Reference Card for Finance and Banking

SOPHOS
Cybersecurity evolved.

The finance and banking sector needs a different approach to defend against advanced cyberthreats that involves multi-layer defenses, enhanced visibility, and security synchronization. This document provides a general reference on how Sophos products assist organizations in the finance and banking sector to meet their cybersecurity requirements, and maintain trust and confidence in financial transactions, safeguard PII, and get support to easily meet the challenge of complying with regulatory requirements like SOX, PCI DSS, GDPR, CIS CSC, and more.

Security Challenge	Sophos Solution	How It Helps
Mitigating risk of unauthorized disclosure by protecting 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 **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	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.

Reference Card for Finance and Banking

SOPHOS
Cybersecurity evolved.

Security Challenge	Sophos Solution	How It Helps
Protecting business-critical data in transit across public or private data networks	**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 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	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.

Reference Card for Finance and Banking

SOPHOS
Cybersecurity evolved.

Security Challenge	Sophos Solution	How It Helps
Identify and authenticate 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. 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. 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.
	Zero Trust Network Access	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.

Reference Card for Finance and Banking

SOPHOS
Cybersecurity evolved.

Security Challenge	Sophos Solution	How It Helps
Secure mobile devices both inside and outside the network perimeter	Sophos Mobile	A rich set of device management capabilities, containers, and market-leading encryption enables protection of sensitive business email and documents on mobile devices – even for users working with personal devices. Leading antivirus and ransomware protection helps to safeguard your users and devices from malicious content and apps.
	Sophos Wireless	Secures the growing number of mobile devices in banking and finance environment with granular visibility into the health of your wireless networks. Automatically restrict Wi-Fi network access for unhealthy and non-compliant endpoints and mobile devices, thereby preventing lateral spread of infection. Separate guest Wi-Fi access from access for your staff with a daily password or time-limited voucher.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
Extending network security to branch offices	Sophos Firewall	Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration. Sophos SD-RED works with Sophos Firewall to allow extension of secure network to other locations easily with no local setup or technical skills required.
Wireless Security	Sophos Wireless	Secures the growing number of mobile devices in banking and finance 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.
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. 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.

Reference Card for Finance and Banking

SOPHOS
Cybersecurity evolved.

Security Challenge	Sophos Solution	How It Helps
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.
	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	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.

Reference Card for Finance and Banking

SOPHOS
Cybersecurity evolved.

Security Challenge	Sophos Solution	How It Helps
Protection against phishing attack	**Sophos Email**	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.phishing attacks, malicious attachments, and snowshoe spam.
	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.
Business continuity and disaster recovery planning	**Sophos Firewall**	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
	Synchronized Security in Sophos products	Sophos products share real-time information via a unique Security Heartbeat™ and then respond automatically to incidents in seconds. It isolates infected endpoints, blocking lateral movement; restricts Wi-Fi for non-compliant mobile devices and infected endpoints; scans endpoints on detection of compromised mailboxes; revokes encryption keys if a threat is detected.
	Sophos Intercept X **Sophos Intercept X for Server**	Includes rollback to original files after a ransomware or master boot record attack.
Audit Trails	**All Sophos products**	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos Firewall	Controls remote access authentication and user monitoring for remote access and logs all access attempts.
	Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud* and mobile* data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.

Reference card for Healthcare

Security Challenge	Sophos Solution	How It Helps
	Sophos Mobile	Creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.
	Sophos Intercept X **Sophos Intercept X for Server**	Creates detailed log events for all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process PII.
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 banking and finance organizations 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

2021-11-22 RC-NA (PS)

SOPHOS