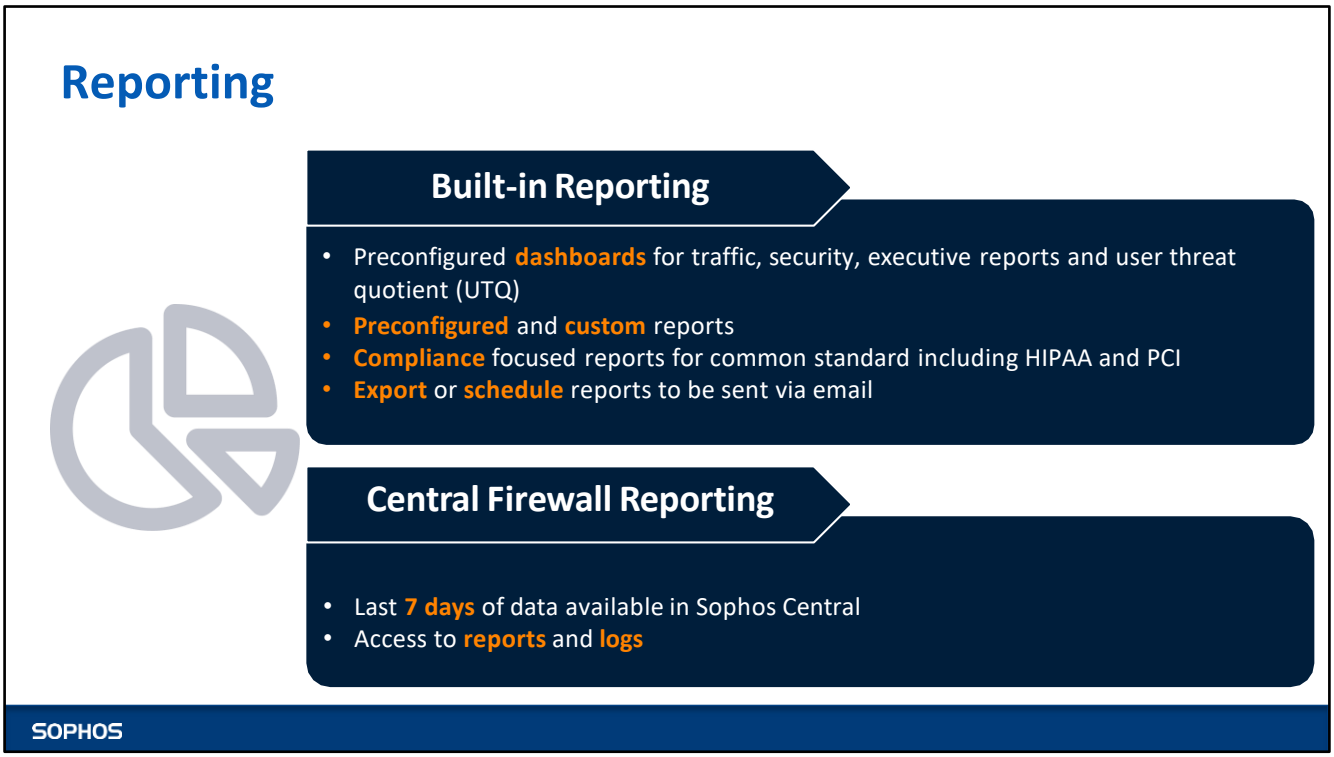
SOPHOS

Running and Customizing Reports on Sophos Firewall

Sophos Firewall
Version: 19.0v1

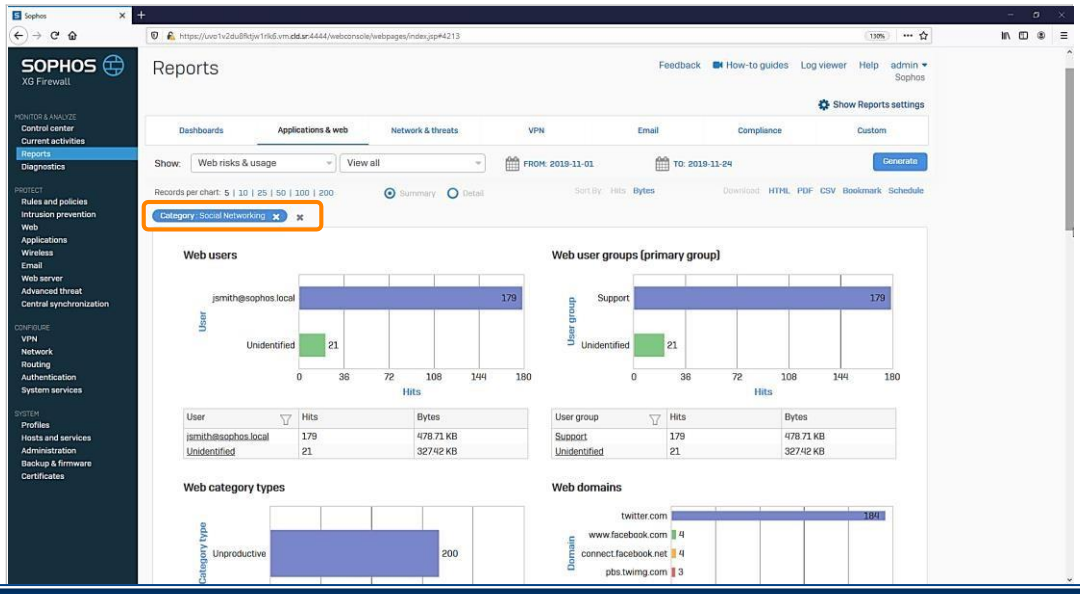


O Sophos Firewall possui relatórios integrados, que fornecem uma visão abrangente do que está acontecendo em sua rede. Existem painéis e relatórios pré-configurados que você pode refinar e detalhar para obter as informações exatas que está procurando. Os relatórios também podem ser exportados ou agendados para serem enviados por e-mail.

Além dos relatórios integrados, o Sophos Firewall pode enviar dados de relatório e log para o Sophos Central.

Observe que os relatórios não estão disponíveis nos modelos XG86 e XG86w.

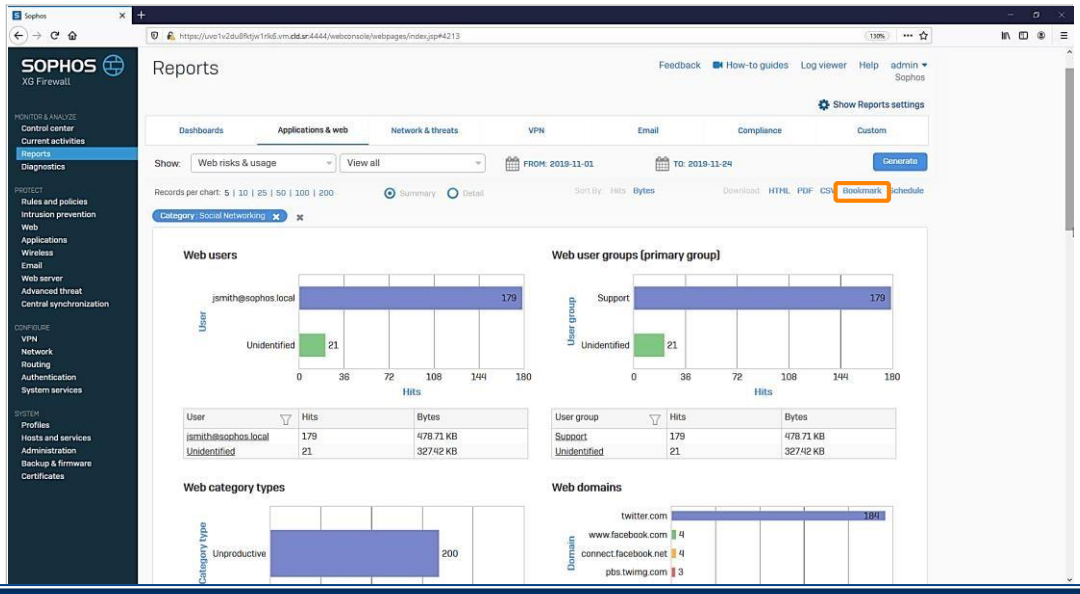
Reports



SOPHOS

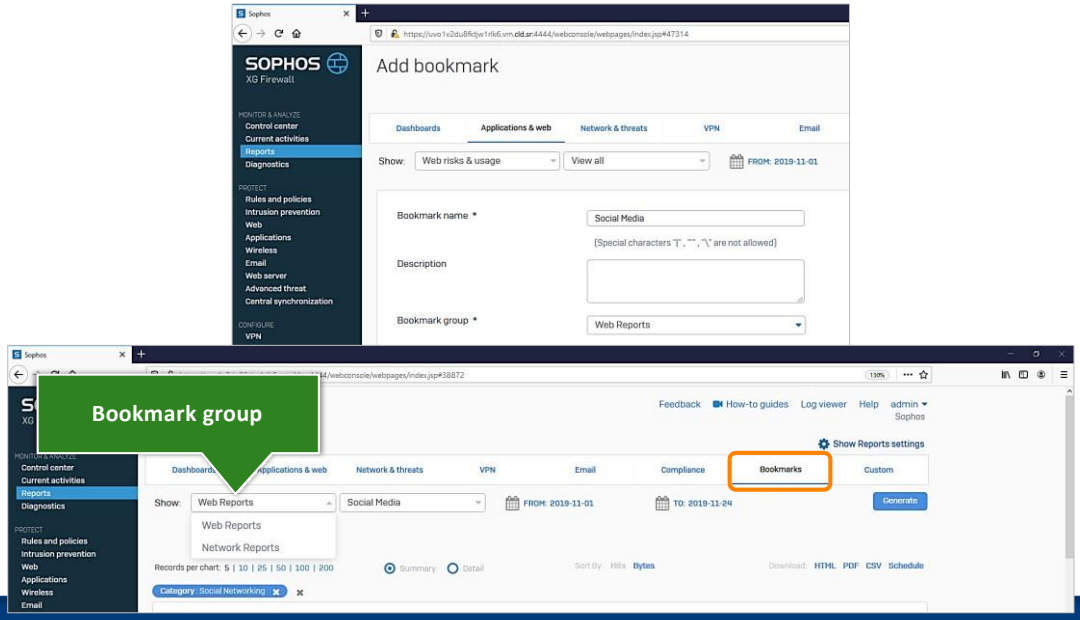
Aqui você pode ver um relatório de exemplo que tem um filtro aplicado. Os filtros podem ser rapidamente adicionados por clicando nos campos dos gráficos e você pode adicionar vários filtros para criar o relatório necessário.

Bookmarks



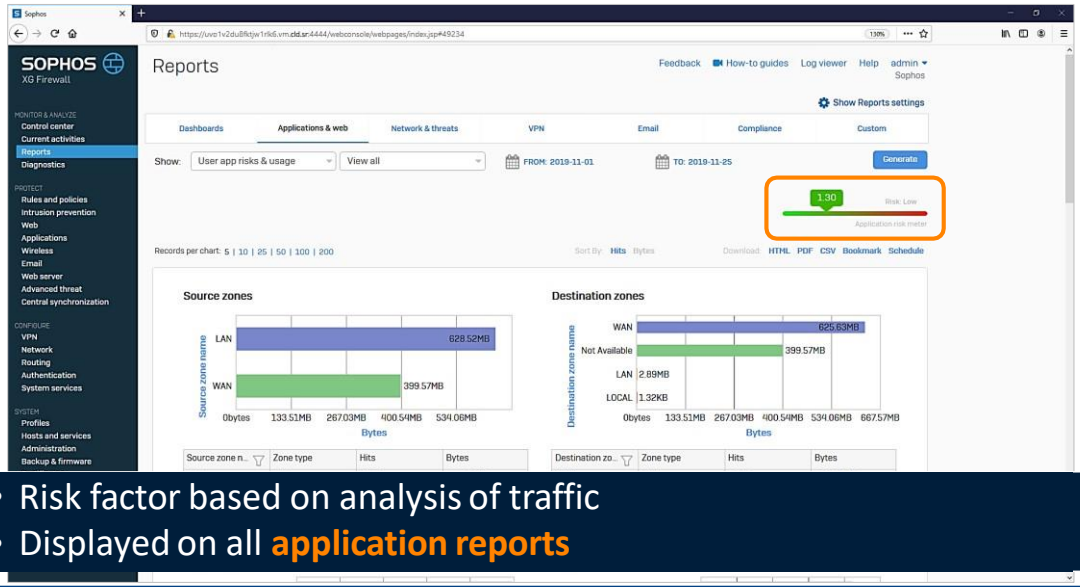
Depois de ter o relatório mostrando os dados desejados, você pode criar um marcador para salvar o para que você possa acessá-lo rapidamente novamente no futuro.

Bookmarks



Ao adicionar o marcador, você pode selecionar um grupo de favoritos; eles são usados para organizar e acessar favoritos. Uma vez que o primeiro marcador tenha sido criado, uma nova guia será criada chamada Favoritos. Ao clicar na guia Favoritos, você pode ver todos os seus relatórios.

Application Risk Meter



- Risk factor based on analysis of traffic
- Displayed on all **application reports**

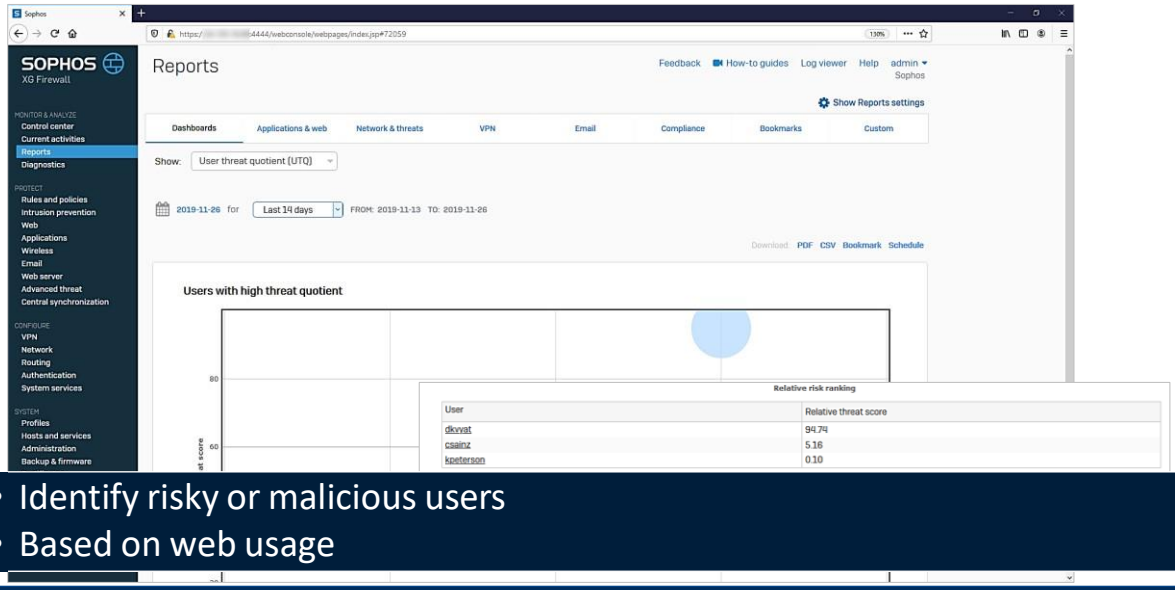
SOPHOS

O Sophos Firewall tem algumas ferramentas de relatórios poderosas para ajudá-lo a identificar aplicativos arriscados e Usuários.

Na guia Aplicativos e relatórios da Web nos relatórios de risco e uso do aplicativo do usuário, você verá o medidor de risco do aplicativo, que fornece uma avaliação de risco com base em uma análise do tráfego que flui pela rede.

A pontuação pode identificar se você precisa reforçar sua segurança ou investigar as ações dos usuários. O medidor de risco varia de 1 sendo de baixo risco e 5 sendo o maior risco.

User Threat Quotient

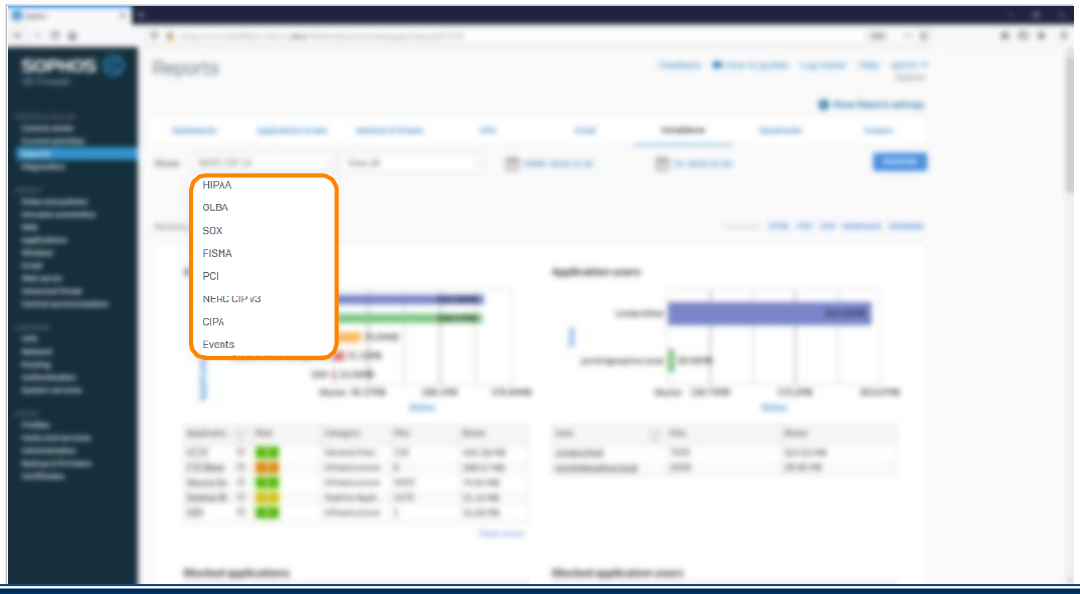


- Identify risky or malicious users
- Based on web usage

SOPHOS

O Sophos Firewall também calcula uma métrica chamada User Threat Quotient (UTQ). A UTQ é baseada nos dados de uso da Web de um usuário e destina-se a ajudá-lo a identificar rapidamente usuários que são arriscados ou mal-intencionados ou que executam ações ingênuas, como responder a tentativas de spear phishing. Isso pode minimizar o esforço necessário para identificar os usuários que precisam ser instruídos sobre como trabalhar com segurança e fornece visibilidade clara dos riscos representados pelos usuários da sua organização.

Compliance Reports



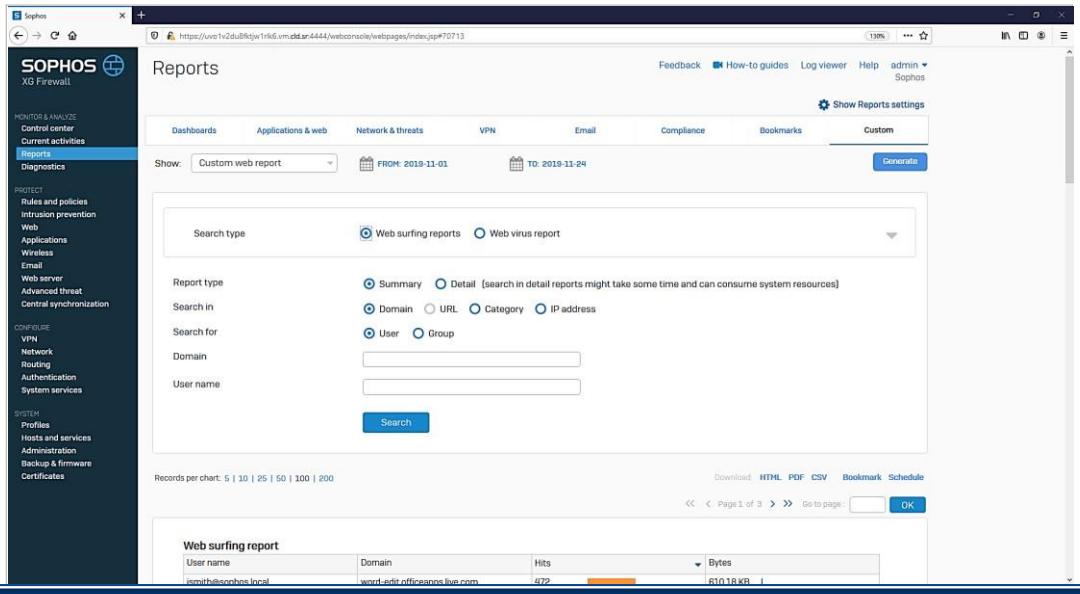
SOPHOS

A conformidade normativa tornou-se uma prioridade para muitas organizações, normalmente exigindo esforço, tempo e custo esmagadores na forma de recuperação e armazenamento de logs e relatórios de vários dispositivos. Correlacionar o grande número de logs e relatórios para concluir o quadro de conformidade é uma tarefa complicada e demorada.

Os relatórios do Sophos Firewall estão prontos para conformidade, facilitando a visualização e o gerenciamento de relatórios baseados em conformidade. Ele fornece relatórios com base em critérios para padrões de conformidade, tais como:

HIPAA (Lei de Portabilidade e Contabilidade de Seguros de Saúde)
GLBA (Lei Gramm-Leach Biley)
SOX (Sarbanes-Oxley)
PCI (Indústria de Cartões de Pagamento)
FISMA (Lei Federal de Gestão de Segurança da Informação)
E vários outros...

Custom Reports

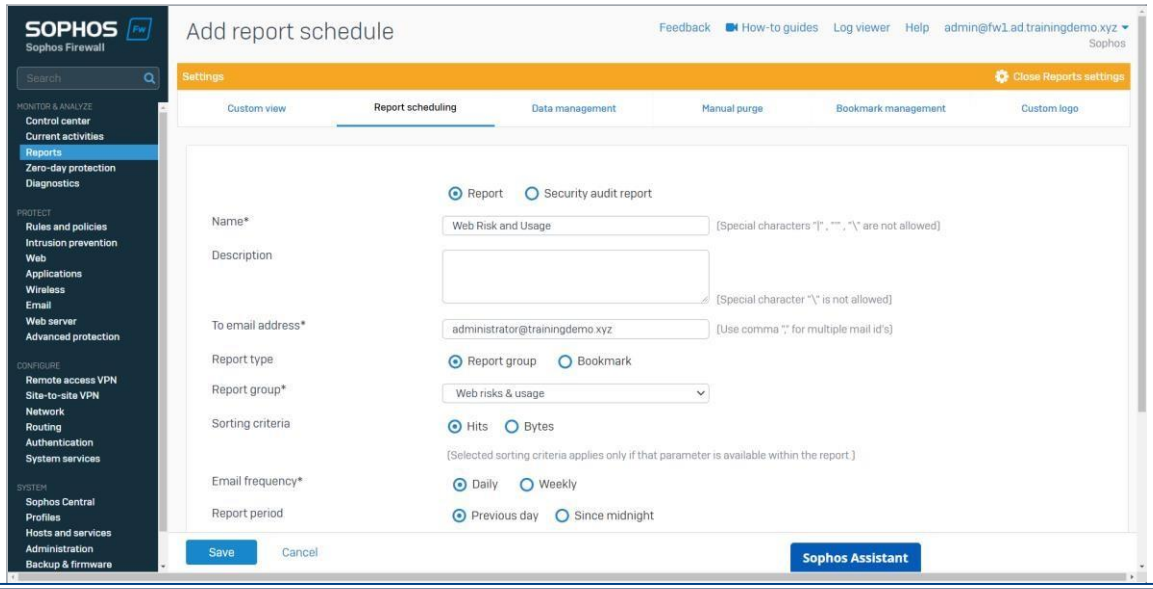


SOPHOS

Na guia Personalizado, você pode configurar relatórios personalizados para web, e-mail, FTP, usuários e servidores web. Dependendo do relatório selecionado, você pode alterar as opções, incluindo o tipo de relatório, os campos a serem pesquisados e os dados específicos a serem pesquisados.

Talvez você queira usar esse controle adicional para investigar melhor as ações de um usuário identificado como arriscado pelo UTQ.

Report Scheduling



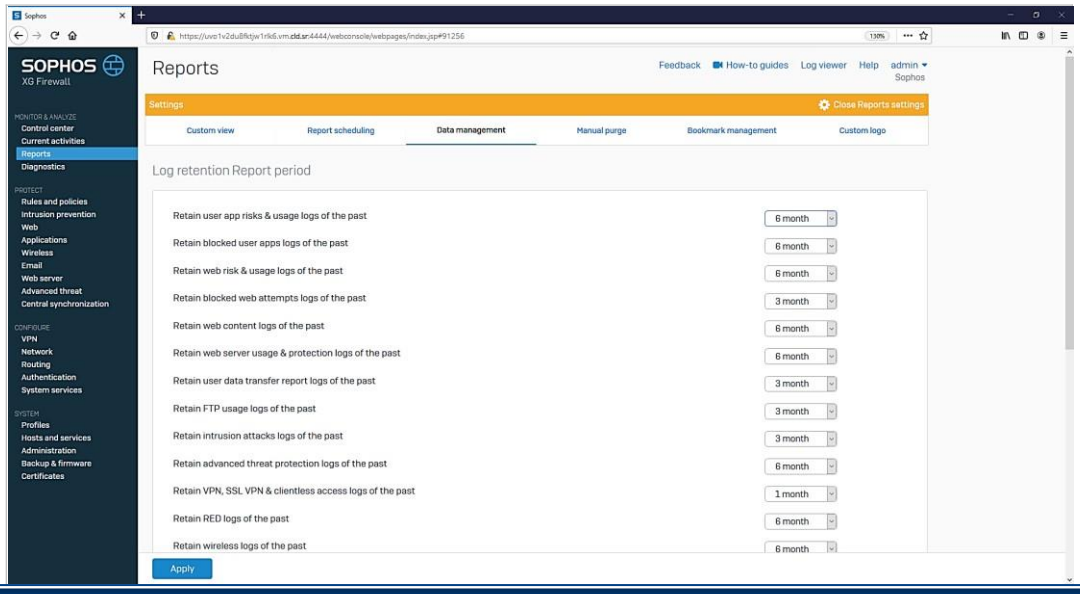
SOPHOS

Na seção de configurações de relatório, você pode controlar várias opções, incluindo agendamento de relatórios, dados retenção e gerenciamento de seus favoritos.

As configurações de relatório são acessadas usando o botão no canto superior direito acima das guias na seção Relatórios. Isso alternará entre configurações de relatório e relatórios.

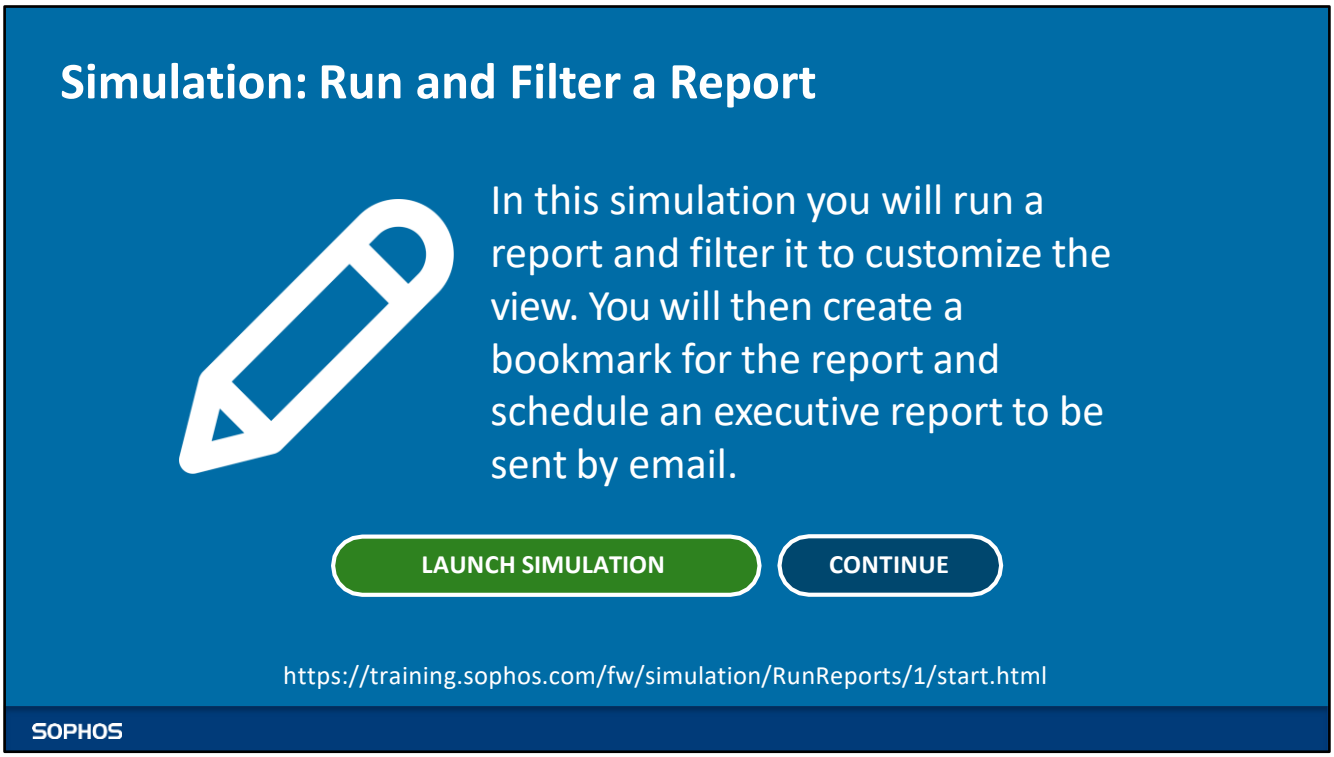
Você pode agendar relatórios a serem enviados por e-mail para qualquer um dos relatórios incluídos ou quaisquer marcadores que você criar. Por favor, note que os relatórios enviados por e-mail conterão um máximo de 50 registros.

Data Management



Com o tempo, o Sophos Firewall armazenará muitos dados, por isso é importante configurar a retenção para permitir que dados antigos sejam limpos.

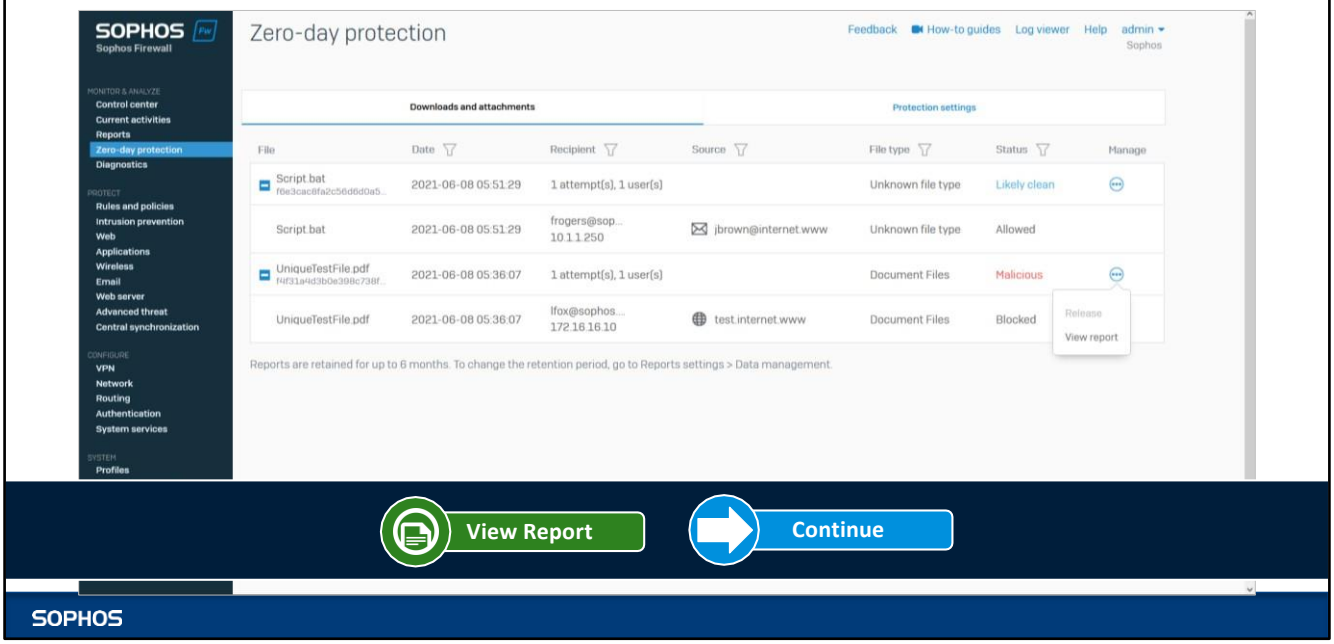
Se o dispositivo estiver com pouco espaço em disco, também é possível executar uma limpeza manual de módulos de relatório específicos ou de todos os módulos de relatório para um período de data específico. Isso é feito em **Reports > Reports settings > Manual purge**.



Nesta simulação, você executará um relatório e o filtrará para personalizar a exibição. Em seguida, você criará um marcar o relatório e agendar um relatório executivo a ser enviado por e-mail.

Zero-Day Protection Reports

Additional information in the notes



Os relatórios de inteligência de ameaças para arquivos que foram encaminhados para proteção de dia zero são acessados De **MONITOR & ANALYZE > Zero-day protection > Downloads and attachments**.

Aqui você pode verificar o status dos arquivos que estão sendo verificados pelo Sandstorm, liberar manualmente um arquivo ou exibir o relatório detalhado.

A atividade de tempestade de areia é agrupada por arquivo. Você pode expandir o arquivo para ver os eventos relacionados a ele, incluindo o usuário e o endereço IP e a origem, que podem ser um site ou e-mail.

Clique no botão para revisar um relatório de exemplo e clique em Continuar quando estiver pronto para continuar.

[Additional Information]
https://training.sophos.com/fw/activity/ThreatReport/1/ThreatReport.html