

Nessus Expert

 **Cherokee**
Segurança em todos os níveis



O Nessus Expert foi desenvolvido diretamente a partir da base do Nessus Professional e **inclui todas as funcionalidades do Nessus Professional**.

A diferença é que o Nessus Expert adiciona recursos que ampliam a capacidade de nossos clientes de resolver questões de segurança com a superfície de ataque moderna. À medida que a Tenable desenvolve tecnologias para lidar com mais desses ambientes, o Nessus Expert as implementará para permitir que os profissionais de segurança tenham uma ferramenta mais completa para avaliar vulnerabilidades contra uma variedade maior de superfícies de ataque.

Principais diferenças funcionais:

- O Nessus Expert oferece a capacidade de verificar infraestrutura como código (IaC). Isso permite que os clientes verifiquem os repositórios de código IaC para identificar quaisquer vulnerabilidades e violações de políticas antes da implementação.
- O Nessus Expert oferece a capacidade de realizar descoberta de superfície de ataque externa. Isso permite que o cliente verifique um domínio de nível superior e identifique todos os domínios filhos acessíveis pela Internet.

Resumindo, o Nessus Expert faz tudo o que o Nessus Professional faz e continuará a fazer mais para aumentar a lista de tipos de superfície de ataque que podem ser abordados pela ferramenta.

https://community.tenable.com/s/question/0D53a00009JTFo0CAH/the-difference-between-nessus-professional-and-nessus-expert?language=en_US



O Nessus tem sido o líder indiscutível na avaliação de vulnerabilidades. Com o lançamento do Nessus Expert, agora você pode proteger-se contra novas ameaças cibernéticas emergentes na infraestrutura de nuvem e entender o que está em sua superfície de ataque externa.

Quando se trata de IaC, o Nessus Expert permite que os usuários detectem programaticamente configurações incorretas e vulnerabilidades da infraestrutura de nuvem nas fases de projeto e criação do ciclo de vida de desenvolvimento de software.

Aproveitando as 500 políticas predefinidas, o Nessus Expert verifica arquivos de configuração e repositórios de código quanto a problemas de segurança e de configuração, antes da produção. Isso permite eliminar erros caros e demorados que possam surgir quando os desenvolvedores, inadvertidamente, enviam vulnerabilidades e configurações incorretas para a produção.

O Nessus Expert permite que os usuários:

- Identifiquem violações de política em pipelines automatizados;
- Aproveitem as 500 políticas predefinidas para verificação da IaC;
- Evitem que configurações incorretas e vulnerabilidades alcancem as instâncias de nuvem;
- Evitem o tempo de inatividade e os custos e recursos adicionais associados à correção do código após a implantação.
- O Nessus Expert também contém a funcionalidade de gerenciamento externo da superfície de ataque para descobrir e inventariar continuamente os ativos voltados para a Internet de uma organização do ponto de vista de um invasor. O Nessus Expert verifica perfeitamente os domínios para descobrir os subdomínios nos quais as equipes de segurança anteriormente tinham pouca ou nenhuma visibilidade. Essa funcionalidade permite aos usuários:
 - Verificação de até cinco domínios a cada 90 dias para entender todos os subdomínios associados;
 - Obter informações contextuais importantes sobre ativos voltados para a Internet, como detalhes de secure socket layer (SSL) das portas e informações do sistema de nomes de domínio (DNS);
 - Comprar domínios adicionais conforme necessário;
 - Iniciar facilmente uma verificação em ativos recém-identificados.

Visão geral dos recursos
















Características	Nessus Professional	Nessus Expert
Projetado para...	<i>Pentesters, consultores, PMEs</i>	<i>Pentesters, consultores, desenvolvedores e PMEs</i>
Atualizações de vulnerabilidades em tempo real	✓	✓
Verificação de vulnerabilidades	✓	✓
Verificação da superfície de ataque externa	X	✓ cinco domínios por trimestre
Possibilidade de adicionar domínios	X	✓
Verificação da infraestrutura de nuvem	X	✓
Auditorias de conformidade da infraestrutura de nuvem	X	500 políticas predefinidas

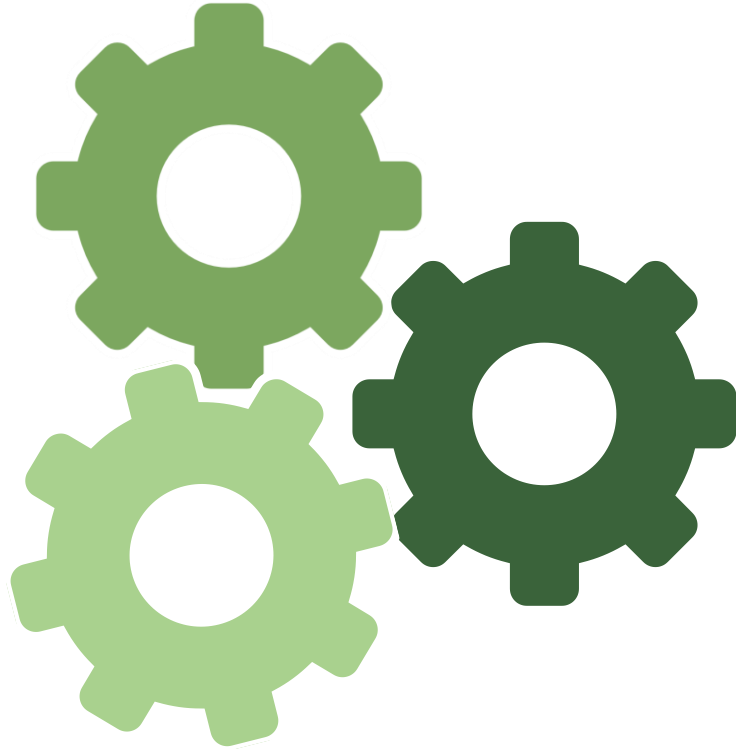
<https://pt-br.tenable.com/blog/introducing-nessus-expert-now-built-for-the-modern-attack-surface>

Comparativo



		
Designed for	Pentesters, consultants, and SMB's	Pentesters, consultants, developers, and SMB's
Real-time vulnerability updates		
Vulnerability scanning		
External attack surface scanning		 5 domains per quarter
Ability to add domains		
Scan cloud infrastructure		
Compliance audits of cloud infrastructure		500 prebuilt policies

<https://s4applications.uk/nessus-pro-vs-nessus-expert-what-is-the-difference/>



Nessus Expert

DataSheet-Nessus_Professional_pt-br,
em anexo

Nessus Pro

Datasheet-Nessus-Expert_pt-br,
em anexo

CONTATO

cherokee.com.br



Rogério Gomes

rogerio.gomes@cherokee.com.br

fone +55 11 97426-6587

Ulisses Donato

ulisses.donato@cherokee.com.br

fone +55 11 96461-0029



NESSUS EXPERT

DESENVOLVIDO PARA A SUPERFÍCIE DE ATAQUE MODERNA

A forma como pensamos hoje sobre a superfície de ataque mudou drasticamente desde 1998, quando o Nessus foi lançado no mercado. Agora, os profissionais, assim como os agentes de ameaças, são desafiados a pensar de forma mais ampla. No caso dos profissionais, precisam pensar em como proteger a organização em um mundo de vulnerabilidades e explorações ilimitadas.

Profissionais de segurança, consultores, desenvolvedores e pentesters precisam de uma solução de avaliação de vulnerabilidades que aborde ameaças que afetam a crescente superfície de ataque. Estão surgindo novos vetores de ataque que vão muito além dos ativos de TI tradicionais, como infraestrutura da nuvem e ativos díspares, que são externos e desconhecidos para a organização.

MAIS FERRAMENTAS PARA O SEU KIT DE AVALIAÇÃO

O Nessus é o verificador de vulnerabilidades mais reconhecido do setor e o Nessus Expert se baseia nesse legado, tornando-se a primeira solução de avaliação de vulnerabilidades para obter visibilidade de toda a superfície de ataque moderna. O Nessus Expert é uma expansão do Nessus Professional para entender os riscos que estão além dos ativos de TI tradicionais. Ele faz uma avaliação das implementações de infraestrutura como código (IaC) e descobre ativos expostos à internet — tudo em um só lugar.

AMPLITUDE E PROFUNDIDADE DE COBERTURA

A Tenable Research trabalha em estreita colaboração com a comunidade de segurança para descobrir novas vulnerabilidades e apresentar perspectivas que ajudem as organizações a consolidar suas práticas de avaliação de vulnerabilidades. A equipe de dia zero da Tenable descobriu mais de 100 vulnerabilidades de dia zero nos últimos três anos.

O NESSUS É O N.º 1 EM AVALIAÇÃO DE VULNERABILIDADES

N.º 1 em precisão

O Nessus apresenta a menor taxa de falsos positivos do setor, com precisão Six Sigma (com 0,32 defeito a cada 1 milhão de verificações).

N.º 1 em cobertura

O Nessus tem a mais profunda e ampla cobertura para mais 62 mil CVEs e mais de 100 novos plug-ins lançados por semana em até 24 horas após a divulgação da vulnerabilidade.

N.º 1 em adoção

O Nessus tem a confiança de mais de 30 mil organizações no mundo todo, incluindo 2 milhões de downloads. Cinquenta por cento (50%) das empresas da Fortune 500 e mais de 30% da Global 2000 confiam na tecnologia do Nessus.

DESCUBRA E AVALIE SEUS ATIVOS DE TI

+

PROTEJA A INFRAESTRUTURA DA NUVEM ANTES DA IMPLEMENTAÇÃO

+

OBTENHA VISIBILIDADE DA SUPERFÍCIE DE ATAQUE VOLTADA À INTERNET

TESTE ANTECIPADO (SHIFT LEFT) E PROTEÇÃO DA INFRAESTRUTURA DA NUVEM

Com o surgimento de infraestrutura e serviços na nuvem, a implementação de novas aplicações e cargas de trabalho pode ser simples. Mas, junto com a velocidade e a agilidade, surgem riscos cibernéticos adicionais e desconhecidos nesses ambientes. Existem soluções projetadas para proteger a nuvem, mas elas são aplicadas tarde demais. O Nessus Expert permite que você verifique os repositórios de código da IaC antes de enviar para a produção para prevenir riscos desconhecidos.

PRINCIPAIS BENEFÍCIOS:

- Estabelecer uma abordagem proativa para a avaliação de vulnerabilidades de cargas de trabalho na nuvem;
- Descobrir problemas de segurança desconhecidos, que fazem parte do ciclo de vida de desenvolvimento de software (SDLC);
- Verificar vulnerabilidades disruptivas e dispendiosas **antes** que o código seja implementado.

OBTENHA VISIBILIDADE DA SUPERFÍCIE DE ATAQUE VOLTADA À INTERNET

A superfície de ataque moderna é composta por ativos voltados à internet que, no geral, são desconhecidos devido à falta de controles de inventário e à capacidade dos desenvolvedores de ativar instâncias da nuvem em questão de minutos. Sob a perspectiva de um invasor, os ativos voltados à internet são uma forma simples, porém furtiva, de investigar vulnerabilidades e se infiltrar na rede, especialmente quando não se sabe a quem eles estão expostos ou nem se sabe que eles existem. O Nessus Expert permite que você descubra e avalie esses ativos desconhecidos.

PRINCIPAIS BENEFÍCIOS:

- Descobrir ativos conectados à internet antes desconhecidos para a organização;
- Iniciar verificações de avaliação de ativos recém-identificados;
- Entender o risco e fechar a lacuna para ativos fora do seu perímetro.

APROVEITE O PODER DA PRIORIZAÇÃO PREDITIVA

Tire proveito do Vulnerability Priority Rating (VPR) da Tenable para focar nas vulnerabilidades que representam o maior risco específico do seu ambiente. O VPR combina os dados de vulnerabilidades coletados pela Tenable com os dados de vulnerabilidades e ameaças de terceiros e faz uma análise deles usando o algoritmo avançado de ciência de dados desenvolvido pela Tenable Research.

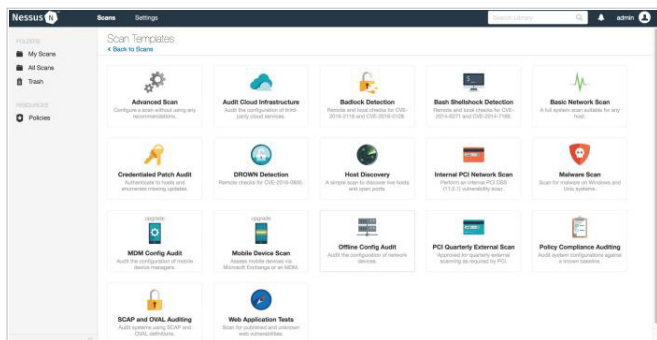
FACILIDADE DE USO

Construído para profissionais de segurança por profissionais de segurança, o Nessus foi criado com um único objetivo: oferecer uma experiência intuitiva para que os profissionais de segurança das linhas de frente encontrem e corrijam as vulnerabilidades com mais rapidez e confiança.

Atualizações na experiência do usuário deixaram a navegação e o processo mais fáceis e intuitivos. O novo centro de recursos do Nessus fornece aos usuários informações relevantes na palma de suas mãos. Guias específicos para o usuário fornecem dicas e orientações práticas com base nas operações e nas funções que estão sendo executadas.

Veja vulnerabilidades rapidamente com políticas e modelos pré-construídos

Modelos pré-configurados e prontos para uso para ativos móveis e de TI, incluindo auditoria de configurações, ajudam você a entender rapidamente onde estão suas vulnerabilidades.



Mais de 450 modelos de conformidade e configuração permitem que você audite a conformidade da configuração com as referências da CIS e outras práticas recomendadas.

Avaliação inteligente de vulnerabilidades com o Live Results

O Live Results faz uma avaliação inteligente de vulnerabilidades em modo off-line em cada atualização de plug-in, sem precisar fazer uma verificação. Basta fazer login e ver os resultados de possíveis vulnerabilidades com base no seu histórico de verificações. Com apenas um clique, você pode executar uma verificação para validar a presença da vulnerabilidade, criando um processo mais rápido e eficiente de avaliar, priorizar e corrigir problemas.

Configure relatórios facilmente

Crie relatórios baseados em exibições personalizadas (ex.: tipos específicos de vulnerabilidades, vulnerabilidades por host/plugin, por equipe/cliente) em diversos formatos (HTML, CSV e Nessus XML).

Exploração e resolução de problemas

Conforme as redes tornam-se mais complexas e sofisticadas, focar em possíveis problemas toma cada vez mais tempo. O recurso de captura de pacotes do Nessus alimenta um poderoso recurso de depuração para solucionar problemas de verificação.

Foco total com a exibição agrupada

Problemas ou categorias semelhantes de vulnerabilidades são agrupados e apresentados em um thread. A suspensão permite que os usuários selecionem problemas para que não sejam mais exibidos por um período de tempo especificado. Isso ajuda na priorização, permitindo que você se concentre apenas nos problemas em que está trabalhando em um determinado momento.

Portátil e flexível

Para fins de portabilidade e facilidade de uso, o Nessus agora está disponível no Raspberry Pi, o que é especialmente útil para pentesters, consultores e outras pessoas cuja função exige mobilidade entre locais.

DISPONIBILIDADE DE SUPORTE AVANÇADO

Os clientes do Nessus Professional podem acessar o suporte por e-mail, portal, bate-papo e telefone 24 horas por dia, 365 dias por ano, com uma assinatura de suporte técnico de nível avançado. Isso também ajuda a garantir um tempo de resposta e resolução mais curto. Os detalhes completos dos planos de suporte podem ser encontrados [aqui](#).

SOBRE A TENABLE

A Tenable®, Inc. é a empresa de Cyber Exposure. Mais de 30 mil organizações no mundo todo contam com a Tenable para entender e reduzir o risco cibernético. Como criadora do Nessus®, a Tenable ampliou sua experiência em vulnerabilidades para oferecer a primeira plataforma do mundo para verificar e proteger qualquer ativo digital em qualquer plataforma computacional. Entre os clientes da Tenable, estão mais de 50% das empresas da Fortune 500, mais de 30% das empresas da Global 2000 e agências governamentais de grande porte. Saiba mais em pt-br.tenable.com.

Para mais informações: acesse pt-br.tenable.com

Fale conosco: envie um e-mail para sales@tenable.com

ou acesse pt-br.tenable.com/contact



NESSUS PROFESSIONAL

O PADRÃO DO SETOR PARA A AVALIAÇÃO DE VULNERABILIDADES

Recursos escassos, tempo limitado, uma superfície de ataque em constante mudança. Para os profissionais de segurança das linhas de frente, é um desafio acompanhar o ritmo dos invasores. Você precisa de uma forma fácil e rápida de localizar e corrigir vulnerabilidades de forma proativa.

O Nessus® Professional automatiza avaliações pontuais para ajudar a identificar e corrigir vulnerabilidades rapidamente, incluindo falhas de software, falta de patches, malware e configurações incorretas em vários sistemas operacionais, dispositivos e aplicações.

O NESSUS É O N.º 1 EM AVALIAÇÃO DE VULNERABILIDADES

N.º 1 em precisão

O Nessus apresenta a menor taxa de falsos positivos do setor, com precisão Six Sigma (com 0,32 defeito a cada 1 milhão de verificações).

N.º 1 em cobertura

O Nessus tem a mais profunda e ampla cobertura, com mais de 62 mil CVEs e mais de 100 novos plug-ins lançados por semana em até 24 horas após a divulgação da vulnerabilidade.

N.º 1 em adoção

O Nessus tem a confiança de mais de 30 mil organizações no mundo todo, incluindo 2 milhões de downloads. Cinquenta por cento (50%) das empresas da Fortune 500 e mais de 30% da Global 2000 confiam na tecnologia do Nessus.

AMPLITUDE E PROFUNDIDADE DE COBERTURA

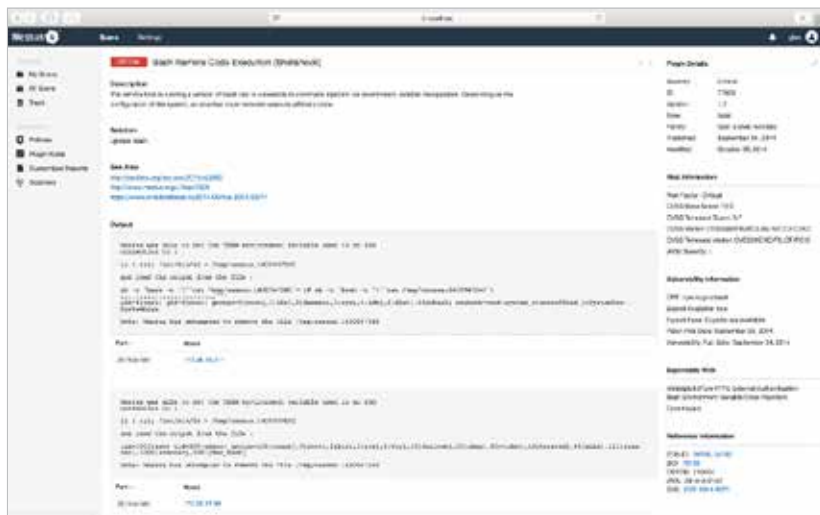
A Tenable Research trabalha em estreita colaboração com a comunidade de segurança para descobrir novas vulnerabilidades e apresentar perspectivas que ajudam as organizações a consolidar suas práticas de avaliação de vulnerabilidades. A equipe de dia zero da Tenable descobriu mais de 100 vulnerabilidades de dia zero nos últimos três anos.

ATUALIZAÇÕES AUTOMÁTICAS E DINÂMICAS DE PLUG-INS DIMINUEM O TEMPO PARA AVALIAR E CORRIGIR

Com mais de 157 mil plug-ins atualizados automaticamente em tempo real, o Nessus ajuda você a economizar um valioso tempo para avaliar, pesquisar e corrigir problemas.

Com o objetivo de oferecer eficiência e precisão, os plug-ins são compilados dinamicamente, o que reduz a base do banco de dados de plug-ins do Nessus em até 75%, ao mesmo tempo em que aumenta o desempenho da verificação.

- Plug-ins personalizados permitem a criação de verificações específicas para avaliar a segurança de aplicações exclusivas da sua organização.
- Arquivos de auditoria personalizados ajudam você a verificar os requisitos de configuração e os padrões de conformidade da sua organização.



"Interface bem organizada, que classifica plug-ins de forma clara, ordenada e estruturada."

– Usuário do Nessus

OS CONSULTORES ADORAM O NESSUS

O Nessus é ideal para consultores de segurança porque oferece:

- **Avaliações ilimitadas:**
Não há limite de quantidade de IPs nem avaliações.
- **Licenças de fácil transferência**
Transfira sua licença com rapidez e facilidade entre computadores. Aproveite a opção do Nessus no Raspberry Pi para alta portabilidade e facilidade de uso.
- **Relatórios personalizáveis**
Personalize facilmente os relatórios com o nome e o logotipo do cliente. Envio de e-mails diretamente para o cliente após cada avaliação.

Cada atualização automática de [plug-ins](#) apresenta um conjunto simples de ações de correção e uma forma rápida e fácil de verificar se os seus sistemas estão vulneráveis.

Perspectivas através de feeds de threat intel

Obtenha informações sobre malware e ransomware possivelmente em execução em hosts de todo o seu ambiente por meio de uma integração simples com diversos feeds de threat intel comercial.

APROVEITE O PODER DA PRIORIZAÇÃO PREDITIVA

Tire proveito da Vulnerability Priority Rating (VPR) da Tenable para ajudar você a identificar as vulnerabilidades que representam o maior risco específico para o seu ambiente. A VPR combina os dados de vulnerabilidades coletados pela Tenable com os dados de vulnerabilidades e ameaças de terceiros e faz uma análise usando o algoritmo avançado de ciência de dados desenvolvido pela Tenable Research.

Visibilidade ampla e profunda das vulnerabilidades

Obtenha visibilidade ampla e profunda de vulnerabilidades em todas as avaliações. O Nessus oferece cobertura para mais de 47 mil ativos exclusivos de TI, incluindo:

- Dispositivos de rede (ex.: Cisco, Juniper, HP, F5 e SonicWall);
- MobileIron e VMware AirWatch para avaliar vulnerabilidades contra as políticas em dispositivos móveis;
- Sistemas operacionais (ex.: Windows, MacOS e Linux);
- Aplicações que variam de pequenos utilitários de atualização de unidades a conjuntos complexos de produtividade do Office.

FACILIDADE DE USO

Desenvolvido para profissionais de segurança por profissionais de segurança, o Nessus foi criado com um único objetivo: oferecer uma experiência intuitiva para que os profissionais de segurança das linhas de frente encontrem e corrijam as vulnerabilidades com mais rapidez e confiança.

Atualizações de UX deixaram a navegação e a experiência do usuário mais fáceis e intuitivas. A nova central de recursos do Nessus oferece aos usuários informações relevantes na palma de suas mãos. Os guias específicos do usuário mostram dicas e orientações práticas com base nas operações e nas funções que estão sendo executadas.

Veja vulnerabilidades rapidamente com políticas e modelos pré-construídos

Modelos pré-configurados e prontos para uso para ativos móveis e de TI, incluindo auditoria de configurações, ajudam você a entender rapidamente onde estão suas vulnerabilidades.



Mais de 450 modelos de conformidade e configuração permitem que você audite a conformidade da configuração com as referências da CIS e outras práticas recomendadas.

Avaliação inteligente de vulnerabilidades com o Live Results

O Live Results faz uma avaliação inteligente de vulnerabilidades em modo off-line em cada atualização de plug-in, sem ter que fazer uma verificação. Basta fazer login e ver os resultados de possíveis vulnerabilidades com base no seu histórico de verificações. Com apenas um clique, você pode executar uma verificação para validar a presença da vulnerabilidade, criando um processo mais rápido e eficiente para avaliar, priorizar e corrigir problemas.

Configure relatórios facilmente

Crie relatórios baseados em visualizações personalizadas (ex.: tipos específicos de vulnerabilidades, vulnerabilidades por host/plug-in, por equipe/cliente) em diversos formatos (HTML, CSV e Nessus XML).

Aprofunde-se e solucione problemas

Conforme as redes se tornam mais complexas e sofisticadas, concentrar-se nos possíveis problemas é algo que toma cada vez mais tempo. O recurso de captura de pacotes do Nessus oferece um potente recurso de depuração para solucionar problemas de verificação.

Foco total com a visualização agrupada

Problemas ou categorias semelhantes de vulnerabilidades são agrupados e apresentados em um thread. A suspensão permite que os usuários selecionem problemas para desaparecer da exibição por um período de tempo especificado. Isso ajuda na priorização, permitindo que você se concentre apenas nos problemas em que está trabalhando em um determinado momento.

Portátil e flexível

Em busca de portabilidade e facilidade de uso, agora o Nessus está disponível no Raspberry Pi, o que é especialmente útil para pentesters, consultores e outros profissionais cuja função requer mobilidade entre os locais.

SUORTE AVANÇADO DISPONÍVEL

Os clientes do Nessus Professional podem acessar o suporte por e-mail, portal, bate-papo e telefone 24 horas por dia, 365 dias por ano, com uma assinatura de suporte técnico de nível avançado. Isso também ajuda a garantir um tempo mais curto de resposta e resolução. Detalhes completos sobre os planos de suporte podem ser encontrados [aqui](#).

SOBRE A TENABLE

A Tenable®, Inc. é a empresa de Cyber Exposure. Mais de 30 mil organizações no mundo todo contam com a Tenable para entender e reduzir o risco cibernético. Como criadora do Nessus®, a Tenable ampliou sua experiência em vulnerabilidades para oferecer a primeira plataforma do mundo para verificar e proteger qualquer ativo digital em qualquer plataforma computacional. Entre os clientes da Tenable, estão mais de 50% das empresas da Fortune 500, mais de 30% das empresas da Global 2000 e agências governamentais de grande porte. Saiba mais em www.pt-br.tenable.com.

Para mais informações: acesse pt-br.tenable.com

Fale conosco: envie um e-mail para sales@tenable.com

ou acesse pt-br.tenable.com/contact

