

Security Responsibilities made simple with Sophos



Shared Responsibility Model	On-Prem	Public Cloud	SaaS	Why?	Sophos Assists
Data classification & accountability				Define and enforce who can access what data.	Sophos Safeguard, DLP and Mobile help secure data and determine access permissions. Both on-premise and in the cloud.
Endpoint protection				Stop data loss and malware propagation.	Sophos Endpoint, Server Protection, Mobile and Intercept X antimalware/anti-exploit on Windows (Servers), OS X, Linux, Android & IOS.
Identity & access management				Enforce authentication, define access restrictions and track credential use.	XG Firewall and UTM enforce in/outbound authentication with SSO and 2FA and provide detailed access reporting.
Application controls				Prevent application compromise through policy, patching and security.	UTM/XG's IPS and Server Protection's HIPS and Lockdown protect against application attacks and unintended application exposure.
Network controls				Track and enforce network access permissions.	UTM/XG Firewall's easy to use interface, powerful packet inspection and Synchronized Security (only on XG) help secure and manage network access and enforce network privileges.
Host infrastructure				Manage and secure operating systems, storage solutions and related services to prevent unpatched bugs and privilege escalations.	Sophos Intercept X protects against 0-day threats by looking at exploit techniques, Server Protection Lockdown enforces runtime restrictions and Sophos XG Sandstorm stops unknown code proliferation.
Physical security				Restrict physical access to systems and design redundancy to prevent SPOF.	Both Sophos UTM and XG Firewall have High Availability deployment options for both physical appliances and on cloud platforms.

Cloud Customer
 Platform Provider

Unparalleled Protection

Automated Incident Response

Real-time Insight and Control

Protect servers, VMs, EC2 instances and S3 buckets

- › Intercept X for Server protects servers and workloads, and their data, from fileless exploits, malware, and ransomware extortion.
- › Whitelists trusted services in minutes, while intelligently allowing updates.
- › Unifies security policies in Sophos Central to manage workloads and their data – secure one and run everywhere!



Reduce firewall complexity



- › XG Firewall provides deep packet inspection with IPS, ATP, URL Filtering and reporting.
- › Bidirectional antivirus for WAF with authentication offloading, path based routing and country-level blocking.
- › Easy to set up and use self-services SSL and HTML5 VPRN technologies allow connecting from anywhere and on any device a reality – without administrative overhead.



- › Sophos UTM provides layers to protect your AWS environment with an all-in-one solution, including granular controls, logging, and reporting.
- › Stateful traffic inspection and control, IPS, Layer 7 application control, VPN connectivity, and WAF. Manage it all with an easy-to-use web-based console.

