SOPHOS
Security made simple.

Sophos and Microsoft Azure: Considerations for Cloud Security

Security in the public cloud

You've chosen to run your applications and workloads in the cloud. Now how do you secure them? Microsoft works hard to protect the Azure cloud, but that's only for the underlying cloud infrastructure. What about your applications and your data itself? As you move workloads to Azure, don't assume they're automatically protected. Microsoft claims responsibility for the security of their cloud, but you are responsible for the security of applications and data you place in their cloud.

This is where Sophos can help. We provide network and server security solutions to help you protect your cloud environment. Sophos XG Firewall is an all-in-one solution that combines advanced networking protections such as Intrusion Prevention (IPS), and web application firewalling (WAF), as well as user and application controls. Sophos Server Protection helps defend Microsoft Windows and Linux virtual machines from malicious attacks using a variety of methods, including CryptoGuard anti-ransomware, Malicious Traffic Detection, and Server Lockdown for application whitelisting.

Microsoft Azure: Welcome to the Shared Responsibility Security Model

For security of the cloud, Microsoft Azure employs the principles of "Protect," "Detect," and "Respond." "Protect" is about controlling access to the platform itself. "Detect" involves monitoring network traffic and other activities on the platform. "Response" is about reacting to security issues.

For security in the cloud, Sophos XG Firewall and Sophos Server Protection communicate and synchronize with each other, creating a security solution that actively blocks advanced threats.

Defending against hacks and attacks

Cybercrime is on the rise, with 38% more security incidents detected in 2015 than 2014. It is estimated that cybercrime will cost businesses $2.1 trillion by 2019. The impacts of a successful hack include financial loss, breach of customer trust, and failure to comply with government or industry regulations.

Sophos and Microsoft Azure provide services that can help you meet your security, privacy, and compliance requirements. The important thing to remember is that when you run your applications and workloads in the cloud, you are also responsible for ensuring protection for those applications and workloads.

As with any infrastructure, whether on-premises or in the cloud, security should be a core functional requirement. Security policies and controls must be implemented to protect mission-critical information from accidental or deliberate theft, leakage, integrity compromise, and deletion. Here are some questions to consider as a starting point:

Security Consideration checklist

- Understand your data. Is it appropriate for the public cloud?
- Know the types of cloud models in use by your company and what your security responsibilities are with each model.
- Research your cloud provider to determine its data security responsibility and the level of security provided.
- Define your organization's security policies, i.e. who has access to the data and how they will access it.
- Ensure that all data is encrypted both in transit and at rest.
- Determine who is holding the data encryption keys.
- Establish the proper layers of protection, such as firewall/intrusion protection, gateway antivirus, etc.
- Implement a consistent and secure data backup plan.

- How is your data routed and what kind of protection do you have for that route?
- How is performance affected by implementing a security solution?
- Where does your data reside? Is it encypted and who has access to it?
- What type of protection do you need? Application-layer, network-layer, server-layer, or all the above?
- Do you have protection in place for known threats? What about threat protection to identify and block the unknown (zero-day) threats?
- Do you understand how your users behave in your cloud infrastructure? How do you identify and separate out risky users?
- What type of policies and rules are you using? Is there overlap or are there ineffective rules? How do you identify more effective ways to manage your security?

Sophos has an ecosystem of partners that are capable of helping you think through security concerns in order to develop and implement controls and protections that are right for your environment.

Sophos XG Firewall

Sophos XG Firewall on Azure combines mutiple security tools into one solution, including Next-Gen Firewall, IPSec, Secure Socket Layer (SSL) Virtual Private Networks (VPN), Network Protection, Wireless Protection, Web Protection, Email Protection, and Web Server Protection. XG Firewall is designed to prevent sophisticated attacks and advanced threats in the cloud while providing secure remote access to the Azure cloud for trusted users.

Sophos XG Firewall complements the infrastructure protection provided by Azure with many advanced management features and deployment capabilities. These include:

- Global deployment options, with the ability to establish separate XG Firewall instances in multiple countries. This is useful for dealing with compliance requirements across different countries, e.g. the EU versus the U.S.
- Sophos Firewall Manager software, which provides fast setup and a single console for the complete central management of the firewall.
- Built-in reports that tell you what's happening with your users and your network.
- User Threat Quotient reports that show you which of your users are putting your Azure-based systems at risk.
- Pre-defined policy templates that let you quickly protect applications like Microsoft Exchange or SharePoint. They set all the inbound/outbound firewall rules and security settings automatically.
- Patented Layer-8 identity control, which enables user-level controls over applications, bandwidth and other network resources regardless of IP-address, location, network or device.

Security Standard Compliance

ISO/IEC 27001

Devised by the International Standards Organization, ISO/IEC 27001 and 27002 are extensive guidelines that give institutions standards of managing IT risk. They help IT professionals implement policies to combat security vulnerabilities. In practice, an organization might begin encrypting its data, set up a policy to manage mobile devices, and use software like that provided by Sophos.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards and sensitive customer banking information. Technical safeguards require firewall protection, encryption of customer data, unique user IDs, development and maintenance of secure systems, antivirus software on all systems, and tracking and monitoring of all system interaction

HIPAA

In the U.S., HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. It refers to any data that can be categorized as personal health information (PHI). Technical safeguards require authorized access, including using unique user IDs, an emergency access procedure, automatic log off, and encryption and decryption. Additionally, network and transmission security are required as well as offsite backup for disaster recovery. Audit reports, or tracking logs, must be implemented to keep records of activity on hardware and software

Sophos Server Protection

Sophos Server Protection is designed to secure the virtual machines that host your business-critical, cloud-based applications and workloads without sacrificing performance. Server protection helps defend Windows and Linux servers from malicious attacks, and complements the infrastructure protection provided by Azure with many advanced management features and deployment capabilities. These include:

- Comprehensive effective protection that prevents, detects, and remediates malware for Windows, Linux, and UNIX VMs, protecting business critical VMs that contain an organization's data and applications against the latest threats, whether known or zero-day. Next-generation protection includes CryptoGuard anti-ransomware, Malicious Traffic Detection, and Server Lockdown for application whitelisting.
- Whether running on VMs on-premises or in the cloud, Sophos Server Protection minimizes the impact on the performance and availability of your servers and server instances. Server-specific policies and groups with granular control of features minimizes the impact. It allows consistent and comprehensive protection of workloads and servers wherever located.
- Simplified deployment with easy to set up, configure, and maintain security management. Get started in minutes with the Sophos Central hosted management console. Server-specific licensing and policies ease management and allow deployment flexibility – whether physical or virtual; on-premises, on the cloud, or hybrid – all with a single license.
- Synchronizes Security across entire organization, coordinating devices and network traffic. As part of Synchronized Security, Sophos Server Protection shares threat, health, and security information across multiple Sophos products in real time, delivering unparalleled protection, automated incident response, and real-time insight and control. Server-specific coordination between Windows or Linux servers and Sophos XG Firewall allows automated and near-instantaneous isolation of the infected server or other endpoint.

Synchronized Security

Synchronized Security enables your defenses to be as coordinated as the advanced attacks they protect against. Sophos XG Firewall and Server Protection communicate and synchronize with each other, creating a security solution that actively blocks advanced threats. Unlike point products that only stop individual elements of an attack, Synchronized Security correlates network traffic with the activities of Virtual Machines (VMs) in Microsoft Azure to thwart multiple prongs of attack, often without administrator intervention. Benefits include:

- Shares real-time threat intelligence between servers, endpoints, and firewalls.
- Protects end-users from accessing potentially compromised servers and network shares and vice versa.
- Creates simple, actionable insights and automatic resolutions across synchronized products.

Contact your Sophos representative today to learn how to access your 30-day free trial of Sophos XG Firewall or visit us at sophos.com/azure

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2017-06-12 SB-NA (MP)

SOPHOS