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 data themselves? Azure manages security of the cloud; security in the cloud is up to you. As you move workloads to Azure, don't assume they're automatically protected.

This is where Sophos can help. We provide solutions to help you properly secure your cloud environment. Sophos XG Firewall is available in the Microsoft Azure Marketplace. You can deploy XG Firewall on Azure to help provide the protection your data needs as it moves through Azure. Sophos XG Firewall gives you additional layers of security from the Azure Virtual Network through the application layer in a single modular solution. XG Firewall is available as a pre-configured, virtual machine in the Azure Marketplace. You can select XG Firewall, apply Azure Resource Manager templates, and easily deploy to your environment.

Microsoft Azure: Welcome To The Shared Responsibility Security Model

For security of the cloud, Microsoft Azure is based on the pillars 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. The "Response" pillar is about reacting to security issues. Yet this is just part of the Shared Responsibity story.

For security in the cloud, Sophos XG Firewall is now available from the Azure Marketplace. When you deploy Sophos in your Azure infrastructure, you can benefit from the security controls offers by both vendors.

Defending Against Hacks and Attacks

Cybercrime is on the rise, with 38% more security incidents detected in 2015 than 2014. [1] It is estimated that cybercrime will cost businesses $2.1 trillion by 2019. [2]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-premise 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 the provider's data security responsibility and the level of security provided.
- Define your organization's security policies, such as who has access to the data and how they will access it.
- Ensure that all data is encrypted in transit and at rest.
- Determine who is holding the data encryption keys.
- Establish the proper layers of protection, such as firewall/intrusion protection and gateway antivirus, for example.
- Implement a consistent and secure data backup plan.

1 "The Global State of Information Security Survey," Joint Survey by CIO, CSO and PwC, 2016.
2 "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation," Juniper Research, 2015.

- How is your data routed, and what kind of protection do you have for that routing?
- How is performance affected by implementing a security solution?
- Where does your data reside? Is it encypted? Who has access to it?
- What type of protection do you need? Web-layer, network-layer, both? More?
- Do you have protection in place for known threats? What about threat protection to identify and block 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 policy and rules are you using? Is there overlap or ineffective rules? How do you identify more effective ways to manage your security?

Sophos has a network of partners 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, such as 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 for 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, anti-virus 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 passed by Congress in 1996. It refers to any data that can be categorized as personal health information (PHI). Technical safeguards require authorized access, such as 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.

Conclusion

Sophos XG Firewall is a "next-generation" firewall you can select and launch from within the Microsoft Azure Marketplace. XG Firewall deploys as 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. XG Firewall is designed to help you protect your Azure-based workloads against advanced threats.

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

2016-09-08 WP-NA (MP)

SOPHOS