CIS Critical Security Controls - Reference Card

SOPHOS

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. This document describes how Sophos, with its proven-in-the-field security technologies, offers effective tools to help address some of the requirements as part of a customer's efforts to comply with CIS Critical Security Controls.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. Use of Sophos products alone does not guarantee legal compliance. The information in this document does 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.

CIS CRITICAL SECURITY CONTROLS	SOPHOS SOLUTION	HOW IT HELPS
Control 1: Inventory and Control of Enterprise Assets *Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.*	Sophos Cloud Optix	Provides accurate inventories and network topologies visualizations of an organization's cloud resources across all production environments including hosts, containers, serverless, IAM, network security groups and more while adding additional visualizations for traffic flows, and deployment of Sophos Cloud workload agents and Sophos virtual firewalls within the environment. With inventory in place, Cloud Optix scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.

Control 2: Inventory and Control of Software Assets *Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*	Sophos Firewall	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 Sophos Firewall identifies all networked applications in the environment running on Sophos Managed Endpoints.
	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 Cloud Optix	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization. Cloud Optix scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	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.
	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.
Control 3: Data Protection *Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.*	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify shared storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central Device Encryption	Enables protection of devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Email	Automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypt messages with just a few clicks. Offers TLS encryption and support for SMTP/S along with push-based encryption to send encrypted emails and attachments as password protected documents direct to the user's inbox, full portal-based pull encryption to manage encrypted messages entirely from a secure portal, and S/MIME to encrypt email messages and add a digital signature to safeguard against email spoofing.

Control 4: Secure Configuration of Enterprise Assets and Software *Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).*	Sophos Firewall	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. Administrators are instructed to change the default password of the "admin" user immediately after deployment. An alert is displayed when the default password for the super administrator is not changed.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration. DevSecOps tools work seamlessly with existing DevOps processes to help prevent security breaches pre-deployment. Sophos Cloud Optix scans container images in ECR, ACR, Docker Hub registries, as well as GitHub and Bitbucket IaC environments to identify operating system vulnerabilities and fixes to prevent threats pre-deployment. Prevents Infrastructure-as-Code (IaC) templates containing insecure configurations as well as embedded secrets and keys from never making it to a test or live production environment.
	Sophos Central	Disables or removes default passwords. Passwords are sufficiently complex to withstand targeted "brute force" attacks and must be rotated periodically.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Intercept X Sophos Intercept X for Server	Endpoint Protection application control policies restrict the use of unauthorized applications. Device Control allows admins to control the use of removable media through policy settings. Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code.
	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.
Control 5: Account Management *Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.*	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.
	Sophos Central	Does not permit shared administrator accounts. Each employee has his or her own account, with explicit permissions granted to each account. Protects privileged and administrator accounts with advanced two-factor authentication.
	Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
	Sophos Email	Delivers granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
	Sophos Mobile	A rich set of device management capabilities, containers, and market-leading encryption keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device.
	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.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.

Control 6: Access Control Management *Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.*	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. 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 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 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.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
Control 7: Continuous Vulnerability Management *Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.*	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	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 XDR	Detects and investigates 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 Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Managed Detection and Response (MDR)	24/7 detection, investigation and neutralization of suspicious activities by human experts enables us to identify and stop exploitation of vulnerabilities by adversaries. Sophos X-Ops experts keep operators up-to-date on the latest threat and vulnerability developments.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.

Control 8: Audit Log Management *Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.*	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.
	Sophos Firewall	Allows 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 feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	Threat hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities.
	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
Control 9: Email and Web Browser Protections *Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.*	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.
	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 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. 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.
Control 10: Malware Defenses *Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.*	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	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 Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	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.

Control 11: Data Recovery *Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.*	Sophos Intercept X Sophos Intercept X for Server	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.
Control 12: Network Infrastructure Management *Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.*	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. 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. Enables administrators to block or limit traffic to certain external systems with port-based or app-based policies. 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.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Wireless	Offers visibility into wireless networks health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy.
	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.
Control 13: Network Monitoring and Defense *Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.*	Sophos Firewall	Allows 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). Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	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 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.
	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.
Control 14: Security Awareness and Skills Training *Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.*	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 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.

Control 15: Service Provider Management *Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.*	Sophos Intercept X with XDR	Provides comprehensive defense in depth against threats that get in via third party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully-managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.
Control 16: Application Software Security *Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.*	Sophos Intercept X Sophos Intercept X for Server	Blocks vulnerabilities in applications, operating systems, and devices with its exploit prevention capabilities.
	Sophos Cloud Optix	DevSecOps tools work seamlessly with existing DevOps processes to help prevent security breaches pre-deployment. Sophos Cloud Optix scans container images in ECR, ACR, Docker Hub registries, as well as GitHub and Bitbucket IaC environments to identify operating system vulnerabilities and fixes to prevent threats pre-deployment. Prevents Infrastructure-as-Code (IaC) templates containing insecure configurations as well as embedded secrets and keys from never making it to a test or live production environment.
Control 17: Incident Response and Management *Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.*	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.
	Sophos Managed Detection and Response (MDR)	Full incident response service included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting.
	Sophos Rapid Response Service	Get fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
Control 18: Penetration Testing *Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.*	Security Consulting	Sophos offers penetration testing and vulnerability assessment of security infrastructure and software deployments; and recommendations for architecture and design changes needed to better use the available infrastructure.
	Sophos Cloud Optix	Allows security teams to focus on and fix their most critical public cloud security vulnerabilities before they are identified and exploited in cyberattacks. By identifying and risk-profiling security, compliance, and cloud spend risks, Cloud Optix enables teams to respond faster, providing contextual alerts that group affected resources with detailed remediation steps.

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

2022-11-25 RC-NA (MP)

SOPHOS