Sophos MDR:

Achieving multiple cyber controls required for cyber insurance

High levels of cyber control are now commonly required by insurance providers as conditions of cover. Their goal: to reduce the likelihood that an organization will experience a major cyber incident and make a claim on their cyber insurance policy. In fact, 54% of IT professionals have experienced an increase in the level of cyber controls required to secure cyber insurance over the last year.*

Sophos Managed Detection and Response (MDR) enables organizations to achieve many of the cyber controls that are key to insurability. With Sophos MDR you benefit from both an expert threat hunting and neutralization service and advanced protection technologies:

- **24/7 threat hunting, detection and response service** delivered by Sophos expert operators
- **Sophos extended detection and response (XDR) tool,** enabling you to access live and historic data across your endpoints and your wider environment for macro-level assessment and granular deep dives
- **Sophos Endpoint protection software,** giving you world-leading cybersecurity for your devices and workloads that stops more threats, faster

For more information and to discuss your requirements, speak to a Sophos representative.

Cyber control	Sophos MDR
Endpoint Detection and Response (EDR)	Sophos Endpoint delivers world-leading protection for your endpoints and workloads, blocking 99.98% of cyber attacks before they can run [AV-TEST].]In parallel, Sophos MDR threat hunting experts monitor your environment 24/7, detecting, investigating and neutralizing even the most advanced, human-led attacks.
Web security	Sophos Endpoint 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.
Privileged Access Management (PAM)	Sophos XDR records all user activity, including authentication and Microsoft 365 audit logs to show changes to privilege settings. It also includes access to the Windows logs from the device and domain controller to see Windows events. Sophos Endpoint protection prevents attempts to harvest or steal user credentials directly from memory.
Cyber incident response planning	Sophos MDR includes incident response cover, so if you experience an event our team of expert responders will step in and address it - at no extra cost.
Hardening techniques, including remote desktop protocol (RDP) mitigation	Sophos XDR enables you to identify and remediate security gaps, including unprotected devices, to harden your environment. Plus it enables you to identify when RDP has been used and provides visibility into the RDP policy on all managed devices and detects changes to the policy. Remote terminal allows administrators to enable/disable RDP policy on devices from any location.
Logging and monitoring	Sophos XDR records up to 90 days of on-disk data and 30 days of data stored in the Sophos Data Lake.
End of life systems replaced or protected	Sophos XDR enables you to identify outdated and unsupported software and systems.
Patch management and vulnerability management	Sophos XDR 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.. It includes queries to check installed applications against online vulnerability information, and queries to identify security posture weaknesses in registry settings.

** Cyber Insurance 2022: Reality from the Infosec Frontline, Sophos*

SOPHOS