

Security in Azure: Sophos Extends Protection



Shared Responsibility Model	On-Prem	Azure	Responsibility	Sophos Assists
Data classification & accountability			Define and enforce who can access what data.	Sophos SafeGuard and Mobile extend data security outside Azure.
Client & end-point protection			Endpoint Protection is critical to stop data loss and malware propagation.	Endpoint antimalware/ anti-exploit on Windows, Windows Server & Linux.
Identity & access management			Enforce authentication, define access restrictions and track credential use.	XG Firewall enforces in/ outbound authentication with SSO and 2FA.
Application level controls			Prevent application compromise through patching and security.	XG and Server Protection provide multiple tools to protect against application attacks
Network controls			Configure and track network access permissions.	XG Firewall extends Azure's NSG with an easy to use interface, deep packet inspection and Synchronized security.
Host infrastructure			Configure, manage and secure storage and platform services.	
Physical security			Leverage Microsoft-supplied redundancy options to avoid SPOF.	

Cloud Customer Microsoft



Server Protection

- Protects your servers, and your data, from malware and ransomware extortion
- Whitelists trusted services in minutes, while intelligently allowing updates
- Unifies policy management in Sophos Central to manage server workloads - Hybrid security made easy!



Sophos XG Firewall

- Deep packet inspection for Azure with IPS, ATP, URL Filtering and in-depth reporting
- Bidirectional antivirus for WAF with authentication offloading, path based routing and country-level blocking
- Easy to set up and easy to use self-services SSL and HTML5 VPRN technologies that make connecting from anywhere and on any device a reality - without administrative overhead.



Synchronized Security

- Real-time intelligence sharing between Server endpoints and XG firewall - in Azure and hybrid environments.
- Security Heartbeat™ includes automated policy actions to effectively isolate and neutralize threats by coordinating efforts of the firewall, servers, endpoints and other components
- Deep analytics and root cause analysis reporting.

Unparalleled Protection

Automated Incident Response

Real-time Insight and Control