BUSINESS WHITE PAPER

EXECUTIVE SUMMARY

One of the key challenges organizations faced, when managing security across the cloud environment, is a lack of visibility. Within their own data centers, organizations can deploy security and monitoring tools to get a complete view of the activities inside their IT environment. However, when they move their workloads to a cloud environment operated by a third-party vendor, they can no longer deploy their monitoring and security tools. To regain visibility and control in the cloud, organizations must unlock the access to the cloud traffic and enable their best of breed security tools to protect their assets in the cloud.

INTRODUCTION

Cloud is a reality. Businesses of all sizes are embracing the cloud in order to gain the speed, agility and cost efficiency to grow their business. Moving to the cloud is no longer just an IT or technology decision. Rather, business executives are driving digital transformation for faster and better business outcomes. In many cases, it's a board room discussion.

However, many organizations may not be aware of their shared responsibility for cloud security with the cloud providers. Cloud providers such as Amazon Web Services and Microsoft Azure are typically responsible for security of their physical infrastructure up to the hypervisor layer. Resources above the hypervisor layer, such as the virtual networks, applications and data are the sole responsibility of the organizations.

The Cloud Security Alliance (CSA) clearly stated that, in its 2017 report Treacherous 12 Top Threats to Cloud Computing Plus: Industry Insights, "Cloud providers often have good security for aspects they take responsibility for but, ultimately customers are responsible for protecting their data in the cloud."

TOP CLOUD SECURITY THREATS

To identify the top concerns, the CSA conducted a survey of industry experts to compile professional opinions on the greatest security issues in cloud computing. Here are the top five cloud security issues (ranked in order of severity per survey results):

1) **Data breaches -** A data breach may be caused by a targeted attack, human error or application vulnerabilities. It might involve information not intended for public consumption, such as personal health information, financial information, personally identifiable information, trade secrets, and intellectual property. An organization's cloud-based data may have value to different parties for different reasons.

2) **Insufficient identity, credential, and access management -** Bad actors masquerading as legitimate users, operators, or developers can read, modify, and delete data. They may snoop on data in transit or release malicious software that appear to originate from a legitimate source. As a result, insufficient identity, credential, or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users.

3) **System vulnerabilities -** System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a system to steal data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system put the security of all services and data at significant risk. With the advent of multi-tenancy in the cloud, systems from various organizations are placed close to each other and given access to shared memory and resources, creating a new attack surface.

4) **Account hijacking -** Account or service hijacking is not new but cloud services add a new threat vector to the landscape. If attackers gain access to a user's credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information and redirect clients to illegitimate sites. With stolen credentials, attackers can often access critical areas of cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

5) **Malicious insiders -** A malicious insider such as a system administrator can access potentially sensitive information, and can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on cloud service providers for security are at greater risk.

THE IMPERATIVE FOR TRAFFIC VISIBILITY

To combat these security threats and minimize risks, organizations need to have access to the cloud traffic in order to gain complete visibility and control of their cloud environment. They cannot secure what they do not see. Imagine if their cloud environment is breached, how are they going to identify the root cause of the problem and respond quickly? Without the ability to examine traffic data before, during, and after the breach, they may not be able to perform proper forensic analysis and take remediation actions in a timely manner. Therefore, having complete visibility of the traffic data inside the cloud is critical in detecting malware, anomalies and data exfiltration in the same way they do in the data centers.

SHORTCOMINGS OF EXISTING TOOLS

The dynamic nature of the cloud environment makes it extremely difficult for security operations teams to monitor activities inside the cloud. A new approach to unlock access to cloud traffic is needed as tools designed for traditional data centers and those provided by the cloud providers fall short of expectations.

Traditional on-premises monitoring tools cannot monitor cloud traffic due to the lack of physical host or static network topology to instrument monitoring devices or probes. While cloud providers offer basic metrics on resource utilization, availability, topology or events, they generally lack sufficient context and intelligence on network activities for real-time operational monitoring and threat detection. Security Information and Event Management (SIEM) tools collect flow logs, traps and alerts to offer analytic metrics. However, they do not capture actual traffic flow among virtualized resources.

Several vendors offer agent-based tools today to capture cloud traffic. However, these tools introduce management overhead and cannot provide visibility into PaaS applications, docker instances, or serverless solutions.

WHERE AND WHEN TO MONITOR CLOUD TRAFFIC

The need to monitor traffic in the cloud is no different than in the traditional data centers. In most cloud usage models, there are five (5) attack surfaces where traffic monitoring and security controls are highly recommended (see figures 1 and 2):

1) Between the organization’s cloud and the corporate network
2) Between the organization’s cloud and any Internet end point with a public IP address
3) Between virtual machines within a subnet, between subnets, and between virtual networks
4) Between the organization’s cloud and third-party cloud services
5) Between PaaS and other cloud services

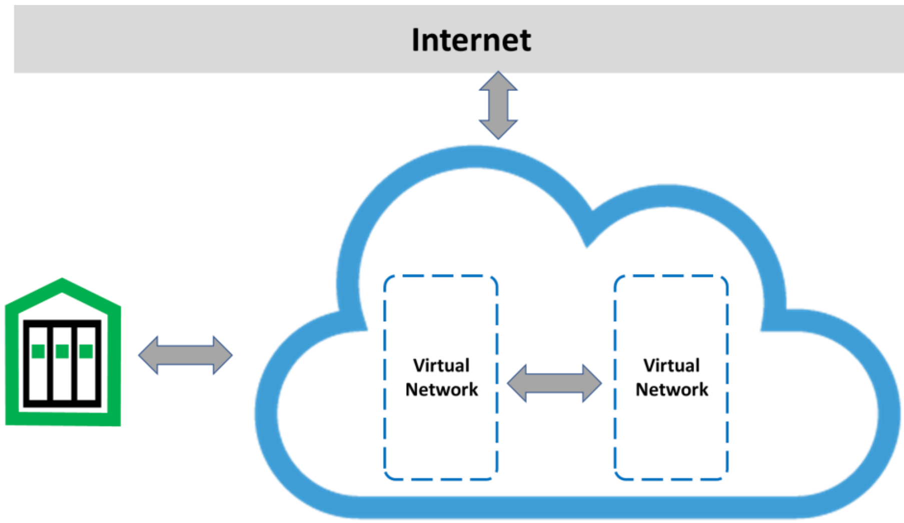

Figure 1. Monitor traffic between the cloud, internet, corporate network and virtual networks

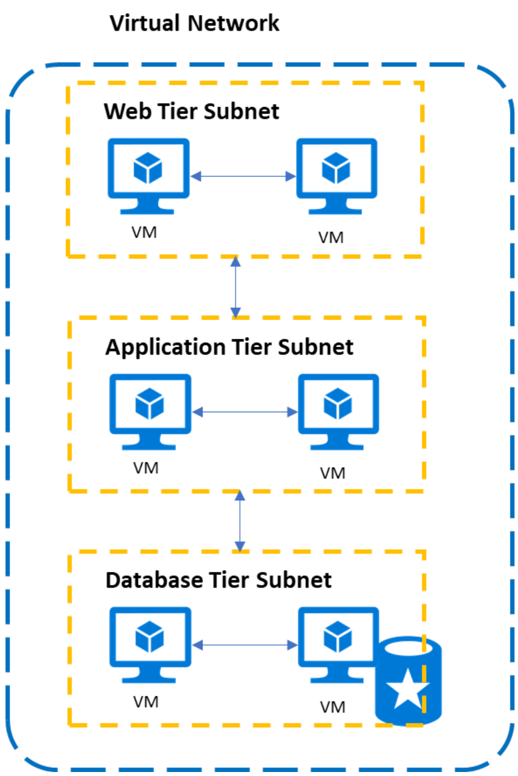

Figure 2. Monitor traffic between VMs and subnets

At each of this inspection point, there is a need to perform full packet capture for incident response and forensic analysis. Depending on the organization's needs and risk profile, traffic monitoring may be event-driven (turn on when an alert is triggered) or turned on 24x7 to provide continuous monitoring.

NUBEVA STRATUSEDGE™

Nubeva StratusEdge™ can capture full traffic packets in IaaS and PaaS environments, between virtual machines, subnets, virtual networks, and even platform services such as .NET/PaaS without agents. It can be deployed in your private account as VM instances and inserted "in-line" as a network tap between the source of communication and the destination. Its intuitive GUI design and RESTful APIs guarantee fast deployment and ease of management. It is resilient, high-performing, and can scale up and down automatically to match your workload demand.

In addition, Nubeva StratusEdge™ can feed traffic data to your existing monitoring and analysis tools, including but not limited to:

- Data Lakes
- Network Packet Brokers
- Security Information and Event Management Tools
- Security Analytics Tools
- Application or Network Monitoring Tools
- Open Source or Custom-built Tools

The data integration feature of Nubeva StratusEdge™ allows security operations teams to run next-generation firewalls or entire security technology stacks without functional compromise inside their public cloud environment, just as they do in the data centers. As a result, they can extend their existing on-premises security investment and policies to the cloud.

A PEACE OF MIND IN CLOUD

In summary, if organizations cannot quickly and accurately see what is going on across their cloud environment, they run the risk of not knowing when they are being attacked and how they can respond effectively. Hence, they need traffic visibility inside the cloud and the ability to 'insert' security control points. With Nubeva StratusEdge™, they can gain complete visibility and control, while leveraging and extending their existing tools and security policies to the cloud. They can accelerate their cloud migration journey with better clarity and confidence.

Learn how to eliminate the visibility blind spots of the public cloud and enable the best of breed security tools to protect valuable assets in the cloud, please visit www.nubeva.com