CIS Critical Security Controls - Reference Card

SOPHOS
Security made simple.

The CIS Critical Security Controls (previously known as the SANS Top 20 security controls) provide a catalog of prioritized guidelines and steps for resilient cyber defense and information security mitigation approaches. Developed by the Center for Internet Security, the set of recommended actions have been assessed and endorsed by leading federal and law-enforcement authorities including the U.S. Department of Homeland Security Federal Network Security Program, the U.S. National Security Agency, the US Department of Energy nuclear energy labs and several other think-tanks. These measures take into account empirical evidence from various cyber-attack incidents and provide guidelines to automate security for improved incident and response. With its proven-in-the-field security technologies, Sophos offers comprehensive capabilities to effectively implement these critical controls.

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
Inventory of Authorized and Unauthorized Devices	Reduce attack surface by applying effective monitoring and configuration management to maintain an up-to-date inventory of endpoint and other devices connected to the network, including workstations, laptops, mobile devices, servers and remote devices	**Sophos Endpoint and Server Protection:** Enforces web, application and device policies for Windows, Mac and Linux systems; When used with Sophos XG Firewall it automatically detects and isolates malware infected endpoint devices from network resources.
		Sophos Mobile: Device management solution for smartphones, tablets etc. Enforces security policies and monitors device health. Automatic remediation assures safety of device and corporate data.
		Sophos XG Firewall with Security Heartbeat™: Allows next generation endpoint and network security to continuously share meaningful information about suspicious events across extended IT ecosystem; detects compromised / unauthorized endpoint device, allows automated and near instantaneous isolation of this endpoint, preventing it from leaking confidential data to a C2 server; drastically improves incident response time.
Inventory of Authorized and Unauthorized Software	Track and control vulnerable, malicious or unproductive application / software to mitigate or root out application-borne risks or attacks	**Sophos Mobile:** Monitor devices for jailbreaking and side-loading of applications and deny access to email, network and other resources if device is not in compliance with policy.
		Sophos Firewall / UTM: Visibility and Control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications / software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints. Full list of controlled software / applications.

CIS Critical Security Controls - Reference Card

SOPHOS
Security made simple.

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Preventing hackers from compromising vulnerable systems, services and configurations; ensuring proper patch management and suitable security configurations for all systems and devices on the network	**Sophos Intercept X, Endpoint and Server Protection:** Exploit prevention capabilities stop vulnerabilities in applications and operating systems from being exploited by attackers.
Continuous Vulnerability Assessment and Remediation	Proactive identification and remediation of application vulnerabilities	**Sophos Mobile:** Proactively monitors Android devices via a Security Advisor and Privacy advisory warns users of potential vulnerabilities.
Controlled Use of Administrative Privileges	Validating administrative access and preventing misuse of administrative credentials	**Sophos Enterprise Console and Sophos Central:** Configurable role-based administration provides granular control of administrator privileges.
		Sophos Mobile: Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Firewall Manager: Centralized security management with extensive administrative controls; Role-based administration with change control and logging.
Maintenance, Monitoring, and Analysis of Audit Logs	Logging and reporting capabilities to enable audit trails and run forensics analysis and detailed investigation or reverse engineering of attacks; capture log information on user actions, network events, device events, network usage and more	**All Sophos products:** Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall: Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos SafeGuard Enterprise: Provides detailed logging of all access attempts.
		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.

CIS Critical Security Controls - Reference Card

SOPHOS
Security made simple.

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
Email and Web Browser Protections	Preventing threats from email and web to compromise network, systems and data	**Sophos Email Appliance:** Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
		Secure Web Gateway: Monitors and blocks web site access for malware infections and execution, and also integrates up-to-date threat intelligence on malicious sites from Sophos.
		Sophos Endpoint and Server Protection: Users can be blocked from visiting restricted and malicious URLs.
Malware Defenses	Deploying safeguards against malicious code or malware attacks to prevent tampering with network access, systems, applications and mission-critical data	**Sophos Intercept X:** Anti-exploit, anti-ransomware and deep learning malware detection protect endpoints from malicious executable code.
		Sophos Endpoint and Server Protection: Integrate innovative technology like malicious traffic detection with real-time threat intelligence to help prevent, detect and remediate threats with ease.
		Sophos Email Appliance: 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.
		Sophos XG Firewall: Includes IPS, APT, AV, Sandboxing with Deep Learning, and Web Protection to monitor and block malware and exploits from accessing any part of your network.
		Sophos Sandstorm: Optional cloud-based technology, it inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
		Sophos Mobile: Delivers secure Unified Endpoint Management (UEM) for mobile devices, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security for Android provides leading antivirus, ransomware, and unwanted app protection for Android devices.

CIS Critical Security Controls - Reference Card

SOPHOS
Security made simple.

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
Limitation and Control of Network Ports, Protocols, and Services	Restricting remote access to select authorized users; permitting only trusted traffic that meet security policy rules; endpoint protection with strong filtering and host-based IPS capabilities	**Sophos Firewall / UTM:** Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization.
		Sophos Mobile: Integration with Sophos UTM and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Intercept X, Endpoint and Server Protection: HIPS and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
Data Recovery Capability	Preventing attack from compromising mission-critical data; ensuring reliable data protection and recovery capabilities	**Synchronized Security:** Stops data-stealing attacks at your network perimeter with Synchronized Security that works side-by-side with endpoint protection to automatically identify and isolate compromised systems.
		Sophos Intercept X, Endpoint and Server Protection: Integrated system of prevention, detection, remediation and encryption technologies.
		SafeGuard Encryption: Proven encryption technology; flexible recovery options for keys, data and forgotten passwords.
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Ensuring standard security configurations and security best practices for network devices to prevent exploit or network hack; keeping the built-in firmware of network devices up-to-date	**Sophos Firewall / UTM:** Unified policy management for web, IPS, app control, traffic shaping, WAF, VPN and more with pre-defined policy templates mapped to best practices.

CIS Critical Security Controls - Reference Card

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
Boundary Defense	Employing effective best practices to protect expanding perimeter and company boundaries from web, email and other threats; capabilities that effectively scan in-bound and out-bound traffic for threats and anomalies	**Sophos Firewall / UTM:** XG Firewall includes IPS, APT, AV, Sandboxing with Deep Learning, and Web Protection to monitor and block malicious, anomalous and exploitive traffic from in-bound or out-bound access. **Secure Email Gateway and Secure Web Gateway:** Round-the-clock threat analysis for protection against the changing nature of email and web-based threats. **Sophos Sandstorm:** An optional cloud-sandbox technology, it can be fully integrated into Sophos security solutions to provide an extra layer of security. Sandstorm inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
Data Protection	Effective data loss prevention capabilities to safeguard mission-critical data while preventing unauthorized access to sensitive information; data protection that helps satisfy compliance needs	**Endpoint Protection:** Data loss prevention policies prevent misuse and distribution of predefined data sets. **SafeGuard Enterprise:** Complete data protection across multiple platforms and devices, including mobile devices; secures data at rest as well as moving data. **Sophos Mobile:** Delivers mobile data protection when integrated with SafeGuard Enterprise to enable access to encrypted content on mobile devices. The secure Sophos Container for email, documents, and content makes sure that protected data stays separate and can be locked down or wiped. **Sophos Email Appliance and XG Firewall:** SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help ensure compliance.
Controlled Access Based on the Need to Know	Enforce role-based access with restricted exposure to network and information resources; validate access to authorized users based on their role and responsibilities	**Sophos XG Firewall:** Offers controlled access to data based on the user-identity technology that governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.

CIS Critical Security Controls - Reference Card

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
		Sophos SafeGuard Enterprise: Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
		Sophos Central: 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).
		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 compliance rules, time, Wi-Fi, or geo-location.
Wireless Access Control	Securing network from unauthorized wireless access; granting access to only authorized devices that meet proper security configuration	**Sophos Wireless and XG Firewall:** Know exactly what's happening with your users and your wireless network with increased visibility and controls from Sophos Wireless. Provide controlled internet access for visitors, contractors, and other guests on your wireless network. Get the status of your wireless networks, access points, connected clients and identify potential issues needing attention on a single dashboard.
Account Monitoring and Control	Reliable authentication for authorized users; identifying attacks impersonating as business users; tracking suspicious user activity and enabling instant incident response	**Sophos Endpoint and Server Protection:** Get detailed log events of malicious activity on endpoint systems, helping to identify suspicious activity on systems that may store or process cardholder data.
		Sophos Server Protection: Prevent unauthorized applications from running with Server Protection that automatically scans your system for known-good applications and whitelists only those applications.
		Sophos Firewall/UTM: Get 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).

CIS Critical Security Controls - Reference Card

SOPHOS
Security made simple.

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
		Sophos iView Reporting: Get 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.
Security Skills Assessment and Appropriate Training to Fill Gaps	Addressing skills gaps with training and demonstration of latest best practices	**Sophos Training and Certifications:** Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
Application Software Security	Protecting mission-critical web and business applications from unauthorized access, web-attacks and tampering	**Sophos UTM/Firewall:** Web Server Protection protects externally facing servers and applications from hackers; secures against more than 350 web-attack patterns. Next-gen IPS provides advanced protection for your critical business applications from hacks and attacks.
		Sophos Mobile: Corporate Browser within Secure Workspace protects corporate websites while delivering secure access to users who need access to applications and corporate websites from their mobile devices.
Incident Response and Management	Proactive incident response plan focused on faster threat discovery, attack remediation and protection of data in the event of attack becoming wide-spread, so that spread of risk is containedand	**Sophos Synchronized Security:** Shares telemetry and health status enabling coordinated isolation, detection and malware remediation across servers, endpoints, and firewalls - stopping advanced attacks.
		Sophos Intercept X: Get the Root Cause Analysis of an attack with complete visibility on how and where of the attack along with recommendations on what your next steps should be.

CIS Critical Security Controls - Reference Card

SOPHOS
Security made simple.

CIS CRITICAL SECURITY CONTROLS	SECURITY CONTROL IMPLICATION	SOPHOS SOLUTION
Penetration Tests and Red Team Exercises	Conducting periodic penetration tests to find out potential vulnerable areas, assess baseline security needs and quality of security posture and readiness of security teams to mitigate risks from attacks	**Professional Services:** Helps customers plan, build and manage a robust security infrastructure. **Security Consulting:** Penetrating testing and vulnerability assessment of security infrastructure and software deployments; recommendations for architecture and design changes needed to better use the available infrastructure. **Health-check Service:** Helps keep Sophos security deployments well- tuned; educates on new threat sources, emerging compliance norms and secure adoption of new technology.

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.

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

SOPHOS