

Integração Sophos com Veeam

Interrompa ameaças direcionadas a dados de backup críticos

Os agentes de ameaças foram capazes de afetar os repositórios de backup em 75% dos ataques de ransomware¹ no decorrer do último ano, manipulando backups e apagando dados para impedir a recuperação. A Sophos e a Veeam simplificam a resiliência cibernética através da troca descomplicada de informações de segurança quando surge uma ameaça aos seus dados de backup, estendendo a visibilidade para auxiliar na detecção, investigação e resposta a ataques ativos.

Casos de uso

1 | DEFESA CONTRA RANSOMWARE

Resultado desejado: obter a melhor proteção contra ataques de ransomware.

Solução: a Sophos oferece tecnologia líder do setor que detecta e interrompe ransomwares antes que impactem seus sistemas, incluindo ataques de novas variantes e criptografia local e remota. Recursos avançados de detecção e prevenção da Sophos, combinados com backups e controle de versão imutáveis fornecidos pela Veeam, asseguram que seus dados de backup permaneçam seguros e recuperáveis.

2 | VISIBILIDADE DE AMEAÇAS ESTENDIDA

Resultado desejado: identificar ameaças potenciais que poderiam afetar seus dados de backup.

Solução: A integração da Sophos com a Veeam está disponível para o serviço Sophos MDR (Managed Detection and Response) e a solução Sophos XDR (Extended Detection and Response). Ela oferece visibilidade das atividades maliciosas que afetam seus backups, incluindo tentativas de apagar repositórios de backup, desabilitar a autenticação multifator, alterar senhas de criptografia e mais.

3 | ASSEGURAR INTEGRIDADE E DISPONIBILIDADE DE BACKUP

Resultado desejado: tranquilidade de saber que seus dados de backup estão disponíveis e protegidos.

Solução: nossa integração poderosa permite que você detecte ameaças, investigue atividades suspeitas e recupere dados rapidamente para manter seus negócios em operação. com a Sophos e a Veeam, você pode assegurar a integridade e a disponibilidade dos seus backups, reduzindo o risco da perda de dados devida a malwares, remoções acidentais, ameaças à segurança interna e outros cenários de perda de dados.

4 | MELHORAR O TEMPO DE RESPOSTA A AMEAÇAS

Resultado desejado: minimizar o tempo de inatividade e garantir a continuidade dos negócios.

Solução: o Sophos MDR é um serviço 24/7 de prevenção, detecção e resposta conduzido por humanos e que defende as organizações contra os ataques mais avançados. Os especialistas da Sophos saem no encalço de ameaças para identificar as técnicas de ataque que tentam burlar as ferramentas de prevenção e executar ações de resposta para interromper ameaças confirmadas em 38 minutos — o melhor tempo médio de resposta do mercado e 96% mais rápido do que a referência do setor.



"Customers' Choice" da Gartner em Serviços Gerenciados de Detecção e Resposta



Líder no Magic Quadrant de 2023 em Plataformas de Proteção de Endpoints em 14 relatórios consecutivos



Fornecedor de alto desempenho na Avaliação MITRE ATT&CK em Serviços Gerenciados de Segurança

Saiba mais:

www.sophos.com/mdr

www.sophos.com/xdr

¹ Veeam 2023 Ransomware Trends Report

© Copyright 2024. Sophos Ltd. Todos os direitos reservados. Registrada na Inglaterra e País de Gales sob o n.º. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido. Sophos é marca registrada da Sophos Ltd. Todos os outros nomes de produtos e empresas mencionados são marcas comerciais ou marcas registradas de seus respectivos proprietários.

O logotipo Gartner Peer Insights é marca comercial e marca de serviço da Gartner, Inc. e/ou de suas afiliadas, usado aqui sob permissão. Todos os direitos reservados. O conteúdo da Gartner Peer Insights consiste em opiniões de usuários finais individuais baseadas em suas próprias experiências com fornecedores listados na plataforma e não deve ser interpretado como uma declaração de fato nem como representação da visão da Gartner ou de suas afiliadas. A Gartner não endossa fornecedores, produtos ou serviços representados neste conteúdo nem estabelece qualquer garantia, expressa ou implícita, em respeito a este conteúdo, sua precisão ou completude, incluindo garantias de comercialização ou de um propósito de uso específico.