Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

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 products can be effective tools to help address some of the requirements as part of a customer's efforts to comply with the ASD Top 35 strategies.

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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**	Svr **Intercept X for Server:** Prevent unauthorized programs running on your servers and receive notification if attempts are made to tamper with critical files. Ep Svr **Intercept X and Intercept X for Server:** Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers. Application Control policies restrict the use of unauthorized applications. Mb **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.	Fw **Sophos Firewall:** Allows user-based policy control over applications, websites, categories, and traffic shaping (QoS). Synchronized Application Control in Sophos Firewall identifies all networked applications in the environment running on Sophos-managed endpoints.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**	Ep Svr **Intercept X and Intercept X for Server:** Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.	
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**	Ep Svr **Intercept X and 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**	Ep Svr **Intercept X and 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.	Fw **Sophos Firewall:** 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.
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**	Ep Svr **Intercept X and Intercept X for Server:** Browser exploit prevention detects and blocks malicious activity attempting to take advantage of software vulnerabilities. Web security and web control scans the web content and can limit access to known sites.	Fw **Sophos Sandstorm:** 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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**	Mb **Sophos Mobile:** Anti-phishing technology in Sophos Secure Email and Sophos Secure Workspace apps protects users from malicious links received in documents or emails.	Em **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**	Ep Svr **Intercept X and Intercept X for Server:** Scans web content and allows category-based web filtering to be enforced both on and off the corporate network. Mb **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.	Fw **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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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		Fw **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	Ep Svr **Intercept X and 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	Svr **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		Fw **Sophos Firewall:** Allows restricted access to Server Message Block through appropriate firewall rule.
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	Ep Svr **Intercept X and 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.	Fw **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.
		Svr **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.	Em **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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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	Ep Svr **Intercept X and Intercept X for Server:** Device Control allows admins to control the use of removable media through policy settings. Mb **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.	
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		Em **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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**		Ph **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.
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**	Ep Svr **Sophos Intercept X and Intercept X for Server:** Uses deep learning technology to detect both known and unknown malware without relying on signatures.	Fw **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.
		Mb **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.	Em **Sophos Email:** Uses behavioral analysis to stop never-before-seen ransomware and boot-record attacks.
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**		Em **Secure Email:** Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**	Enc **Sophos Central Device Encryption:** Offers role-based management to separate authorization levels, as well as detailed logging of all access attempts.	Fw **Sophos Firewall:** Offers centralized security management with extensive administrative controls; role-based administration to delegate control by job function.
		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).	ZT **Zero Trust Network Access:** Continuously validates user identity, device health, and compliance before granting access to applications and data.
		Mb **Sophos Mobile:** Role-based administration ensures user privacy and appropriate credentials for altering compliance or device/data access.	
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**	Ep Svr **Intercept X and Intercept X for Server:** Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.	MTR **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.
			RR **Sophos Rapid Response Service:** Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**	Enc **Sophos Central Device Encryption:** Authenticates users for access to specific files/folders with the use of user- or group-specific keys.	Fw **Sophos Firewall:** 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.
		Sophos Central: Protects privileged and administrator accounts with advanced two-factor authentication.	ZT **Zero Trust Network Access:** Continuously validates user identity, device health, and compliance before granting access to applications and data.
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**		Fw **Sophos Firewall:** 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. 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.
			ZT **Zero Trust Network Access:** 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.	Fw **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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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		Fw **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	Mb **Sophos Mobile:** The Corporate Browser in Sophos Secure Workspace delivers secure browsing access to pre-defined websites and domains from their mobile devices. Ep Svr **Sophos Intercept X and 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.	Fw **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.
Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.	Very Good	Svr **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.	Fw **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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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		Fw **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. Em **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.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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**	**Sophos Central Management:** Sophos Central provides powerful centralized management and reporting for all Sophos products from a single console.	**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).
		Synchronized Security in Sophos products: Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.	**Sophos Managed Threat Response:** Monitors and investigates detections from Sophos endpoint, network, and cloud platform solutions to identify, investigate, contain, and neutralize active threats.
		Intercept X with 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.	
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**	**Intercept X for Server:** Provides integrated server application whitelisting and Server Lockdown with advanced anti-malware and HIPS.	**Sophos Firewall:** Next-gen protection technologies like deep learning and intrusion prevention to keep your organization secure.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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	Ep **Intercept X:** Protects Office applications vulnerabilities being exploited through malicious abnormalities delivered through Office files. XDR Svr **Intercept X Advanced with XDR and Intercept X Advanced for Server with XDR:** Inspect your endpoints and servers, both on-premises and in the cloud across Windows, MacOS*, and Linux operating systems. Get the tools you need for advanced threat hunting and IT security operations hygiene. XDR **Intercept X Advanced with XDR:** It 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. Quickly find indicators of compromise (IoCs) across your estate. Remotely access, investigate, and remediate devices. Perform guided threat hunting and response.	
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	XDR **Intercept X Advanced with XDR:** It 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. Quickly find indicators of compromise (IoCs) across your estate. Remotely access, investigate, and remediate devices. Perform guided threat hunting and response.	MTR **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. RR **Sophos Rapid Response Service:** Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Australian Signals Directorate (ASD) Top 35 Reference Card

SOPHOS
Cybersecurity evolved.

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Limited		Fw **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	XDR **Intercept X Advanced with 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. **Sophos Central Management:** Sophos Central provides powerful centralized management and reporting for all Sophos products from a single console. **Synchronized Security in Sophos products:** Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.	Fw **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).

Australian Signals Directorate (ASD) Top 35 Reference Card

Mitigation Strategy	Relative Security Effectiveness Rating	Endpoint	Network
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		Em **Sophos Email:** 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			
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).	Fw **Sophos Firewall:** 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.

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

2022-03-17 RC-NA (PC)

SOPHOS