Visão Geral do Intercept X, XDR e MTR

SOPHOS
Cybersecurity evolved.

Gerenciado pelo Sophos Central

		PONTOS DE DESTAQUE	INTERCEPT X ESSENTIALS	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X WITH MTR STANDARD	INTERCEPT X WITH MTR ADVANCED
	GERENCIAMENTO	Políticas múltiplas		✓	✓	✓	✓
		Atualizações controladas		✓	✓	✓	✓
PREVINA	REDUÇÃO DA SUPERFÍCIE DE ATAQUE	Controle de Aplicativos		✓	✓	✓	✓
		Controle de periféricos		✓	✓	✓	✓
		Controle da Web / Bloqueio de URL por categoria		✓	✓	✓	✓
		Reputação de download	✓	✓	✓	✓	✓
		Serviço de segurança	✓	✓	✓	✓	✓
	ANTES QUE SEJA EXECUTADO NOS DISPOSITIVOS	Detecção de malware com Deep Learning	✓	✓	✓	✓	✓
		Varredura de arquivo por anti-malware	✓	✓	✓	✓	✓
		Proteção em tempo real	✓	✓	✓	✓	✓
		Análise de comportamento de pré-execução (HIPS)	✓	✓	✓	✓	✓
		Bloqueio de aplicativo potencialmente indesejado (PUA)	✓	✓	✓	✓	✓
		Sistema de Prevenção de Invasão (IPS)	✓	✓	✓	✓	✓
	DETENÇÃO DA EXECUÇÃO DE AMEAÇAS	Prevenção contra a perda de dados	✓	✓	✓	✓	✓
		Análise de comportamento de tempo de execução (HIPS)	✓	✓	✓	✓	✓
		Antimalware Scan Interface (AMSI)	✓	✓	✓	✓	✓
		Detecção de tráfego malicioso (MTD)	✓	✓	✓	✓	✓
		Prevenção contra exploração (detalhes na página 5)	✓	✓	✓	✓	✓
		Mitigações contra usuários ativos (detalhes na página 5)	✓	✓	✓	✓	✓
		Proteção de arquivos contra ransomware (CryptoGuard)	✓	✓	✓	✓	✓
		Proteção a registro de inicialização e disco (WipeGuard)	✓	✓	✓	✓	✓
		Proteção contra Man-in-the-Browser (Safe Browsing)	✓	✓	✓	✓	✓
		Bloqueio de aplicativos aprimorado	✓	✓	✓	✓	✓

Recursos continuam na próxima página

Visão Geral do Intercept X, XDR e MTR

SOPHOS
Cybersecurity evolved.

Gerenciado pelo Sophos Central (continuação)

		PONTOS DE DESTAQUE	INTERCEPT X ESSENTIALS	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH XDR	INTERCEPT X WITH MTR STANDARD	INTERCEPT X WITH MTR ADVANCED
DETECTAR E INVESTIGAR	DETECTAR	Live Discover (consulta SQL patrimonial para caça a ameaças e higiene das operações de segurança de TI)			✓	✓	✓
		Biblioteca de Consultas SQL (consultas pré-gravadas e totalmente personalizáveis)			✓	✓	✓
		Acesso rápido, armazenamento de dados em disco (até 90 dias)			✓	✓	✓
		Fontes de dados entre produtos, por exemplo, Firewall, Email			✓	✓	✓
		Consulta entre produtos			✓	✓	✓
		Sophos Data Lake (armazenamento de dados na nuvem)			30 dias	30 dias	30 dias
		Consultas agendadas			✓	✓	✓
	INVESTIGUE	Casos de ameaças (análise da causa raiz)		✓	✓	✓	✓
		Análise de malware com Deep Learning			✓	✓	✓
		SophosLabs Threat Intelligence por demanda avançado			✓	✓	✓
		Exportação de dados forenses			✓	✓	✓
RESPONDA	REMEDIAÇÃO	Remoção automatizada de malware	✓	✓	✓	✓	✓
		Security Heartbeat sincronizado	✓	✓	✓	✓	✓
		Sophos Clean	✓	✓	✓	✓	✓
		Live Response (Acesso a terminal remoto para investigação aprofundada e resposta)			✓	✓	✓
		Isolamento de endpoint por demanda			✓	✓	✓
		Comando de um clique "Eliminar e Bloquear"			✓	✓	✓
SERVIÇO GERENCIADO	CAÇA A AMEAÇAS E RESPOSTA CONDUZIDAS POR HUMANOS	Caça de ameaças conduzida por indícios 24/7				✓	✓
		Verificações de integridade da segurança				✓	✓
		Retenção de dados				✓	✓
		Relatório de atividades				✓	✓
		Detecções adversas				✓	✓
		Neutralização e correção de ameaças				✓	✓
		Caça de ameaças conduzida sem indícios 24/7					✓
		Resposta a ameaças conduzida pela equipe					✓
		Chamada direta para assistência					✓
		Gerenciamento proativo de postura de segurança					✓

Visão Geral do Intercept X, XDR e MTR

SOPHOS
Cybersecurity evolved.

Comparação de sistemas operacionais

		PONTOS DE DESTAQUE	WINDOWS	macOS
PREVINA	REDUÇÃO DA SUPERFÍCIE DE ATAQUE	Serviço de segurança	✓	✓
		Reputação de download	✓	
		Controle da Web / Bloqueio de URL por categoria	✓	✓
		Controle de periféricos	✓	✓
		Controle de Aplicativos	✓	✓
	ANTES QUE SEJA EXECUTADO NOS DISPOSITIVOS	Detecção de malware com Deep Learning	✓	
		Varredura de arquivo por anti-malware	✓	✓
		Proteção em tempo real	✓	✓
		Análise de comportamento de pré-execução (HIPS)	✓	
		Bloqueio de aplicativo potencialmente indesejado (PUA)	✓	✓
		Sistema de Prevenção de Invasão (IPS)	✓	
	DETENÇÃO DA EXECUÇÃO DE AMEAÇAS	Prevenção contra a perda de dados	✓	
		Análise de comportamento de tempo de execução (HIPS)	✓	
		Antimalware Scan Interface (AMSI)	✓	
		Detecção de tráfego malicioso (MTD)	✓	✓
		Prevenção contra exploração (detalhes na página 5)	✓	
		Mitigações contra usuários ativos (detalhes na página 5)	✓	
		Proteção de arquivos contra ransomware (CryptoGuard)	✓	✓
		Proteção a registro de inicialização e disco (WipeGuard)	✓	
		Proteção contra Man-in-the-Browser (Safe Browsing)	✓	
		Bloqueio de aplicativos aprimorado	✓	

Recursos continuam na próxima página

Visão Geral do Intercept X, XDR e MTR

SOPHOS
Cybersecurity evolved.

Comparação de sistemas operacionais (continuação)

		PONTOS DE DESTAQUE	WINDOWS	macOS
DETECTE E INVESTIGE	DETECTE	Live Discover (consulta SQL patrimonial para caça a ameaças e higiene das operações de segurança de TI)	✓	✓
		Biblioteca de Consultas SQL (consultas pré-gravadas e totalmente personalizáveis)	✓	✓
		Acesso rápido, armazenamento de dados em disco (até 90 dias)	✓	✓
		Fontes de dados entre produtos, por exemplo, Firewall, Email	✓	Em breve
		Consulta entre produtos	✓	Em breve
		Sophos Data Lake (armazenamento de dados na nuvem)	✓	Em breve
		Consultas agendadas	✓	Em breve
	INVESTIGUE	Casos de ameaças (análise da causa raiz)	✓	✓
		Análise de malware com Deep Learning	✓	
		SophosLabs Threat Intelligence por demanda avançado	✓	
		Exportação de dados forenses	✓	
RESPONDA	CORRIJA	Remoção automatizada de malware	✓	✓
		Security Heartbeat sincronizado	✓	✓
		Sophos Clean	✓	
		Live Response (Acesso a terminal remoto para investigação aprofundada e resposta)	✓	✓
		Isolamento de endpoint por demanda	✓	
		Comando de um clique "Eliminar e Bloquear"	✓	✓
SERVIÇO GERENCIADO	CAÇA A AMEAÇAS E RESPOSTA CONDUZIDAS POR HUMANOS	Caça de ameaças conduzida por indícios 24/7	✓	✓
		Verificações de integridade da segurança	✓	✓
		Retenção de dados	✓	✓
		Relatório de atividades	✓	✓
		Detecções adversas	✓	✓
		Neutralização e correção de ameaças	✓	✓
		Caça de ameaças conduzida sem indícios 24/7	✓	✓
		Resposta a ameaças conduzida pela equipe	✓	✓
		Chamada direta para assistência	✓	✓
		Gerenciamento proativo de postura de segurança	✓	✓

Recursos do Sophos Intercept X

SOPHOS
Cybersecurity evolved.

Detalhes dos recursos incluídos com Intercept X

	Pontos de destaque	
PREVENÇÃO CONTRA EXPLORAÇÃO	Prevenção de execução de dados imposta	✓
	Aleatoriedade de layout de espaço de endereço compulsória	✓
	ASLR ascendente	✓
	Página nula (Proteção de deferência nula)	✓
	Alocação de heap spray	✓
	Heap spray dinâmico	✓
	Pivô de pilha	✓
	Executável de pilha (MemProt)	✓
	Mitigações ROP com base em pilhas (Chamador)	✓
	Mitigações ROP com base em ramificações (Assistido por hardware)	✓
	Substituição por manipulador de exceção estruturado (SEHOP)	✓
	Filtragem na importação da tabela de endereços (IAF)	✓
	Biblioteca de carga	✓
	Injeção DLL refletiva	✓
	Shellcode	✓
	VBScript God Mode	✓
	Wow64	✓
	Syscall	✓
	Hollow Process	✓
	Sequestro de DLL	✓
	Squiblydoo Applocker Bypass	✓
	Proteção APC (Double Pulsar / AtomBombing)	✓
	Escalonamento de privilégio de processamento	✓
	Proteção dinâmica de shellcode	✓
	EFS Guard	✓
	CTF Guard	✓
	ApiSetGuard	✓
MITIGAÇÕES DE ADVERSÁRIO ATIVO	Proteção contra roubo de credenciais	✓
	Mitigação de Code Cave	✓
	Proteção contra Man-in-the-Browser (Safe Browsing)	✓
	Detecção de tráfego mal-intencionado	✓
	Detecção de shell em Meterpreter	✓

	Pontos de destaque	
ANTI-RANSOMWARE	Proteção de arquivos contra ransomware (CryptoGuard)	✓
	Recuperação automática de arquivo (CryptoGuard)	✓
	Proteção a registro de inicialização e disco (WipeGuard)	✓
BLOQUEIO DE APLICATIVOS	Navegadores da Web (incluindo HTA)	✓
	Plug-ins de navegadores da Web	✓
	Java	✓
	Aplicativos de mídia	✓
	Aplicativos de escritório	✓
PROTEÇÃO COM DEEP LEARNING	Detecção de malware com Deep Learning	✓
	Bloqueio de aplicativo potencialmente indesejado (PUA) com Deep Learning	✓
	Supressão de falso-positivo	✓
RESPONDA INVESTIGUE REMOVA	Casos de ameaças (análise da causa raiz)	✓
	Sophos Clean	✓
	Security Heartbeat sincronizado	✓

Managed Threat Response (MTR)

SOPHOS
Cybersecurity evolved.

O Sophos Managed Threat Response oferece busca, detecção e resposta a ameaças 24 horas, fornecidas por uma equipe de especialistas como um serviço totalmente gerenciado. Clientes MTR também recebem o Intercept X Advanced with XDR.

Sophos MTR: Standard

Caça de ameaças conduzida por indícios 24/7

Atividades ou artefatos maliciosos confirmados (sinais fortes) são bloqueados ou encerrados automaticamente, liberando os peritos para sair na captura de ameaças. Esse tipo de busca de ameaças envolve agregar e investigar eventos causadores e adjacentes (sinais fracos) para descobrir novos Indicadores de Ataque (IoA) e Indicadores de Comprometimento (IoC) que possam ter sido detectados anteriormente.

Verificação de integridade da segurança

Mantenha os seus produtos Sophos Central – a começar pelo Intercept X Advanced for with XDR – operando com capacidade máxima, com exames proativos de suas condições operacionais e melhorias recomendadas à sua configuração.

Relatório de atividades

Um resumo das atividades de casos permite priorizar e comunicar, de modo que a sua equipe saiba quais ameaças foram detectadas e quais ações foram adotadas dentro de cada período de registro.

Detecções adversas

Os ataques mais bem-sucedidos contam com a execução de um processo que pode parecer legítimo para as ferramentas de monitoramento. Utilizando técnicas de investigação proprietárias, nossa equipe determina a diferença entre um comportamento legítimo e as táticas, técnicas e procedimentos (TTPs) usados pelos invasores.

Sophos MTR: Advanced *Inclui todos os recursos da versão Standard, mais:*

Caça de ameaças conduzida sem chumbo 24/7

Com a aplicação de dados científicos, inteligência de ameaças e muita intuição gerada por experts em captura, combinamos o perfil da sua empresa, informações de importância e usuários de alto risco para antecipar o comportamento do invasor e identificar novos Indicadores de Ataque (IoA).

Telemetria aprimorada

As investigações de ameaças são complementadas com a telemetria de outros produtos Sophos Central que se estendem além do endpoint para montar o cenário completo das atividades adversas.

Melhoria proativa da postura

Melhore de forma proativa a sua postura de segurança e fortaleça as suas defesas seguindo uma orientação prescritiva para lidar com vulnerabilidades de configuração e arquitetura que diminuem as suas funcionalidades gerais de segurança.

Liderança dedicada à resposta a ameaças

Quando um incidente é confirmado, um líder de resposta a ameaças é indicado para colaborar diretamente com os seus recursos locais (pessoal interno ou parceiro externo) até que a ameaça ativa seja neutralizada.

Chamada direta para assistência

Seu pessoal tem acesso direto ao nosso Centro de Operações de Segurança (SOC). Nossa equipe de operações de MTR está disponível initerruptamente, e recebe o apoio de equipes espalhadas em 26 localidades mundo afora.

Descoberta de patrimônio

De informações patrimoniais sobre versões de SO, aplicativos e vulnerabilidades à identificação de patrimônios gerenciados e não gerenciados, fornecemos valiosos insights durante avaliações de impacto, captura de ameaças e como parte das recomendações proativas de melhoria da postura.