SonicWall Analytics

Transformação de dados em informações, informações em conhecimento, conhecimento em decisões e decisões em ações

O SonicWall Analytics fornece um olhar clínico sobre tudo o que acontece no ambiente de segurança de rede SonicWall, tudo isso por meio de uma única tela. Em seu núcleo está um potente mecanismo de análise orientado por inteligência que automatiza a agregação, a normalização, a correlação e a contextualização de dados de segurança que fluem por todos os firewalls SonicWall e pontos de acesso wireless. O painel interativo da aplicação usa várias formas de gráficos e tabelas de uso de tempo para criar representações de conhecimento dos modelos de dados.

O Analytics apresenta os resultados de maneira significativa, prática e fácil de consumir. Isso permite que equipes de segurança, analistas, auditores, diretorias e diretores executivos descubram, interpretem, priorizem, tomem decisões baseadas em provas e executem ações defensivas e corretivas apropriadas contra riscos e ameaças à medida que surgirem no processo de descoberta.

O Analytics fornece às partes interessadas insights em tempo real e visibilidade, autoridade e flexibilidade em uma única tela. Como resultado, elas podem executar análise profunda investigativa e forense do tipo drilldown de tráfego na rede, acesso de usuário, conectividade, aplicações e utilização, estado de ativos de segurança, eventos de segurança, perfis de ameaça e outros dados relacionados a firewall.

Benefícios:

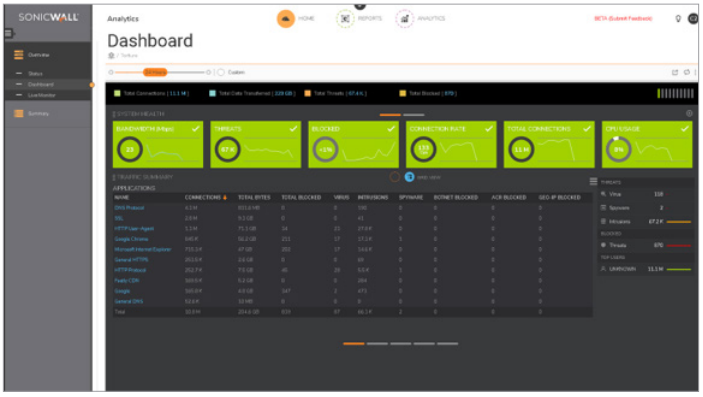
- Obtenha visibilidade em tela única e conscientização situacional completa do ambiente de segurança de rede
- Tenha autoridade e flexibilidade completas para realizar análise profunda investigativa e forense
- Obtenha conhecimento e compreensão mais profundos sobre riscos e ameaças potenciais e reais
- Corrija riscos com maior clareza, certeza e velocidade
- Reduza o tempo de incident response (IR) com threat intelligence prática em tempo real

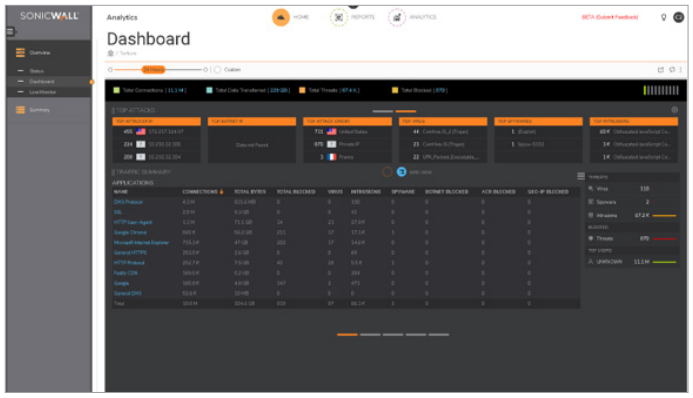
Serviços ativados por parceiros

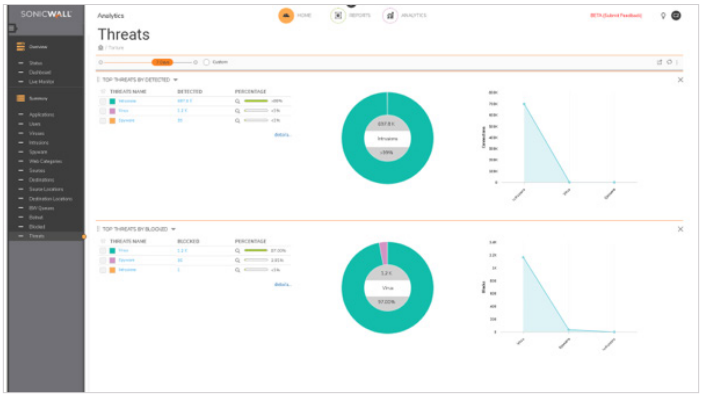
Precisa de ajuda para planejar, implementar ou otimizar sua solução SonicWall? Os Parceiros de serviços avançados da SonicWall são treinados para fornecerem a você serviços profissionais de nível mundial. Saiba mais em www.sonicwall.com/PES.

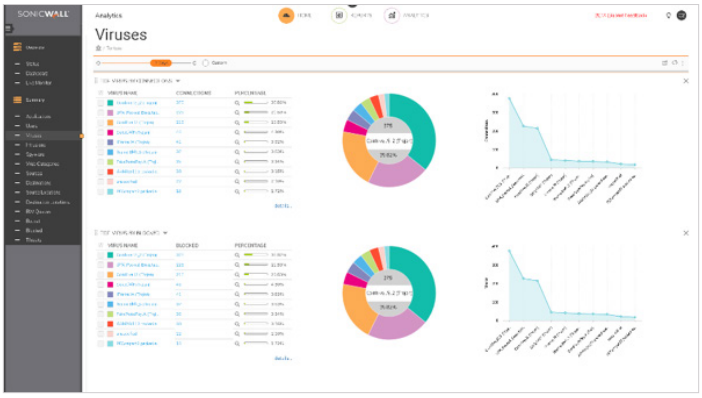
Esse conhecimento e entendimento profundos do ambiente de segurança fornecem a inteligência e a capacidade para desvendar e orquestrar a correção dos riscos de segurança, além de monitorar e rastrear os resultados com maior clareza, certeza e velocidade.

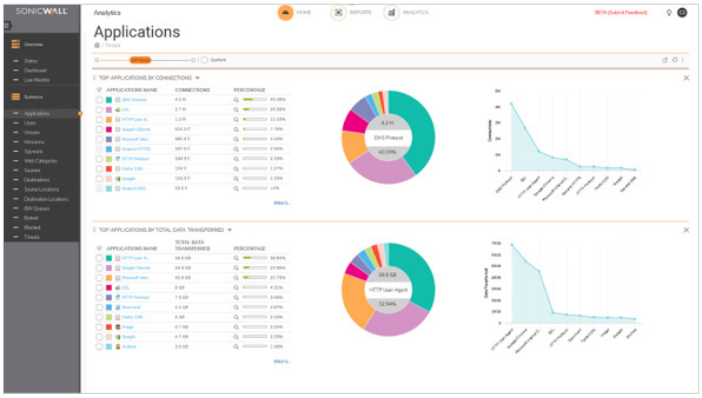
A integração do Analytics ao processo de negócio ajuda a operacionalizar a análise ao transformar dados em informações, informações em conhecimento e conhecimento em decisões para obter automação da segurança.











SONICWALL®

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 Zero-Touch	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 painel único 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.
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 painel único de toda a infraestrutura de segurança da rede.
Relatórios HIPAA, PCI e SOX	Inclui modelos de relatórios PCI, HIPAA e SOX predefinidos para satisfazer as auditorias de conformidade de segurança.
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 dados de segurança de rede são continuamente processados, correlacionados e analisados em tempo real e os resultados são ilustrados em um painel 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.

Resumo dos recursos

Painel de resumo com visualizações e gráficos

- Taxa de largura de banda
- Utilização da CPU
- Contagem de conexões
- Taxa de conexão por segundo
- Índice de risco (escala de um a dez)
- Porcentagem de bloqueio
- Total de conexões
- Total de dados transferidos
- Principais aplicações
- Principais intrusões
- Principais categorias de URL
- Principais vírus
- Número de vírus, intrusões, spyware, botnets

Streaming de monitor em tempo real com gráficos de áreas/barras

- Aplicações
- Entrada/saída da interface, média, mín., pico
  - Largura de banda
  - Taxa de pacotes
  - Tamanho do pacote
  - Taxa de conexão
- Uso
  - Contagem de conexões
  - Monitor com múltiplos núcleos

Principais painéis de resumo com drilldowns

- Aplicações
- Usuários
- Vírus
- Intrusões
- Spyware
- Categorias da Web
- Fontes
- Destinos
- Locais das fontes
- Locais dos destinos
- Filas de BW
- Botnet

Relatórios com drilldowns, exportação para pdf/csv e envio de e-mail agendado

- Aplicações/Usuários/Fontes/Destinos
  - Conexões
  - Total de conexões travadas
  - Conexões travadas por regra de acesso
  - Conexões travadas por ameaça
  - Conexões travadas por filtro de botnet
  - Conexões travadas por filtro de GeoIP
  - Conexões travadas por Content Filtering Service
  - Vírus
  - Intrusões
  - Spyware
  - Total de dados transferidos
  - Dados enviados
  - Dados recebidos
- Vírus/Intrusões/Spyware/Categorias da Web/Locais das fontes/Locais dos destinos/Filas de BW
  - Conexões
  - Total de dados transferidos
  - Dados enviados
  - Dados recebidos
- Botnet
  - Conexões
- Exportação
  - .pdf
  - .csv
- Relatórios agendados
  - Relatório de fluxo
  - Capture Threat Assessment (SWARM)
  - Diária/Semanal/Mensal
  - Arquivo/E-mail/PDF

Visualizador de sessão do Analytics com drilldowns, filtragem, exportação de dados de sessões individuais

- Análise de tráfego em qualquer combinação de:
  - Aplicação
  - Categoria da aplicação
  - Risco da aplicação
  - Assinatura
  - Ação
  - IP do iniciador/respondente
  - País do iniciador/respondente
  - Porta do iniciador/respondente
  - Bytes do iniciador/respondente
  - Interface do iniciador/respondente
  - Índice do iniciador/respondente
  - Gateway do iniciador/respondente
  - MAC do iniciador/respondente
  - Protocolo
  - Taxa (Kbit/s)
  - ID do fluxo
  - Intrusão
  - Vírus
  - Spyware
  - Botnet
- Análise de ameaças/travamentos em qualquer combinação de:
  - Nome da ameaça
  - Tipo de ameaça
  - ID da ameaça
  - Aplicação
  - Categoria da aplicação
  - Risco da aplicação
  - Assinatura
  - Ação
  - IP do iniciador/respondente
  - País do iniciador/respondente
  - Porta do iniciador/respondente
  - Bytes do iniciador/respondente
  - Interface do iniciador/respondente
  - Índice do iniciador/respondente
  - Gateway do iniciador/respondente
  - MAC do iniciador/respondente
  - Protocolo
  - Taxa (Kbit/s)
  - ID do fluxo
  - Intrusão
  - Vírus
  - Spyware
  - Botnet

Análise de URL/travamentos em qualquer combinação de:

- URL
- Categoria da URL
- Domínio da URL
- Aplicação
- Categoria da aplicação
- Risco da aplicação
- Assinatura
- Ação
- IP do iniciador/respondente
- País do iniciador/respondente
- Porta do iniciador/respondente
- Bytes do iniciador/respondente
- Interface do iniciador/respondente
- Índice do iniciador/respondente
- Gateway do iniciador/respondente
- MAC do iniciador/respondente
- Protocolo
  - Taxa (Kbit/s)
  - ID do fluxo
  - Intrusão
  - Vírus
  - Spyware
  - Botnet

Monitor do fluxo de análise - drilldown e giro nos parâmetros de fluxo

- Aplicações
  - Nomes
  - Categorias
  - Assinaturas
- Usuários
  - Nome
  - Endereço IP
  - Nomes de domínios
  - Tipos de autenticação
- Atividades da Web
  - Sites
  - Categorias da Web
  - URLs
- Fontes
  - Endereços IP
  - Interfaces
  - Países
- Destinos
  - Endereços IP
  - Interfaces
  - Países
- Ameaças
  - Intrusões
  - Vírus
  - Spyware
  - Spam
  - Botnets
- VoIP
  - Tipos de mídia
  - IDs dos chamadores
- Dispositivos
  - Endereços IP
  - Interfaces
  - Nomes
- Conteúdo
  - Endereços de e-mail
  - Tipos de arquivos
- Gerenciamento da largura de banda
  - Entrada
  - Saída
  - Todos
  - URL
  - Sessões
  - Total de pacotes
  - Total de bytes
  - Ameaças

Gráficos em estrela - visualizações de ponto a ponto, drilldowns e giros

- Fontes/Usuários/Locais/Dispositivos
  - Para/de
    - » Destinos
    - » Aplicações
    - » Atividades da Web
    - » Ameaças
  - Filtrado por
    - » Número de conexões
    - » Dados transferidos
    - » Pacotes trocados
    - » Número de ameaças
  - Realce com halo para
    - » Ameaças
    - » Dados > 1 MB
    - » Conexões >1000
    - » Pacotes >1000

Licenciamento e pacotes

Capture Security Center (CSC)		Camada de licença			
		CSC Management Lite	CSC Management	CSC Management e Reporting	CSC Análise
Requisito de licenciamento	Disponível para clientes com a assinatura AGSS/CGSS ativa	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Gerenciamento	Tela única	✓	✓	✓	
	Backup/restauração	✓	✓	✓	
	Programação de tarefas		✓	✓	
	Gerenciamento de firewall de grupo		✓	✓	
	Herança - para frente/reversa		✓	✓	
	Sem intervenção		✓	✓	
	Downloads de assinatura de firewall off-line		✓	✓	
	Fluxo de trabalho		✓	✓	
Relatórios	Monitor em tempo real, painéis de resumo			✓	
	Relatórios para download: Aplicações, Ameaças, CFS, Usuários, Tráfego, etc.			✓	
	Relatórios agendados			✓	
Análise	Analytics (retenção de 30 dias)				✓
	Cloud App Security (retenção de 30 dias)				✓

Informações para pedidos do Capture Security Center

Produto	SKU
SonicWall Capture Security Center Management para Série TZ, NSv 10 a 100, 1 ano	01-SSC-3664
SonicWall Capture Security Center Management para Série TZ, NSv 10 a 100, 2 anos	01-SSC-9151
SonicWall Capture Security Center Management para Série TZ, NSv 10 a 100, 3 anos	01-SSC-9152
SonicWall Capture Security Center Management para NSA 2600 a 6650 e NSv 200 a 400, 1 ano	01-SSC-3665
SonicWall Capture Security Center Management para NSA 2600 a 6650 e NSv 200 a 400, 2 anos	01-SSC-9214
SonicWall Capture Security Center Management para NSA 2600 a 6650 e NSv 200 a 400, 3 anos	01-SSC-9215
SonicWall Capture Security Center Management and Reporting para Série TZ, NSv 10 a 100, 1 ano	01-SSC-3435
SonicWall Capture Security Center Management and Reporting para Série TZ, NSv 10 a 100, 2 anos	01-SSC-9148
SonicWall Capture Security Center Management and Reporting para Série TZ, NSv 10 a 100, 3 anos	01-SSC-9149
SonicWall Capture Security Center Management and Reporting para NSA 2600 a 6650 e NSv 200 a 400, 1 ano	01-SSC-3879
SonicWall Capture Security Center Management and Reporting para NSA 2600 a 6650 e NSv 200 a 400, 2 anos	01-SSC-9154
SonicWall Capture Security Center Management and Reporting para NSA 2600 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 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

- SonicWall Network Security Appliances: appliances NS*a* 2600 a NS*a* 6650 e Série TZ
- SonicWall Network Security Virtual Appliances: NSv 10 a NSv 400

Sobre nós

A SonicWall tem combatido o setor do crime cibernético por mais de 26 anos ao defender desde pequenas e médias empresas até grandes corporações mundialmente. A nossa combinação de produtos e parceiros propiciou uma solução de defesa cibernética em tempo real, associada às necessidades específicas de mais de 500.000 empresas globalmente, em mais de 150 países, o que permite que você faça mais em seu negócio com menos preocupações.

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

Datasheet-Analytics-US-VG-MKTG4305

SONICWALL®