Reference Card for Government

SOPHOS

Government institutions and agencies are responsible for huge amounts of sensitive information that is under threat from advanced cyberattacks levelled by nation states, cybercriminals, and hactivists. Successful defense against these attacks depends on the comprehensiveness of their IT security solutions, the capability of their firewall and endpoint to communicate with one another in real time to quickly respond to cyberattacks and kickstart remedial measures, and the ability of the cybersecurity infrastructure to address security vulnerabilities at the network or endpoint level that are commonly exploited to access sensitive data.

Sophos offers a range of high-performance cybersecurity solutions that meet exacting requirements of mission-critical government IT infrastructure.

CHALLENGE	SOPHOS PRODUCT	HOW IT HELPS
Protecting mission-critical or sensitive data at rest	Sophos XG Firewall SG UTM Sophos Intercept X	Data Leakage Prevention (DLP) capabilities in Sophos products can detect and prevent leaks of critical government data via email, uploads, and local copying.
	Sophos Email Appliance Sophos XG Firewall SG UTM	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
	Sophos Mobile	Sophos Secure Workspace secures work documents with AES-256 encryption, allowing a secure way to manage, distribute, and edit business documents and view web content on mobile devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.
Securing sensitive or mission-critical data in transit	Sophos SafeGuard Encryption	Encrypts information at rest and in transit on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption for information stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All encrypted data remains encrypted as files move across the network.
	Sophos Wireless Sophos XG Firewall SG UTM	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots.

	Sophos XG Firewall SG UTM	Allows for policy-based encryption for VPN tunnels, protecting information in transit.
	Sophos Email Appliance Sophos XG Firewall SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
Lateral Movement Protection – preventing further access to valuable data or systems	Sophos XG Firewall	Isolates and prevents threats or attackers from moving laterally across the network to other systems, even if they are on the same network segment or broadcast domain where the firewall can't normally intervene. It's an extremely simple and effective solution to the challenge of active adversaries operating on your network.
Seamless intelligence sharing between endpoint and firewall	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls, stopping advanced attacks.
Rich and easy central management capabilities	Sophos Central	Manage all your Sophos products from a single interface. Ability for remote management and deployment of all Sophos products through a single integrated cloud-based management console.
Stop phishing attacks before they reach your employees' inbox	Sophos Email	Automate phishing imposter defense with Sophos Email authentication. Protect your employees from phishing attacks using fraudulent email addresses that impersonate trusted contacts and domains before they reach the inbox. Using a combination of SPF, DKIM, and DMARC authentication techniques and email header analysis, Sophos Email allows you to identify and allow legitimate emails from trusted partners and block the imposter – so you can trust your inbox again.
	Sophos Phish Threat	Sophos Phish Threat provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to IT training and compliance topics, malware and mobile device risks, password protection, and more.
Block suspicious/malicious URLs and web-borne threats	Sophos XG Firewall SG UTM	Benefit from fully transparent proxy for anti-malware and web-filtering and a URL filter database with millions of sites across 90+ categories, backed by continuously updated database from SophosLabs. Advanced web protection engine intelligently scans web content and blocks the latest web threats by using advanced techniques like JavaScript emulation, behavioral analysis, context-sensitive inspection, and dynamic URL analysis for both HTTP and HTTPS traffic.

Protection against ransomware and other types of advanced malware	**Sophos Intercept X** **Sophos Intercept X for Server**	Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code. Integrates innovative technology like deep learning, anti-exploit, and adversary mitigation feature into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease. Includes rollback to original files after a ransomware or master boot record attack, along with Sophos Clean which provides forensic-level remediation by eradicating malicious code, as well as eliminating nasty registry key changes created by malware.
	Sophos Mobile	Delivers Unified Endpoint Management (UEM) and security management for traditional and mobile endpoints, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security provides Mobile Threat Defense for Android and iOS devices, including app, network, and device protection. Leading anti-malware and anti-ransomware protection powered by deep learning for Android devices.
	Sophos XG Firewall	Includes APT and sandboxing with deep learning to monitor and block malicious, anomalous, and exploitive traffic from in-bound or out-bound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Email Appliance	Uses real-time threat intelligence to detect and block unwanted email right at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
Protection against insider threats	**Sophos XG Firewall**	User Threat Quotient (UTQ) helps identify users who pose a risk based on suspicious web behavior and threat and infection history. A user's high UTQ risk score could be an indication of unintended actions due to lack of security awareness, a malware infection, or intentional rogue actions.
	Sophos XG Firewall **SG UTM**	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Sophos XG Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised/unauthorized endpoint device; and allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data.

	Sophos SafeGuard Encryption	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication. Supports risk management by authenticating users for access to specific files/folders with the use of user- or group-specific encryption keys.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Sophos Mobile	Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device health, compliance rules, time, Wi-Fi, or geo-location.
Extending corporate IT security beyond network perimeter: Mobile workforce and remote branch offices	**Sophos Mobile**	Provides enterprise mobility and security management capabilities for traditional and mobile endpoints, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.
	Sophos XG Firewall **SG UTM**	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos RED (Remote Ethernet Device) extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
	Sophos SafeGuard Encryption	Encrypts information at rest and in transit on Macs, Windows, and mobile devices. Manages BitLocker and FileVault full disk encryption as well as always-on file encryption for information stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted remains encrypted as files move across the network.
	Sophos Email Appliance **Sophos XG Firewall** **SG UTM**	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.

Protecting network integrity	**Sophos XG Firewall** **SG UTM**	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports, and protocols except those explicitly allowed and defined as appropriate and necessary for the organization.
	Sophos Mobile	Integration with Sophos UTM, Sophos Wireless access points, and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
	Sophos Intercept X **Sophos Intercept X for Server**	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
Complying with global best-practices such as NIST Cybersecurity Framework, NIS Directive and more	**All Sophos products**	Sophos security products support an organization's need to meet a range of cybersecurity compliance best practices, especially expected from government entities. Refer to Sophos compliance page for more information.
Cloud infrastructure security	**Sophos Cloud Optix**	An AI-powered, next-generation cloud infrastructure security platform, it delivers continuous security monitoring, compliance, analytics, and remediation across multiple public cloud accounts and multiple public cloud platforms.

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

© Copyright 2019. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2019-05-09 RC (PC)

SOPHOS