Guia de Licenças do Sophos Workload Protection

SOPHOS
Cybersecurity delivered.

Visão geral do Intercept X for Server, XDR, Cloud Native Security e MTR

Gerenciado pelo Sophos Central

Pontos de destaque	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Gerenciamento						
Políticas múltiplas		✓	✓	✓	✓	✓
Atualizações controladas		✓	✓	✓	✓	✓
Redução da superfície de ataque						
Controle de Aplicativos		✓	✓	✓	✓	✓
Controle de periféricos		✓	✓	✓	✓	✓
Controle da Web / Bloqueio de URL por categoria		✓	✓	✓	✓	✓
Aplicativos em lista branca (Bloqueio de Servidor)		✓	✓	✓	✓	✓
Reputação de download	✓	✓	✓	✓	✓	✓
Serviço de segurança	✓	✓	✓	✓	✓	✓
Antes que seja executado no dispositivo						
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, Potentially Unwanted Application)	✓	✓	✓	✓	✓	✓
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)	✓	✓	✓	✓	✓	✓

Pontos de destaque	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
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	✓	✓	✓	✓	✓	✓
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			✓	✓	✓	✓
Lista priorizada de detecções			✓	✓	✓	✓
Sophos Data Lake (armazenamento de dados na nuvem)			30 dias	30 dias	30 dias	30 dias
Consultas agendadas			✓	✓	✓	✓
Detecções e visibilidade do contêiner em tempo de execução			✓	✓	✓	✓
Investigue						
Casos de ameaças (análise da causa raiz)		✓	✓	✓	✓	✓
Análise de malware com Deep Learning			✓	✓	✓	✓
SophosLabs Threat Intelligence por demanda avançado			✓	✓	✓	✓
Exportação de dados forenses			✓	✓	✓	✓
Investigações guiadas por IA			✓	✓	✓	✓

Pontos de destaque	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Remediação						
Remoção automatizada de malware	✓	✓	✓	✓	✓	✓
Security Heartbeat sincronizado	✓	✓	✓	✓	✓	✓
Sophos Clean	✓	✓	✓	✓	✓	✓
Live Response (Acesso a terminal remoto para investigação aprofundada e resposta)			✓	✓	✓	✓
Isolamento de servidor por demanda			✓	✓	✓	✓
Comando de um clique "Eliminar e Bloquear"			✓	✓	✓	✓
Detecções e visibilidade do contêiner em tempo de execução			✓	✓	✓	✓
Controle						
Controle Sincronizado de Aplicativos (visibilidade de aplicativos)	✓	✓	✓	✓	✓	✓
Cache de Atualização e Retransmissor de Mensagem	✓	✓	✓	✓	✓	✓
Exclusões Automáticas de Varredura	✓	✓	✓	✓	✓	✓
Monitoramento de Integridade de Arquivos			✓	✓	✓	✓
Ambientes na nuvem						
Monitoramento do ambiente de nuvem: registros AWS, Azure, GCP, Kubernetes, IaC e Docker Hub		Um por provedor	Um por provedor	Ilimitado	Um por provedor	Um por provedor
Monitoramento de segurança (regras de boas práticas CSPM)		Varreduras diárias	Varreduras diárias	Varreduras agendáveis, diárias e sob demanda	Varreduras diárias	Varreduras diárias
Inventário de patrimônio		✓	✓	✓	✓	✓
Recursos de pesquisa avançada		✓	✓	✓	✓	✓
Detecção de anomalias por IA		✓	✓	✓	✓	✓
Alertas de tráfego mal-intencionado do SophosLabs Intelix		✓	✓	✓	✓	✓
E-mails de alerta		✓	✓	✓	✓	✓
Integrações de serviços nativos AWS (Amazon GuardDuty, AWS Security Hub, Amazon Inspector etc.)		✓	✓	✓	✓	✓
Integrações de serviços nativos Azure (Azure Sentinel e Advisor)		✓	✓	✓	✓	✓
Proteção de carga de trabalho na nuvem: Agente de descoberta do Sophos Intercept X Server		✓	✓	✓	✓	✓

Pontos de destaque	Intercept X Essentials for Server	Intercept X Advanced for Server	Intercept X Advanced for Server with XDR	Cloud Native Security	Intercept X Advanced for Server with MTR Standard	Intercept X Advanced for Server with MTR Advanced
Proteção de carga de trabalho na nuvem: Remoção automática do agente do Sophos Intercept X Server		✓	✓	✓	✓	✓
Relatórios e políticas de conformidade		CIS Benchmarks	CIS Benchmarks	CIS Benchmarks, ISO 27001, EBU R 143, FEDRAMP FIEC, GDPR, HIPAA, PCI DSS, SOC2, Práticas recomendadas da Sophos	CIS Benchmarks	CIS Benchmarks
Políticas personalizadas				✓		
Visualização de rede		✓	✓	✓	✓	✓
Visualização de IAM		✓	✓	✓	✓	✓
Monitoramento de gastos		✓	✓	✓	✓	✓
Integrações de gerenciamento de alertas (Jira, ServiceNow, Slack, Teams, PagerDuty, Amazon SNS)		✓	✓	✓	✓	✓
Integrações SIEM (Splunk, Azure Sentinel)		✓	✓	✓	✓	✓
API Rest		✓	✓	✓	✓	✓
Varredura de modelo de Infraestrutura como Código		✓	✓	✓	✓	✓
Controle de acesso ao ambiente		✓	✓	✓	✓	✓
Varredura de imagem do contêiner (ECR, ACR, Docker Hub, API)		✓	✓	✓	✓	✓
Serviço gerenciado						
Caça de ameaças conduzida por chumbo 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						✓
Proteção de arquivos contra ransomware (CryptoGuard)						✓

Comparação de recursos e sistemas operacionais

Pontos de destaque	Windows	Linux*
Gerenciamento		
Políticas múltiplas	✓	✓
Atualizações controladas	✓	✓
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	✓	
Aplicativos em lista branca (Bloqueio de Servidor)	✓	
Antes que seja executado no dispositivo		
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, Potentially Unwanted Application)	✓	
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)	✓	Veja a nota
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	✓	

Pontos de destaque	Windows	Linux*
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	✓	✓
Lista priorizada de detecções	✓	✓
Sophos Data Lake (armazenamento de dados na nuvem)	✓	✓
Consultas agendadas	✓	✓
Detecções e visibilidade do contêiner em tempo de execução		✓
Investigue		
Casos de ameaças (análise da causa raiz)	✓	
Análise de malware com Deep Learning	✓	
SophosLabs Threat Intelligence por demanda avançado	✓	
Exportação de dados forenses	✓	
Investigações guiadas por IA	✓	✓
Remediação		
Remoção automatizada de malware	✓	
Security Heartbeat sincronizado	✓	Veja a nota
Sophos Clean	✓	
Live Response (Acesso a terminal remoto para investigação aprofundada e resposta)	✓	✓
Isolamento de servidor por demanda	✓	
Comando de um clique “Eliminar e Bloquear”	✓	
Controle		
Controle Sincronizado de Aplicativos (visibilidade de aplicativos)	✓	
Cache de Atualização e Retransmissor de Mensagem	✓	
Exclusões Automáticas de Varredura	✓	
Monitoramento de Integridade de Arquivos	✓	

Pontos de destaque	Windows	Linux*
Serviço gerenciado		
Caça de ameaças conduzida por chumbo 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	✓	✓
Melhoria proativa de postura de segurança	✓	✓

*Linux inclui duas opções de implantação. 1) A implantação do Sophos Protection para Linux dá acesso aos recursos marcados na tabela. 2) A implantação do Sophos Anti-Virus para Linux, que inclui: Anti-malware, Proteção em tempo real, Detecção de tráfego mal-intencionado e Segurança sincronizada. Observe que as duas opções de implantação não podem ser usadas juntas.

Visão geral do Sophos Protection

Detalhes dos recursos de proteção de carga de trabalho incluídos com o Intercept X e Cloud Native Security

Pontos de destaque	
Exploit Prevention	
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	✓

Pontos de destaque	
CTF Guard	✓
ApiSetGuard	✓
Mitigação de adversários ativos	
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	✓
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 (inclusive 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	✓
Resposta Investigação Remoção	
Casos de ameaças (análise da causa raiz)	✓
Sophos Clean	✓
Security Heartbeat sincronizado	✓

Managed Threat Response (MTR)

O Sophos Managed Threat Response (MTR) oferece 24 horas de busca, detecção e resposta a ameaças, sete dias por semana, ditadas por um time de especialistas nos moldes de um serviço totalmente gerenciado. Clientes MTR também recebem o Intercept X Advanced for Server with XDR.

Sophos MTR: Standard

Caça de ameaças conduzida por chumbo 24/7
Atividades ou artefatos maliciosos confirmados (sinais fortes) são bloqueados ou terminados 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 Server with XDR – operando à sua 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 medidas de ação foram tomadas 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.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

22-07-25 PTBR (DD)

SOPHOS