IBM Tivoli Endpoint Manager for Core Protection

Protege terminais contra malware e contra outras ameaças maliciosas

Destaques

- Oferece proteção a terminais em tempo real contra vírus, cavalos de troia, spyware, rootkits e outros malwares
- Protege através de métodos que incluem reputação de arquivo e da Web, monitoramento de comportamento e firewall pessoal
- Fornece reconhecimento de virtualização para reduzir problemas de contenção em infraestruturas virtuais
- Utiliza tecnologias IBM e Trend Micro™, líderes de segmento de mercado, com uma infraestrutura de gerenciamento de console único

Embora o volume sempre crescente e a frequência de ataques de malware representem desafios contínuos para a proteção de terminais e de dados, esses não são os únicos perigos. A velocidade dos ataques aumentou significativamente, o que permite aos invasores se beneficiar das brechas imediatamente após a descoberta.

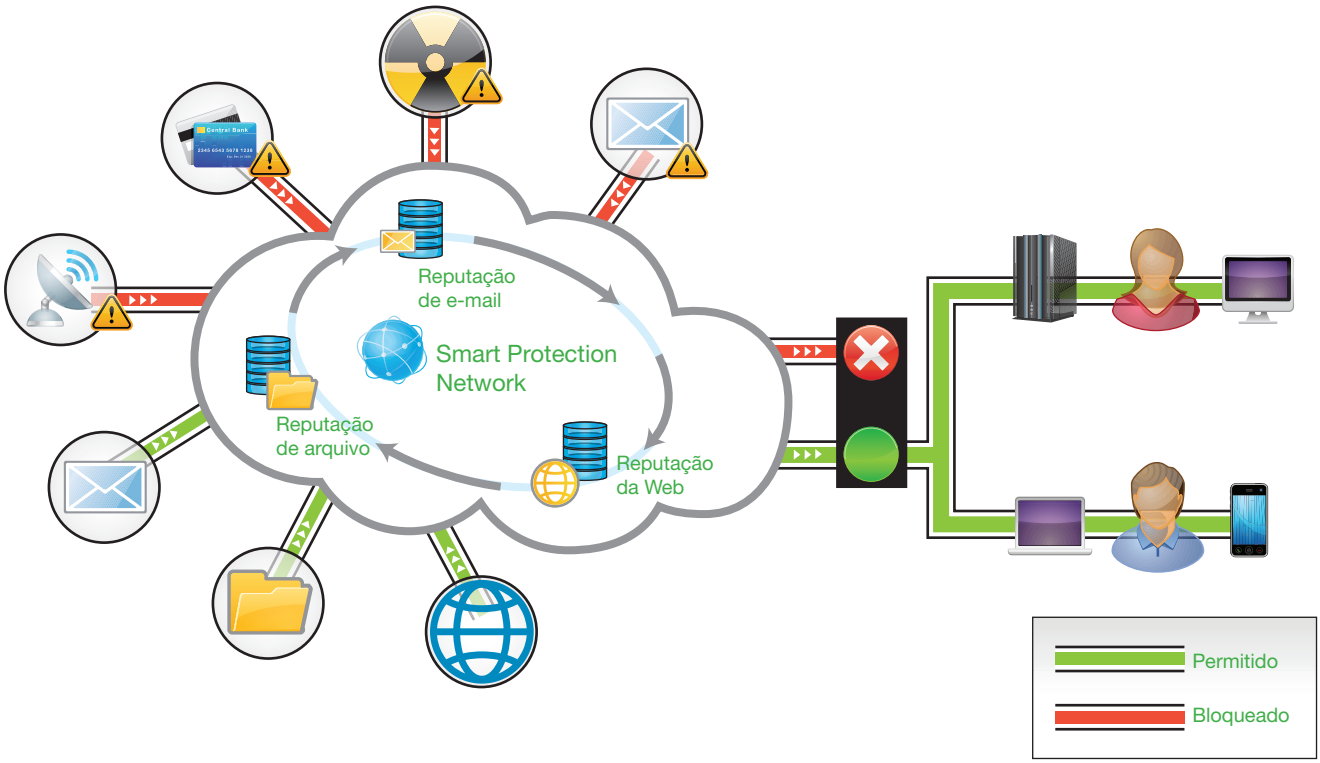
As organizações geralmente são criteriosas ao implementarem medidas para se protegerem de ataques, pois estas muitas vezes fazem parte do problema, à medida que geram camadas complexas de distribuição de produtos pontuais que não podem responder de maneira suficientemente rápida.

O IBM Tivoli Endpoint Manager for Core Protection oferece às organizações de TI uma solução automatizada e fácil de usar para detectar e remover malware antes que possam explorar as vulnerabilidades. A partir de um único console, fornece funções de proteção como detecção e remoção de malware, reputação de arquivo e da Web e firewall pessoal.

Proteção aprimorada para terminais distribuídos

Essa solução IBM protege terminais físicos e virtuais de danos causados por vírus, cavalos de troia, worms, spyware, rootkits, ameaças da Web e suas novas variantes. Reduz interrupções nos negócios que podem resultar de infecção de terminal, roubo de identidade, perda de dados, indisponibilidade de rede, produtividade perdida e violações de conformidade.

Planilha de dados



O Tivoli Endpoint Manager for Core Protection interrompe ameaças antes que elas surjam, buscando potencial malicioso em arquivos, URLs e e-mails em tempo real.

O Tivoli Endpoint Manager for Core Protection faz referência cruzada às informações de ameaças com um amplo banco de dados baseado em nuvem criado pela Trend Micro e continuamente atualizado através de terminais Smart Protection Network™ para Windows da Trend Micro. Em tempo real, a solução verifica arquivos e URLs em relação a esse banco de dados em busca de potencial malicioso, além de oferecer proteção antimalware para terminais Mac e Windows conforme necessário.

O Tivoli Endpoint Manager for Core Protection fornece segurança para terminais fixos, móveis, conectados à rede e conectados à Internet. O monitoramento constante baseado em agente é uma maneira comprovadamente eficaz para combater a vulnerabilidade extrema de terminais móveis. Um laptop utilizado em um aeroporto, por exemplo, pode receber proteção baseada em nuvem, em qualquer lugar, a qualquer momento contra ameaças ocultas em Web sites que visita ou em arquivos que recebe.

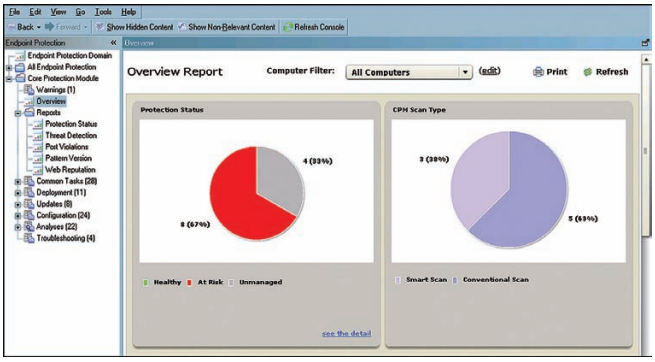
Proteção mais inteligente e mais segura projetada para reduzir riscos

A chave para o sucesso da solução é a capacidade de funcionar em múltiplos níveis de proteção às ameaças, incluindo o bloqueio das ameaças antes que elas surjam. O Tivoli Endpoint Manager for Core Protection, por exemplo,

pode varrer URLs em e-mails, verificá-las em relação aos bancos de dados de ameaças conhecidas e bloquear o acesso, se necessário. Tais medidas de linha de frente integradas a outros recursos protegem a infraestrutura e os terminais contra ataques à medida que eles ocorrem. O resultado foi que os recursos combinados do Tivoli Endpoint Manager for Core Protection capturaram 100% das ameaças nos últimos testes, enquanto a solução concorrente capturou apenas 77%.*

Esses recursos incluem:

- **Proteção superior contra malware:** A solução protege contra uma ampla gama de malwares e varre em busca de ameaças nas pastas do Microsoft Outlook e nos e-mails POP3. Livra automaticamente os terminais de malware, incluindo rootkits, spyware, processos e entradas de registros que estão ocultas ou bloqueadas.
- **Reputação de arquivo:** Consultando até os dados secundários em um banco de dados baseado em nuvem (uma implementação privada de nuvem oferecida pela Trend Micro também é suportada), esse recurso pode determinar a segurança de um arquivo e evitar que os usuários abram documentos infectados. Isso reduz o volume de esforços de gerenciamento necessários e o impacto da proteção no desempenho do terminal enquanto fornece proteção imediata dentro ou fora da rede.
- **Reputação da Web:** Esse recurso determina automaticamente a segurança de milhões de Web sites classificados de maneira dinâmica para proteger terminais contra malware baseado na Web, roubo de dados, perda de produtividade e danos à reputação. Fornece proteção em tempo real independentemente do tipo de conexão e pode aprimorar o desempenho da Web com sua sincronização baseada em nuvem.
- **Monitoramento de comportamento:** A solução identifica atividades suspeitas do sistema como o uso de memória flash para alteração de registro. Se ativado por um evento como esse, o recurso pode bloquear a execução para evitar atividades potencialmente prejudiciais.



Uma inovadora interface gráfica com o usuário permite que os administradores entendam facilmente seu status de proteção e identifiquem terminais em risco.

Gerenciamento de terminais simplificado com visibilidade aprimorada

A partir de um único console, o Tivoli Endpoint Manager for Core Protection pode aprimorar o gerenciamento com a visibilidade total de todos os terminais. Isso simplifica e centraliza o gerenciamento para terminais físicos e virtuais e suporta a delegação de tarefas com administração granular baseada em função.

Utilizar a infraestrutura Tivoli Endpoint Manager proporciona maior proteção através do cumprimento de políticas para assegurar que os serviços antivírus sempre estejam instalados, em funcionamento e atualizados. As organizações podem obter eficiências operacionais através do único console centralizado e reduzir os custos de servidor de gerenciamento e distribuição através da enorme escalabilidade proporcionada pela solução IBM.

Segurança que se adapta à organização

O Tivoli Endpoint Manager se adapta às necessidades de aumento e evolução dos ambientes de terminal. Tecnologias prospectivas como virtualização de desktop e serviços baseados em nuvem que aumentam a agilidade e simplificam as implementações enquanto reduzem carga operacional são recursos significativos da solução.

- **Reconhecimento de virtualização:** Para iniciativas de transição de desktops e laptops para máquinas virtuais, a solução IBM oferece proteção ao reconhecer automaticamente se um agente está em um terminal físico ou virtual. Se estiver em um terminal virtual, há algumas providências para evitar problemas como "sobrecargas de antivírus", nas quais a varredura executada simultaneamente em grandes quantidades de máquinas pode ocasionar uma interrupção nas redes e nos terminais. Ao invés disso, a solução serializa varreduras e atualizações para evitar conflitos. Isso também diminui o tempo da varredura ao listar imagens de base e conteúdo previamente analisado. O Tivoli Endpoint Manager for Core Protection se integra às soluções de virtualização existentes das organizações, incluindo Citrix XenDesktop e VMware View para aprimorar o retorno sobre investimento para projetos de virtualização em andamento.
- **Área de cobertura superficial:** O Tivoli Endpoint Manager for Core Protection libera recursos com capacidades baseadas em nuvem para implementação e gerenciamento da segurança. Em uma solução convencional, as atualizações de assinaturas de grande porte necessárias para acompanhar os crescentes números de ameaças podem prolongar a implementação, sobrecarregar os terminais e afetar a produtividade do usuário. Com a solução IBM, as assinaturas permanecem na nuvem, reduzindo a carga em terminais individuais.

Uma maneira inteligente de oferecer proteção a terminais

No mundo interconectado, instrumentado e inteligente de hoje, onde a complexidade do gerenciamento de terminal e a importância da segurança estão aumentando constantemente, o Tivoli Endpoint Manager for Core Protection oferece visibilidade e proteção atualizadas de terminal. Essa solução fácil de usar pode detectar e remover uma ampla gama de malwares antes que eles possam explorar as vulnerabilidades dos terminais através de funções de proteção como reputação de arquivo e da Web.

As organizações podem obter valor significativo ao implementarem produtos adicionais da família Tivoli Endpoint Manager, além do Tivoli Endpoint Manager for Core Protection. Por exemplo, ataques de malware geralmente visam vulnerabilidades sem patch. O Tivoli Endpoint Manager fornece recursos de gerenciamento de patch abrangentes para disponibilizar patches de uma ampla gama de fornecedores de aplicativos e sistemas operacionais para terminais distribuídos. Esse recurso pode diminuir o prazo de entrega de patches e atualizações, sem perda de funcionalidade do terminal, mesmo com baixa largura de banda ou redes globalmente distribuídas.

E a ampla solução Tivoli Endpoint Manager atende à convergência do gerenciamento do sistema e dos requisitos de segurança ao oferecer recursos de gerenciamento de vulnerabilidade, gerenciamento de configuração de segurança, descoberta de ativos, inventário, distribuição de software, implementação de sistema operacional, análise de utilização de software, relatório de conformidade, entre outros. O único console do Tivoli Endpoint Manager é utilizado para gerenciar todos esses recursos, incluindo os fornecidos pelo Tivoli Endpoint Manager for Core Protection. Essa solução abrangente fornece uma visão holística do status de segurança dos terminais da organização.

Visão Geral do Tivoli Endpoint Manager for Core Protection
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 pelo agente: • Microsoft Windows, incluindo XP, 2003, Vista, 2008, 2008 R2, 7, XP Embedded e Embedded Point-of-Sale • Mac OS X

Para mais informações

Para saber mais sobre o IBM Tivoli Endpoint Manager for Core Protection, entre em contato com o seu representante de vendas IBM ou Parceiro de Negócios IBM, ou visite: **ibm.com**/tivoli/endpoint

Sobre o software Tivoli da IBM

O software Tivoli da IBM ajuda as organizações de maneira eficaz e eficiente a gerenciar recursos, tarefas e processos de TI que vão ao encontro das constantes mudanças nos requisitos de negócios e entrega um gerenciamento de serviço de TI flexível e responsivo, enquanto ajuda a reduzir custos. O portfólio Tivoli inclui software para segurança, conformidade, armazenamento, desempenho, disponibilidade, configuração, operações e gerenciamento do ciclo de vida de TI e é apoiado pelos serviços, suporte e pesquisa de alto nível da IBM.

Adicionalmente, as soluções financeiras do IBM Global Financing podem possibilitar um gerenciamento de caixa eficiente, proteção contra obsolescência de tecnologia, melhora no custo total de propriedade e retorno do investimento. Nosso Global Asset Recovery Services também ajuda a abordar questões ambientais com soluções novas e mais econômicas em termos de energia. Para mais informações sobre o IBM Global Financing, visite: **ibm.com**/financing

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

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

IBM, o logotipo IBM, ibm.com e Tivoli são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos, em outros países, ou em ambos. Se a primeira ocorrência desses e de outros termos de marcas registradas da IBM for marcada com um símbolo de marca registrada (® ou ™), esses símbolos indicam marcas registradas ou de direito consuetudinário nos Estados Unidos de propriedade da IBM no momento da publicação destas informações. Tais marcas registradas também podem ser marcas registradas ou de direito consuetudinário em outros países. Uma lista atualizada das marcas registradas da IBM encontra-se disponível na Web no item "Copyright and trademark information" em:
ibm.com/legal/copytrade.shtml

Microsoft e Windows são marcas registradas da Microsoft Corporation nos estados Unidos, em outros países ou em ambos.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviços de terceiros.

Referências nesta publicação a produtos, programas ou serviços IBM não significam que a IBM pretenda torná-los disponíveis em todos os países nos quais a IBM opera.

Nenhuma parte desse documento pode ser reproduzida ou divulgada em qualquer formato sem permissão por escrito da IBM Corporation.

Dados do produto foram revisados para exatidão conforme data da publicação inicial. Dados do produto estão sujeitos à mudança sem prévio aviso. Quaisquer instruções sobre a direção ou intenção futura da IBM estão sujeitas à alteração ou à retirada sem aviso prévio e somente representam as metas e objetivos.

As informações nesse documento são fornecidas "no estado em que se encontram" sem nenhuma garantia, seja expressa ou implícita. A IBM renuncia expressamente quaisquer garantias de comercialização e adequação para um determinado objetivo ou não infração. Os produtos IBM são garantidos de acordo com os termos e condições dos acordos (por exemplo, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) sob os quais foram fornecidos.

Por favor, recicle

O cliente é responsável por assegurar a conformidade com requisitos legais. É responsabilidade de o cliente obter assistência da assessoria jurídica competente, além de identificar e interpretar quaisquer leis ou requisitos regulatórios relevantes que possam afetar os negócios do cliente e quaisquer ações que o cliente necessite tomar para atender a tais leis. A IBM não fornece conselho jurídico ou representa ou garante que seus serviços e produtos assegurarão que o cliente está em conformidade com qualquer lei ou regulamento.

* "Trend Micro Enterprise Endpoint Comparative Report," AV-Test, janeiro de 2011. http://us.trendmicro.com/us/trendwatch/core-technologies/competitive-benchmarks/avtest/

Produzido nos Estados Unidos da América
Maio de 2011

© Copyright IBM Corporation 2011
Todos os direitos reservados.

Tivoli software

TID14081-BRPT-00