.4 billion, up 12 per cent from 2008. This growth has been fueled primarily by demand for content security services (e.g. web, email and archiving).

So what's the reality behind the predictions?

Cloud solutions offer some great opportunities in security, particularly in email and web security; and there are some exciting developments in cloud services in these areas. But it is important to remember that you can't provide complete network security purely from the cloud. The cloud is likely to play a more important role in security in the future, but needs to be combined with on-site security systems to provide a completely secure network.

What the cloud does well

We consider that there are four main areas of network security that are ideally suited for delivery via the cloud.

Email security

Email security, including anti-spam, anti-virus and anti-phishing - is well suited to being handled in the cloud; and Network Box provides this service for many enterprises and SMEs that want the ability to scale rapidly and host email security remotely. It also has the benefit of providing the customer with a form of email disaster recovery which is useful if the local email server is down for any reason.

Email encryption

For those companies requiring additional security the cloud can also provide email encryption for all emails passing through an organisation's network and across the Internet. By encrypting the email on the cloud servers, it can be downloaded to the recipient if the recipient has the necessary authentication details. Neither end needs special software to do this and the email can even remain on the cloud servers whilst the recipient reads it. This ensures the email will not be kept unencrypted by the recipient.

Email Archiving

With growing commercial, legal and compliance demands for emails to be stored for various time periods, the ability to archive email is one area in which the cloud excels. Rapid search and retrieval makes a cloud archiving solution operationally attractive and a highly competitive hosting market makes it affordable. Companies should be aware that some countries, such as Germany, require them to archive all information and data in country. Offsite backup is always a good thing, and this will secure the archive with professional providers replicating data to geographically disparate sites.

Another consideration for any IT manager is that with a cloud solution processes are in place that ensures that company personnel cannot alter the data and there should be clear logs provided showing who searched for what, and what they did with it.

Web Cleansing

Web cleansing is always a controversial topic from an employee's point of view. However, it is crucial in protecting the organisation from drive-by downloads, malicious scripts and virulent applications. Also many companies want to protect themselves from legal liabilities, while improving productivity, and managing bandwidth usage. By filtering in the cloud, companies can be confident that the web content their employees are surfing (whether in the office or on the road) complies with their internet and social media policies; and will not be damaging to employees, the business or its network.

What can't be secured in the cloud

While there are obvious advantages of providing services like email and web cleansing and control in the cloud, there are security operations that have to be serviced on site.

Firewall

The most obvious security element to start with is the firewall. Even when de-perimeterisation of the network is becoming more common, the firewall remains the central component of any network's defense and protection. Whilst email and web can be protected in the cloud, if the firewall is not configured correctly, managed and updated, an organisation will be at risk from its network being comprised in a plethora of ways. These attacks could include hackers, viruses or worms. In addition, the misconfiguration of the firewall could negate the effectiveness of the cloud solutions and usually changes to the firewall are needed to deliver the full benefit of the cloud.

Intrusion Detection

Online criminals are becoming ever more inventive in the approaches that they are using to access data illegally or to extort money through numerous ploys like denial of service attacks. This makes the use of effective on-site intrusion detection and prevention systems ever more important, providing alerts on abuse – either on internal or external threats. This is crucially important in analyzing data after security events have occurred. Combine this with the viruses being introduced to the network through USB keys and laptops used remotely and intrusion detection becomes a critical part of a comprehensive security and protection strategy. With the Conficker outbreak IDS was central in identifying infected systems, allowing organizations to isolate and clean infected systems.

Remote Access

Remote access by user can also be a major security concern. Many companies leave themselves open to abuse by the unsecured use of remote desktop or similar easy but insecure access techniques. However, companies frequently find the setting up of secure virtual private networks to be difficult and the temptation to use less secure options is quite strong. Obviously, this critical function cannot be provided by the cloud and yet can be central to an organisation's productivity. It is also very important that the remote users only have access on the agreed protocols so if the remote user gets infected, the organisation is protected.



Security Policy

One of the benefits of the cloud model is peace of mind for the IT team. If someone else is handling that aspect of the network security, it takes the burden off the IT team. But this doesn't replace the need for a robust and comprehensive security policy that covers and governs a wide range of issues including data access, web-browsing habits, use of passwords and encryption, email attachments and more. Although the process of developing these policies can be outsourced to an expert, their implementation and management must be done in-house for them to be relevant, effective and current.

Despite clear company security policies, no user likes having to remember a large number of passwords, and many of the ones they do use are not as secure as they could be. But passwords remain a critical first line of defense and how they are managed on the ground is crucial. We had an incident reported to us recently of a NHS worker being able to reset their password for a NHS email web portal on the phone without being asked any security questions – driving a horse and cart through the carefully planned security policies and procedures. Making sure that this sort of mistake does not occur requires that the security policy is followed which requires management and monitoring.

Routing

The best laid network security plans can easily be undermined by a failure to understand where data is being routed to and from. Incorrect routing can result in security measures being bypassed or reduced. If it is not known how the data is routed or where it might be routed, it can leave the company open to direct attacks. An all too common error is to have two gateways where one is tied down and complies with best practice; the second is not so carefully managed and is doing port forwarding to internal servers. If one of these servers happens to be the email server, the company can find itself as a spam relay within minutes or, more worryingly, compromised if vulnerabilities exist or weak passwords being used.

Device security

Another area of network security that the cloud cannot address is device security. The growth in the use of USB sticks to transfer data or the provision of information by suppliers on sticks and discs create security risks when these are plugged into a workstation. This threat is likely to grow as more smart phones are connected to company LANs without due care and process.

Hand-in-hand with the introduction of viruses onto the network via USB keys and infected files is the unauthorised downloading of data onto a portable device and that device being lost or stolen. Our experience is that one of the biggest causes of data loss is DVDS, USB keys and laptops being lost or stolen from users while they are out of the office. Unfortunately, no matter how sophisticated your cloud protection might be it can not address the vagaries of human behavior.

Updates

The daily updates to hardware and software – routers, firewalls and office applications etc. - that are so much a part of IT management are not ideally suited to be handled through the cloud and without them you cannot be confident that your security is up to date and fully operational. Alongside these updates sits the encryption of databases, and data held on desktops and laptops which unless the database is provided as software as a service cannot be encrypted in the cloud.



NETWORK BOX
Managed Security Services
Tel: 0800 107 6098

Summary

In summary, the cloud is, and will continue to be, a critical part of many companies' security strategy. This role is likely to grow as a raft of new services are developed and commercialised and users' level of familiarity and comfort with this approach to service delivery develops and grows. But it is also likely, that the most effective network security strategies will be a hybrid model that takes the best that the cloud has to offer and combines it with the skills and focus of experts working on the ground.