E-BOOK

DESAFIOS NA SEGURANÇA DE ENDPOINTS

SONICWALL®

Introdução

O gerenciamento e a segurança de endpoints são críticos no clima empresarial atual. Com usuários finais que iniciam e encerram as sessões na rede usando dispositivos com vulnerabilidade sem patches de segurança e com ameaças criptográficas que chegam aos endpoints sem controle, os dispositivos devem ser protegidos tanto nos endpoints em si como na rede como um todo. Uma vez que ransomware e roubos de credenciais estão cada vez mais disseminados, endpoints se tornaram um campo de batalha no cenário atual de ameaças.

Apesar da grande quantidade de soluções no mercado atual, os administradores ainda têm dificuldades com a visibilidade e com o gerenciamento de seu sistema de segurança. Além disso, enfrentam o desafio de garantir segurança consistente ao cliente e, ao mesmo tempo, oferecer funções de inteligência e relatórios acionáveis e fáceis de usar. A seguir apresentaremos alguns dos desafios que você poderá encontrar quando formular sua estratégia de proteção de endpoints.

Soluções de segurança antiquadas

Os administradores têm que garantir que os endpoints estejam executando a versão correta dos componentes do software de segurança de acordo com a política de conformidade. Este problema se agrava ao se utilizarem soluções antivírus tradicionais baseadas em banco de dados com assinaturas atualizadas para se defender contra as últimas ameaças. Soluções de proteção avançada de endpoints (AEP) que atuam examinando o comportamento do sistema (heurística) são mais efetivas contra esses ataques e também conseguem bloquear scripts maliciosos, como os observados em ataques sem arquivos.

"91% das aplicações comerciais contêm componentes de código aberto antiquados ou abandonados"

Referência: Sinopse do relatório Open Source Security and Risk Analysis (OSSRA) 2020

SONICWALL®

Reforço de políticas e Conformidade na rede

Administradores encontram dificuldades para mitigar os riscos que surgem com os funcionários usando seus dispositivos em redes terceirizadas: em casa, nas lanchonetes, em hotéis ou aeroportos. Ao mesmo tempo enfrentam desafios no momento de reforçar a política da empresa sobre o uso da rede quando se está fora do escritório. Fora do lugar de trabalho, os funcionários estão mais propensos a acessar sites maliciosos e a visitar sites improdutivos. Se seus usuários transmitirem todos os seus dados pelo centro de dados corporativos via VPN, há a necessidade de limitar o conteúdo intenso de largura de banda, tais como vídeos. No início da pandemia, os administradores de rede reclamavam que suas redes estavam sendo inundadas por TikTok, YouTube, Netflix e outros serviços provenientes de streaming – e este problema continua crescendo à medida que a qualidade da imagem melhora e a confiança no uso desses aplicativos como entretenimento aumenta.

"30 a 40 por cento das atividades dos funcionários na internet não estão relacionadas ao trabalho"

Referência: Estudos IDC

SONICWALL®

Obtenção de relatórios e gerenciamento de acesso

Em alguns casos, os administradores podem gerenciar multitenants através de firewalls, mas seus usuários estão configurados em um único grupo. Isso complica a obtenção de um single-sign-on (SSO) de um administrador de firewall ou de um console de gerenciamento quando se tenta gerenciar as políticas de um cliente. Ao mesmo tempo, os regulamentos de conformidade impõem frequentemente que todas as funções de administradores sigam o princípio do privilégio mínimo. Assim um pacote de gerenciamento de cliente unificado que não consegue administrar os controles de acesso baseados em funções dará muitos problemas. Por exemplo, alguém pode estar limitado a duas funções; uma que tem acesso de leitura e escrita e outra somente com o de leitura.

Ameaças que vêm de canais criptografados

Com mais aplicações protegidas por canais criptografados, como HTTPS, e o malware também recorrendo à criptografia para burlar a inspeção baseada em rede, a inspeção profunda de tráfico SSL/TLS (DPI/SSL) se tornou extremamente necessária. No entanto, isto não ocorre facilmente sem a implementação em massa dos certificados de SSL/TLS em todos os endpoints confiáveis, para evitar experiência de usuário e problemas de segurança.

SONICWALL®

Entender alertas e passos para resolução

Geralmente os usuários finais são menos conscientes dos riscos de segurança do que os profissionais em segurança. Assim eles não entendem os alertas na maioria dos clientes de segurança de endpoints. Além do mais, a maioria dos clientes não inclui informações de autoajuda, o que faz com que ignorem o problema ou que recorram ao departamento de TI. Por exemplo, se o dispositivo do usuário não cumpre as políticas e ele está em quarentena, tal usuário não saberá quais as ações exigidas para voltar a cumprir as normas.

Gerenciamento de licenças

Um dos problemas de back-end do software de segurança de endpoints é que os administradores, especialmente no caso de MSSPs, não podem garantir que seu software esteja licenciado corretamente. Se as informações de licenças relacionadas aos clientes não forem monitoradas e armazenadas de maneira centralizada, podem haver interrupções e lacunas na segurança. Adicionalmente, os administradores podem ter dificuldades para executar relatórios de conformidade contra todas as licenças terceirizadas implementadas para pagar seus parceiros.

SONICWALL®

Parar as ameaças avançadas, tais como ransomware

Muitas vezes os enfoques tradicionais de segurança de endpoints podem deixar lacunas no cumprimento das exigências administrativas. A abordagem de longa data baseada em assinaturas das tecnologias antivírus tradicionais fracassou em acompanhar o desenvolvimento de malwares e das novas técnicas de evasão de malwares. Muitas soluções antigas não conseguem oferecer detecção avançada de ameaças e também não têm suporte para segurança em camadas nos endpoints, incluindo integração com o ambiente de sandboxing.

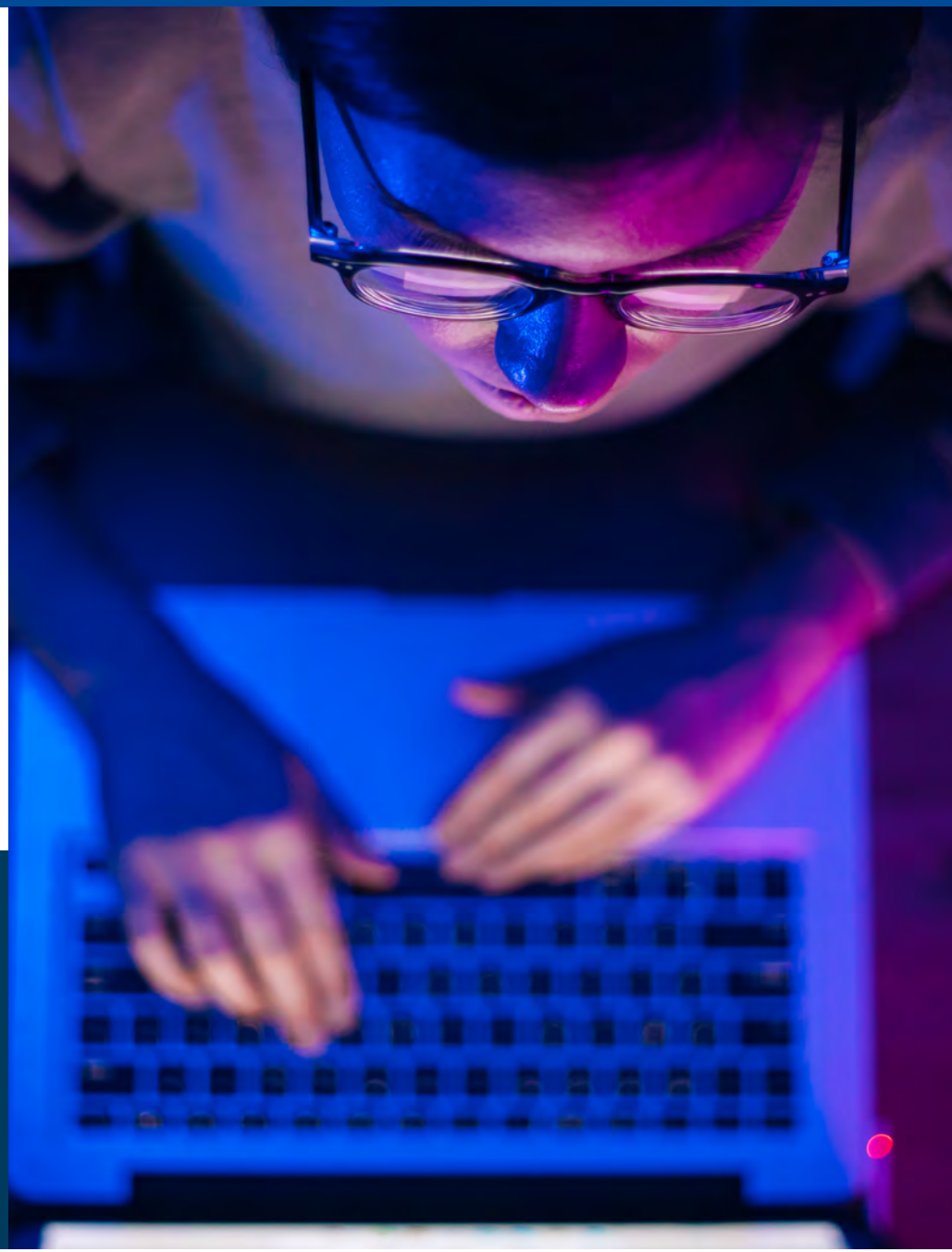
"No final do 3º trimestre de 2020, ransomware aumentou 40% em relação ao mesmo período de 2019."

Referência: Dados de Ameaças da SonicWall do 3º trimestre

SONICWALL®

Onde estão as vulnerabilidades críticas?

Com o grande aumento em aplicações empresariais, a ameaça de vulnerabilidades das aplicações tem crescido exponencialmente, dando dores de cabeça aos administradores de TI e resultando em falhas na segurança. Muitas organizações ainda não têm como identificar o número e a classificação das vulnerabilidades, o que dificulta a criação de um plano, tanto para fornecer patches como para desinstalar as aplicações de risco.



"Somente em 2019, as CNAs atribuíram pontuações CVSS críticas de 9,0+ a mais de 16.000 vulnerabilidades."

Referência: NIST National Vulnerability Database

Conclusão

Devido ao grande número de desafios potenciais, a elaboração de um plano de proteção de endpoints parece ser quase impossível, mas uma grande quantidade de recursos está disponível para simplificar o processo. Para identificar qual é a solução mais adequada à sua organização leia nosso resumo executivo, "O que os administradores devem buscar na hora de comprar uma solução de segurança de endpoints."

LEIA O RESUMO EXECUTIVO

SONICWALL®

Sobre SonicWall

A SonicWall fornece o modelo Boundless Cybersecurity na era da computação hiper distribuída em uma realidade de trabalho onde todos estão remotos, móveis e inseguros. SonicWall protege organizações que se mobilizaram conduzir os negócios “no novo normal” com proteção perfeita que impede a maioria dos ataques cibernéticos mais evasivos em pontos de exposição ilimitados e nas forças de trabalho cada vez mais remotas, móveis e habilitadas para a nuvem. Ao revelar ameaças ainda desconhecidas, fornecendo visibilidade em tempo real e, possibilitando a contínua inovação da economia, a SonicWall resolve as falhas na segurança cibernética para empresas, governos e SMBs em nível mundial. Para mais informações, visite www.sonicwall.com ou nos siga no Twitter, LinkedIn, Facebook e Instagram.

Se tiver dúvidas com relação ao possível uso deste material, contate:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Faça referência ao nosso website para informação adicional.
www.sonicwall.com