SOPHOS

Top Cybersecurity Controls Required to Secure Cyber Insurance and How Sophos Can Help

Cyber insurance providers increasingly require organizations to deploy strong cybersecurity controls as a condition of providing cover. Strengthening your defenses reduces your risk of making a claim following a major cyber incident, while incident response planning and testing reduces the cost and impact of an attack.

This table details the top cybersecurity controls that are commonly considered key to insurability, mitigation, and resilience by cyber insurance providers, and how Sophos can help. Without a positive response in the first five categories, organizations may not be able to secure coverage.

A Sophos Solution Brief. February 2022

Top Cybersecurity Controls Required to Secure Cyber Insurance and How Sophos Can Help

Cyber Control	How Sophos Can Help	Detail
Multifactor authentication for remote access and admin/privileged controls	**Sophos ZTNA**	Enables MFA to access your applications from any location.
	Sophos Firewall	Supports MFA for remote access VPN.
	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for Root user and IAM user access with MFA disabled and provides guided remediation.
	Sophos Central	Enforces MFA for your IT security management, securing access to all your protection solutions.
Endpoint Detection and Response (EDR)	**Sophos XDR** (Extended Detection and Response)	Enables organizations to conduct advanced threat hunting and neutralization. Detections can come from all over your environment: endpoint, server, firewall, email, cloud, mobile, Microsoft 365, and more.
	Sophos MDR (Managed Detection and Response)	24/7/365 threat hunting, detection and response delivered by an expert team as a fully-managed service.
Secured, encrypted, and tested backups	**Sophos Workload Protection**	Secures backups in cloud and on premises environments.
	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
Privileged access management (PAM)	**Sophos Cloud Optix**	Enables IT teams to manage the large number of configurations and policies in a cloud environment, providing superior visibility, governance, compliance, and oversight of cloud IAM role entitlements, whether human or non-human cloud services and, ultimately, achieve a state of least privilege access across their cloud environments.
	Sophos XDR (Extended Detection and Response)	Records all user activity, including authentication and Microsoft 365 audit logs to show changes to privilege settings. Also includes access to the Windows logs from the device and domain controller to see Windows events.
	Sophos Endpoint and **Sophos Workload Protection**	Prevents attempts to harvest or steal user credentials directly from memory.
Email filtering and web security	**Sophos Email**	Removes malware, malicious URLs, credential harvesting, and impersonation attacks while keeping mail flowing.
	Sophos Endpoint and **Sophos Workload Protection**	Protects against malicious downloads and suspicious payloads delivered via browsers. Control features enable administrators to warn or block websites based on their category, block risky file types, and apply data leakage controls against web-based email and file sharing. Web Control for Cloud Workload environments secures data when users access virtual desktops that don't sit behind a traditional web gateway.
	Sophos Firewall	Protects from compromised sites, pharming attacks, and malicious downloads with extensive machine learning and sandboxing inspection for file downloads. Integrated email protection also provides anti-spam, anti-virus, encryption, and DLP message protection.
Cyber incident response planning and testing	**Sophos Rapid Response**	Provides lightning fast, 24/7 incident response delivered by Sophos specialists.
	Sophos MDR (Managed Detection and Response)	Provides 24/7 threat hunting, detection and response delivered by an expert team as a fully-managed service.

Top Cybersecurity Controls Required to Secure Cyber Insurance and How Sophos Can Help

Cyber Control	How Sophos Can Help	Detail
Cybersecurity awareness training and phishing testing	Sophos Phish Threat	Improves security awareness and educates users with phishing attack simulations, automated security awareness training, and comprehensive reporting. Integration with Sophos Email enables security teams to efficiently identify and fast track the training of users who have been warned or blocked from visiting a website due to its risk profile.
Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	Sophos Firewall	Enables IT teams to easily manage and lock down RDP.
	Sophos Cloud Optix	Proactively identifies exposed RDP ports via public cloud security benchmark assessments. Guided remediation instructs administrators on how to address these security misconfigurations.
	Sophos XDR (Extended Detection and Response)	Monitors all RDP connections and logs the activity. Remote terminal allows administrators to enable/disable RDP policy. Provides visibility into the RDP policy on all managed devices and detect changes to it.
Logging and monitoring/ network protections	Sophos XDR (Extended Detection and Response)	Records up to 90 days of on-disk data and 30 days of data stored in the Sophos Data Lake.
	Sophos Cloud Optix	Continually monitors public cloud resources to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
	Sophos Firewall	Includes extensive built-in logging and reporting included at no extra charge. Additional centralized cloud-based logging and monitoring is also available, as well as Sophos XDR and Sophos MDR integration for advanced cross estate threat hunting and response.
End of life systems replaced or protected	Sophos XDR (Extended Detection and Response)	Identifies outdated and unsupported software and systems.
Patch management and vulnerability management	Sophos Cloud Optix	Proactively identifies and mitigates security vulnerabilities and network access misconfigurations in AWS public cloud environments with integration to Amazon Inspector, including virtual machine ports exposed to the internet, remote root login being enabled, or vulnerable software versions installed. Receives patch status for Amazon virtual machines with integration to AWS Systems Manager. Extends vulnerability scanning to cloud native containers across Azure, AWS and Docker by scanning container images for OS vulnerabilities. Automatically detects security configuration vulnerabilities pre-deployment with infrastructure-as-code template scanning in development pipelines, including scans for embedded secrets, passwords, and keys to proactively prevent breaches.
	Sophos XDR (Extended Detection and Response)	Provides access to all applications on the device, version info, SHA256, patch info and their logs, including the application execution history, network connections, parent/child processes etc.. Includes queries to check installed applications against online vulnerability information, and queries to identify security posture weaknesses in registry settings.

To discuss how Sophos can help you put in place the cyber controls required by insurance providers, speak to a Sophos representative.

2023-07-10 (SB-PS)

SOPHOS