Reference Card for Retail

SOPHOS

Retailers hold a goldmine of sensitive customer and payment information. Retail businesses, regardless of their size, are facing cybersecurity attacks such as phishing, credential stuffing, ransomware and DDoS attacks, supply chain attacks, and more, to gain access to their systems and valuable credit card and payment information. Such attacks can lead to heavy penalties for retailers for non-compliance with regulatory mandates like PCI DSS and GDPR, and data, financial, and reputational losses.

This document provides a general reference on how Sophos solutions help retail organizations to meet their unique cybersecurity requirements and support them in simplifying compliance with stringent regulatory mandates and industry best practices.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing stored confidential data such as credit card information, customer personal data, and more	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Sophos Firewall with Security Heartbeat™ allows next-generation endpoint and network security to continuously share meaningful information about suspicious events across the extended IT ecosystem; detects compromised / unauthorized endpoint device; allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential 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 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 your endpoint devices. Our data loss prevention (DLP) capabilities identify your sensitive data and prevent leaks via email, uploads, and local copying.
	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 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.
Securing distributed retail 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.
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.
Ensuring 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.
Preventing Business Email Compromise (BEC) scams	Sophos Email	Uses advanced Natural Language Processing (NLP) machine learning to block targeted impersonation and Business Email Compromise attacks. For added protection, Sophos Email also includes a setup assistant that integrates with AD Sync to automatically identify the individuals within an organization who are most likely to be impersonated. It scans all inbound mail for display name variations associated with those users, further extending protection against phishing imposters.
Securing against phishing scams	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	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.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
Securing against POS system attacks	Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop hackers from exploiting vulnerabilities in applications and operating systems. Sophos Server Workload Protection automatically scans your system for known good applications, whitelisting only those applications and blocking unauthorized applications from running in the system.
	Sophos Cloud Optix	Continually monitors your multi-cloud environments to detect unsanctioned activity, vulnerabilities, and misconfigurations and provides detailed threat remediation steps for security of your cloud POS systems.
	Sophos XDR	Gives you the most complete view of your cybersecurity posture by pulling in rich data from your network, email, cloud, and mobile data sources and helping you locate systems and devices that are unpatched or have out-of-date software.
	Sophos Managed Detection and Response (MDR)	Continuously monitors signals from across your security environment to help you detect potential cybersecurity events quickly and accurately. Detects, investigates, and correlates anomalous behaviors and code use to identify malicious activities and quickly neutralize the event.
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.
Preventing advanced malware and threats	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. 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.
	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.

SECURITY CHALLENGE	SOPHOS SOLUTION	HOW IT HELPS
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.
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 Cloud Optix	Eliminates compliance gaps with a single view of your compliance posture across AWS, Azure, and Google Cloud environments. Continuously monitors compliance with custom or out-of-the-box templates and audit-ready reports for standards such as FFIEC, GDPR, HIPAA, PCI DSS, and SOC2.

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

2023-04-27 RC-NA (PS)

SOPHOS