RESUMO DA SOLUÇÃO

Um ganha-ganha: segurança mais forte, relacionamentos mais sólidos

Como o SonicWall Endpoint Security ajuda MSPs a aumentar a lucratividade enquanto aprofunda a confiança dos clientes.

Todo MSP enfrenta o mesmo desafio: os clientes esperam uma segurança cada vez mais robusta a cada ano, mas nem sempre estão dispostos a pagar mais por isso. As margens ficam apertadas, os stacks de ferramentas se tornam complicados e o trabalho de manter tudo funcionando consome o tempo que você poderia dedicar ao crescimento do negócio. A tendência costuma ser buscar a combinação mais barata de ferramentas que atenda aos requisitos, mas juntar antivírus gratuito com uma solução de detecção e resposta de endpoint (EDR) separada e de baixo custo geralmente gera mais custos e riscos do que resolve.

O SonicWall Endpoint Security segue um caminho diferente. Ele combina antivírus de última geração (NGAV) e detecção e resposta avançada em endpoint (EDR) em um único agente leve, oferecendo proteção de nível corporativo por um preço pensado para as pequenas e médias empresas que você atende. O resultado é uma oferta de segurança mais fácil de operar, mais barata de entregar e mais valiosa para seus clientes — assim, tanto o seu negócio quanto o relacionamento com os clientes saem ganhando.

O problema de lucratividade com segurança fragmentada

MSPs preocupados com o orçamento costumam combinar antivírus gratuito com um EDR de baixo custo para proteger a margem. Embora isso possa parecer eficiente, operar dois sistemas desconectados significa dois consoles, dois conjuntos de políticas, dois ritmos de atualização e o dobro de chances de uma configuração incorreta passar despercebida. Essa complexidade resulta em horas extras de engenheiros, triagem de falsos positivos e incidentes que poderiam ter sido evitados.

O mercado de EDR está crescendo rapidamente porque o antivírus básico já não é suficiente contra malwares impulsionados por IA, ataques sem arquivo, e explorações de dia zero. A dúvida para um MSP é se oferecer um EDR confiável precisa significar mais custo e complexidade. Com o SonicWall Endpoint Security, não precisa.

Cinco maneiras pelas quais o SonicWall Endpoint Security impulsiona a lucratividade das MSPs

1 Consolide sua stack e reduza custos

NGAV e EDR funcionam em um único agente leve em um único console multi-tenant. Você elimina o trabalho de integração, as licenças duplicadas e a sobrecarga operacional de manter ferramentas paralelas — e ainda ganha reversão contra ransomware com até 40% de economia em comparação com soluções concorrentes. Um custo menor para entregar significa mais margem em cada endpoint que você protege.

2 Adicione fontes de receita

EDR avançado, busca de ameaças em tempo real e histórica, e relatórios detalhados são serviços que você pode empacotar e precificar — não apenas recursos cujos custos você precisa absorver. Cada funcionalidade é uma oportunidade para migrar um cliente para um nível de serviço superior e aumentar a receita mensal recorrente usando capacidades que normalmente são reservadas para plataformas corporativas muito mais caras.

3 Cresça sem aumentar o quadro de funcionários

A gestão multi-tenant, o controle granular de políticas e a integração com as principais ferramentas de PSA, RMM e SIEM permitem que uma equipe enxuta atenda muitos clientes a partir de uma única plataforma. Você pode expandir sua carteira de clientes sem aumentar sua folha de pagamento na mesma proporção.

4 Ofereça um nível totalmente gerenciado com faturamento mensal

As ameaças cibernéticas não dormem e, por isso, os alertas de endpoint também não. Mais empresas do que nunca precisam de monitoramento 24 horas por dia. O SonicSentry MDR para SonicWall Endpoint Security adiciona um centro de operações de segurança (SOC) 24x7, caça proativa a ameaças e resposta especializada — todos os benefícios de um SOC sem que você precise montar um por conta própria. Ele é vendido mensalmente, sem contratos ou mínimos, para que você possa começar pequeno e aumentar ou reduzir conforme a demanda. Esse é um serviço de alto valor e padrão corporativo que você pode oferecer sem grandes investimentos em infraestrutura ou pessoal.

5 Transforme a proteção em uma vantagem de confiança e seguro

Parceiros que adicionam o SonicSentry MDR junto com um firewall SonicWall e Cloud Threat Analytics se qualificam para cobertura de garantia cibernética incorporada de até US$ 1 milhão. Eles também se tornam imediatamente elegíveis para seguro cibernético com desconto e tarifa fixa por meio da parceria da SonicWall com a Cysurance. Ajudar clientes a atender requisitos de conformidade e seguro faz de você um parceiro estratégico, não apenas um fornecedor.

Segurança mais forte constrói relacionamentos mais sólidos

Lucratividade e confiança do cliente não são uma escolha: a mesma plataforma oferece ambos. Quando suas ferramentas são mais simples e confiáveis, seus clientes enfrentam menos incidentes, recebem respostas mais rápidas e contam com relatórios mais claros sobre a proteção pela qual estão pagando.

- **Menos surpresas:**
  A reversão de ransomware restaura arquivos criptografados indevidamente a partir de cópias de sombra do VSS, enquanto o isolamento do dispositivo contém as ameaças antes que elas se espalhem, ajudando a minimizar os danos causados por ataques.
- **Valor visível:**
  A busca de ameaças em tempo real e histórica, junto com relatórios unificados, permite mostrar aos clientes exatamente o que o investimento deles em segurança está proporcionando.
- **Confiança o tempo todo:**
  Com o SOC 24x7 opcional como parte do SonicSentry MDR, você e seus clientes podem ter tranquilidade sabendo que especialistas estão monitorando e mitigando ameaças mesmo enquanto vocês dormem.
- **Um nome que eles reconhecem:**
  O SonicWall Endpoint Security conta com mais de 30 anos de pesquisa em cibersegurança e é desenvolvido internamente, conferindo às suas recomendações uma credibilidade difícil de ser replicada.

Feito para a forma como os MSPs trabalham

O SonicWall Endpoint Security combina a tecnologia patenteada Real-Time Deep Memory Inspection (RTDMI) com detecção multimotor baseada em comportamento, bloqueando ameaças tanto antes quanto depois da execução. A telemetria avançada potencializa a busca histórica por ameaças, e tudo é gerenciado a partir do já conhecido console SonicWall Unified Management, que sua equipe já domina. Seja implantando como EDR independente ou integrando MDR totalmente gerenciado, a plataforma foi projetada para se adaptar aos seus fluxos de trabalho existentes — não para forçar você a reconstruí-los.

Pronto para aumentar suas margens e fortalecer relacionamentos?

Veja como o SonicWall Endpoint Security pode simplificar seu stack, abrir novas receitas e fortalecer a confiança que seus clientes depositam em você. **Fale com um representante da SonicWall hoje mesmo para ver a solução em ação.**

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 | Consulte nosso site para obter mais informações.

© 2026 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 especificados no contrato de licença deste produto, a SonicWall e/ou suas afiliadas não assumem nenhuma responsabilidade e rejeitam toda e qualquer garantia expressa, implícita ou legal relacionada aos seus produtos, incluindo, mas não se limitando, à garantia implícita de comercialização, adequação a um propósito específico ou não violação de direitos. 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.

Endpoint Security_MSP Profitability_SolutionBrief_12551

sonicwall.com

SONICWALL®