Serviço SonicWall Capture Advanced Threat Protection

Descubra e pare ataques do tipo zero-day e outros ataques desconhecidos

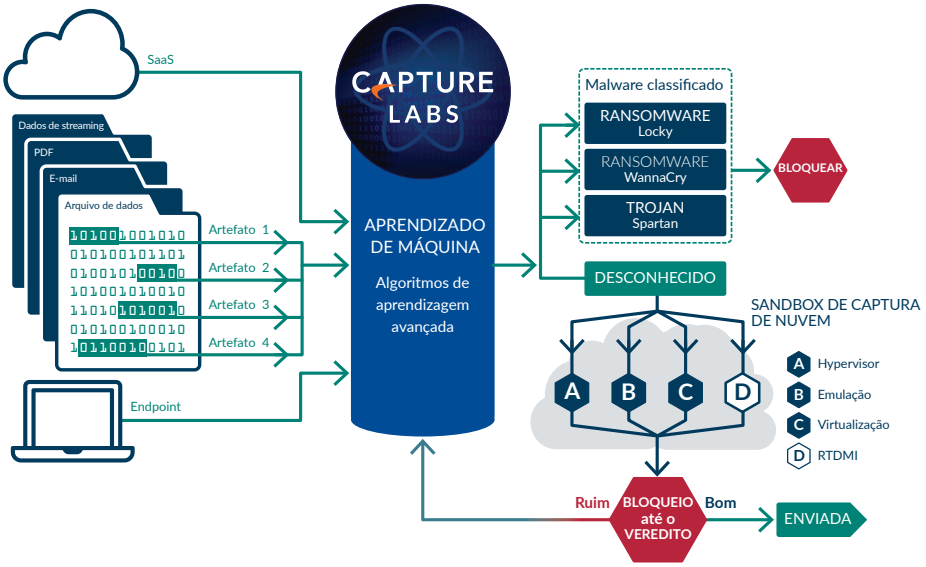
Para proteção eficaz contra ameaça zero-day, as organizações precisam de soluções que incluam tecnologias de análise de malware e que possam detectar ameaças avançadas evasivas e malware, hoje e futuramente.

Para proteger clientes contra os perigos cada vez maiores de ameaças zero-day, o Serviço SonicWall Capture Advanced Threat Protection (ATP), um serviço baseado em nuvem disponível com os firewalls SonicWall, detecta e pode bloquear ameaças avançadas no gateway até o veredito. Esse serviço é a única oferta de detecção de ameaça avançada que combina sandboxing de múltiplas camadas, inclusive Real-Time Deep Memory Inspection (RTDMI™) da SonicWall, emulação completa do sistema e técnicas de virtualização, para analisar o comportamento de código suspeito. Essa combinação eficiente detecta mais ameaças do que soluções de sandbox de mecanismo único, que são específicas do ambiente de computação e susceptíveis à evasão.

A solução verifica o tráfego e extrai o código suspeito para análise, mas diferentemente de outras soluções de gateway, analisa um grande intervalo de tamanhos e tipos de arquivos. A infraestrutura de threat intelligence global implementa rapidamente assinaturas de correção para ameaças recém-identificadas a todos os appliances de segurança de rede da SonicWall, o que evita a infiltração adicional. Os clientes se beneficiam da eficácia de alta segurança, tempos de resposta rápidos e custo total de propriedade reduzido.

Benefícios:

- Alta eficácia de segurança contra ameaças desconhecidas
- Implementação de assinatura praticamente em tempo real protege contra ataques futuros
- Redução do custo total de propriedade
- Bloqueio de arquivos no gateway até o veredito
- Múltiplos mecanismos processam arquivos em paralelo para vereditos rápidos
- O mecanismo RTDMI da SonicWall bloqueia malware desconhecido em grande escala ao utilizar técnicas de inspeção em tempo real baseadas em memória



Uma solução de múltiplos mecanismos baseada em nuvem para interromper ataques de zero-day e desconhecidos no gateway

Para melhor proteção contra ameaça zero-day, a solução é arquitetada para adicionar dinamicamente novas tecnologias de análise de malware à medida que o cenário de ameaça evolui.

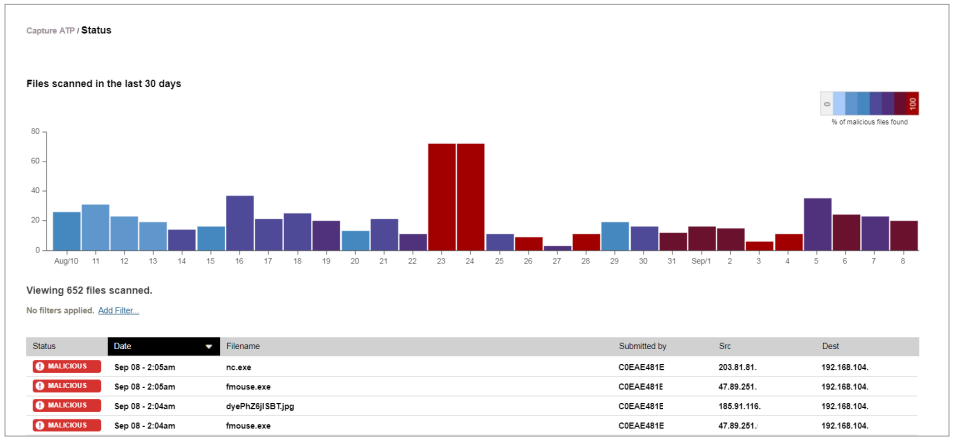
Recursos

Análise de ameaça avançada contra múltiplos mecanismos: o Serviço SonicWall Capture ATP estende a proteção contra ameaça ao firewall para detectar e evitar ataques do tipo zero-day. O firewall inspeciona o tráfego, detecta e bloqueia intrusões e malwares conhecidos. Os arquivos suspeitos são enviados à nuvem do SonicWall Capture ATP para análise. A plataforma de sandbox com múltiplos mecanismos, que inclui RTDMI, sandboxing virtualizado, emulação completa do sistema e tecnologia de análise no nível hypervisor, executa código suspeito, analisa o comportamento e fornece visibilidade abrangente da atividade mal-intencionada, ao mesmo tempo que resiste às táticas de evasão e maximiza a detecção de ameaça zero-day.

Real-Time Deep Memory Inspection (RTDMI): nossa tecnologia Real-Time Deep Memory Inspection com patente pendente aprimora o serviço Capture ATP com múltiplos mecanismos da SonicWall. O mecanismo RTDMI detecta e bloqueia de forma proativa malware em grande escala, de ameaças zero-day e desconhecido ao inspecionar a memória diretamente. Devido à arquitetura em tempo real, a tecnologia SonicWall RTDMI é precisa, minimiza falsos positivos e identifica e mitiga ataques sofisticados.

Análise ampla de tipo de arquivo: o serviço oferece suporte à análise de um amplo tamanhos e tipos de arquivos, inclusive programas executáveis (PE), DLL, PDFs, documentos MS Office, arquivos, JAR e APK, além de múltiplos sistemas operacionais, inclusive Windows e Android. Os administradores podem personalizar a proteção ao selecionar ou excluir arquivos para serem enviados à nuvem para análise por tipo de arquivo, tamanho de arquivo, remetente, destinatário ou protocolo. Além disso, os administradores podem enviar arquivos manualmente ao serviço de nuvem para análise.

Bloqueia até o veredito: para evitar que arquivos potencialmente mal-intencionados entrem na rede, os arquivos enviados ao serviço de nuvem para análise podem ser mantidos no gateway até um veredito final.



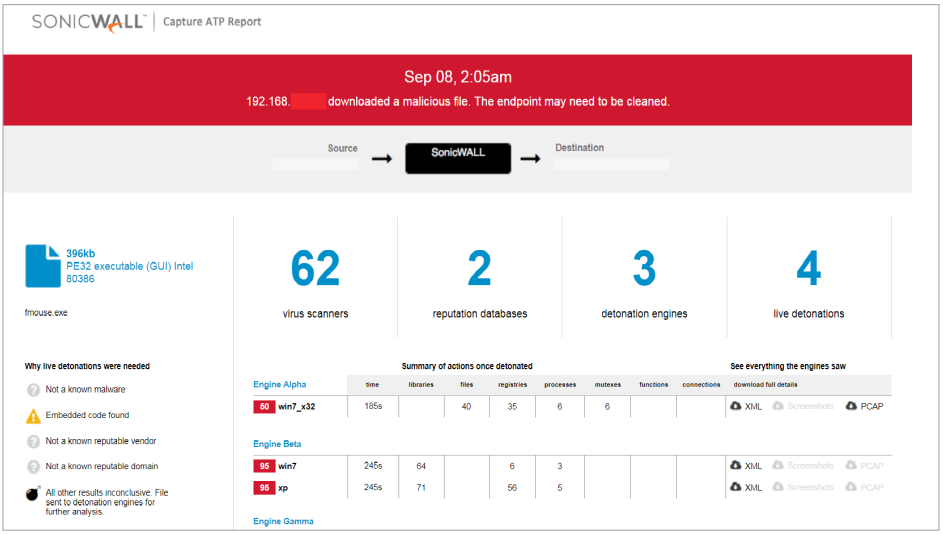
A página do relatório do SonicWall Capture ATP exibe resultados diários de visualização rápida. Barras coloridas no relatório indicam os dias em que o malware foi descoberto. Os administradores podem clicar em resultados diários individuais e aplicar filtros para ver rapidamente arquivos mal-intencionados com os resultados.

Implementação rápida de assinaturas de correção: quando um arquivo é identificado como mal-intencionado, é disponibilizada uma assinatura imediatamente para firewalls com SonicWall Capture ATP para evitar ataques posteriores. Além disso, o malware é enviado à equipe de pesquisa de ameaças do Laboratório SonicWall Capture para análise adicional e inclusão de informações da ameaça nos bancos de dados de assinatura de antivírus do gateway e de IPS. Além disso, ele é enviado aos bancos de dados de reputação de URL, de IP e de domínio no prazo de 48 horas.

Relatórios e alertas: o Serviço SonicWall Capture ATP fornece um painel de análise de ameaça de visualização rápida e relatórios que detalham os resultados de análises dos arquivos enviados ao serviço, inclusive fonte, destino e um resumo, além de detalhes de ação de malware após a detonação. Os alertas do registro de firewall fornecem notificação sobre arquivos suspeitos enviados ao Serviço SonicWall Capture ATP e veredito de análise dos arquivos.

Sobre nós

A SonicWall tem combatido o setor do crime cibernético por mais de 27 anos ao defender desde pequenas e médias empresas até grandes corporações mundialmente. Nossa combinação de produtos e parceiros possibilitou uma solução de defesa cibernética em tempo real ajustada às necessidades específicas de mais de 500.000 empresas em mais de 215 países e territórios, o que permite que você faça mais negócio com menos preocupações.



O relatório detalhado da análise também está disponível para arquivos analisados para facilitar a correção.

PLATAFORMAS COM SUPORTE

O Serviço SonicWall Capture ATP tem suporte nos firewalls a seguir da SonicWall que executam o SonicOS 6.2.6 e superiores:

NS*sp* 12800
NS*sp* 12400

NS*a* 9650
NS*a* 9450
NS*a* 9250
NS*a* 6650
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

Série TZ600
Série TZ500
Série TZ400
Série TZ300

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

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

DataSheet-CaptureAdvancedThreatProtection-US-VG-MKTG4093