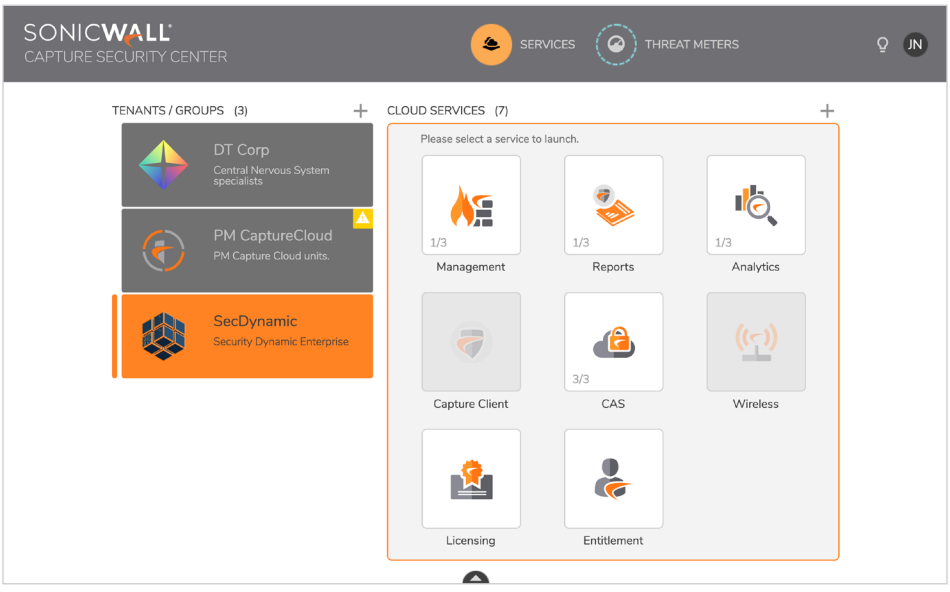
SONICWALL CAPTURE SECURITY CENTER

Análise e gerenciamento unificado através de interface única em nuvem, para segurança de redes, endpoint e nuvem

O SonicWall Capture Security Center é um software de gerenciamento de segurança aberto, escalável e baseado em nuvem, oferecido como uma oferta de serviço com custo reduzido, para organizações e provedores de serviços de vários tamanhos e casos de uso. Oferece o que há de mais novo em visibilidade, agilidade e capacidade para controlar de forma centralizada todo o ecossistema de segurança SonicWall com mais clareza, precisão e velocidade, tudo isso a partir de uma interface de nuvem que pode ser acessada de qualquer local e em qualquer dispositivo ativado para a Web. Essa arquitetura voltada para a nuvem e serviços unifica e conecta os serviços de segurança e as ferramentas de gerenciamento SonicWall para ajudar a obter melhores eficiências e elasticidades operacionais, ao mesmo tempo em que oferece suporte a uma estratégia de defesa cibernética mais ampla.

Guiado por processos de negócios e requisitos de nível de serviço, o Capture Security Center ajuda os Centros de Operações de Segurança (SOCs) a formar a base para uma estratégia unificada de controle de segurança, conformidade e gerenciamento de riscos. Ao estabelecer uma abordagem holística e conectada à orquestração de segurança, o Capture Security Center associa os aspectos operacionais de segurança de rede, endpoint e nuvem por meio de uma estrutura de gerenciamento simples e comum. Isso simplifica e, em muitos casos, automatiza várias tarefas para promover uma melhor coordenação de segurança e tomada de decisão, enquanto reduz a complexidade, o tempo e as despesas da execução de tarefas de operações e administração de segurança. Essas tarefas incluem provisionamento, configuração, monitoramento, relatórios, patches, auditoria e análise de dados e tráfego de firewall e de endpoint, que são inestimáveis para a detecção e resposta a problemas de segurança antes que eles ocorram.



Benefícios:

- Gerenciar de forma centralizada seu ambiente de segurança SonicWall, tudo de um só lugar
- Reduzir silos de segurança com experiência de tela única
- Melhorar as eficiências operacionais com automação do gerenciamento de políticas sem erros
- Facilitar e acelerar o provisionamento de firewalls remotos com Implementação sem intervenção
- Facilitar a criação de relatórios de conformidade para PCI, HIPPA e SOX
- Identificar falhas riscos na segurança usando análise detalhada e precisa
- Responder a riscos rapidamente com informações de ameaças com tempo como fator crucial

O Capture Security Center fornece acesso de login único para licenciar, provisionar e gerenciar todos os seus serviços de segurança de rede, endpoint e de nuvem. Esses serviços incluem a Gestão de Firewalls o Analytics, o Capture Client e o Cloud Application Security. Nossa visão de unificar toda a gama do portfólio de segurança da SonicWall sob uma ferramenta de gerenciamento de simples integração inclui serviços de segurança da Web, wireless, e-mail, móveis e IoT[1]. A combinação desses serviços de nuvem fornece defesa cibernética crítica em camadas, inteligência contra ameaças análise e colaboração e gerenciamento, relatórios e análise comuns que funcionam em sincronia. Com atualizações de software e suporte incluídos em um serviço de assinatura ativo, o acesso a quaisquer inovações e aprimoramentos mais recentes é imediato. Isso ajuda a gerenciar os riscos de segurança, ajuda a cumprir obrigações regulamentares e a se defender contra as mais novas vulnerabilidades e ameaças de maneira automatizada. Com escalabilidade e flexibilidade ilimitadas, o Capture Security Center se adapta prontamente à capacidade e às mudanças de negócio sob demanda.

Gerenciamento de riscos cibernéticos

Integrado ao Capture Security Center encontra-se o SonicWall Risk Meters, uma ferramenta eficiente de gerenciamento de informações e risco de segurança. O Risk Meters fornece dados de ameaças e pontuações de risco personalizados que revelam falhas nas camadas defensivas, promove planejamento de segurança decisivo e facilita ações necessárias para uma defesa cibernética ideal. Isso ajuda a amplificar as defesas de rede, nuvem, Web e endpoint enquanto reduz a superfície de ameaça do ambiente e a suscetibilidade a ataques cibernéticos.

Além disso, o Risk Meters atualiza de forma contínua a pontuação de risco calculada e o nível de ameaça baseados em dados de ameaça em tempo real relativos a recursos de defesa existentes. Essas pontuações lógicas poderão então ser usadas para guiar as decisões de planejamento, política e orçamento de segurança.

Capture Client

O SonicWall Capture Client, uma plataforma client unificada que oferece múltiplos recursos de proteção de endpoint, é acessado dentro do Capture Security Center. Com um mecanismo de proteção contra malware de próxima geração com tecnologia SentinelOne, o Capture Client aplica técnicas avançadas de proteção contra ameaças, como aprendizado de máquina e reversão do sistema. Isso protege contra malware baseado em arquivo e sem arquivo, ao mesmo tempo em que oferece uma visão de ataque de 360 graus com inteligência acionável relevante para investigações.

Combinado com os firewalls SonicWall, o Capture Client também adiciona visibilidade ao tráfego criptografado, por meio do gerenciamento de certificados SSL confiáveis usados para inspeção profunda de pacotes de tráfego SSL/TLS.

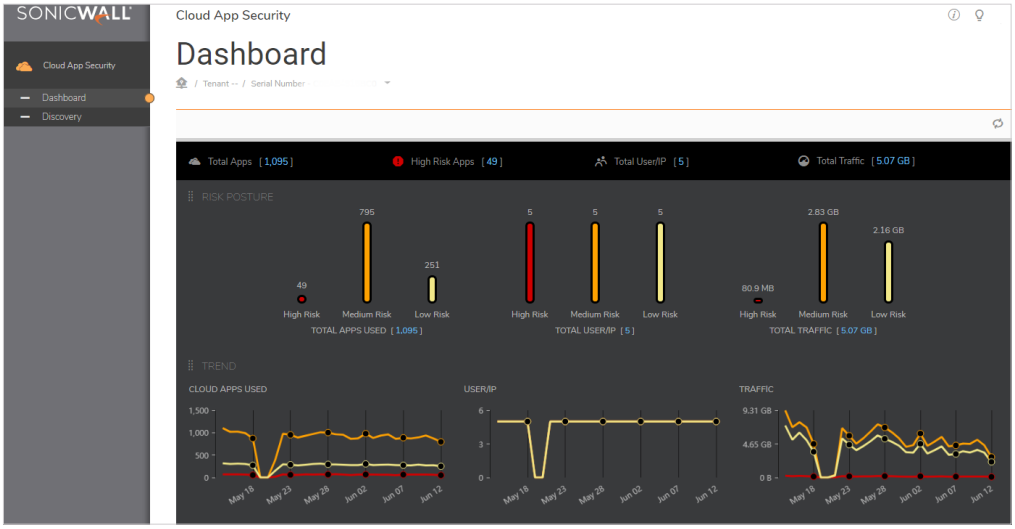
[1] *Os serviços de segurança da Web, wireless, e-mail, móvel e IoT serão totalmente integrados a essa plataforma em anúncios futuros de produtos.*

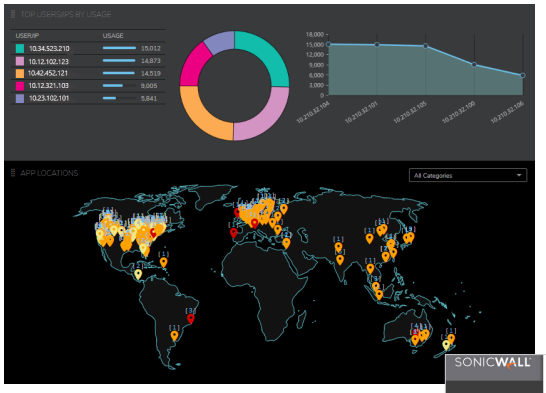
Cloud App Security

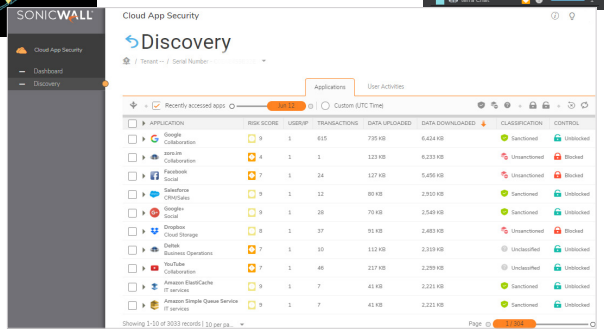
O pacote de assinatura do SonicWall Capture Security Center Analytics capacita os clientes com visibilidade de Shadow IT e controle sobre o uso de aplicações na nuvem. O SonicWall Cloud App Security oferece funcionalidade semelhante a CASB. Ele permite que os administradores descubram o uso de aplicações arriscadas, acompanhem a atividade do usuário e definam políticas de permissão/bloqueio para aplicações de TI sancionadas e não sancionadas em firewalls gerenciados para proteger dados confidenciais.

A descoberta de Shadow IT, a visibilidade em tempo real e a classificação e o controle de aplicações são os principais recursos do serviço Cloud App Security. O serviço garante a adoção segura de aplicações SaaS sem afetar a produtividade dos funcionários e com um baixo custo total de propriedade.

1. **Descoberta de Shadow IT:** utilize arquivos de registro do firewall existentes para automatizar a descoberta de nuvem para identificar as aplicações que estão sendo usadas e sua postura de risco.
2. **Visibilidade da aplicação em tempo real:** monitore o uso em tempo real com uma visualização intuitiva do painel que fornece detalhes das aplicações em uso, volume de tráfego, atividade do usuário e local de uso.
3. **Classificação e controle da aplicação:** classifique as aplicações de nuvem não gerenciadas em Aplicações sancionadas (aprovadas pela TI) ou Aplicações não sancionadas (não aprovadas pela TI) e defina políticas de permissão/bloqueio com base na pontuação de risco da aplicação.





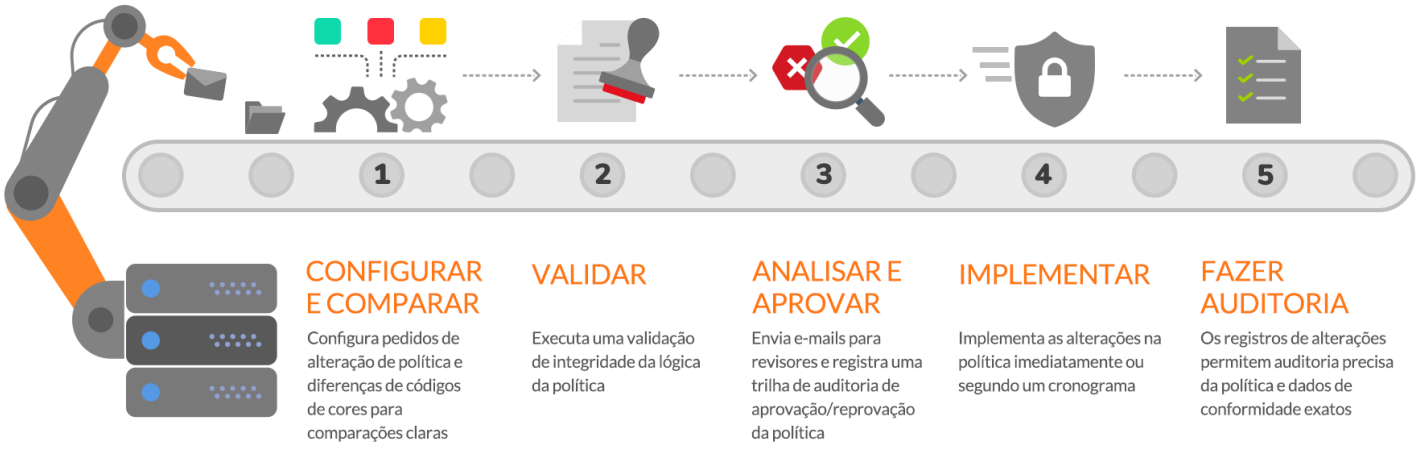


SONICWALL®

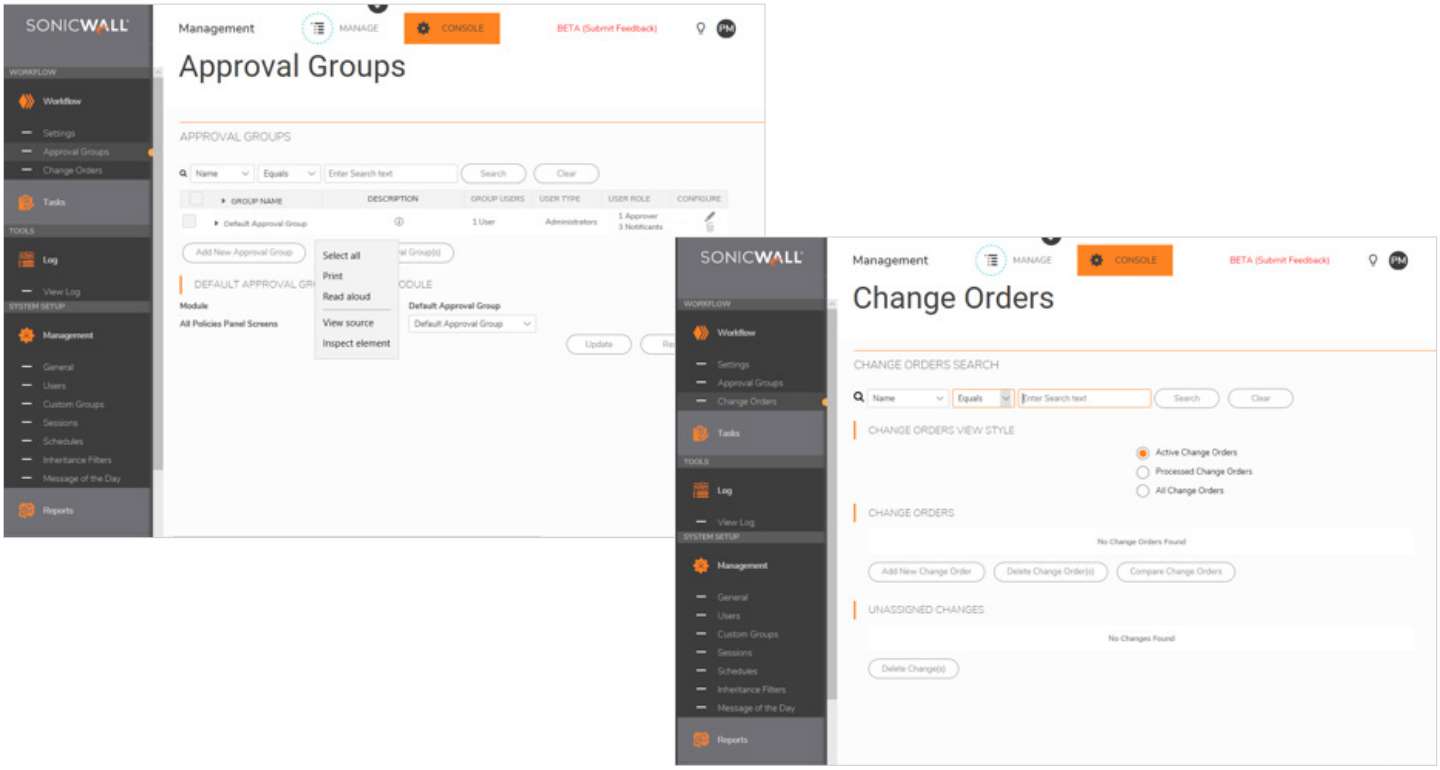
Automação do fluxo de trabalho

Ao empregar a automação do fluxo de trabalho nativo, o Capture Security Center ajuda aos SOCs a atender aos requisitos de auditoria e gerenciamento de mudanças da política de firewall de várias regulamentações, como PCI, HIPPA e GDPR. Ele permite alterações de políticas aplicando uma série de procedimentos rigorosos para configurar, comparar, validar, revisar e aprovar políticas de firewall antes da implementação. Os grupos de aprovação são flexíveis para cumprir diversos procedimentos de autorização e auditoria de diferentes tipos de organizações. A automação do fluxo de trabalho implementa programaticamente políticas de segurança para melhorar a eficiência operacional, reduzir riscos e eliminar erros.

O Capture Security Center fornece uma abordagem holística para controle de segurança, conformidade e gerenciamento de riscos.

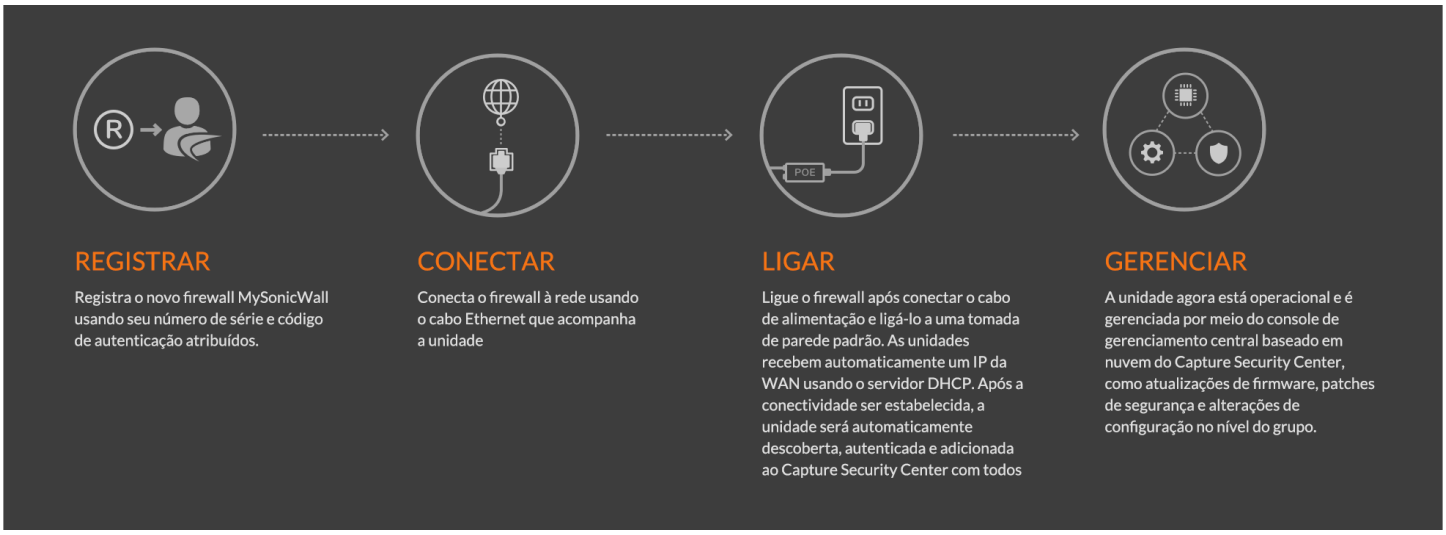


Automação do fluxo de trabalho: cinco etapas para o gerenciamento de políticas sem erros



Implementação sem intervenção

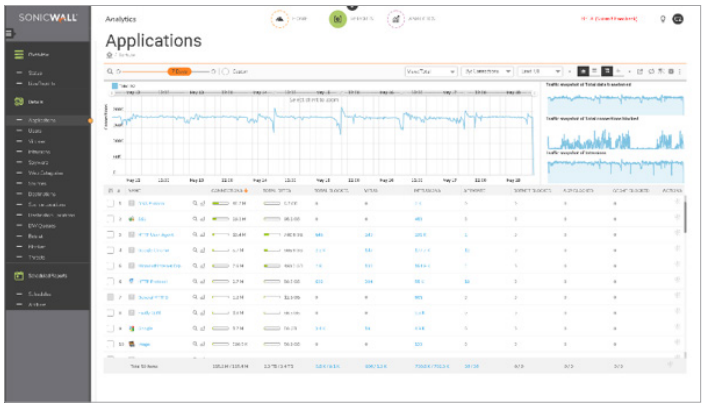
Integrado ao Capture Security Center está o serviço de Implementação sem intervenção (zero-touch), que simplifica e agiliza o processo de provisionamento para firewalls SonicWall em locais remotos e de filiais. O processo requer intervenção mínima do usuário e é totalmente automatizado para operacionalizar os firewalls em escala, em quatro etapas fáceis de implementação. Isso reduz significativamente o tempo, o custo e a complexidade associados à instalação e à configuração, enquanto a segurança e a conectividade ocorrem de maneira instantânea e automática.

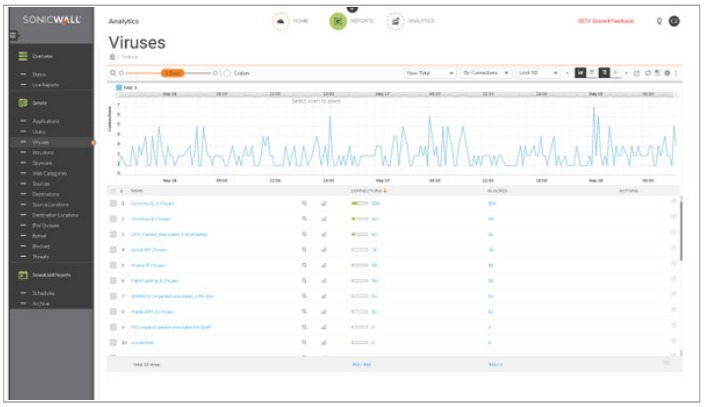


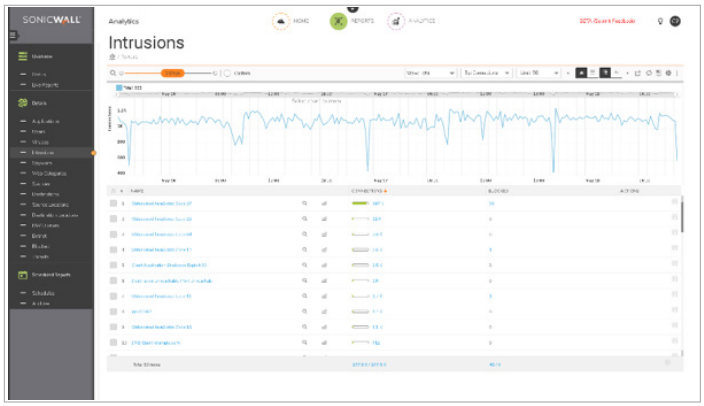
Implementação sem intervenção: operacionalize o firewall em quatro etapas simples

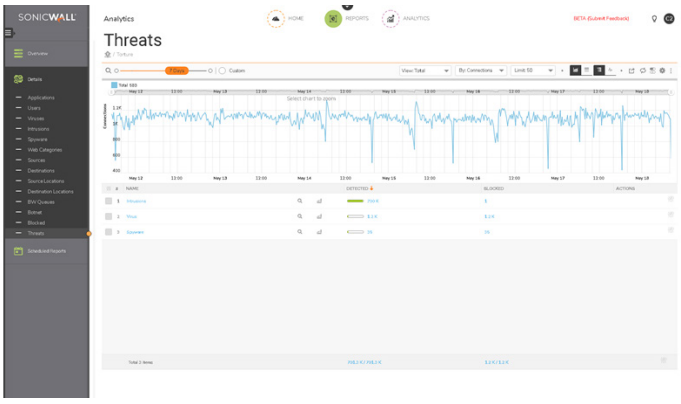
Relatórios

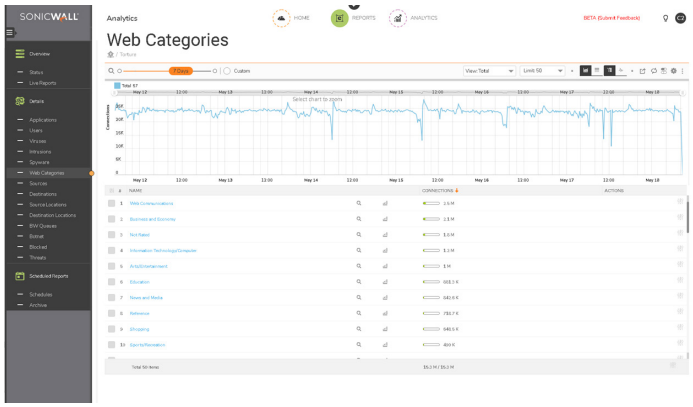
O Capture Security Center oferece mais de 140 relatórios pré-definidos, assim como a flexibilidade para criar relatórios personalizados usando qualquer combinação de dados auditáveis para adquirir vários resultados de caso de uso. Esses resultados incluem percepção geral e detalhada de eventos de rede, atividades de usuários, ameaças, problemas operacionais e de desempenho, eficácia de segurança, riscos e lacunas de segurança, prontidão de conformidade e até análise post mortem. Cada relatório é projetado com a contribuição coletiva de muitos anos de colaborações de clientes e parceiros da SonicWall. Isso fornece a granularidade, o escopo e o conhecimento profundos dos SOCs de dados do syslog e do IPFIX/NetFlow para rastrear, medir e executar uma operação efetiva de rede e segurança.







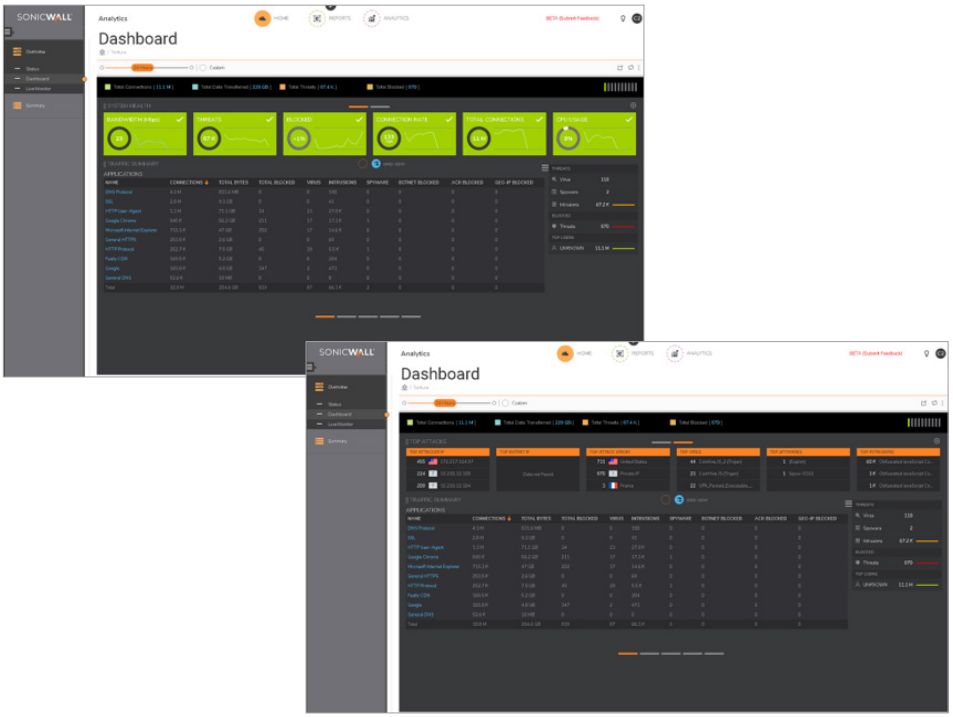


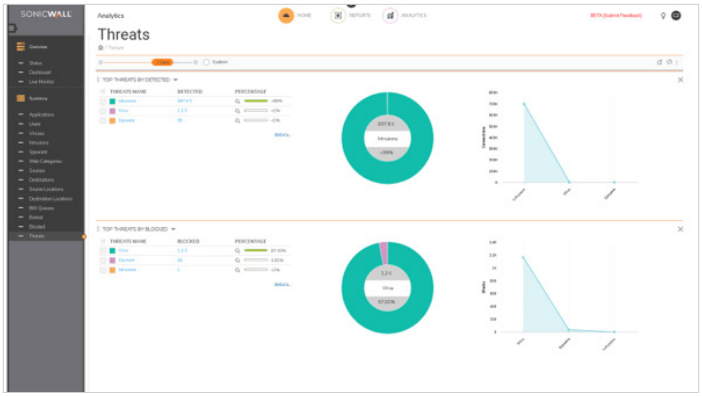


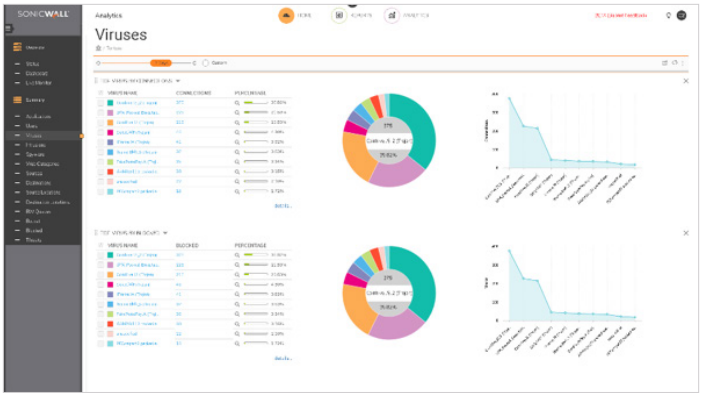
Análise

O SonicWall Analytics é um mecanismo de análise de Big Data baseado em inteligência que automatiza a agregação, a normalização, a correlação e a contextualização de dados de segurança que passam por todos os firewalls gerenciados. Ele oferece às organizações um insight em tempo real sobre tudo o que está acontecendo em suas redes. Os resultados, apresentados de forma estruturada, significativa, acionável e facilmente consumível, capacitam a equipe de segurança, os analistas, os auditores, as diretorias, os C-Suites e as partes interessadas a descobrir, interpretar, priorizar, tomar decisões e tomar ações defensivas e corretivas apropriadas.

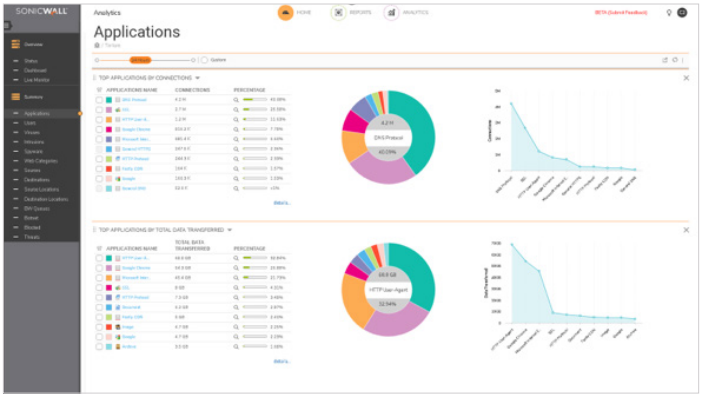
O Analytics apresenta visualização, monitoramento e alertas em tempo real de dados de segurança aprimorados por meio de uma interface única. Ele possui ferramentas eficientes que dão aos clientes total autoridade, agilidade e flexibilidade para executar uma análise de drilldown de tráfego na rede, atividades do usuário, eventos de segurança, perfil de ameaças, utilização de aplicações e uma infinidade de outros dados de firewall contextuais. Essa profunda visibilidade, conhecimento e compreensão do ambiente de segurança oferece aos clientes um insight valioso e a capacidade de descobrir não apenas riscos de segurança, mas também orquestrar a correção, enquanto monitora e controla os resultados com maior clareza e velocidade. O Analytics permite aos clientes operacionalizar a análise de segurança e integrá-la aos processos de negócios para transformar dados em informações, informações em conhecimento e conhecimento em decisões que permitem alcançar a automação de segurança completa.

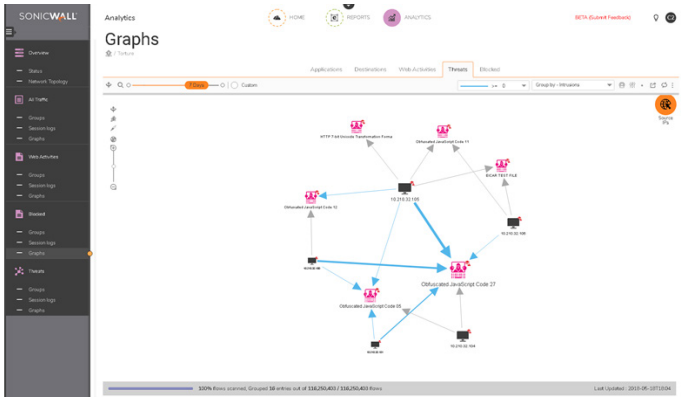


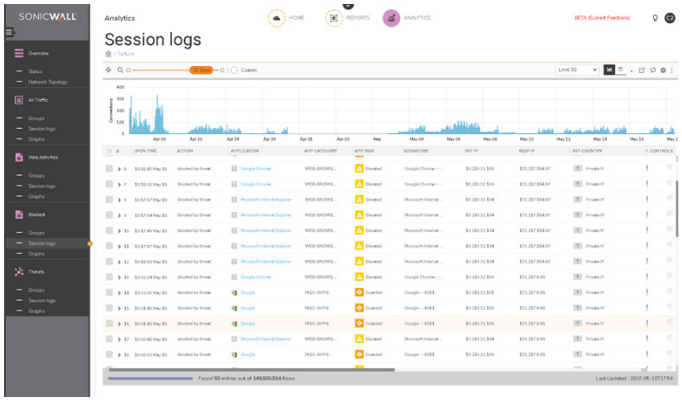

Analytics
Threats


Analytics
Viruses


Analytics
Graphs


Analytics
Applications


Analytics
Graphs

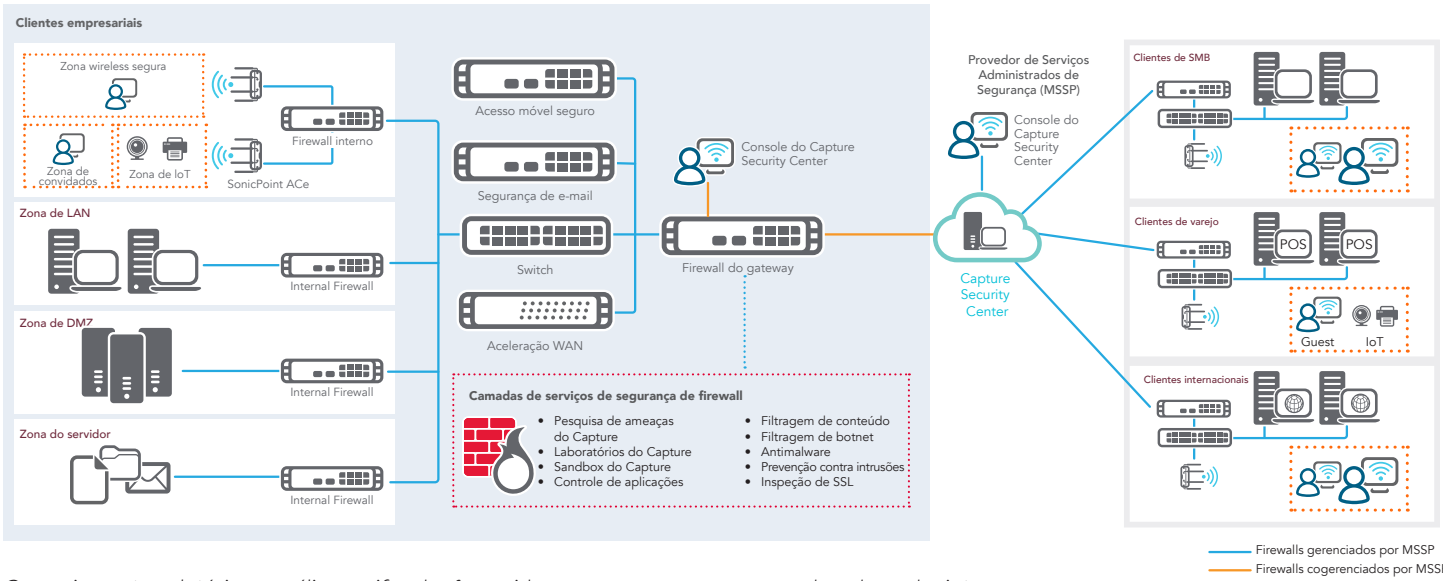

Analytics
Session logs

SONICWALL®

Arquitetura de nuvem escalável

A arquitetura distribuída do Capture Security Center facilita a disponibilidade e a escalabilidade ilimitadas do sistema. Oferecendo suporte para pequenas a grandes empresas, telecomunicações, operadoras e provedores de serviços com um ecossistema de vários usuários, o Capture Security Center pode ajustar a escala sob demanda para oferecer suporte a milhares de dispositivos de segurança SonicWall sob seu gerenciamento, independentemente do local. No nível voltado para o cliente, seus painéis universais altamente interativos são carregados com dados de monitoramento, relatórios e análises em tempo real para ajudar a orientar decisões inteligentes de políticas de segurança e impulsionar a colaboração, comunicação e conhecimento em toda a estrutura de segurança compartilhada. Com uma visão corporativa do ambiente de segurança e inteligência de segurança em tempo real alcançando as pessoas certas na organização, ações precisas de políticas e controles de segurança podem ser tomadas em direção a uma postura de segurança adaptativa mais forte.

O Capture Security Center fornece uma plataforma completa e escalável de gerenciamento, análise e relatórios de segurança para organizações distribuídas e provedores de serviços (por exemplo, operadoras, telecomunicações e MSPs).



Gerenciamento, relatórios e análises unificados fornecidos na nuvem para segurança de rede, endpoint e nuvem.

Recursos

Recursos de gerenciamento e monitoramento de segurança	
Recurso	**Descrição**
Gerenciamento centralizado de segurança e rede	Ajuda os administradores a implementar, gerenciar e monitorar um ambiente de segurança de rede distribuído.
Configuração de política federada	Facilmente define políticas para milhares de firewalls SonicWall, pontos de acesso wireless, segurança de e-mail, dispositivos de acesso remoto seguro e switches de um local central.
Gerenciamento de pedido de mudança e fluxo de trabalho	Garante a correção e a conformidade das mudanças de políticas, aplicando um processo para configurar, comparar, validar, revisar e aprovar políticas antes da implementação. Os grupos de aprovação podem ser configurados pelo usuário para conformidade com a política de segurança da empresa. Todas as alterações de políticas são registradas em um formato auditável que garante que o firewall esteja em conformidade com os requisitos regulamentares. Todos os detalhes granulares de quaisquer alterações feitas são historicamente preservados para ajudar na conformidade, na auditoria e na solução de problemas.
Implementação sem intervenção	Simplifica e acelera a implementação e o provisionamento remoto de firewalls SonicWall remotamente usando a nuvem. Envia políticas automaticamente, executa atualizações de firmware e sincroniza licenças.
Implementação e configuração de VPN sofisticada	Os switches Dell da Série X agora podem ser gerenciados facilmente nos firewalls das séries TZ, NSa e SuperMassive para oferecer gerenciamento de interface única de toda a infraestrutura de segurança da rede.
Gerenciamento off-line	Simplifica e acelera a implementação e o provisionamento remoto de firewalls SonicWall remotamente usando a nuvem. Envia políticas automaticamente, executa atualizações de firmware e sincroniza licenças.

Recursos de gerenciamento e monitoramento de segurança (continuação)	
Recurso	Descrição
Gerenciamento de licenças simplificado	Simplifica a ativação da conectividade VPN e consolida milhares de políticas de segurança.
Painel universal	Apresenta widgets personalizáveis, mapas geográficos e relatórios centrados no usuário.
Monitoramento e alerta de dispositivos ativos	Fornece alertas em tempo real com recursos integrados de monitoramento e facilita os esforços de solução de problemas, permitindo que os administradores tomem medidas preventivas e forneçam correção imediata.
Suporte a SNMP	Oferece interceptações eficientes e em tempo real para todos os dispositivos e aplicações de Transmission Control Protocol/Internet Protocol (TCP/IP) e SNMP, aprimorando bastante os esforços de solução de problemas para identificar e responder a eventos críticos da rede.
Visualização e inteligência de aplicações	Mostra relatórios históricos e em tempo real de quais aplicações estão sendo usadas e por quais usuários. Os relatórios são totalmente personalizáveis usando recursos intuitivos de filtragem e drilldown.
Opções ricas de integração	Oferece interface de programação de aplicações (API) para serviços da Web, suporte à interface de linha de comando (CLI) para a maioria das funções e suporte a interceptações SNMP para provedores de serviços e empresas.
Gerenciamento de switch Dell Networking Série X	Os switches Dell da Série X agora podem ser gerenciados facilmente nos firewalls das séries TZ, NSa e SuperMassive para oferecer gerenciamento de interface única de toda a infraestrutura de segurança da rede.
Risk Meters	Exiba araques ao vivo em tempo real juntamente com gráficos e tabelas detalhados que capturam atividades maliciosas na camada de defesa específica. • Categorizar ações maliciosas de invasores na camada de defesa específica • Restringir o foco de ataques recebidos em um ambiente específico • Atualizar a pontuação de risco calculada e o nível de ameaça baseados em dados de ameaça em tempo real relativos a recursos de defesa existentes • Destacar falhas de segurança atuais pelas quais ameaças evitáveis passam devido à ausência de defesas • Promover ações defensivas imediatas em resposta para evitar todas as ameaças recebidas
Relatórios	
Recurso	Descrição
Relatórios de botnet	Inclui quatro tipos de relatórios: Tentativas, Destinos, Iniciadores e Linha do tempo contendo contexto de vetor de ataque, como ID de Botnet, Endereços IP, Países, Hosts, Portas, Interfaces, Iniciador/Destino, Origem/Destino e Usuário.
Relatório de Geo IP	Contém informações sobre o tráfego bloqueado com base no país de origem ou destino do tráfego. Inclui quatro tipos de relatórios: Tentativas, Destinos, Iniciadores e Linha do tempo contendo contexto de vetor de ataque, como ID de Botnet, Endereços IP, Países, Hosts, Portas, Interfaces, Iniciador/Destino, Origem/Destino e Usuário.
Relatório de endereço MAC	Mostra o endereço de Controle de Acesso à Mídia (MAC) na página do relatório. Inclui informações específicas do dispositivo (Iniciador MAC e Respondente MAC) em cinco tipos de relatórios: • Uso de dados > Iniciadores • Uso de dados > Respondentes • Uso de dados > Detalhes • Atividade do usuário > Detalhes • Atividade da Web > Iniciadores
Relatório do Capture ATP	Mostra informações detalhadas sobre comportamento de ameaças para responder a uma ameaça ou infecção.
Relatórios HIPAA, PCI e SOX	Inclui modelos de relatórios PCI, HIPAA e SOX predefinidos para satisfazer as auditorias de conformidade de segurança.

Relatórios (continuação)	
Recurso	Descrição
Relatórios de ponto de acesso wireless invasor	Mostra todos os dispositivos wireless em uso, assim como o comportamento não autorizado de redes ad-hoc ou peer-to-peer entre hosts e associações acidentais para usuários que se conectam a redes vizinhas invasoras.
Relatórios inteligentes e visualização de atividades	Fornece gerenciamento abrangente e relatórios gráficos para firewalls SonicWall, segurança de e-mail e dispositivos de acesso móvel seguros. Permite um insight mais amplo sobre tendências de uso e eventos de segurança, ao mesmo tempo em que oferece uma marca coesa para os provedores de serviços.
Registros centralizados	Oferece um local central para a consolidação de eventos e registros de segurança para milhares de appliances, fornecendo um único ponto para conduzir a perícia da rede.
Relatórios de syslog em tempo real e históricos de próxima geração	Por meio de um aprimoramento revolucionário na arquitetura, agiliza o processo de sumarização que consome tempo, permitindo relatórios quase em tempo real sobre as mensagens recebidas do syslog. Também fornece a capacidade de detalhar dados e personalizar relatórios extensivamente.
Relatórios universais agendados	Agenda relatórios que são criados automaticamente e enviados por meio de múltiplos appliances de vários tipos para destinatários autorizados.
Análise	
Recurso	Descrição
Agregação de dados	O mecanismo analítico orientado por inteligência automatiza a agregação, a normalização, a correlação e a contextualização dos dados de segurança que passam por todos os firewalls.
Contextualização de dados	A análise acionável, apresentada de forma estruturada, significativa e facilmente consumível, capacita a equipe de segurança, o analista e as partes interessadas a descobrir, interpretar, priorizar, tomar decisões e tomar ações defensivas apropriadas.
Análise de streaming	Streams de segurança de rede são continuamente processados, correlacionados e analisados em tempo real e os resultados são ilustrados em uma interface visual dinâmico e interativo.
Análise do usuário	Análise detalhada das tendências de atividade dos usuários para obter visibilidade total de sua utilização, acesso e conexões em toda a rede.
Visualização dinâmica em tempo real	Por meio de uma única tela, a equipe de segurança pode realizar análises investigativas drilldown e análises forenses de dados de segurança com maior precisão, clareza e velocidade.
Detecção e correção rápidas	Recursos de investigação para perseguir atividades inseguras e gerenciar e corrigir rapidamente os riscos.
Análise e relatórios de fluxo	Fornece um agente de relatório de fluxo para análise de tráfego de aplicações e dados de uso por meio de protocolos IPFIX ou NetFlow para monitoramento em tempo real e histórico. Oferece aos administradores uma interface eficaz e eficiente para monitorar visualmente sua rede em tempo real, fornecendo a capacidade de identificar aplicações e sites com alta demanda de largura de banda, visualizar o uso da aplicação por usuário e antecipar ataques e ameaças encontrados pela rede. • Um Visualizador em tempo real com personalização de arrastar e soltar • Uma tela de relatório em tempo real com filtragem de um clique • Um painel de controle de fluxo superior com botões de um clique Visualizar por • Uma tela Relatórios de fluxo com cinco guias adicionais de atributo de fluxo • Uma tela de Análise de fluxo com eficientes recursos de correlação e giro • Um Visualizador de sessão para drilldowns profundos de sessões e pacotes individuais.
Análise de tráfego de aplicações	Oferece às organizações um insight eficiente do tráfego de aplicações, da utilização de largura de banda e das ameaças de segurança, ao mesmo tempo em que fornece recursos eficientes de solução de problemas e análise forense.
Cloud App Security	
Recurso	Descrição
Painel em tempo real	Obtenha representação visual em tempo real das aplicações em uso, volume de tráfego, atividade do usuário e local de uso.
Descoberta de aplicação	Automatize a descoberta de aplicações na nuvem aproveitando seus arquivos de registro do firewall SonicWall para identificar atividades de shadow IT na rede.
Avaliação de riscos da aplicação	Tome decisões informadas para bloquear/desbloquear aplicações com base na avaliação de riscos.
Classificação e controle de aplicações	Classifique aplicações em aplicações sancionadas ou não sancionadas e defina políticas para bloquear aplicações perigosas.

Resumo dos recursos

Management

- Acesso onipresente
- Alertas e notificações
- Ferramentas de diagnóstico
- Sessões com múltiplos usuários simultâneos
- Gerenciamento off-line e programação
- Gerenciamento de políticas de segurança de firewall
- Gerenciamento de políticas de segurança de VPN
- Gerenciamento de políticas de segurança de e-mail
- Gerenciamento de políticas de Acesso remoto seguro/SSL VPN
- Gerenciamento de serviços de segurança de valor agregado
- Definição de modelos de políticas no nível de grupos
- Replicação de políticas de um dispositivo para um grupo de dispositivos
- Replicação de políticas do nível de grupos para um único dispositivo
- Redundância e alta disponibilidade
- Gerenciamento de provisionamento
- Arquitetura distribuída e escalável
- Visualizações dinâmicas de gerenciamento
- Gerenciador unificado de licenças
- Interface de linha de comando (CLI)
- Interface de programação de aplicações (API) para serviços da Web
- Gerenciamento com base em funções (usuários, grupos)
- Painel universal
- Backup de arquivos de preferência dos appliances de firewall

Monitoramento

- Fluxos de dados IPFIX em tempo real
- Suporte a SNMP
- Monitoramento e alerta de dispositivos ativos
- Gerenciamento de retransmissão SNMP
- Monitoramento de status de firewall e VPN
- Alertas e monitoramento do Syslog em tempo real
- Risk Meters

Relatórios

- Conjunto abrangente de relatórios gráficos
- Relatório de conformidade
- Relatórios personalizáveis com recursos de detalhamento
- Registros centralizados
- Relatórios de várias ameaças
- Relatórios voltados para o usuário
- Relatórios de uso das aplicações
- Relatórios mais granulares sobre serviços
- Nova inteligência contra ataques
- Relatório de largura de banda e serviços por interface
- Relatórios para appliances de firewall UTM SonicWall
- Relatórios para appliances VPN SSL do SonicWall SRA
- Relatórios universais agendados
- Relatórios de Syslog e IPFIX de próxima geração
- Relatórios flexíveis e granulares praticamente em tempo real
- Relatórios de largura de banda por usuário
- Relatório de atividades VPN do cliente
- Relatório de resumo detalhado dos serviços por VPN
- Relatórios de ponto de acesso wireless invasor
- Relatórios do Web Application Firewall (WAF) de SRA para pequenas e médias empresas
- Relatórios do Cloud App Security (CAS)
- Relatórios do Capture Client

Análise

- Agregação de dados
- Contextualização de dados
- Análise de streaming
- Análise do usuário
- Visualização dinâmica em tempo real
- Detecção e correção rápidas

Licenciamento e pacotes

Os serviços baseados em nuvem de CSC Management, Reporting, Analytics e CAS estão disponíveis nas opções de pacotes abaixo. O requisito de uso mínimo é que cada firewall gerenciado deve ter uma assinatura AGSS ou CGSS ativa.

1. CSC Basic Management (Lite)

Esta versão é mais adequada para backup/restauração de sistema ou de preferências de firewall e para atualização de firmware. Qualquer firewall com assinatura AGSS ou CGSS pode ter essa funcionalidade básica de gerenciamento ativada para ajudar a administrar firewalls.

2. CSC Management

Essa opção de assinatura paga ativa os recursos completos de gerenciamento, incluindo os recursos de Automação de fluxo de trabalho e Implementação sem intervenção.

3. CSC Management e Reporting

Essa opção de licença é ideal para instituições maiores com muitos firewalls implementados em locais geograficamente dispersos que estão sob gerenciamento baseado em grupos ou locatários. Isso inclui organizações de médio porte, empresas distribuídas, setor público e instituições de ensino com muitos distritos e campi, e provedores de serviços gerenciados (MSPs).

Além dos recursos completos de gerenciamento, essa opção de assinatura oferece recursos completos de relatórios para realizar análises e auditorias periódicas ou sob demanda de segurança e desempenho da rede. Isso pode ser feito usando uma interface interativa universal na tela com gráficos e tabelas em tempo real ou fora da tela com relatórios exportados programados.

4. CSC Analytics

Esse é um eficiente serviço suplementar para todas as opções de assinatura do Capture Security Center. A ativação do serviço fornece acesso total às ferramentas e serviços do SonicWall Analytics e SonicWall Cloud App Security para conduzir a perícia na rede e a detecção de ameaças usando recursos abrangentes de drilldown e pivotamento.

	Recursos	CSC Management Lite	CSC Management	CSC Management e Reporting	CSC Análise
Management	Backup/Restauração – Sistema de firewall	Sim	Sim	Sim	Sim
	Backup/Restauração – Preferências de firewall	Sim	Sim	Sim	Sim
	Atualização de firmware	Apenas do arquivo local	Apenas do arquivo local ou MySonicWall	Sim	Apenas do arquivo local
	Programação de tarefas	—	Sim	Sim	—
	Gerenciamento de firewall de grupo	—	Sim	Sim	—
	Herança – Para frente/reversa	—	Sim	Sim	—
	Implementação sem intervenção[1]	—	Sim	Sim	—
	Downloads de assinatura de firewall off-line	—	Sim	Sim	—
	Fluxo de trabalho	—	Sim	Sim	—
	Licenças agrupadas – Pesquisa, compartilhamento, inventário de código de ativação usado	—	Sim	Sim	—
Relatórios (com base em Netflow/IPFIX)	Agendar relatórios, monitoramento em tempo real, painéis de resumo	—	—	Sim	Sim
	Download de relatórios: aplicações, ameaças, CFS, usuários, tráfego, origem/destino (relatório de fluxo de um ano)	—	—	Sim	Sim
Análise (com base em Netflow/IPFIX)	Rede de caça forense e ameaças usando drilldown e dinâmica	—	—	—	Sim
	Segurança de aplicação na nuvem	—	—	—	Sim
	Retenção de dados de tráfego por 30 dias	—	—	—	Sim
Suporte técnico		Somente casos da Web	Suporte 24x7	Suporte 24x7	Suporte 24x7

1 Suporte para SOHO-W com firmware 6.5.2+; séries TZ, NSA e NSa 2650-6650 com firmware 6.5.1.1+. Não tem suporte para as séries SOHO ou NSv.

Modelos de firewall com suporte

O Capture Security Center está disponível somente para clientes AGSS/CGSS com firewalls SOHO-W, Série TZ, Série NSA, NS*a* 2650-6650, e Série NSv. Para o SuperMassive Série 9000, NS*a* 9250 a 9650 e NS*sp* 12400 a 12800, a opção de assinatura do CSC Management é ativada automaticamente como parte de sua ativação de assinatura de AGSS correspondente.

Capture Security Center			
	Management	Geração de relatórios	Análise
FW básico	SOHO-W, Série TZ, NSv 10-100	Série TZ, NSv 10-100	Série TZ, NSv 10-100
FW intermediário	Série NSA, NS*a* 2650-6650, NSv 200-400	Série NSA, NS*a* 2650-6650, NSv 200-400	Série NSA, NS*a* 2650-6650, NSv 200-400
FW de tecnologia avançada	SuperMassive série 9000, NS*sp* série 12000, NS*a* 9250-9650, NSv 800-1600		

Informações para pedidos

Produto	SKU
SonicWall Capture Security Center Management para Série TZ, SOHO-W, NSv 10 a 100, 1 ano	01-SSC-3664
SonicWall Capture Security Center Management para Série TZ, SOHO-W, NSv 10 a 100, 2 anos	01-SSC-9151
SonicWall Capture Security Center Management para Série TZ, SOHO-W, NSv 10 a 100, 3 anos	01-SSC-9152
SonicWall Capture Security Center Management para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 1 ano	01-SSC-3665
SonicWall Capture Security Center Management para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 2 anos	01-SSC-9214
SonicWall Capture Security Center Management para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 3 anos	01-SSC-9215
SonicWall Capture Security Center Management e Reporting para Série TZ, NSv 10 a 100, 1 ano	01-SSC-3435
SonicWall Capture Security Center Management e Reporting para Série TZ, NSv 10 a 100, 2 anos	01-SSC-9148
SonicWall Capture Security Center Management e Reporting para Série TZ, NSv 10 a 100, 3 anos	01-SSC-9149
SonicWall Capture Security Center Management e Reporting para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 1 ano	01-SSC-3879
SonicWall Capture Security Center Management e Reporting para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 2 anos	01-SSC-9154
SonicWall Capture Security Center Management e Reporting para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 3 anos	01-SSC-9202
SonicWall Capture Security Center Analytics para Série TZ, NSv 10 a 100, 1 ano	02-SSC-0171
SonicWall Capture Security Center Analytics para NSA 2600 a 6600, NSa 2650 a 6650 e NSv 200 a 400, 1 ano	02-SSC-0391

Navegadores da Internet

- Microsoft® Internet Explorer 11.0 ou superior (não usar modo de compatibilidade)
- Mozilla Firefox 37.0 ou superior
- Google Chrome 42.0 ou superior
- Safari (versão mais recente)

Appliances com suporte do SonicWall gerenciados pelo Capture Security Center

- Appliances de segurança de rede da SonicWall: appliances NS*a* 2600 a NS*a* 6650 e da Série TZ
- Appliances virtuais de segurança de rede SonicWall: NSv 10 a NSv 400
- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)

Sobre nós

A SonicWall tem combatido o setor de crime cibernético há mais de 27 anos, defendendo pequenas, médias e grandes empresas em todo o mundo. Nossa combinação de produtos e parceiros possibilitou uma solução automatizada de detecção e prevenção de violação em tempo real ajustada às necessidades específicas de mais de 500.000 organizações em mais de 215 países e territórios, o que permite que você faça mais negócio com menos preocupações. Para obter mais informações, visite **www.sonicwall.com** ou siga-nos no Twitter, no LinkedIn, no Facebook e no Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte o nosso site para informações adicionais.
www.sonicwall.com

DataSheet-CaptureSecurityCenter-US-KJ-MKTG4268