IBM Tivoli Endpoint Manager for Security and Compliance

Uma solução única para o gerenciamento da segurança de terminais em toda a organização

Destaques

- Forneça visibilidade e controle atualizados a partir de um único console de gerenciamento
- Utilize um único agente multiuso e inteligente que avalia e corrige os problemas para garantir a segurança e a conformidade de forma contínua
- Gerencie centenas de milhares de terminais, físicos e virtuais, independentemente da localização, tipo de conexão ou status
- Gerencie automaticamente os patches em múltiplos sistemas operacionais e aplicativos

Em um mundo onde o número de terminais e as ameaças que podem comprometê-los crescem em um ritmo sem precedentes, o IBM Tivoli Endpoint Manager for Security and Compliance oferece visibilidade unificada, em tempo real e reforço para a proteção do seu ambiente complexo e altamente distribuída.

Desenvolvido para garantir a segurança dos terminais em toda a organização, o Tivoli Endpoint Manager for Security and Compliance pode auxiliar sua organização a proteger os terminais e assegurar aos reguladores que você está cumprindo as normas de segurança. Ele proporciona uma solução de fácil gerenciamento e de rápida implementação que suporta a segurança em um ambiente que pode incluir uma grande variedade e uma grande quantidade de terminais – de servidores a desktops, laptops conectados à Internet em "roaming" e equipamentos especializados como dispositivos de PDV (ponto de venda), caixas eletrônicos e quiosques de autoatendimento.

O Tivoli Endpoint Manager for Security and Compliance pode reduzir os custos e a complexidade do gerenciamento de TI, pois aumenta a agilidade dos negócios, a velocidade de correção e a precisão. Seu baixo impacto sobre as operações de terminais pode aumentar a produtividade e aperfeiçoar a experiência do usuário. Por meio de um constante reforço de política de conformidade onde atuam os terminais, o Tivoli Endpoint Manager for Security and Compliance auxilia na redução dos riscos e no aumento da visibilidade da auditoria para uma conformidade contínua.

Atendendo às necessidades de segurança em toda a organização

O Tivoli Endpoint Manager for Security and Compliance enfrenta os desafios de segurança em ambientes distribuídos e de desktop. Ao fornecer gerenciamento de terminais e de segurança em uma única solução, garante proteção e conformidade contínuas. Por exemplo, ele pode diminuir drasticamente as lacunas nas exposições de segurança em questão de minutos, utilizando os patches de software. Pode também auxiliar na resolução da lacuna entre as funções, como as que estabelecem e executam a estratégia e a política, as que gerenciam os dispositivos em tempo real e aquelas que geram relatórios sobre questões de segurança e conformidade.

Entre os recursos do Tivoli Endpoint Manager for Security and Compliance está sua capacidade em:

- Proporcionar uma visibilidade precisa, exata e atualizada, além de um reforço contínuo das configurações de segurança e dos patches.
- Centralizar o gerenciamento de antimalwares de terceiros e de proteção de firewall.
- Fornecer as melhores práticas prontas para uso que atendam às regulamentações da FDCC (U.S. Federal Desktop Configuration Control) e da DISA STIGs (Defense Information Systems Agency Security Technical Implementation Guides).
- Suportar SCAP (Security Content Automation Protocol); o Tivoli Endpoint Manager é o primeiro produto certificado pelo NIST (National Institute of Standards and Technology) para avaliações e correções.
- Transmitir com segurança as instruções de terminais de acordo com NIAP CCEVS EAL3 e FIPS 104-2, certificações de Nível 2.
- Suportar o padrão OVAL (Open Vulnerability and Assessment Language) para promover a segurança de conteúdo aberto e publicamente disponível.
- Receber e atuar nos alertas de vulnerabilidade e de risco de segurança divulgados pelo SANS Institute.
- Mostrar a tendência e a análise das mudanças de configuração de segurança através de relatórios avançados.

Os recursos adicionais fornecidos para todos os produtos da família Tivoli Endpoint Manager, desenvolvidos com tecnologia BigFix, possuem a capacidade de:

- Descobrir os terminais dos quais as organizações não estavam cientes de que estavam em seu ambiente – até 30% a mais em alguns casos.
- Fornecer um único console para funções de gerenciamento, configuração, descoberta e segurança, simplificando as operações.
- Direcionar ações específicas para um determinado tipo de configuração de terminal ou de usuário, além de utilizar praticamente qualquer hardware ou software proprietário para isso.
- Utilizar uma infraestrutura unificada de gerenciamento de coordenação entre as operações de TI, segurança, desktop e servidor.
- Alcançar os terminais, independentemente da localização, tipo de conexão ou status com um gerenciamento abrangente de todos os principais sistemas operacionais, aplicativos de terceiros e patches baseados em políticas.

O Tivoli Endpoint Manager for Security and Compliance possibilita processos automatizados e altamente direcionados que fornecem controle, visibilidade e velocidade para realizar alterações e gerar relatórios sobre a conformidade. Os ciclos de correção são curtos e rápidos e os problemas de malware e de vírus são resolvidos com recursos de gerenciamento de patch rápido.

Entregando uma ampla gama de funções de segurança eficientes

O Tivoli Endpoint Manager for Security and Compliance possui as funções essenciais a seguir e fornece a você a capacidade de adicionar facilmente outras funções específicas, conforme a necessidade, sem aumentar os custos de infraestrutura ou de implementação.

Gerenciamento de patch

O gerenciamento de patch possui recursos abrangentes para o fornecimento de patches para Microsoft® Windows®, UNIX®, Linux® e Mac OS e para fornecedores de aplicativos como Adobe®, Mozilla, Apple e Java™ para terminais distribuídos, independentemente da sua localização, tipo de

conexão ou status. Um único servidor de gerenciamento pode suportar até 250 mil terminais, reduzindo os períodos para patches sem perda de funcionalidade do terminal, mesmo em redes com baixa largura de banda ou globalmente distribuídas . Relatórios em tempo real fornecem informações sobre quais patches foram implementados, quando foram implementados e quem os implementou, bem como a confirmação automática de que os patches foram implementados em uma solução completa não segmentada para o processo de correção.

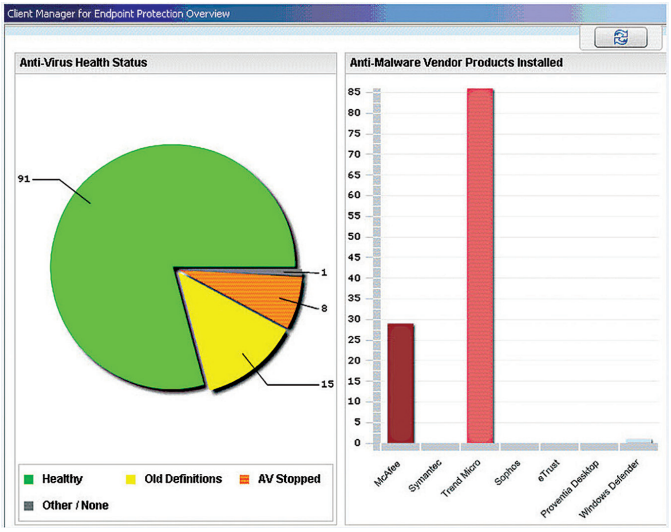
Gerenciamento de configuração de segurança

Validados pelo National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia), os recursos da configuração de segurança da solução oferecem uma biblioteca abrangente de controles técnicos que podem ajudá-lo a atingir a conformidade de segurança, detectando e reforçando as configurações de segurança. As bibliotecas de política suportam o reforço contínuo das linhas de base de configuração; relatam, corrigem e confirmam a correção da não conformidade de terminais em tempo real e asseguram uma visão verificada em tempo real de todos os terminais.

Esse recurso fornece informações importantes sobre a integridade e a segurança dos terminais, independentemente da localização, sistema operacional, conexão (inclusive computadores desktop ou laptops conectados à internet móvel irregularmente), ou ainda aplicativos instalados. Auxilia na consolidação e na unificação do ciclo de vida da conformidade, reduzindo os períodos de configuração e de correção.

Gerenciamento da vulnerabilidade

O gerenciamento da vulnerabilidade permite que você descubra, avalie e corrija as vulnerabilidades antes que os terminais sejam afetados. O recurso avalia os sistemas em relação às definições padronizadas de vulnerabilidade OVAL (open source security language) e aos relatórios em tempo real sobre as políticas de não conformidade. O resultado é a visibilidade aperfeiçoada e a integração completa em todos os estágios do fluxo de trabalho: descobrir – avaliar – corrigir – relatar.



O Tivoli Endpoint Manager for Security and Compliance fornece relatórios que auxiliam as organizações a visualizar os problemas que afetam a eficiência dos esforços de segurança e de conformidade.

A equipe de TI pode identificar e eliminar, utilizando ações automatizadas ou manuais, as vulnerabilidades conhecidas em todos os terminais. Ao utilizar uma única ferramenta para descobrir e eliminar as vulnerabilidades, os administradores podem aumentar a velocidade e a precisão, reduzindo os ciclos de implantação de patch, atualizações de software e correções de vulnerabilidade. Os administradores podem ampliar o gerenciamento de segurança para clientes móveis dentro ou fora da rede, configurando alarmes para identificar rapidamente os recursos com problemas e tomar medidas para localizá-los para correção ou remoção.

Descoberta de ativo

Com o Tivoli Endpoint Manager for Security and Compliance, a descoberta de ativo não é mais um exercício instantâneo minucioso. Ele cria uma consciência situacional dinâmica sobre a mudança das condições da infraestrutura. A capacidade de sondar frequentemente toda a rede proporciona visibilidade e controle abrangentes, e garante que as organizações identifiquem rapidamente todos os dispositivos com endereço IP (máquinas virtuais, dispositivos de rede e periféricos como impressoras, scanners, roteadores e switches, além de terminais de computador) com um impacto mínimo na rede. Essa função auxilia na manutenção da visibilidade em todos os terminais da empresa, incluindo computadores laptops e notebooks móveis em roaming fora da rede corporativa.

Gerenciamento de proteção de terminal multifornecedor

Este recurso dá aos administradores um ponto único de controle para gerenciar terminais de segurança clientes de terceiros de fornecedores como Computer Associates, McAfee, Sophos, Symantec e Trend Micro. Com esse recurso de gerenciamento centralizado, as organizações podem aperfeiçoar a escalabilidade, a velocidade e a confiabilidade das soluções de proteção. O recurso monitora a integridade do sistema para assegurar que os terminais de segurança clientes estejam sempre em execução e que as assinaturas de vírus estejam atualizadas. Além de fornecer uma visão unificada das diferentes tecnologias, facilita a migração de terminais de uma solução para outra com remoção e reinstalação de software com um só clique. A verificação em circuito fechado garante que as atualizações e outras mudanças sejam concluídas, inclusive a verificação habilitada para Internet para terminais desconectados da rede.

Autoquarentena da rede

O Tivoli Endpoint Manager for Security and Compliance avalia automaticamente os terminais em relação às configurações necessárias de conformidade, e se o terminal for considerado fora de conformidade, a solução pode configurar o terminal para que seja colocado na quarentena da rede até que a conformidade seja alcançada. O servidor do Tivoli Endpoint Manager possui acesso de gerenciamento ao terminal, mas todos os outros acessos estão desativados.

Serviço de antimalware e de reputação da Web (complemento opcional)

A grande integração com o CPM (Core Protection Module) da Trend Micro oferece recursos para proteger os terminais contra vírus, cavalos de tróia, worms, spyware, rootkits, novas variações de malware e de sites maliciosos por meio de consulta em tempo real e inteligência de ameaça na nuvem para eliminar quase completamente a necessidade de arquivos de assinaturas no terminal. A tecnologia de reputação da Web impede que os usuários acessem sites maliciosos, seja por suas próprias ações, ocultas ou automáticas realizadas por algum malware.

A família Tivoli Endpoint Manager

Você pode adicionar posteriormente outras ferramentas, reduzir o número de agentes terminais e os custos de gerenciamento, ampliando o seu investimento no Tivoli Endpoint Manager for Security and Compliance para incluir outros componentes da família do Tivoli Endpoint Management. Uma vez que todas as funções operam a partir dos mesmos consoles, servidor de gerenciamento e agente terminal, o acréscimo de mais serviços é uma simples questão de mudança da chave de licença.

- **Tivoli Endpoint Manager for Power Management** – Esta opção permite a execução de políticas de conservação de energia em toda a organização, com a granularidade necessária para permitir a aplicação de políticas em um único computador.
- **Tivoli Endpoint Manager for Lifecycle Management** – Esta opção abrangente e poderosa promove a convergência atual das funções de TI, oferecendo visibilidade em tempo real do estado dos terminais do sistema e proporcionando aos administradores recursos avançados para o gerenciamento desses terminais.

Tivoli Endpoint Manager: Desenvolvido com tecnologia BigFix

A força por trás de todas as funções do Tivoli Endpoint Manager está na abordagem única da infraestrutura que permite a tomada de decisões externamente aos terminais, proporcionando benefícios extraordinários em toda a família da solução, com as seguintes funcionalidades:

- **Um agente inteligente** – O Tivoli Endpoint Manager utiliza uma abordagem líder de mercado que coloca um agente inteligente em cada terminal. Esse agente único executa funções múltiplas que incluem a aplicação da autoavaliação e o reforço da política continuamente, com um impacto mínimo no desempenho do sistema. Diferentemente da arquitetura tradicional cliente-servidor que aguarda por instruções de um ponto central de controle, esse agente inicia as ações de forma inteligente, enviando mensagens de forma ascendente para o servidor de gerenciamento central e baixando as correções, configurações ou outras informações para o terminal, quando necessárias para a conformidade com política pertinente. Como resultado da inteligência e velocidade do agente, o servidor de gerenciamento central sempre conhece a conformidade e a mudança de status dos terminais, gerando relatórios de conformidade rápidos e atualizados.
- **Relatórios** – O console unificado desenvolvido no Tivoli Endpoint Manager proporciona um alto nível de visibilidade que inclui relatórios em tempo real e contínuos e análise a partir dos agentes inteligentes nos terminais da organização.
- **Recursos de retransmissão** – A arquitetura escalável e leve do Tivoli Endpoint Manager permite que qualquer agente seja configurado como um retransmissor entre outros agentes e o console. Essa função de retransmissão permite a utilização dos servidores ou estações de trabalho existentes na transferência de pacotes através da rede, reduzindo a necessidade de servidores.
- **Mensagens IBM Fixlet** – A Fixlet Relevance Language é uma linguagem de comando publicada que permite aos clientes, parceiros de negócios e desenvolvedores a criação de políticas e serviços personalizados para terminais gerenciados por soluções Tivoli Endpoint Manager.

Ampliando o compromisso do Tivoli com a segurança

O Tivoli Endpoint Manager for Security and Compliance é parte do abrangente portfólio de segurança da IBM e auxilia no enfrentamento dos desafios de segurança de toda a organização. Ao oferecer suporte para operações de TI inteligentes, instrumentadas e interconectadas em um planeta mais inteligente, as soluções de segurança da IBM ajudam a garantir visibilidade em tempo real, controle centralizado e maior segurança para toda a infraestrutura de TI, inclusive os terminais distribuídos globalmente.

Destaques da família Tivoli Endpoint Manager

Requisitos do servidor:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Requisitos do console:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Plataformas suportadas para o agente:

- Microsoft Windows, inclusive XP, 2000, 2003, Vista, 2008, 2008 R2, 7, CE, Mobile, XP Embedded e Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX
- Linux em IBM System z
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Oracle Enterprise Linux
- CentOS Linux
- Debian Linux
- Ubuntu Linux

Para mais informações

Para saber mais sobre o IBM Tivoli Endpoint Manager for Security and Compliance, entre em contato com seu representante IBM ou Parceiro de Negócios IBM, ou acesse ibm.com/tivoli/endpoint

Sobre o software Tivoli da IBM

O software Tivoli da IBM auxilia as organizações a gerenciar de forma eficiente e eficaz os recursos, tarefas e processos de TI para atender às necessidades de negócios em constante mudança e entregar um gerenciamento de serviços flexível e ágil, ao mesmo tempo em que auxilia na redução de custos. O portfólio do Tivoli abrange softwares para gerenciamento da segurança, conformidade, armazenamento, desempenho, disponibilidade, configuração, operações e ciclo de vida de TI, e é apoiado por serviços, suporte e pesquisa de nível internacional da IBM.

Produzido nos Estados Unidos da América
Fevereiro de 2011

IBM Brasil Ltda.
Rua Tutoia, 1157
CEP 04007-900
São Paulo – Brasil

A home page da IBM pode ser encontrada em:
ibm.com

Por favor, recicle

Tivoli software

TID14075-BRPT-00