# Reference Card for Government

Cybersecurity in government organizations is important to protect national security and citizens' trust. However, it is under constant attack from nation states, hactivists and cybercriminals interested in espionage and financial gains. At the same time, many countries have undertaken rapid digital transformation to speed up government operations and enhance citizen services, which is increasing the attack surface in this sector. Government organizations need to secure large volumes of classified data, and ensure application and network availability for smooth functioning of their operations.

This document provides a general reference on how Sophos products assist organizations in the government sector by offering them advanced protection to safeguard cybersecurity and secure the mission-critical government IT infrastructure.

| Challenge | Sophos Product | How it helps |
|---|---|---|
| **Securing classified data at rest** | Sophos Firewall | Uses AI-powered threat detection technology to prevent attacks from reaching sensitive customer data, financial transactions, and other parts of your ecosystem. Automatic threat response instantly identifies and isolates compromised systems on the network to stop threats from spreading. |
| | Sophos Intercept X<br>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.<br>Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.<br>Endpoint Protection application control policies restrict the use of unauthorized applications.<br>Server Lockdown allows only trusted whitelisted applications and associated files to run. |
| | Sophos Central Device Encryption | Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance. |
| | Sophos Zero Trust Network Access (ZTNA) | Validates user identity, device health, and compliance before granting access to resources. |
| | Sophos Email | Encrypts personally identifiable information, corporate and other sensitive data, stopping both accidental and malicious data breaches. |
| | 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. |
| **Securing sensitive or mission-critical data in transit** | Sophos Email | Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode. |

SOPHOS

| Challenge | Sophos Product | How it helps |
|---|---|---|
| | Sophos Mobile | Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device.<br>A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection safeguards your users and devices from malicious content and apps. |
| | Sophos Central Device Encryption | Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance. |
| | Sophos Firewall | Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. |
| | Sophos Zero Trust Network Access (ZTNA) | Validates user identity, device health, and compliance before granting access to resources. |
| | Sophos Wireless | Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos managed networks and hotspots. |
| **Automate incident response** | Sophos Synchronized Security | Brings together all of Sophos' endpoint, network, mobile, Wi-Fi, email, and encryption products to share threat, health, and security information in real time. Synchronized Security is powered by the Sophos Adaptive Cybersecurity Ecosystem (ACE) that leverages automation and human operations to deliver protection that constantly learns and improves. |
| **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.<br>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<br>Lateral Movement Protection, a Synchronized Security feature, prevents the threat or hacker from spreading to other systems, stealing data, or communicating back to the host. |
| | 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 | Synchronized Security is a complete portfolio of world-class Sophos security products that work together, responding automatically to incidents and delivering enhanced security insights. Zero-touch incident response slashes exposure to threats while the integrated product portfolio minimizes security gaps. Enhanced insight into network traffic lets you identify and address hidden risks. Centralized management enables you to focus on priority alerts. |
| | Sophos Intercept X<br>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.<br>Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.<br>Endpoint Protection application control policies restrict the use of unauthorized applications.<br>Server Lockdown allows only trusted whitelisted applications and associated files to run. |
| | Sophos Managed Threat Response (MTR) | Proactively hunt threats 24x7 and neutralize even the most sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf. |
| | Sophos Rapid Response Service | Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders. |

| Challenge | Sophos Product | How it helps |
|---|---|---|
| **Securing multi-cloud environments** | Sophos Intercept X for Server with XDR | Offers cloud workload protection that secures business-critical virtual machines and virtual desktops without sacrificing performance. Protect cloud workloads from the latest threats, including ransomware, fileless attacks, and server-specific malware, with XDR included to hunt down suspicious activities and perform critical IT operations tasks. Control exactly which applications can and can't run on your virtual machines and receive notifications for any unauthorized change attempts to critical files and folders with inbuilt application control. |
| | Sophos Cloud Optix | Sophos' Cloud Security Posture Management solution enables teams to proactively reduce organizational risk from unsanctioned activity, vulnerabilities, misconfigurations, and insecure identities in multi-cloud environments. |
| | Sophos Firewall | Protects environments from the latest network threats and vulnerabilities with a complete cloud edge firewall solution featuring IPS, ATP, and URL filtering. Extend your secure network with flexible SD-WAN and VPN connectivity options, while Sophos Web Application Firewall (WAF) hardens cloud workloads against hacking attempts. |
| | Sophos Zero Trust Network Access (ZTNA) | Constantly verifies the user — typically with multi-factor authentication and an identity provider — and validates health and compliance of the device for users to securely connect to corporate resources from any location. It elevates protection and minimizes the risk of lateral movement within the network by continually assessing identity and device health before allowing access. |
| | Sophos Managed Threat Response (MTR) | Helps take the weight of 24/7 threat monitoring and response. Receiving telemetry from Sophos products running on AWS, Azure and GCP this experienced team continuously monitors your cloud environments, analyzes and triages security events to prevent them from compromising your data and systems. |
| **Protection against threats posed by risky insider activities** | Sophos Firewall | Correlates each user's surfing habits and activity with advanced threat triggers and history to identify users with risky online behavior. You can schedule reports to identify users at risk and get details about their activities, including what and where they are posting or what sites they are visiting.<br>Automatically isolates compromised systems to stop active attacks in their tracks, denying further intrusion into the network. 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. |
| **Controlled 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 | 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.<br>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.<br>And 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 Zero Trust Network Access (ZTNA) | Continuously validates user identity, device health, and compliance before granting access to applications and data. |
| | Sophos Central Device Encryption | Authenticates users for access to specific files/folders with the use of user- or group-specific keys. |
| | Sophos Mobile | Encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy. |

| Challenge | Sophos Product | How it helps |
|---|---|---|
| **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 Threat Response (MTR) | 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 Zero Trust Network Access (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



2021-11-24 RC (PC)

SOPHOS