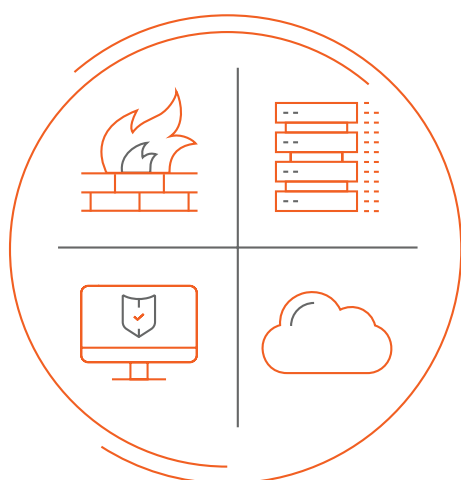




Managed Detection and Response (MDR) da SonicWall

A segurança de seus endpoints.
Nossos recursos especializados.



O Managed Detection and Response (MDR) é um serviço abrangente que inclui o monitoramento de ameaças 24x7, a captura das ameaças e resposta mediante detecção. O serviço de MDR da SonicWall, oferecido pela Solutions Granted, potencializa análises avançadas, inteligência em ameaças e especialização humana para realizar uma investigação e uma resposta sofisticada e completa a incidentes. A validação de incidentes, juntamente com serviços de resposta remota como a contenção de ameaças, também estão disponíveis. Você pode ficar tranquilo, sabendo que mesmo no pior dos cenários, você estará nas mãos do melhor serviço possível.

- A detecção avançada de ameaças a endpoints que vai superar todas as suas outras defesas
- Prestação de serviços de segurança proativa para seus clientes, com um SOC 24x7 realizado por especialistas, utilizando a mais recente inteligência em ameaças
- Evite a disseminação de ransomware com o isolamento automático de redes e o cancelamento de processos de ransomware
- Supere a fadiga de alertas e reduza a incidência de falsos positivos
- Seja um usuário do SonicWall Capture Client para trabalhar com uma plataforma de gestão unificada, de fácil utilização, ou em conjunto com o Windows Defender ou SentinelOne já instalados

"O SOC da Solutions Granted detectou atividades suspeitas no servidor de um cliente às 2:00 h. Conseguimos conter a violação no estágio inicial. Eu dormi melhor à noite, sabendo que a Solutions Granted está inspecionando minhas redes".

DAN BROWNE, CEO, DMB NETWORKS

Descubra como funciona uma parceria verdadeira com um fornecedor de serviços de segurança: Aumente a visibilidade em todo o seu ecossistema e acesse as respostas rapidamente como a nossa equipe completa de SOC 24x7x365.

Para saber mais sobre a ampla gama de benefícios desfrutados pelos parceiros do SecureFirst da SonicWall, entre em contato conosco hoje mesmo! partnerdevelopment@sonicwall.com

TECNOLOGIAS COMPROVADAS. PROTEÇÃO SUPERIOR.

Veja como o MDR da SonicWall melhora a segurança, ao mesmo tempo otimizando os recursos:

IMPLEMENTAÇÃO BASEADA EM AGENTES

Agentes leves são instalados em endpoints, oferecendo acesso persistente e contínuo e ao mesmo tempo habilitando o monitoramento e a coleta de dados em tempo real.

DETECÇÃO COM BASE EM ANOMALIAS

Com o uso de análises estatísticas, heurística e aprendizagem de máquina, o agente destaca qualquer evento ou característica atípica em um artefato ou arquivo, auxiliando na detecção de ameaças avançadas ou de dia zero.

A Detecção com base em anomalias inclui:

- Monitoramento de processos e scripts em tempo real
- Análise de memória ao vivo e contínua
- Detecção de PowerShell e outras técnicas prejudiciais do tipo Living Off the Land (LOTL)
- Evita abusos em contas de usuários e legítimas ferramentas administrativas
- Interrompe ameaças em movimentações laterais

DETECÇÃO COM BASE NO COMPORTAMENTO

O mecanismo de análises comportamentais inspeciona comportamentos suspeitos em processos e eventos legítimos. Essas irregularidades são então mapeadas conforme táticas, técnicas e procedimentos (TTPs) conhecidos dos criminosos, conforme descritos pela estrutura MITRE ATT&CK. Concentrando-se em 20 das técnicas mais comuns observadas da ATT&CK, o MDR da SonicWall é altamente eficaz na captura de elementos prejudiciais no ato.

ANÁLISE DE STATUS FORENSE

O agente é capaz de coletar e analisar dados periciais de endpoints ao vivo, incluindo a memória volátil e não-volátil. Isto permite uma inspeção proativa de milhares de hosts em busca de ações prejudiciais atuais e históricas, e ajuda a identificar a causa-raiz dos ataques detectados. As análises podem ser conduzidas sem agentes ou utilizando o agente ARR.

A Análise de Status Forense inclui:

- Processos e scripts ativos
- Triagem da memória volátil
- Registro e execuções automáticas (chaves de execução, pastas de inicialização, arquivos com links, schtasks/cron, etc.)
- Artefatos de execução (shimcache, amcache, prefetch)
- Subversão de SO (ganchos de api, controles desabilitados)
- Triagem de registros de eventos locais
- Contas privilegiadas
- Aplicativos e vulnerabilidades instaladas
- Conexões e observadores de hosts ativos

MONITORAMENTO CONTÍNUO DE ENDPOINTS, RESPOSTA E PERÍCIA

A captura e o monitoramento de ameaças avançadas acrescenta outra camada de segurança. Este recurso se concentra na identificação de comportamentos significativos, observados durante um ataque e depois dele. A análise pericial automatizada permite aos nossos especialistas que confirmem proativamente a integridade dos endpoints e que determinem rapidamente uma causa-raiz assim que uma violação é identificada. O MDR simplifica e acelera a identificação, investigação e resposta a ataques cibernéticos sofisticados.

Sobre a SonicWall

A SonicWall oferece cibersegurança estável, escalonável, sem transtornos na era da hiperdistribuição e uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao conhecer o desconhecido, oferecer visibilidade em tempo real e possibilitar economia disruptiva, a SonicWall preenche as lacunas de cibersegurança para grandes empresas, governos e PMEs em todo o mundo. Para obter mais informações, visite www.sonicwall.com.



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 950305
Consulte nosso site na internet para obter informações adicionais.
www.sonicwall.com

SONICWALL®

© 2024 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.

SonicWall é uma marca registrada da SonicWall Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as demais marcas e marcas registradas são de propriedade dos respectivos titulares. As informações deste documento foram fornecidas em relação aos produtos da SonicWall Inc. e/ou de suas afiliadas. Nenhuma licença, expressa ou implícita, por preclusão ou de qualquer espécie, para qualquer direito de propriedade intelectual será concedida por meio deste documento ou em relação à venda de produtos da SonicWall. Salvo na forma estabelecida nos termos e condições, conforme especificado no contrato de licenciamento deste produto, a SonicWall e/ou suas afiliadas presumem isenção de responsabilidade, qualquer que seja, e de qualquer garantia expressa, implícita ou prevista em lei relacionada a seus produtos, incluindo, entre outras, a garantia implícita de comerciabilidade, adequação a um objetivo específico ou não violação. Em hipótese alguma, a SonicWall e/ou suas afiliadas se responsabilizam por qualquer tipo de dano direto, indireto, consequencial, cominatório, especial ou eventual (incluindo, entre outros, danos por lucros cessantes, interrupção de negócios ou perda de informações) decorrentes da utilização ou da incapacidade de utilizar este documento, mesmo se a SonicWall e/ou suas afiliadas tiverem sido orientadas da possibilidade de ocorrência de tais danos. A SonicWall e/ou suas afiliadas não fazem qualquer declaração nem oferecem garantias em relação à precisão ou integridade do conteúdo deste documento e reservam para si o direito de realizar alterações nas especificações e descrições de produtos a qualquer momento e sem aviso prévio. A SonicWall Inc. e/ou suas afiliadas não assumem qualquer compromisso pela atualização das informações contidas neste documento.