

POR QUE PROTEGER SUA FORÇA DE TRABALHO REMOTA COM ACESSO MÓVEL SEGURO É UM IMPERATIVO DA MISSÃO ESTRATÉGICA

O acesso móvel garante que as operações e serviços essenciais não sejam interrompidos em um mundo dinâmico e incerto

Resumo

Globalmente, a força de trabalho remota veio para ficar - e está crescendo. Os benefícios em agilidade, continuidade e produtividade tornam o acesso móvel seguro estrategicamente imperativo para as agências e departamentos governamentais de hoje. No entanto, para dar suporte eficaz a essa força de trabalho, a TI enfrenta vários desafios, incluindo uma explosão de endpoints, ameaças mais inteligentes e a necessidade de acessar recursos sensíveis, tudo isso enquanto opera com um orçamento enxuto.

Introdução

As manchetes de cada dia podem trazer desafios disruptivos que exigem soluções de tecnologia dinâmicas. Emergências de saúde pública; eventos naturais e as crises políticas podem restringir a equipe de viajar ou acessar recursos em um local físico. Para garantir a continuidade das atividades, as agências devem ter agilidade para conduzir as operações de qualquer lugar, a qualquer momento.

Mesmo quando não enfrentam pandemias, muitas agências buscam se beneficiar do aumento da produtividade da força de trabalho da equipe, bem como minimizar os custos operacionais de manutenção das instalações físicas do escritório, capacitando o pessoal para trabalhar com segurança de qualquer lugar, a qualquer hora.

Como resultado, as agências governamentais têm contado cada vez mais com o acesso remoto a recursos de dispositivos autorizados e BYOD fora de seus perímetros de rede tradicionais.

A cibersegurança eficaz deve incluir acesso móvel seguro

Fornecer acesso remoto em qualquer lugar / a qualquer hora, no mundo hiper distribuído de hoje, abre uma explosão de pontos de exposição em uma infinidade de dispositivos de endpoints móveis potencialmente inseguros.

A falibilidade humana e os riscos no comportamento on-line exigem que os funcionários não sejam confiáveis para garantir a segurança de seus próprios dispositivos móveis.

Além disso, a variedade de tipos de ameaças está se expandindo, se aprofundando e ficando mais inteligente, incluindo ransomware direcionado, ameaças nunca antes vistas, malware baseado em memória, ataques de canal lateral e ameaças criptografadas.

Em última análise, a segurança de sua rede remota deve corresponder à de sua rede com fio. Isso requer uma postura zero-trust em relação a qualquer dispositivo remoto que tente se conectar com recursos da agência, sejam esses recursos no local ou na nuvem. O acesso móvel seguro é um componente central de uma abordagem zero-trust para proteger o acesso em qualquer lugar e a qualquer hora.

A TI também deve proteger o acesso a partir desses endpoints móveis, com orçamentos limitados e recursos humanos qualificados. Isso significa agilizar a implantação, a disponibilidade e o suporte para reduzir o custo total de propriedade. Para ser eficaz, a cibersegurança deve fornecer aos funcionários remotos acesso fácil e seguro 24 horas por dia, 7 dias por semana, aos principais recursos das empresas públicas e privadas de forma ágil, fácil de usar, econômica e escalonável.

Conclusão

Seja para garantir a continuidade operacional ou aumentar a produtividade da força de trabalho, o acesso móvel seguro é uma necessidade. A solução SonicWall Secure Mobile Access (SMA) permite acesso seguro em qualquer lugar e a qualquer hora em operações hiper-distribuídas. Isso dá à sua agência a agilidade para permanecer operacional, independentemente do que as manchetes de amanhã possam trazer.

Saiba mais em www.sonicwall.com/products/remote-access.

A SonicWall é uma marca comercial ou marca registrada da SonicWall Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as outras marcas comerciais e marcas registradas são de propriedade dos respectivos proprietários.

As informações contidas neste documento são fornecidas em conexão com a SonicWall Inc. e/ou com os produtos de suas afiliadas. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a algum direito de propriedade intelectual é concedida por este documento ou em conexão com a venda de produtos da SonicWall. EXCETO CONFORME ESTABELECIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NO CONTRATO DE LICENÇA DESTE PRODUTO, A SONICWALL E/OU SUAS AFILIADAS NÃO ASSUMEM NENHUMA RESPONSABILIDADE E EXIMEM-SE DE TODA GARANTIA EXPRESSA, IMPLÍCITA OU JURÍDICA RELATIVA A SEUS PRODUTOS, ENTRE ELAS, A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA DETERMINADA FINALIDADE OU NÃO VIOLAÇÃO. EM NENHUMA CIRCUNSTÂNCIA A SONICWALL E/OU SUAS AFILIADAS SERÃO RESPONSÁVEIS POR PERDAS E DANOS,

MULTA COMPENSATÓRIA, DANOS EMERGENTES OU IMPREVISTOS (ENTRE ELAS, DANOS POR LUCROS CESSANTES, INTERRUPTÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) DECORRENTES DO USO OU DA IMPOSSIBILIDADE DE USO DESTE DOCUMENTO, MESMO QUE A SONICWALL E/OU SUAS AFILIADAS TENHAM SIDO INFORMADAS SOBRE A POSSIBILIDADE DE TAIS DANOS.

A SonicWall e/ou suas afiliadas não fazem declarações ou garantias quanto à exatidão ou à integridade do conteúdo deste documento e reservam-se o direito de fazer alterações às especificações e descrições de produtos a qualquer momento sem notificação prévia. A SonicWall Inc. e/ou suas afiliadas não assumem nenhum compromisso de atualizar as informações contidas neste documento.

Sobre a SonicWall

A SonicWall oferece Boundless Cybersecurity ou Cibersegurança sem Limites para a era da hiperdistribuição, em uma realidade de trabalho em que todos estão remotos, têm mobilidade e estão menos seguros. Com o conhecimento do desconhecido, a disponibilização de visibilidade em tempo real e a viabilização de uma economia disruptiva, a SonicWall fecha a lacuna de cibersegurança para corporações, governos e pequenas e médias empresas no mundo inteiro. Para obter mais informações, visite www.sonicwall.com.

Se você tiver alguma dúvida sobre o uso potencial deste material, entre em contato:

SonicWall, Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consulte nosso website para obter informações adicionais.
www.sonicwall.com/pt-br/