Australian Signals Directorate (ASD) Top 35 Reference Card

Sophos provides data sovereignty and security solutions for organizations in Australia that have strict national or local regulatory or policy requirements, with a dedicated data center in Sydney, Australia. This provides organizations across all industries with the ability to store, manage and access data locally from Sophos Central, the cloud management platform that supports Sophos' portfolio of advanced, next-generation cybersecurity solutions and services.

The Australian Signals Directorate (ASD) published its "Strategies to Mitigate Targeted Cyber Intrusions" based on its analysis of incidents across the Australian Government. First published in 2010, an update of these strategies was released in February 2017. Initially aimed at government organizations, the strategies are equally valuable for commercial organizations seeking to protect their networks and users.

Each strategy is assigned a "Relative Security Effectiveness Rating" of either Essential, Excellent, Very Good, Good, and Limited to help organizations prioritize their efforts and to focus limited resources where they are most needed. Accordingly, the strategies that are with a rating of Essential form the **Essential Eight Maturity Model** which is the foundational defense against cyber security threats and represents "the most effective of these mitigation strategies". The Essential Eight Maturity Model offers a guideline to assess the progress of implementing each strategy, from a scale of Zero (Not aligned) to four (higher risk environments). The ASD recommends organizations target level three (Fully aligned) as a baseline.

This document describes how Sophos solutions can be effective tools to support the customer's efforts to comply with the ASD requirements.

SOPHOS

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Mitigation strategies to prevent malware delivery and execution			
Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs, including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Essential	Sophos Intercept X Sophos Intercept X for Server	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. Sophos Intercept X for Server does not permit unauthorized applications from running, automatically scanning your system for known good applications, and whitelisting only those applications.
		Sophos Firewall	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. Delivers advanced protection from the latest drive-by and targeted web malware, URL/ Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
		Sophos Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
		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.
		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.
Patch applications e.g. Flash, web browsers, Microsoft Office, Java, and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	Essential	Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk level and prioritize response. Average time to detect and investigate is just 26 minutes.
Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Essential	Sophos Intercept X Sophos Intercept X for Server	Application Control policies restrict the use of unauthorized applications. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.
User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads, and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers, and PDF viewers.	Essential	Sophos Intercept X Sophos Intercept X for Server	Application Control policies restrict the use of unauthorized applications. Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.
		Sophos Firewall	Provides complete application visibility and control over all applications on your network with deep-packet scanning technology and Synchronized App Control that can identify all the applications that are currently going unidentified on your network. Sophos' Web Protection engine is backed by SophosLabs and includes advanced web protection, Potentially unwanted App control, and more, to identify and block the latest web threats and unwanted apps.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Automated dynamic analysis of email and web content run in a sandbox, blocked if suspicious behaviour is identified, such as network traffic, new or modified files, or other system configuration changes.	Excellent	Sophos Sandboxing	Sophos Zero-day dynamic file analysis uses next-gen cloud-sandbox technology powered by deep learning and the best technology from Intercept X to protect your organization against zero-day threats like the latest ransomware and targeted attacks coming in through phishing, spam, or web downloads.
Email content filtering. Whitelist allowed attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDFs, and Microsoft Office attachments. Quarantine Microsoft Office macros.	Excellent	Sophos Email	Sophos Email Content Control allows customers to filter inbound and outbound messages for keywords and file types – identifying specific keywords in email subject lines, message content, and file names. The content inspection capabilities will recursively unpack archives so that the contained files are inspected independently. The solution is able to identify PDF using their true file-type and set policy around those file types. Time-of-Click URL rewriting analyzes all URLs at the moment they are clicked, and automatically removes dangerous emails to protect against these post-delivery techniques. Sophos Email Search and Destroy capabilities take this one step further, directly accessing Office 365 mailboxes, to identify and automatically remove emails containing malicious links and malware at the point the threat state changes and before a user ever clicks on them – removing the threat automatically.
Web content filtering. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks, and free domains.	Excellent	Sophos Intercept X Sophos Intercept X for Server	Scans web content and allows category-based web filtering to be enforced both on and off the corporate network.
		Sophos Intercept X for Mobile	Web filtering and URL checking stops access to known bad sites on mobile devices, while SMS phishing detection spots malicious URLs.
		Sophos Firewall	Full visibility and control over all web traffic with flexible enforcement tools that work the way you need, with options for user and group enforcement of activity, quotas, schedules, and traffic shaping. Blocks known malicious domains and IP addresses through configuration of its web protection rule and FQDN host appropriately. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
Deny corporate computers direct Internet connectivity. Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.	Excellent	Sophos Firewall	Creates identity-based IPv6-capable firewall rule that can enforce strict authentication to access the internet resources.
Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR), and Enhanced Mitigation Experience Toolkit (EMET)	Excellent	Sophos Intercept X Sophos Intercept X for Server	Exploit technique mitigation is applied to the operating system and applications, going well beyond the capabilities offered in EMET. Intercept X offers the perfect replacement and alternative to EMET now that Microsoft has stopped active development of the tool.
Server application hardening especially Internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive or high-availability) data.	Very Good	Sophos Intercept X for Server	Integrates server application whitelisting/lockdown with advanced anti-malware and HIPS that lets you whitelist your applications at the click of a button and permits only trusted applications.
Operating system hardening (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD.	Very Good	Sophos Firewall	Allows restricted access to Server Message Block through appropriate firewall rule.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Antivirus software using heuristics and reputation ratings to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.	Very Good	Sophos Intercept X Sophos Intercept X for Server	Prevents malware before it can execute with heuristic evaluation, traditional signature matching with known malware, file reputation scoring, emulation, sandboxing, and more.
		Sophos Intercept X for Server	Integrates server application whitelisting/lockdown with our advanced anti-malware and HIPS to offer effective protection against zero-day attacks, along with heuristic evaluation, traditional signature matching with known malware, and file reputation scoring.
		Sophos Email	Employs the latest antivirus and phishing detection technology that constantly updates in real-time to detect the latest threats. Reputation filtering blocks unwanted spam right at the gateway.
		Sophos Firewall	Offers advanced Web Malware Protection with its advanced technology like real-time JavaScript emulation, behavioral analysis, context-sensitive inspection, and dynamic URL analysis for both HTTP and HTTPS traffic.
Control removable storage media and connected devices. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G devices.	Very Good	Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
		Sophos Wireless	Monitors the health status of any Sophos-managed endpoint or mobile device and automatically restricts web access on trusted Wi-Fi networks for those with serious compliance issues.
		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 keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices.
Block spoofed emails. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.	Very Good	Sophos Email	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. It spots and blocks phishing emails before they reach your users. Sophos Email also uses advanced machine learning to detect targeted impersonation and Business Email Compromise attacks. Utilizing the deep learning neural network created by Sophos AI, Sophos Email analyzes email body content and subject lines for tone and wording to identify suspicious conversations.
User education. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.	Good	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 Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
		Sophos Intercept X Sophos Intercept X for Server	Device Control allows admins to control the use of removable media through policy settings.
Antivirus software with up-to-date signatures identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	Limited	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		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.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
		Sophos Firewall	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. Delivers advanced protection from the latest drive-by and targeted web malware, URL/ Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
TLS encryption between email servers to help prevent legitimate emails from being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.	Limited	Sophos Email	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
Mitigation strategies to limit the extent of cybersecurity incidents			
Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	Essential	Sophos Cloud Optix	Sophos Cloud Optix, Cloud Security Posture Management solution, 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 Firewall	Offers centralized security management with extensive administrative controls; role-based administration to delegate control by job function.
		Sophos Mobile	Role-based administration ensures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Central	Configurable role-based administration provides granular control of administrator privileges. Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	Essential	Sophos Intercept X Sophos Intercept X for Server	Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.
		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. Locate systems and devices that are unpatched or have out-of-date software.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk level and prioritize response. Average time to detect and investigate is just 26 minutes.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.	Essential	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
		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. Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
Disable local administrator accounts or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.	Excellent	Sophos Central	Prevents shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account.
Network segmentation. Deny network traffic between computers unless required. Constrain devices with low assurance e.g. BYOD and IoT. Restrict access to network drives and data repositories based on user duties.	Excellent	Sophos Firewall	Flexible and powerful segmentation options via zones and VLANs provide ways to separate levels of trust on your network while enabling added protection against lateral movement between different parts of your network.
		Sophos Switch	Allows configuration of VLANs to segment your internal traffic and reduce the attack surface in case of an infection or breach. 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.
		Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
Protect authentication credentials. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Credential Guard. Change default passphrases. Require long complex passphrases.	Excellent	Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
		Sophos Firewall	Allows strong passphrase policy to be applied for admin accounts in terms of complexity, length, password reuse and use of a single dictionary word.
Non-persistent virtualised sandboxed environment, denying access to important (sensitive or high-availability) data, for risky activities e.g. web browsing, and viewing untrusted Microsoft Office and PDF files.	Very Good	Sophos Firewall	Supports next-gen cloud-sandbox technology for protection from ransomware and targeted attacks.
Software-based application firewall, blocking incoming network traffic that is malicious/unauthorised, and denying network traffic by default e.g. unneeded/ unauthorised RDP and SMB/NetBIOS traffic.	Very Good	Sophos Intercept X Sophos Intercept X for Server	Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
		Sophos Firewall	Offers complete visibility into risky users, evasive and unwanted applications, and suspicious payloads. Synchronized Application Control automatically identifies all unknown, evasive, and custom applications running on your network so you can easily prioritize the ones you want, and block the ones you don't.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.	Very Good	Sophos Intercept X for Server	Denies attackers by blocking the exploits and techniques used to distribute malware, steal credentials and escape detection. Prevent unauthorized programs running on your servers and receive notification if attempts are made to tamper with critical files.
		Sophos Firewall	Offers complete visibility into risky users, evasive and unwanted applications, and suspicious payloads. 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.
Outbound web and email data loss prevention. Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns.	Very Good	Sophos Firewall	Blocks and logs unapproved cloud computing services and applications. Offers policy-based outbound email DLP; and flexible, user-based monitoring and control of keyword content and downloadable content, including files types via FTP, HTTP, or HTTPS.
		Secure 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.
Mitigation strategies to detect cybersecurity incidents and respond			
Continuous incident detection and response with automated immediate analysis of centralized, time-synchronised logs of permitted and denied: computer events, authentication, file access and network activity.	Excellent	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
		Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Firewall	Provides real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading, and persistence.	Very Good	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
		Sophos Firewall	Next-gen protection technologies like deep learning and intrusion prevention to keep your organization secure.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Endpoint detection and response software on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.	Very Good	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
Hunt to discover incidents based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.	Very Good	Sophos Firewall	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 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.
		SophosLabs	Delivers the global threat intelligence advantage with Sophos' state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, Live Protection and Live Anti-spam offer the data and expert analysis from SophosLabs in real time.
		Sophos Managed Detection and Response (MDR)	Sophos MDR investigates suspicious signals, correlating data and behaviors and leveraging Sophos X-Ops threat intelligence for context and insights. On notification of vulnerabilities, Sophos MDR proactively hunts for exposure to enable swift remediation.
		Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Limited	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.
Capture network traffic to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.	Limited	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.
		Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.
		Sophos Firewall	Provides real-time insights into network and user events, quick and easy access to historical data, easy integration with third-party remote management and monitoring tools (RMMs).
		Sophos Managed Detection and Response (MDR)	Threat hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high caliber, actional signals across the network infrastructure to optimize cyber defenses.

Mitigation Strategy	Relative Security Effectiveness Rating	Sophos Solution	How It Helps
Mitigation strategies to recover data and system availability			
Business continuity and disaster recovery plans which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.	Very Good	Synchronized Security in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and cleanup devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
		Sophos Managed Detection and Response (MDR)	Sophos MDR swiftly contains and neutralizes incidents, with average time to detect, investigate and respond to just 38 minutes. Clients choose the level of response they wish us to take.
		Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
		Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
Mitigation strategy specific to preventing malicious insiders			
Personnel management e.g. ongoing vetting, especially for users with privileged access; immediately disable all accounts for departing users; and remind users of their security obligations and penalties.	Very Good	Sophos Central	Keeps access lists and user privileges information up-to-date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).

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

2022-12-06 CC (PC)

SOPHOS