SOLUTION BRIEF

Securing Your Microsoft Azure Virtual Networks

IPS security for public cloud deployments

It's no surprise that public cloud infrastructure has experienced fast adoption. It is quick and easy to spin up a workload, often taking only a few minutes, with additional capacity being readily available to add as needed. Microsoft Azure is a popular choice for cloud infrastructure and platform services. The agility Azure offers fits well within the context of modern, global markets and economies.

Connect With Us

Public clouds offer convenience, cost savings, and the opportunity to shift from a capital expenditure to an operational expense model. They also offer highly scalable and flexible infrastructure, often more than most organizations could accomplish on their own. Despite these gains, you are still responsible for protecting your data and the software you run in the cloud.

While Azure provides world-class services that are secure at the infrastructure level, such as the physical elements of storage and databases, they make it clear through their Shared Responsibility Model that their customers are ultimately responsible for protecting everything they are deploying in the Azure infrastructure—which translates into everything above the physical infrastructure and hypervisors. Azure provides security "of" the cloud, and enterprises must protect what they are deploying "in" the cloud.

Almost all organizations use additional security products for their Azure deployments, but many do not realize that the virtual networks accompanying Azure workloads are part of their security responsibility. Deep inspection of traffic bound for workloads, looking for remote calls, application denials of service, or even evidence of callbacks, is out of scope for the infrastructure protection Azure provides.

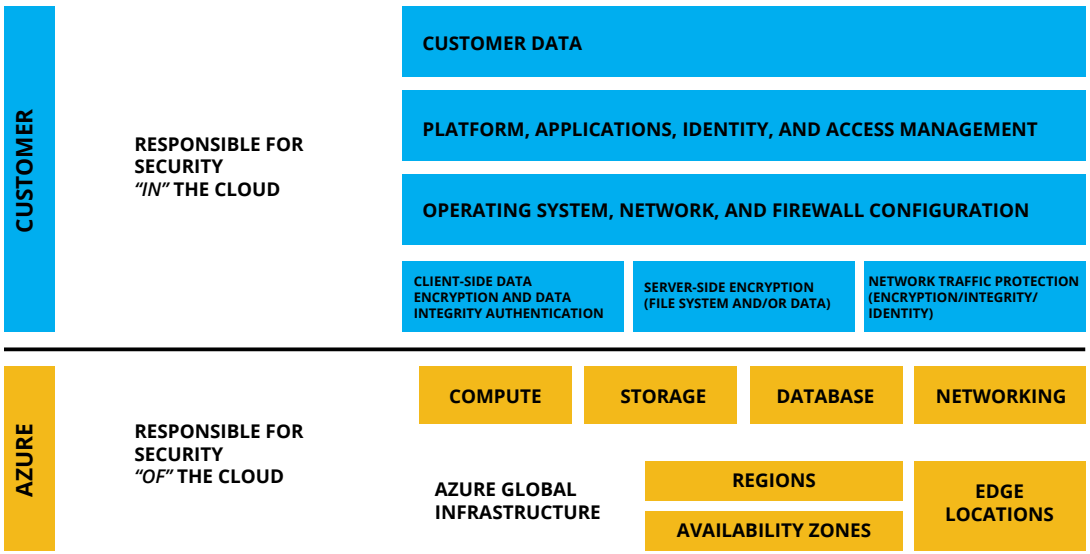

Figure 1. Azure Shared Responsibility Model (https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91)

Top Challenges for Protecting Workloads in Azure

Organizations typically lack the capability to detect and block known and unknown threats across virtual networks in public cloud environments such as Azure. Here are some of the top challenges:

- Protection of the organization's public cloud deployment:
  - Performing microsegmentation to apply appropriate security policies to different workloads
  - Ensuring that security policies stay in place and move along with dynamic workloads
  - Protecting the operating system and applications from known exploits, malware, and zero-day attacks
  - Protecting virtual networks such as Azure Virtual Network (VNet)
- Detection of threats that successfully infiltrate public cloud environments:
  - Visibility of malicious activity in the public cloud
  - Detecting not just north-south, but also east-west attacks

In addition, many organizations have insufficient staffing, and those available may not have the expertise in virtualized, public clouds to properly secure the environment.

What's Different About Cloud

Scalability

The public cloud provides organizations with benefits such as nearly unlimited scalability with on-demand resources readily available as needed, so any changes in activity level can be handled very easily.

IT point of view: What IT desires is security that can scale along with their workloads, since cloud workloads scale dynamically and security must be able to scale with increasing demands, while at the same time be lightweight enough to not impact performance of the applications running in the cloud.

Protection and Detection

Traditional security solutions were not designed for the public cloud, and something that works well for on-premises deployments is often not appropriate.

IT point of view: IT is seeking to understand how to properly protect their public cloud workloads and ensure that they can continue to protect the business, including these off-premises deployments.

Manageability and Automation

Security administrators are struggling to deliver security at the same speed of current cloud automation workflows. Cloud automation enables infrastructure to scale rapidly, but security automation is still lagging behind.

IT point of view: IT is looking for a way for administrators to view all cloud workloads and apply the proper network security controls, ideally using a single

console from where they can manage not only public cloud security but also protect their on-premises deployments. To keep up with cloud deployment practices such as automation, security needs to embrace automation since manually managing highly elastic cloud deployments is not feasible.

The McAfee Solution

McAfee understands the complexity of public cloud and has designed a security architecture specifically for Azure. This includes not only new processes and techniques to protect the entire stack and capabilities to inspect north-south as well as east-west traffic, but also the ability to manage across hybrid environments with one management tool and with one security policy.

McAfee® Virtual Network Security Platform (McAfee vNSP) addresses the customer responsibility for applying Network Traffic Protection in Azure with an advanced level of security. It provides a full-featured, software-only intrusion prevention system (IPS) for Azure cloud deployments. It is a complete IPS and intrusion detection system (IDS) that protects applications and operating systems from known and unknown threats.

McAfee vNSP supports today's leading public cloud service—Azure—delivering complete visibility to data traversing through a network gateway, as well as bi-directional east-west traffic to protect against intrusion to critical assets. With this threat intelligence in hand, administrators can reduce visibility gaps, increase security, and extend compliance into public cloud architectures.

Key Benefits

McAfee Virtual Network Security Platform provides a set of key benefits when protecting deployments in the Azure public cloud infrastructure:

- **Scalability:** McAfee vNSP scales based upon the changing dynamics of virtualized workloads in clouds such as Azure. In the event of a network burst causing increased traffic, McAfee vNSP automatically scales to meet workload demands by deploying additional sensors as needed to meet the required throughput performance. With support for network virtualization, administrators can quickly deliver network protection to new, existing and moving workloads.
- **Protection and Detection:** McAfee vNSP scales across the virtual data center to protect against advanced threats and lateral movement with true east-west network protection in addition to north-south traffic inspection. McAfee Virtual Network Security Platform's signature-less engines intelligently identify the intent of network traffic and can block attacks for which no signatures exist, such as advanced targeted attacks or new threats that have not been seen before.
- **Manageability and automation:** McAfee vNSP provides security administrators with a single pane of glass that enables visibility and control for workloads across all cloud environments. Furthermore, instead of needing to process an abundance of alerts, McAfee Virtual Network Security Platform displays actionable data via preconfigured, guided workflows. This approach reduces expertise needed to monitor and investigate.

Key Advantages

- Virtual deployment built to protect public cloud workloads
- Advanced threat prevention
- Signature-less, advanced malware analysis
- Automatic scaling of sensors to meet performance demands
- In-line browser and JavaScript emulation
- Advanced botnet and malware callback detection
- Behavior-based analysis and DDoS protection
- Integration with McAfee® Advanced Threat Defense

It is worth diving a bit deeper into McAfee Virtual Network Security Platform's capabilities to protect Azure cloud deployments and the manageability advantages provided to security administrators. More details about these benefits are discussed below.

Threat Detection and Protection

McAfee Virtual Network Security Platform is based on a next-generation inspection architecture designed to deliver deep inspection of virtual network traffic. It uses a combination of advanced inspection technologies—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent both known and zero-day attacks on the network.

- No single malware detection technology can prevent all attacks, which is why McAfee vNSP layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc in your clouds. Most network threat solutions rely on signature-based inspection. However, today's advanced targeted attacks are usually new and unknown. Since no signatures exist for these attacks, they are often missed.
- McAfee vNSP delivers numerous inspection technologies, like in-line emulation of Browser, JavaScript, and Adobe files, botnet and malware callback detection, behavior-based distributed denial-of-service (DDoS) detection, and protection from advanced attacks like cross-site scripting and SQL injection. McAfee also supports the use of Snort signatures to detect and protect against malware.
- McAfee vNSP can also identify and block the stealthiest of files via integration with McAfee Advanced Threat Defense in Azure environments, where files are submitted for in-depth behavior analysis.

McAfee Virtual Network Security Platform provides many other benefits, such as web application firewalling (WAF) to protect against application DDos, SQL injections and more. For a complete set of features, please refer to the **datasheet**.

North-south and east-west traffic protection

McAfee Virtual Network Security Platform provides north-south as well as east-west traffic inspection between Azure cloud servers. With these methods, it can inspect for threats that attempt to move laterally. Unlike current solutions in the market, McAfee delivers a full-protection mode IPS for Azure.

In addition, McAfee vNSP provides east-west traffic inspection, which helps prevent malware from spreading laterally. Without this protection, threats could spread swiftly without being detected.

Cloud-Ready Architecture

- An innovative approach to Azure inspection provides true east-west traffic protection in the public cloud
- Single centralized management console for on-premises physical and virtual IPS sensors in Azure
- One license allows throughput sharing across any combination of public and private clouds

Intelligent Security Management

- Intelligent alert correlation and prioritization
- Robust malware investigation dashboards
- Preconfigured investigation workflows
- Scalable web-based management

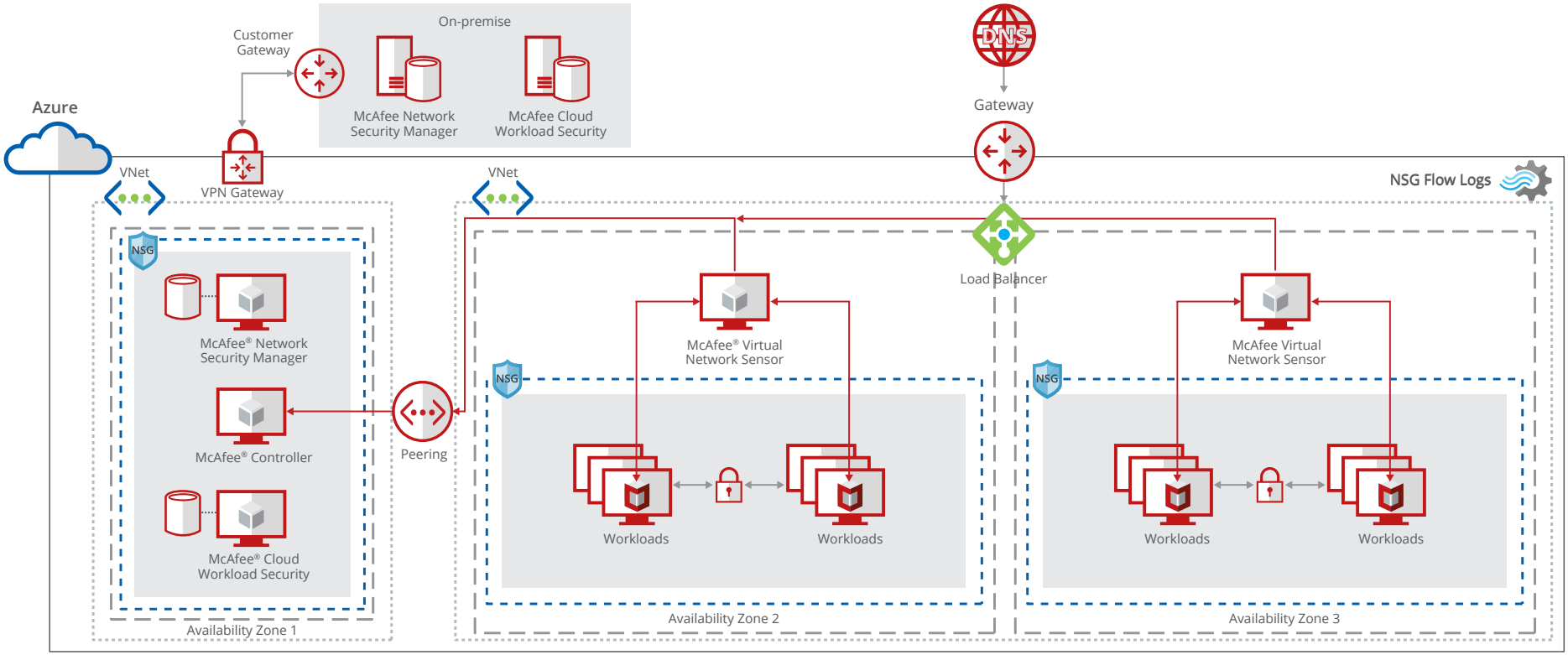

Figure 2. McAfee Virtual Network Security Platform protects north-south and east-west traffic in Azure.

When traffic flows to a virtual machine, the virtual probe that is installed in the virtual machine intercepts traffic and forwards it to the virtual IPS sensor for inspection. The sensor then scans the traffic for any malicious activity. If there is no threat, the traffic is returned back to the virtual machine. If a threat is found, depending on the policy configuration, the sensor will either drop the traffic or return the traffic after generating an alert in the McAfee® Network Security Manager.

Security Management

Streamline workflows and analytics

Discover and block the most sophisticated threats with ease. McAfee vNSP includes advanced analytics and integrations with additional security solutions to create a truly comprehensive and connected network threat detection and mitigation platform.

Modern threats can generate large volumes of alerts, quickly outpacing a security operator's ability to prioritize and track them. If the dots are not connected in time, real threats can slip by undetected. McAfee® Network Security Platform includes out-of-the-box advanced analytics and actionable workflows correlate multiple IPS alerts into a single, actionable event, helping administrators rapidly cut through the noise and get to relevant, actionable information.

With intelligent workflows centered on malware detection and breach discovery, alert noise is reduced, user error is minimized, and operators are allowed to focus on the key data needed to protect their environment.

Centralized Management with Real-Time Control of Real-Time Data

A single McAfee Network Security Manager appliance delivers centralized, web-based management and unrivaled ease of use. The state-of-the-art console and enhanced graphical user interface put you in control of real-time data. You can easily manage, configure, and monitor not only your virtual IPS appliance but also all McAfee Network Security Platform appliances, virtual or physical, as well as McAfee® Network Threat Behavior Analysis appliances across your traditional, private, and public cloud resources—from a single console.

In summary, McAfee Virtual Network Security Platform is a complete network threat and intrusion prevention system (IPS) solution built for the unique demands of Azure environments. It helps discover and block sophisticated threats in cloud architectures with accuracy and simplicity, enabling organizations to restore compliance and embrace the cloud with confidence.

Advanced technologies include signature-less detection, in-line emulation, signature-based vulnerability patching, and support for Azure and network virtualization. With streamlined workflows, multiple integration options, and simplified licensing, organizations can easily manage and scale their security in the most complex cloud architectures.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com