Reference Card for Government

SOPHOS

Government agencies hold a large volume of classified data on national security and critical infrastructure along with personally identifiable information (PII) on citizens. The data must be protected to preserve national security and the privacy of citizens' data. But government agencies are under constant attack from nation states, hacktivists, and cybercriminals looking at financial and political gains. At the same time, governments around the world have undergone rapid digital transformation to speed up government operations and improve citizen services. This, along with the shrinking budget and resources at IT teams' disposal, has increased the attack surface in this sector.

Sophos helps government agencies to protect their systems and data wherever they exist with our next-gen services and technologies, enabling them to consolidate their security management with a single vendor. This document provides a general reference on how Sophos delivers advanced cybersecurity solutions that enable the government sector to manage and reduce cyber risks.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing citizens' and classified data	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying.
	Sophos Firewall	Flexible and powerful segmentation options via zones and VLANs help you separate levels of trust on the network to reduce cyber-risk exposure to the data stores.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos Intercept X Sophos Intercept X for Server	Mitigate known vulnerabilities and stop the latest cybersecurity threats such as ransomware, file-less attacks, exploits, and malware across all endpoint devices.
	Sophos Central Device Encryption	With the huge number of laptops lost, stolen, or misplaced every day, a crucial first line of defense against the loss or theft of devices and the data therein is full-disk encryption. Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
	Sophos Email	Prevent data loss by creating multi-rule DLP policies for groups and individual users to ensure the protection of sensitive information with discovery of confidential contents in all emails and attachments.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing sensitive or mission-critical data in transit	Sophos Email	Encrypt messages and add a digital signature to verify sender identity with S/MIME, or select from customizable encryption options, including TLS encryption, attachment and message encryption (PDF and Office), or add-on full web portal encryption.
	Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
Protection against phishing attacks	Sophos Email	Scans all inbound messages for key phishing indicators such as brand spoofing and impersonation attempts in real-time using SPF, DKIM, and DMARC authentication techniques and email header anomaly analysis. This helps to spot and block phishing emails before they reach your users.
	Sophos Phish Threat	Educates and tests end users against phishing, credential harvesting, or attachment attacks, through automated attack simulations, quality security awareness training, and actionable reporting metrics.
	Sophos Intercept X Sophos Intercept X for Server	Get complete protection for all your endpoints – Windows, Mac, Linux, and virtual machines – multiple layers of protection technologies including credential theft protection, exploit protection, anti-ransomware protection, and tamper protection, that optimize your defenses.
Protection against hacktivism	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Offers powerful segmentation options via zones and VLANs. This provides ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.
	Sophos XDR	Helps you keep the systems and apps updated with regular patch management by offering the most complete view of your cybersecurity posture. By pulling in rich data from your network, email, cloud, and mobile data sources, it helps you locate systems and devices that are unpatched or have out-of-date software.
	Sophos Managed Detection and Response (MDR)	Reduces the threat response time dramatically for government agencies with a fully managed 24/7/365 service delivered by experts that are armed with critical visibility and context for seeing the entire attack path, enabling a faster, more comprehensive response to security threats that technology solutions alone cannot prevent. Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect citizens' data and classified information wherever it resides.
Automated incident response	Sophos Synchronized Security	Combines all Sophos products to share threat, health, and security information in real time and automatically respond to incidents. Synchronized Security is powered by the Sophos Adaptive Cybersecurity Ecosystem (ACE), which encompasses Sophos threat intelligence, next-gen technologies, data lake, APIs, and Sophos Central management platform to deliver constantly learning and improving cyber protection.
Securing remote access environments	Sophos Secure Access portfolio	Includes Sophos ZTNA to support secure access to applications, Sophos SD-RED remote Ethernet devices to safely extend your network to branch offices and remote devices, Sophos Wireless access points for easy and secure wireless networking, and Sophos Switch for secure access on the LAN. Everything is managed through a single cloud-based security platform – Sophos Central.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Protection against advanced malware attacks	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also identifies and protects users and applications on the network. Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
	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 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. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Endpoint Protection application control policies restrict the use of unauthorized applications. Server Lockdown allows only trusted whitelisted applications and associated files to run.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
Securing resources in the cloud	Sophos Cloud Native Security	Provides complete multi-cloud security coverage across environments, workloads, and identities. It protects your cloud infrastructure and data with flexible host and container workload security for Windows and Linux. Multi-layered technologies protect against ransomware and other advanced attacks including cloud-native behavioral and exploit runtime detections that identify threats such as container escapes, kernel exploits, and privilege-escalation attempts.
Ensuring application and network availability	Sophos Firewall	Delivers advanced protection from the latest drive-by and targeted web malware, URL/malicious site filtering, and cloud-based filtering for offsite protection, backed by industry-leading machine learning technology and powered by SophosLabs Intelix. Combined with our enterprise-class web application firewall, it protects your critical business applications from hacks and attacks while enabling authorized access.
	Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Besides, the endpoint protection application control policies restrict the use of unauthorized applications in government systems.
	Sophos Managed Detection and Response (MDR)	Provides 24/7 detection, investigation, and neutralization of suspicious activities by human threat experts who are kept up to date on the latest threat and vulnerability developments by Sophos X-Ops.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Protection against insider threats	Sophos Firewall	Protects your sensitive data from accidental or malicious disclosure with complete policy control over web categories, applications, removable media, and mobile devices used in your network. Offers insights into your riskiest users and applications to ensure that your policies are enforced before your security is compromised with actionable intelligence from Sophos User Threat Quotient (UTQ). Offers the most extensive set of user authentication options available on any firewall, including Active Directory integration, and even our unique and easy-to-use Synchronized User ID solution that facilitates seamless user authentication across the firewall and endpoints to offer tighter, granular user access, blocking an external attacker as well as a malicious insider from gaining access to sensitive systems or data.
	Sophos Cloud Optix	Connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real-time that can help you identify credential misuse or theft. An IAM visualization tool that provides a complete map of IAM relationships allows your IT teams to identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks quickly and easily.
Controlling access to system components	All Sophos Products	Sophos' user-identity-based policy technology allows organizations to enforce role-based user-level controls over network resources and other organization's assets.
	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security Posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
Minimizing the risk of supply chain attacks	Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.

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

2023-04-24 RC-NA (PS)

SOPHOS