Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity made simple.

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.

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
Mitigation strategies to prevent malware delivery and execution				
1	**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**	**Server Protection:** Server Lockdown allows only trusted whitelisted applications and associated files to run. **Intercept X:** 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 Firewall/UTM:** Allows user-based policy control over applications, websites, categories, and traffic shaping (QoS). Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints.
2	**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**	**Intercept X:** Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.	

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
3	**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	Endpoint & Server Protection: Application Control policies restrict the use of unauthorized applications. Intercept X: Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.	
4	**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	Endpoint & Server Protection: Application Control policies restrict the use of unauthorized applications. Intercept X: Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.	
5	**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	Intercept X: Browser exploit prevention detects and blocks malicious activity attempting to take advantage of software vulnerabilities. Endpoint & Server Protection: Web security and web control scans the web content and can limit access to known sites.	Sophos Sandstorm: Complements Sophos web and email security products and Sophos Firewall/UTM by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
6	**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 Mobile**: Anti-phishing technology in Sophos Secure Email and Sophos Secure Workspace apps protects users from malicious links received in documents or emails.	**Sophos Email Appliance***: Secures against email threats and phishing attacks; provides advanced DLP and easy policy-based encryption.
7	**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	**Endpoint & Server Protection**: Scans web content and allows category-based web filtering to be enforced both on and off the corporate network.	**Sophos Firewall/UTM**: Blocks known malicious domains and IP addresses through configuration of its web protection rule and FQDN host appropriately.
			Sophos Mobile: Centrally-managed web filtering in Sophos Mobile Security app provides category-based web filtering for Android devices.	**Secure Web Gateway***: 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.
8	**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/UTM**: Creates identity-based IPv6-capable firewall rule that can enforce strict authentication to access the internet resources.

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
9	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR), and Enhanced Mitigation Experience Toolkit (EMET)	**Excellent**	**Intercept X**: 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.	
10	**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**	**Server Protection**: 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.	
11	**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/UTM**: Allows restricted access to Server Message Block through appropriate firewall rule.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity made simple.

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
12	**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**	**Endpoint Protection:** Prevents malware before it can execute with heuristic evaluation, traditional signature matching with known malware, file reputation scoring, emulation, sandboxing, and more. **Server Protection:** Sophos Server Protection 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.	**Secure Web Gateway*:** 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. **Sophos Email Appliance and Sophos Email on Sophos Central*:** 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.
13	**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**	**Endpoint & Server Protection:** Device Control allows admins to control the use of removable media through policy settings. **SafeGuard Encryption:** Provides complete data protection across multiple platforms and devices, including mobile devices; secures data at rest as well as in transit.	

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
			Sophos Mobile: Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps.	
14	**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		**Secure Email Appliance Gateway*:** Support for Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) ensures spam and phishing attacks attempting to spoof legitimate sender domains are blocked.
15	**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.	**Secure Email Appliance and Sophos Email on Sophos Central*:** Detects threats and allows administrators to quarantine email for review and follow-up education with the user.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity made simple.

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
16	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	Limited	**Endpoint & Server Protection:** Integrates innovative technology like malicious traffic detection with real-time threat intelligence to help prevent, detect and remediate threats with ease.	**Secure Web Gateway*:** Monitors and blocks web site access for malware infections and execution; also integrates up-to-date threat intelligence on malicious sites from Sophos.
			Sophos Mobile: The Sophos Mobile Security app offers leading anti-malware and antivirus protection together with Potentially Unwanted App detection for Android devices.	**Sophos Email Appliance and Sophos Email on Sophos Central*:** Uses real-time threat intelligence to detect and block viruses and phishing emails that may include malware.
17	**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		**Secure Email Appliance Gateway*:** Offers TLS encryption and support for SMTP/S. IMAP supported with Email Appliance.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity made simple.

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
Mitigation strategies to limit the extent of cybersecurity incidents				
18	**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	**SafeGuard Encryption:** Offers role-based management to separate authorization levels, as well as detailed logging of all access attempts. **Sophos Enterprise Console/Sophos Central:** Configurable role-based administration provides granular control of administrator privileges. **Sophos Mobile:** Role-based administration ensures user privacy and appropriate credentials for altering compliance or device/data access.	**Sophos Firewall Manager:** Offers centralized security management with extensive administrative controls; role-based administration to delegate control by job function.
19	**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	**Intercept X:** Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.	

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
20	**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	**SafeGuard Encryption:** Authenticates users for access to specific files/folders with the use of user- or group-specific keys for SafeGuard encryption. **Sophos Central:** Protects privileged and administrator accounts with advanced two-factor authentication.	**Sophos Firewall/UTM:** Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
21	**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.	
22	**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/UTM:** Limits access between untrusted devices and critical servers with segmentation of the internal network and by applying policies, adding a layer of protection and logging to disrupt the attack chain.
23	**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/UTM:** Allows strong passphrase policy to be applied for admin accounts in terms of complexity, length, password reuse and use of a single dictionary word.

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
24	**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/UTM:** Supports next-gen cloud-sandbox technology for protection from ransomware and targeted attacks.
25	**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 Mobile:** The Corporate Browser in Sophos Secure Workspace delivers secure browsing access to pre-defined websites and domains from their mobile devices. **Endpoint & Server Protection:** 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/UTM:** Offers visibility and control over thousands of applications with granular controls based on category, risk, technology, and other characteristics.
26	**Software-based application firewall, blocking outgoing network traffic** that is not generated by approved/trusted programs, and denying network traffic by default.	Very Good	**Server Protection:** Gives automated application security with pre-defined policy templates while minimizing false positives with Sophos Server Protection's Server Lockdown.	

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity made simple.

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
27	**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		**Secure Web Gateway*:** Blocks and logs unapproved cloud computing services and applications. **Sophos Email Appliance:** Protect information by blocking messages containing sensitive data or by encrypting them before they leave the network gateway, with filters available for the following: ‣ Offensive language ‣ Bulk mail ‣ Total email size ‣ Attachment size ‣ Country/GeoIP
Mitigation strategies to detect cybersecurity incidents and respond				
28	**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:** All Sophos products are capable of generating security event logs that can be integrated into a centralized monitoring program for incident detection and response.	**Sophos Firewall/UTM:** 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).

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
				Sophos iView Reporting: Provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.
29	**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	**Server Protection**: Provides integrated server application whitelisting and Server Lockdown with advanced anti-malware and HIPS.	
30	**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	**Endpoint & Server Protection**: Creates detailed log events of all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process sensitive data. Detects and prevents malicious code execution on the Endpoint. **Intercept X**: Protects Office applications vulnerabilities being exploited through malicious abnormalities delivered through Office files.	

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity made simple.

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
32	**Network-based intrusion detection/ prevention system** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Limited		**Sophos Firewall/UTM**: 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.
33	**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	**Endpoint & Server Protection**: Creates detailed log events of all malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process PHI and PII.	**All Sophos Products**: Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response. **Sophos Firewall/UTM**: 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 iView Reporting**: Provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.

Australian Signals Directorate (ASD) Top 35 Reference Card

SR. NO.	MITIGATION STRATEGY	RELATIVE SECURITY EFFECTIVENESS RATING	ENDPOINT	NETWORK
Mitigation strategies to recover data and system availability				
35	**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		**Sophos Email on Sophos Central:** In the event of third-party cloud email service provider outages, alerts are provided if mail can't be delivered to a server/service; email is then queued for delivery to ensures no email is lost, and access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is 5 days.
Mitigation strategy specific to preventing malicious insiders				
37	**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).	**Sophos Firewall/UTM:** User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth and other network resources.

Specifications and descriptions subject to change without notice. Sophos disclaims in full all warranties and guarantees. This document and the information in it do not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

* Also available on Sophos XG Firewall and SG UTM

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

Oxford, UK

2018-05-08 RC-NA (PS)

SOPHOS