Sophos frente a Microsoft

FUNCIONES	Sophos	Microsoft
Superficie de ataque, pre y posejecución		
Reducción de la superficie de ataque, con múltiples tecnologías para la protección web, el control de aplicaciones y el control de dispositivos que eliminan los vectores de ataque y protegen contra la pérdida de datos	✓	Parcialmente incluido
Defensas que se adaptan automáticamente a los ataques perpetrados por humanos	✓	Parcialmente incluido
Verificación automatizada del estado de la cuenta para mantener una postura de seguridad sólida	✓	✓
Security Heartbeat para compartir información sobre estados de seguridad y amenazas entre múltiples productos	✓	Parcialmente incluido
Mitigaciones de exploits		
Mitigaciones activadas por defecto en el sistema operativo Windows	7	7
Mitigaciones activadas por defecto en el producto	60	0
Mitigaciones desactivadas por defecto que requieren una configuración manual	0	32
Detección de ransomware con reversión automática de documentos	✓	Parcialmente incluido
Bloqueo y reversión remota de ransomware	✓	✗
Igualdad de funciones entre Windows, macOS y Linux	Parcialmente incluido	Parcialmente incluido
Administración, investigación y remediación		
Una única consola de administración para la gestión y creación de informes	✓	✗
Clasificación de alertas y asistencia	✓	✓
Amplias capacidades de búsqueda e investigación de amenazas	✓	✓
Adecuado para clientes sin SOC interno	✓	Parcialmente incluido
Adecuado para grandes empresas con un SOC interno completo	✓	✓
Búsqueda y respuesta a amenazas		
Funcionalidad de detección y respuesta para endpoints (EDR)	✓	✓ (E5 requerido)
La integración de la detección y respuesta ampliadas (XDR) permite a los analistas buscar y responder a amenazas en todo su entorno, correlacionar información y alternar entre datos de endpoints, servidores, redes, dispositivos móviles, correo electrónico, la nube pública y Microsoft 365.	✓	✓ (E5 requerido)
El servicio MDR ofrece búsqueda, detección y remediación ilimitada de amenazas 24/7 a organizaciones de todos los tamaños, con asistencia disponible por teléfono o correo electrónico	✓	✓
Respuesta a incidentes incluida en el nivel superior de MDR	✓ (IR opcional en niveles inferiores de MDR)	✗
Integración con controles de seguridad de terceros para aprovechar sus inversiones en seguridad existentes y proporcionar una visibilidad total de su entorno y detecciones y alertas a su equipo y al equipo de MDR	✓	✓ (Requiere compra adicional y no es aplicable a MDR)
Análisis del tráfico de red cifrado (NDR)	✓	✗

Prevención de exploits predeterminada

Nada más instalarlo, Sophos amplía la protección básica ofrecida por Windows con 60 mitigaciones de exploits adicionales preconfiguradas, ajustadas y activadas de manera automática. Con Microsoft, debe activar y ajustar manualmente las mitigaciones, lo que aumenta el riesgo de errores de configuración y puede crear una falsa sensación de protección.