SONICWALL

RESUMO DE SOLUÇÃO: UMA ABORDAGEM UNIFICADA PARA GERENCIAR GOVERNANÇA, RISCO E CONFORMIDADE

Integrando o gerenciamento global da segurança de rede

Resumo

Uma abordagem conectada à orquestração, controle, análise e relatórios de segurança não é apenas fundamental para uma boa prática de segurança preventiva, mas também a base para uma estratégia unificada de governança, conformidade e gerenciamento de riscos de segurança.

Um quadro geral mais simples e coerente

A simplicidade na prática de gerenciamento de segurança promove melhor coordenação e decisões de segurança. Isso requer liberar a desordem e a rotina manual das operações diárias.

Uma das melhores maneiras de remover essas complexidades é utilizar o software de gerenciamento inteligente como base. Este software deve ser sistemático em seus métodos e fluxo de trabalho para reduzir o número de intervenções pessoais ao gerenciar o ambiente de segurança. Em vez de se esforçar para reagir quando os sistemas desenvolvem problemas ou quando são feitas alterações não autorizadas nas regras de firewall, o software inteligente reconhece e relata automaticamente esses tipos de riscos de segurança e ajuda a resolvê-los rapidamente.

Além disso, não ter um quadro geral coerente e abrangente de todo o ecossistema de segurança deixa as organizações em risco para ataques cibernéticos ou violações de conformidade evitáveis. A adoção dessa plataforma comum oferece a organizações de qualquer porte, incluindo empresas distribuídas e provedores de serviços, um insight mais profundo para tomar decisões de segurança mais informadas. Ele também permite que as equipes de segurança avancem e impulsionem a colaboração, a comunicação e o conhecimento em toda a estrutura de segurança compartilhada.

Gerenciamento integrado, seguro e extensível

Para simplificar e unificar, **uma solução ideal forneceria** uma arquitetura baseada em nuvem integrada, segura e extensível para gerenciar todo o portfólio de segurança. Essa plataforma de nuvem unificada permitiria que as equipes de segurança consolidassem facilmente o gerenciamento de dispositivos de segurança e federassem todos os aspectos operacionais da infraestrutura de segurança. Isso inclui o gerenciamento e a aplicação centralizados de políticas, monitoramento de eventos em tempo real, atividades de usuários, controle de aplicações, uso de dados, dados de drilldown e análise de fluxo, assim como análise forense, conformidade e auditoria, entre outros. Isso também atenderia aos requisitos de gerenciamento de mudança de firewall das empresas por meio de um recurso de automação de fluxo de trabalho.

Governança, conformidade e gerenciamento de riscos

Uma abordagem abrangente formaria a base para uma estratégia unificada de governança, conformidade e gerenciamento de riscos de segurança. Seria ideal estabelecer uma abordagem holística e conectada à orquestração de segurança para federar todos os aspectos operacionais do ecossistema de segurança de rede. Isso deveria simplificar e automatizar várias tarefas para promover uma melhor coordenação de segurança reduzindo a complexidade, o tempo e as despesas da execução de operações e administração de segurança. Tais tarefas incluem:

- Segurança e provisionamento de rede
- Aplicação de política
- Patching
- Descoberta de dispositivo
- Inventário
- Configuração e diagnóstico
- Monitoramento
- Geração de relatórios
- Análises
- Auditoria
- Coleta de estatísticas de segurança

Automação do fluxo de trabalho

O processo de fluxo de trabalho garante a correção e a conformidade das mudanças de política por meio de procedimentos rigorosos de validação e execução antes da implementação. Os grupos de aprovação devem ser flexíveis e estar em conformidade com as diretrizes de segurança de pessoal da empresa. Isso ajudará a reduzir riscos e erros, aperfeiçoar a eficiência e garantir alta eficácia na segurança. Com a automação adequada do fluxo de trabalho e a auditoria das mudanças de políticas, as equipes de segurança teriam a agilidade e a confiança de implantar as políticas de firewall corretas, no momento certo e em conformidade com os regulamentos de conformidade.

Implementação *zero touch*

Ao utilizar a nuvem, uma solução ideal simplificaria e aceleraria a implementação e o provisionamento de firewalls remotamente. Isso reduziria o tempo, o custo e a complexidade associados à configuração do dispositivo. Ao mesmo tempo, a segurança e a conectividade poderiam ocorrer de maneira instantânea e automática. Os administradores poderiam operacionalizar um grande número de firewalls em escala, com o mínimo de intervenção do usuário. De um único console de gerenciamento baseado na Web, por exemplo, pode-se enviar políticas, executar atualizações de firmware e sincronizar licenças.

Análises

Uma solução eficaz permitiria que a TI realizasse análises investigativas e forenses profundas de dados de segurança enriquecidos. Isso capacitaria as partes interessadas com visibilidade de painel único e conscientização situacional do ambiente de segurança de rede.

> As equipes de segurança devem ter agilidade e confiança na implantação das políticas corretas de firewall no momento certo e em conformidade com os regulamentos de conformidade.

Eles estariam capacitados a tomar decisões informadas sobre políticas de segurança baseado em informações de ameaças críticas e consolidadas no tempo. A TI poderia calibrar políticas e controles de segurança à medida que riscos e ameaças potenciais são descobertos. Como resultado, reduziria o tempo de resposta a incidentes com inteligência de ameaças acionável em tempo real.

Conclusão

Com a plataforma de gerenciamento de segurança baseada em nuvem correta, as organizações e os provedores de serviços podem estabelecer uma estratégia totalmente coordenada de governança de segurança, conformidade e gerenciamento de riscos. A plataforma correta também pode reduzir as despesas operacionais e as complexidades de suportar uma infraestrutura de propriedade exclusiva, proporcionando o máximo em visibilidade, agilidade e capacidade para controlar todo o ecossistema de segurança de rede SonicWall com maior clareza, precisão e velocidade - tudo em um só lugar.

Saiba como o Serviço do SonicWall Capture Security pode melhorar seus resultados em sonicwall.com/capture-security-center.

Sobre nós

A SonicWall tem combatido o setor do crime cibernético por mais de 25 anos, defendendo 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, em mais de 150 países, o que permite que você faça mais negócios com menos preocupações.

Se você tiver dúvidas sobre o possível uso deste material, entre em contato com:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Acesse o nosso site para obter mais informações.
www.sonicwall.com

SolutionBrief-AUnifiedApproach-US-KJ-MKTG2444