You Cannot Secure What You Cannot See

How to make your hybrid cloud environment visible and secure

Publication Date: June 13, 2018

Author: Maxine Holt

Summary

Ovum view

Cloud can transform enterprises, yet simultaneously it creates new security challenges. Although the security posture of an organization may be strong, bringing cloud into the equation creates a new attack vector – and this is a vector that the organization doesn't have the same level of control over.

Yet enterprises remain responsible for the security of their data, applications, and services in the cloud. As such, security and network professionals are keen to have sight of the traffic relevant to their organization in these environments. Traffic data can be "backhauled" to a customer's data center for analysis, but this can be time-consuming and expensive. Instead, organizations can choose to monitor traffic directly in the cloud.

Visibility of traffic can help enterprises identify potential threats earlier in the cyberattack chain. Acting quickly is essential to limit any possible financial, reputational, and legislative damage that could be caused by a compromise of data, applications, or services in a cloud environment.

Key messages

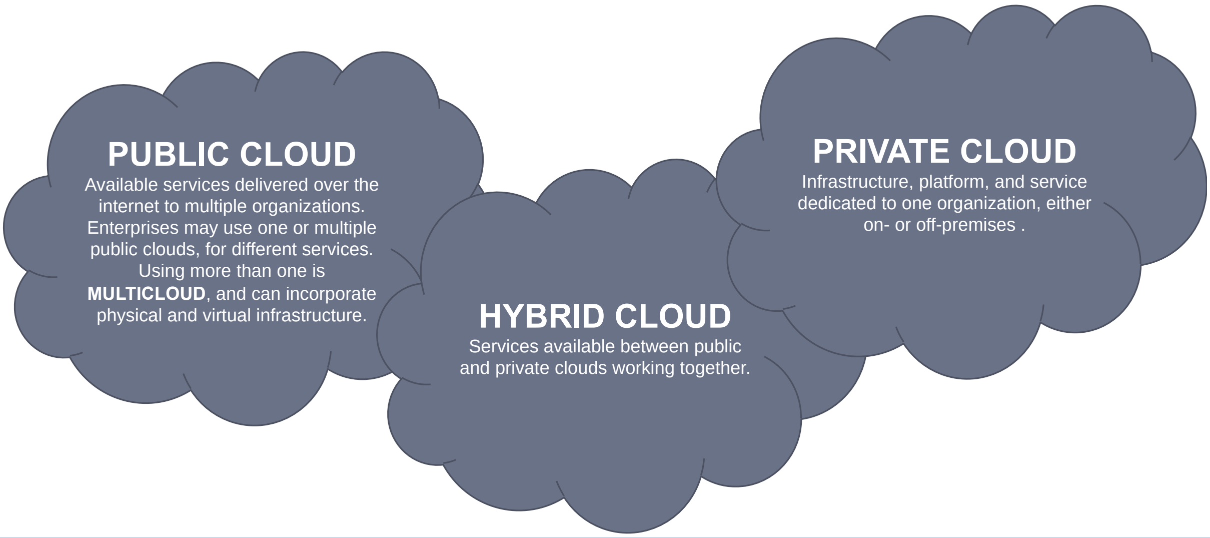
- Cloud can be transformative – but security may be an afterthought.
- Cloud adds another vector to an organization's attack surface.
- A lack of visibility and monitoring can lead to delays in resolving security failures.
- Organizations must take responsibility for the security of their data, applications, and services in the cloud.
- Be prepared and act quickly to identify and contain attacks.
- Enhance visibility and security, rapidly and cost-effectively, by monitoring packet data in the cloud.

Cloud can be transformative – but security may be an afterthought

In the rush to create digital capability using cloud computing and services, security is often an afterthought, if not forgotten completely. Without doubt, the power of cloud can transform enterprises, yet simultaneously it creates new security challenges.

In response to the rush toward cloud, some larger organizations have developed clear cloud strategies in recent years. McKinsey reports that leading organizations have migrated more than 50% of their processing workloads. This has resulted in a more strategic and organization-wide approach to cloud adoption via a managed program, rather than the opportunistic line-of-business uses seen in the early years of cloud. Today, enterprises have three main cloud environments available for use (see Figure 1).

Figure 1: Cloud environments used by enterprises



PUBLIC CLOUD
Available services delivered over the internet to multiple organizations. Enterprises may use one or multiple public clouds, for different services. Using more than one is **MULTICLOUD**, and can incorporate physical and virtual infrastructure.

HYBRID CLOUD
Services available between public and private clouds working together.

PRIVATE CLOUD
Infrastructure, platform, and service dedicated to one organization, either on- or off-premises .

Source: Ovum

Enterprises typically use a combination of their own data center and cloud environments to store and process data.

Most cloud providers comply with many security requirements (e.g. ISO/IEC 27017 security for public cloud services, ISO/IEC 19086 cloud service agreements and service-level agreements [SLAs], and ISO/IEC 27036-4 information security risks) and actively manage their own security – since suffering a security incident could cause untold reputational damage. The established security practices of cloud providers include protecting data behind a high-grade firewall, locating their data centers in a physically secure environment unknown to most individuals and organizations, and dealing with attacks on their infrastructure and services.

However, using cloud environments does not transfer risk from the cloud user to the provider, and enterprises remain responsible for the security of the data, applications, and services in any cloud they use. Potential security challenges in the cloud include the following:

- Data in transit over the public internet, unless encrypted, could be vulnerable to breaches.

- Direct governance is lost when some control is given to the cloud service provider, potentially without an adequate SLA to ensure that security issues are dealt with appropriately.
- Network data is not visible and security threats remain unmonitored.
- Responsibilities are not made clear to the cloud user by the service provider, potentially leaving gaps in security defenses.
- An attacker could tamper with or delete corporate information.

Security is a shared responsibility between the cloud provider and the customer organization.

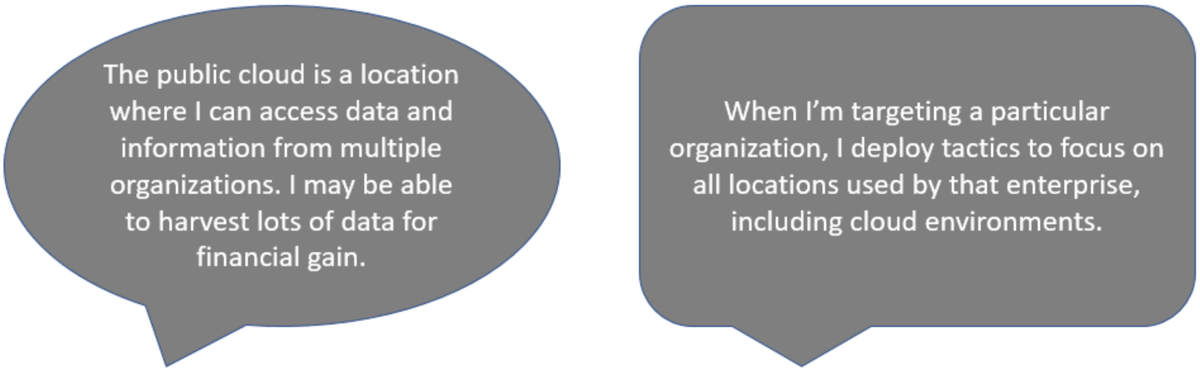
An increased attack surface requires increased vigilance

Cloud adds another vector to an organization's attack surface

Attackers are already taking malicious advantage of the possibilities that cloud environments present, particularly public and hybrid clouds, where multiple parties use one underlying environment.

Threats range from organized criminal groups and petty criminals seeking to generate revenue, to hacktivists and individuals bent on wreaking havoc. As an extension to an organization's infrastructure and applications used to operate on a day-to-day basis, cloud adds another vector to an organization's attack surface. Consider a couple of potential perspectives of an attacker, shown in Figure 2.

Figure 2: Potential perspectives of an attacker

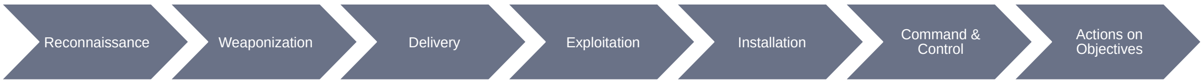


The public cloud is a location where I can access data and information from multiple organizations. I may be able to harvest lots of data for financial gain.
When I'm targeting a particular organization, I deploy tactics to focus on all locations used by that enterprise, including cloud environments.

Source: Ovum

Attackers follow a fairly regular process – often referred to as the cyber kill chain or cyberattack chain – when targeting systems or information. Originally developed by Lockheed Martin, the chain is shown in Figure 3. Each stage presents an opportunity to detect and react to an attack. The closer to the beginning of the chain that an attack can be stopped, the better.

Figure 3: Cyberattack chain



Source: Lockheed Martin

In cloud environments, attackers progress through the above chain in the same way as when they target on-premises infrastructure, systems, and data. After performing reconnaissance and building malicious code that can be delivered through a back door, attackers can launch their operation. Installing malware on the target gives attackers access to the systems needed to reach their objectives.

Using tactics including social engineering and more sophisticated means (e.g. exploiting technical vulnerabilities, modifying compromised accounts, and escalating privileges), malicious actors can masquerade as legitimate users and steal information or compromise systems. User access and – even worse – privileged access is often used by attackers throughout the chain to infiltrate public cloud services and subsequently exploit their security gaps.

Occasionally, line-of-business users deploy cloud services that the IT and security functions are unaware of, to get faster access to needed resources. This is often referred to as "shadow IT," and the use of such cloud services outside the control of IT expands the organization's attack surface.

A lack of visibility and monitoring can lead to delays in resolving security failures

Although cloud adopters have limited access to the cloud provider's infrastructure, they are still responsible for the security of their data, applications, and services in the cloud.

In addition to the (already discussed) established security practices of reputable cloud providers, organizations are keen to have visibility of the traffic that is passing through this public/hybrid extension to their IT infrastructure, platforms, and services. Without this visibility, those responsible for an organization's network and security cannot spot potential problems or respond to threats.

Used in conjunction with an understanding of the cyberattack chain, traffic analysis can highlight unexpected or suspicious behavior, help identify potentially malicious actors who are snooping around, point out a potentially damaging payload being executed, and so on.

However, the ability of a cloud user to analyze traffic moving between the virtual resources supplied by cloud providers is often limited. In public and hybrid cloud environments, the traffic flowing between endpoints and cloud-based services is not directly observable because it is traveling on infrastructure that is not under the direct control of the enterprise. Digital footprints are still generated – by both legitimate and malicious traffic – but they are effectively invisible to an organization's security and performance monitoring tools and staff.

A lack of visibility can mean that important clues pointing to underlying issues go unnoticed, such as malware moving laterally through an organization, an unusually large number of database requests coming from a particular user due to a compromise of that user's credentials, or an employee/temporary worker sending sensitive data to an unapproved file-sharing service to access while working from home later. Many breaches have occurred due to a misconfiguration of cloud resources or an exposure caused by an application interface.

Accept responsibility, act quickly, and enhance visibility

Organizations must take responsibility for the security of their data, applications, and services in the cloud

Security is about much more than technology. User communities (the workforce, customers, partners, and suppliers), governance, risk, compliance, people, and process are all levers that affect security. Recognizing these levers and adapting accordingly means that organizations need to strengthen their ability to quickly detect a threat or breach, contain the attack, and initiate recovery – all while limiting the impact on application performance.

Organizations must update their security practices to reflect a world increasingly dominated by cloud computing and continually subject to cyberthreats. Most enterprises have moved at least some operations to the cloud, so gaining visibility into traffic in these environments should be addressed sooner rather than later.

A visibility platform that can directly access, aggregate, filter, and deliver traffic from an organization's many clouds helps monitoring solutions perform more efficiently. Furthermore, the packet data that the visibility platform provides can help security analysis and forensics in the detection of sophisticated attacks.

Good practice suggests that an organization's security professionals should regularly test the security of the cloud environments in use. This can help to identify gaps in responsibilities and consequently ensure that vulnerabilities are addressed. It can also improve the speed of detection and containment of attacks.

Be prepared and act quickly to identify and contain attacks

Many organizations expect that their cyber defenses, and those of their cloud providers, will protect the enterprise from incidents and breaches. However, annual security research has shown that data breaches and cyberattacks will continue as long as there is an incentive for hackers.

Some organizations are unprepared for such events – often referred to as a lack of cyber-readiness. Cyber-readiness must extend across an organization's entire IT estate, including cloud environments. A security incident management framework is necessary, to provide a plan to help resolve security incidents and breaches quickly and effectively.

The Cloud Security Alliance (CSA), an organization dedicated to security best practices, notes that the ability to identify, obtain, preserve, and analyze potential digital evidence is now a critical business capability required to support breach investigations. Cloud forensics are also important when performing root cause analysis, for rebuilding systems lost during accidents or disasters, and for complying with regulation or legal proceedings. In all of these circumstances, an organization requires a highly effective platform for accessing the digital traffic that impacts their business, irrespective of the environments that the traffic crosses.

Enhance visibility and security, rapidly and cost-effectively, by monitoring packet data in the cloud

It is possible for a cloud provider to send log data to the relevant data center of a customer organization for analysis. However, analyzing log data can be time-consuming for the customer and require the purchase of new tools. In addition, the more advanced security solutions use detailed packet data, as opposed to log data, to correlate events and identify attacks.

Gaining granular visibility of cloud traffic is essential for organizations using clouds in production. Cloud visibility solutions access packets moving between virtual resources, to eliminate blind spots that can result from east-west traffic. In addition, having access to packet-level traffic data provides information about the context of the interaction, which can help identify the root cause of an issue or the source of an attack more quickly. Some enterprises have adopted a single visibility platform with access to traffic in all of their operating environments, and can use that single solution to deliver filtered data to all of their security and forensics solutions, both in the cloud and in the data center. Using a single platform has obvious benefits for efficiency and management, as well as helping the many organizations facing security workforce shortages.

A cloud-agnostic, cloud-native visibility platform offers

- visibility of all traffic (including east-west and server-to-server) moving through any public, hybrid, or private cloud
- the elimination of blind spots that can harbor threats and multistage attacks throughout the cyberattack chain
- aggregated and integrated visibility of traffic in hybrid environments
- unlimited scalability to keep up with cloud deployment
- fast, direct delivery to cloud-based tools and solutions, to avoid the cost of data backhaul
- the ability to filter raw packet data, aiding the efficiency of monitoring solutions.

Taking these benefits into consideration, organizations with operations in the cloud should investigate visibility architecture and platforms.

Appendix

Author

Maxine Holt, Research Director, Infrastructure Solutions

maxine.holt@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.informa.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo