SOPHOS
Cybersecurity delivered.

Top Ransomware Controls and How Sophos Can Help

The ransomware challenge continues to grow. The proportion of organizations hit by ransomware has almost doubled in twelve months, up from 37% in 2020 to 66% in 2021. Adversaries have also become more successful at encrypting data, with 65% of attacks resulting in data encryption last year*.

Stopping ransomware requires efforts to prevent both advanced, hands-on-keyboard attacks executed by skilled adversaries as well as the growing success of the Ransomware-as-a-Service model, which significantly extends the reach of ransomware by reducing the skill level required to deploy an attack.

This guide details the top cybersecurity controls that minimize ransomware exposure and impact and how Sophos can help.

A Sophos Solution Brief. April 2022

CYBER CONTROL	HOW SOPHOS CAN HELP	DETAIL
Proactive threat hunting to detect and neutralize human-led attacks before the ransomware is deployed	Sophos XDR (Extended Detection and Response)	Enables organizations to conduct threat hunting and neutralization across their environment. Detections can come from endpoint, server, cloud workloads, firewall, email, public cloud environments, mobile, Microsoft 365, and more.
	Sophos MTR (Managed Threat Response)	24/7/365 threat hunting, detection and response delivered by an expert Sophos team as a fully-managed service. Connectors to a range of security and IT solutions, including Microsoft 365, extend our operators' visibility across the customer estate, increasing their ability to defend against attacks.
Automatic blocking of ransomware threats before they can be deployed	Sophos Endpoint and Sophos Workload Protection	Provides advanced ransomware protection capabilities that disrupt the whole attack chain, including: › Deep learning artificial intelligence to prevent both known and unknown ransomware › Exploit protection to block the exploits and techniques used to distribute malware, steal credentials, and escape detection › Application control to block applications from running on cloud workloads that could be used by adversaries to launch attacks › Server lockdown which takes a known, good configuration of cloud workloads and locks that state to prevent unauthorized programs from running. › Anti-ransomware technology that detects and rolls-back unauthorized encryption, shutting down the processes before they can spread across your network. Protects against both file-based and master boot record ransomware.
	Sophos Email	Automatically analyzes all file processes, file activity, registry activity, and network connections to block ransomware and other forms of malware. Advanced phishing protection, URL scanning, and post-delivery protection ensure only safe senders reach your inbox and if the threat state of delivered messages change, they are automatically removed.
	Sophos Firewall	Protects from compromised sites and malicious downloads with extensive machine learning and sandboxing inspection for file downloads to identify even new, previously unseen ransomware attacks.

CYBER CONTROL	HOW SOPHOS CAN HELP	DETAIL
Identifying and closing down security gaps to harden your environment, for example unpatched devices, unprotected machines, and more.	Sophos XDR (Extended Detection and Response)	Identifies outdated and unsupported software and systems. Provides access to all applications on the device, version info, SHA256 file hashes, 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.
	Sophos ZTNA	Enables secure, granular remote access to systems and applications, eliminating the attack surface area and potential for attacks to move laterally.
Locking down Remote Desktop Protocol to prevent adversaries using it to gain access	Sophos Firewall	Enables IT teams to easily manage and lock down RDP.
	Sophos ZTNA	Enables secure remote access to RDP and other applications without exposing these systems to attack.
	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)	Detects 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 detects changes to it.
Cyber incident response planning to minimize impact if an attack occurs	Sophos Rapid Response	Provides lightning fast, 24/7 incident response delivered by Sophos specialists.
	Sophos MTR (Managed Threat Response)	Provides 24/7 threat hunting, detection, and response delivered by an expert team as a fully-managed service.
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.

CYBER CONTROL	HOW SOPHOS CAN HELP	DETAIL
Identifying and mitigating vulnerabilities in cloud environments to prevent exploitation by adversaries	Sophos Cloud Optix	Proactively identifies and mitigates security vulnerabilities, over-privileged IAM roles, and network access misconfigurations in 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 security scans to CI/CD pipelines with Infrastructure as Code scanning while analyzing containers registries across Azure, AWS, and Docker Hub for OS vulnerabilities.

To discuss your cyber resilience and how Sophos can help you strengthen your ransomware defenses, speak to a Sophos representative.

** The State of Ransomware 2022, Sophos, Survey of 5,600 IT professionals in 31 countries*

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2022-04-08 (SB-NP)

SOPHOS