

Principais controles contra ransomware e como a Sophos pode ajudar

O desafio do ransomware continua a crescer. A proporção de organizações atingidas por ransomwares quase duplicou em 12 meses: de 37% em 2020 para 66% em 2021. Os adversários também estão tendo mais sucesso na criptografia de dados, com 65% de ataques resultando em dados criptografados no último ano*.

Deter os ransomwares exige esforços para prevenir os ataques avançados via teclado praticados por adversários bem-preparados e também o sucesso crescente do modelo Ransomware como Serviço, que amplia significativamente o alcance de um ransomware ao reduzir o nível de aptidão necessário para lançar um ataque.

Este guia detalha os principais controles de segurança cibernética que minimizam a exposição a ransomwares e o seu impacto e como a Sophos pode ajudar.

Principais controles contra ransomware e como a Sophos pode ajudar

CONTROLE CIBERNÉTICO	COMO A SOPHOS PODE AJUDAR	DETALHE
Caça a ameaças proativa para detectar e neutralizar ataques conduzidos por humanos antes que o ransomware seja lançado	Sophos XDR [Extended Detection and Response]	Permite que as organizações conduzam a caça a ameaças e a neutralização em todo o seu ambiente. As detecções podem se originar de endpoints, servidores, cargas de trabalho na nuvem, firewalls, e-mails, ambientes de nuvem pública, aparelhos móveis, Microsoft 365 e outros mais.
	Sophos MTR [Managed Threat Response]	Busca, detecção e resposta a ameaças, 24 horas por dia, sete dias por semana, 365 dias por ano, ditadas por um time de especialistas da Sophos como um serviço totalmente gerenciado. Conectores ligados a diferentes soluções de segurança e TI, incluindo Microsoft 365, estendem a visibilidade de nossos operadores de todo o patrimônio de nossos clientes, aumentando sua habilidade de defesa contra ataques.
Bloqueio automático das ameaças de ransomware antes que possam ser lançadas	Sophos Endpoint e Sophos Workload Protection	Oferece capacidade avançada de proteção contra ransomware que desmantela toda a cadeia de ataque, incluindo: - Inteligência artificial com Deep Learning para evitar ransomwares conhecidos e desconhecidos. - Proteção contra exploit para bloquear as explorações de vulnerabilidades e as técnicas usadas para distribuir malwares, roubar credenciais e fugir da detecção. - Controle de aplicativos para impedir que aplicativos sejam executados nas cargas de trabalho na nuvem que poderiam ser usados pelos adversários para lançar ataques. - Bloqueio de servidores, que tomam as cargas de trabalho na nuvem em boas condições e bem configuradas e mantém esse estado para impedir a execução de programas não autorizados. - A tecnologia anti-ransomware, que detecta e reverte a criptografia não autorizada, interrompendo o processo antes que possa se espalhar pela sua rede. Protege contra ransomwares baseados em arquivo e registro mestre de inicialização.
	Sophos Email	Analisa automaticamente todos os processos de arquivos, atividades com arquivos, atividades de registro e conexões de rede para bloquear ransomwares e outras formas de malware. Proteção avançada contra phishing, varredura de URL e proteção pós-entrega asseguram que apenas remetentes confiáveis cheguem até a sua caixa de entrada, e se o estado de ameaça das mensagens entregues mudar, elas são removidas automaticamente.
	Sophos Firewall	Protege contra sites comprometidos e downloads maliciosos com o uso extensivo de Machine Learning e inspeção de sandbox no download de arquivos para identificar ataques novos de ransomware, porém nunca antes vistos.

Principais controles contra ransomware e como a Sophos pode ajudar

CONTROLE CIBERNÉTICO	COMO A SOPHOS PODE AJUDAR	DETALHE
Identificar e eliminar as lacunas na segurança para reforçar o seu ambiente, como, por exemplo, dispositivos sem patches, máquinas sem proteção e muito mais.	Sophos XDR [Extended Detection and Response]	Identifica softwares e sistemas desatualizados e sem suporte. Oferece acesso a todos os aplicativos no dispositivo, informações de versão, hashes de arquivo SHA256, informações de patch e logs, incluindo o histórico de execução do aplicativo, conexões de rede, processos matriz/secundário etc. Inclui consultas para verificar os aplicativos instalados em relação a informações de vulnerabilidade online e consultas para identificar as deficiências de postura nas configurações de registro.
	ZTNA da Sophos	Habilita o acesso remoto seguro e granular a sistemas e aplicativos, eliminando a superfície de ataque e o potencial para ataques se moverem lateralmente.
Bloqueio do Remote Desktop Protocol para impedir que os adversários o utilizem para obter acesso	Sophos Firewall	Capacita a sua equipe de TI para gerenciar e bloquear facilmente o RDP.
	ZTNA da Sophos	Permite o acesso remoto seguro ao RDP e a outros aplicativos sem expor esses sistemas ao ataque.
	Sophos Cloud Optix	Identifica proativamente portas RDP expostas através de avaliações de benchmark de segurança na nuvem pública. A correção guiada orienta os administradores sobre como tratar as configurações incorretas da segurança.
	Sophos XDR [Extended Detection and Response]	Detecta conexões RDP e logs de atividade. O terminal remoto permite que os administradores ativem/desativem a política de RDP. Oferece visibilidade da política de RDP em todos os dispositivos gerenciados e detecta alterações a ela.
Planejamento de resposta a incidentes cibernéticos para minimizar o impacto no caso de acontecer um ataque	Sophos Rapid Response	Oferece resposta imediata a incidentes 24/7, entregue por especialistas da Sophos.
	Sophos MTR [Managed Threat Response]	Oferece busca, detecção e resposta a ameaças, 24 horas por dia, sete dias por semana, ditadas por um time de especialistas como um serviço totalmente gerenciado.
Treinamento de conscientização em segurança cibernética e testes de phishing	Sophos Phish Threat	Melhora a conscientização em segurança e educa os seus usuários através de simulações de ataques de phishing, treinamento e conscientização em segurança automatizada, e relatórios abrangentes. A integração com o Sophos Email permite que as equipes de segurança identifiquem eficientemente e rastreiem com rapidez o treinamento dos usuários que foram alertados ou impedidos de acessar um site devido a seu perfil de risco.

Principais controles contra ransomware e como a Sophos pode ajudar

CONTROLE CIBERNÉTICO	COMO A SOPHOS PODE AJUDAR	DETALHE
Identificação e mitigação de vulnerabilidades nos ambientes em nuvem para prevenir a exploração pelos adversários	Sophos Cloud Optix	Identifica e mitiga de forma proativa as vulnerabilidades de segurança, funções do IAM com excesso de privilégios e erros de configuração de acesso à rede em ambientes de nuvem pública com integração ao Amazon Inspector, incluindo portas de máquinas virtuais expostas à internet, login de root remoto ativado ou versões de software vulneráveis instaladas. Recebe o status de patch das máquinas virtuais da Amazon com integração ao AWS Systems Manager. Amplia as varreduras de segurança aos pipelines CI/CD com Infraestrutura como Código fazendo a varredura enquanto analisa registros de contêineres em busca de vulnerabilidades de SO no Azure, AWS e Docker Hub.

Para estabelecer a sua resiliência cibernética e como a Sophos pode ajudar a fortalecer as suas defesas contra ransomwares, [fale com um representante da Sophos](#).

** O Estado do Ransomware 2022, Sophos. Pesquisa com 5.600 profissionais de TI em 31 países*

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.