Reference Card for Retail

Retailers are being hit hard by cyber attackers who see them as a goldmine of vast amounts of sensitive customer and payment information in their databases. Retail businesses, regardless of size, are facing cybersecurity challenges in the form of ransomware attacks, data loss, insider threats, DDoS attacks and more. No other vertical sees brand equity, customer retention, and business continuity more dependent on cybersecurity than retail does. This document provides a general reference on how Sophos products assist retail organizations with robust cybersecurity and support them to simplify compliance with stringent regulatory mandates and industry best practices.

Challenge	Sophos Product	How it helps
Loss of stored confidential data such as credit card information, customer personal data, and more	Sophos Firewall	Uses AI-powered threat detection technology to prevent attacks from reaching sensitive customer data, POS systems, 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 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 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.
Loss of sensitive 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 Mobile	Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. 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

Challenge	Sophos Product	How it helps
	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.
Secure distributed retail environments	Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED works with Sophos Firewall to connect remote sites and individuals to your main network. It's ideal for branch offices, stores, and other third-party partners with no local setup or required technical skills, as well as for people with highly sensitive data.
	Sophos Zero Trust Network Access (ZTNA)	Provides full control over access to your applications and data by putting identity at the center of defense, constantly validating the user, the device, and policy compliance.
Minimize 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.
Wireless security	Sophos Wireless	Secures the growing number of mobile devices in retail organizations with granular visibility into the health of your wireless networks and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy. Monitors and acts upon the health status of the device connecting to the wireless network. It automatically restricts Wi-Fi network access for unhealthy and non-compliant endpoints and mobile devices, thereby preventing lateral spread of infection. Enhanced Rogue AP Detection classifies neighboring Wi-Fi networks to identify threats and prevent attempts to infiltrate an organization via Wi-Fi.
Stop attackers moving through your POS network at will	Sophos Firewall	Prevents attackers from moving through your POS networks and compromising POS machines. Segments your network so you can strengthen your network security, creating separate levels of trust on your network, making lateral movement difficult.
Malicious insider activity	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. 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.
Ransomware and other 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. 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.

Challenge	Sophos Product	How it helps
	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 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 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.
Supporting regulatory compliance	Sophos Central	Provides flexible reporting tools that allow visualization of network activity and security over time. It offers several built-in compliance reports as well as easy tools to create custom reports.
	Sophos Central Device Encryption	Makes it easy to verify encryption status and demonstrate compliance which is especially useful in cases of lost or stolen devices where retailers must prove that these missing devices are encrypted.

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

2021-11-25 RC (PC)

SOPHOS