IBM Software
White Paper de Liderança de Ideias

Fevereiro de 2011

Reescrevendo as regras de gerenciamento de patches

O IBM Tivoli Endpoint quebra o paradigma de patches

Conteúdo

Introdução

Os ataques de Malware estão em uma corrida contra o tempo para explorar sistemas vulneráveis de computadores antes que os fornecedores de software publiquem correções e seus clientes possam aplicá-las. Quando o malware vence a corrida, as organizações perdem produtividade e correm o risco de perda de dados sensíveis, processos judiciais em potencial e multas regulamentares. A enormidade absoluta do problema é alarmante – a batalha contínua entre hackers e empresas de software custa à economia dos Estados Unidos aproximadamente U$266 bilhões de dólares ao ano, segundo o Cyber Secure Institute, um grupo de advocacia com base em Washington D.C.[1]

Para combater essa ameaça, mais e mais fornecedores de software estão publicando mais correções em uma tentativa de acompanhar o furor das explorações de malware. Infelizmente, a maioria das organizações não está equipada para lidar com este ataque violento de correções a tempo e com custo reduzido. Devido aos processos organizacionais, os departamentos de TI levam semanas ou até meses para implementarem correções em todo o ambiente. Segundo algumas estimativas, as organizações podem levar até quatro meses para atingir uma taxa de 90 a 95 por cento de conformidade de correção. Até que isso aconteça, inúmeras correções adicionais foram publicadas, o que significa que as organizações estão sempre correndo alto risco e fora de conformidade – e a situação apenas piora ao longo do tempo.

O gerenciamento de patches sempre foi uma subida íngreme devido à grande complexidade envolvida. Apesar dos riscos, algumas organizações são relutantes à correção, devido ao tempo e trabalho requeridos, além de uma possível perturbação das operações de negócio. Em uma organização com ambiente de software e hardware heterogêneos, ficar no topo da grande quantidade de correções – e publicá-las em tempo hábil – pode extrapolar o orçamento e a equipe de TI. É preciso uma solução de gerenciamento de patches baseada em política, rapidamente implementável e com custo reduzido que:

- Funcione para todos os terminais em organizações de todos os tamanhos, incluindo as muito grandes.
- Suporte diversos fornecedores, sistemas operacionais, aplicativos e plataformas.
- Funcione com conexões de baixa velocidade e suporte dispositivos que funcionem fora da rede organizacional.
- Minimize a demanda pela equipe de TI.
- Opere em tempo real, implementando correções em toda a organização em horas.

O IBM Tivoli® Endpoint Manager, desenvolvido com a tecnologia BigFix®, combina as partes separadas do quebra-cabeça do gerenciamento de patches em uma solução simplificada e inteligente que simplifica e otimiza o processo de pesquisa, avaliação, correção, confirmação, aplicação e geração de relatório sobre correções.

O enigma do gerenciamento de patches

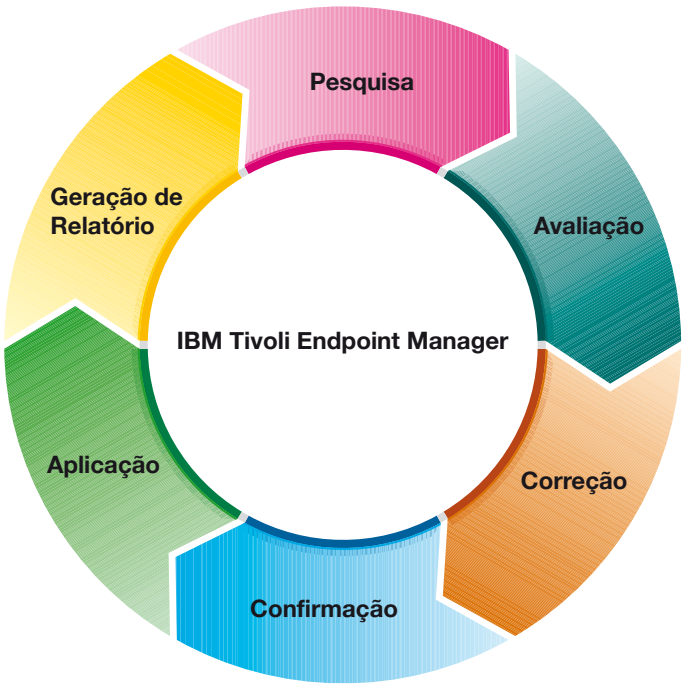
O gerenciamento de patches parece direto, mas ainda é um dos mais complexos e críticos desafios que uma organização enfrenta. As nuances de um gerenciamento de patches efetivo vão muito além de possuir simplesmente um administrador de sistemas que empurra as correções ou de depender de mecanismos de correções fornecidos por fornecedores e esperar que eles sejam aplicados com sucesso, mas sem nunca saber com certeza. O enigma do gerenciamento de correções levanta questões que muitas organizações podem considerar difíceis – se não impossíveis – de responder. Por exemplo:

- Como uma organização deveria implementar correções críticas "fora da banda" que cheguem com urgência e fora do planejamento de correção de rotina?
- Como os administradores de sistemas podem manter o controle de correções em um ambiente com centenas ou centenas de milhares de terminais executando uma variedade de sistemas operacionais e aplicativos?
- Como os administradores de sistemas deveriam monitorar o status de laptops e outros dispositivos móveis?
- Quanto tempo o processo de correção levará do início ao fim e como os administradores do sistema confirmarão (e provarão) que cada terminal presente na infraestrutura foi corrigido adequadamente – e permanecerá assim?
- Como os administradores do sistema podem testar correções rapidamente antes de implementá-las e revertê-las caso elas causem problemas?
- Como as correções podem ser implementadas sem interferirem na experiência com o usuário final e na produtividade?

Enquanto as pesquisas de opinião mostram que o gerenciamento de correção é uma das prioridades de segurança mais importantes para as organizações, essas questões indicam apenas quantas barreiras as organizações enfrentam ao implementar práticas efetivas de gerenciamento de correção. Entre uma falta de visibilidade e equipe, impacto nos negócios em potencial, limitações de largura da banda da rede, falta de gerenciamento, longas horas de correção, problemas de escalabilidade e cobertura para diferentes plataformas, aplicativos de terceiros e terminais móveis, os obstáculos são muitos.

Felizmente, esses obstáculos são superáveis. O Tivoli Endpoint Manager remove esses obstáculos com uma solução abrangente que é construída sob medida para ambientes altamente distribuídos e heterogêneos. Com essa solução, as organizações podem, finalmente, consultar, alterar, impingir e gerar relatórios sobre status de conformidade de correção em tempo real, em uma escala global, por meio de um único console.

Processo de gerenciamento de patches



Com o Tivoli Endpoint Manager, o gerenciamento de patches se torna um processo completamente unificado em um circuito fechado que ajuda a aprimorar a segurança e a economizar dinheiro.

Alterando o paradigma de gerenciamento de patches

Enquanto não há uma única boa prática oficial de gerenciamento de pacthes, a abordagem geral envolve um processo de circuito fechado com seis etapas básicas: pesquisa, avaliação, correção, confirmação, aplicação e geração de relatório. Historicamente, muitas dessas etapas foram implementadas por meio de tecnologias não integradas e separadas, tornando praticamente impossível a criação um processo de gerenciamento de correção em tempo real em um circuito fechado.O Tivoli Endpoint Manager fornece todas essas etapas como parte de um processo completamente integrado e unificado que pode ajudar a aprimorar a segurança e a economizar dinheiro, tempo e recursos.

Segue um olhar do antes e depois sobre como esta solução altera as regras para o gerenciamento de correção.

Etapa 1: Pesquisa

Antes: A primeira etapa no processo de gerenciamento de patches envolve a descoberta de quais correções estão disponíveis. Isso inclui pesquisar disponibilidade de patches por meio de mensagens de e-mail do fornecedor, notificações pop-up dos aplicativos, Web sites, blogs e uma variedade de outras fontes. Esse processo deve ser repetido semanalmente – ou até mesmo diariamente – para centenas de correções, entre pontuações de sistema operacional e fornecedores de aplicativos e antimalware. Uma alternativa – confiar nas atualizações automáticas padrão do fornecedor – pode levar a erros que podem ter consequências negativas, porque a aceitação automática de correções sem testá-las pode colocar as organizações em grande risco, não há controle corporativo sobre sincronização e geração de relatório e confiar nos usuários para aplicar atualizações é arriscado e falível.

Uma abordagem melhor é possuir um fornecedor de gerenciamento de patches que forneça um fluxo consolidado das correções mais comuns, para que a organização precise apenas avaliar cada carga de correções conforme eles chegam, testá-las com relação à compatibilidade com o ambiente organizacional e, em seguida, implementá-las por meio de políticas altamente granulares, destinadas a perfis específicos de máquinas, pois elas permitem especificar as correções a serem aplicadas apenas nos terminais que precisam delas. O problema com essa abordagem é que, se ela não for automatizada, será necessária uma quantidade significativa de tempo e de recursos que as organizações podem não possuir.

Depois: A IBM adquire, testa, empacota e distribui correções de fornecedores de sistema operacional, aplicativos comuns de terceiros e antimalware diretamente aos clientes, removendo um considerável gasto adicional com pesquisa no gerenciamento de correção. Quando um fornecedor suportado libera uma nova correção, a IBM recebe a correção, conduz análises preliminares e cria políticas de correção, chamadas mensagens do IBM Fixlet®, que une a atualização com informações de política, tais como dependências da correção, sistemas aplicáveis e nível de gravidade. Assim, os Fixlets são enviados automaticamente aos servidores de clientes do Tivoli Endpoint Manager. A solução também fornece um processo em que os clientes podem configurar o produto para transferir as correções por download diretamente dos sites dos fornecedores ou armazenar o conteúdo da correção localmente; os clientes também podem criar seus próprios Fixlets customizados usando uma interface orientada por assistente. Esse processo funciona praticamente para qualquer atualização, inclusive correções internas de aplicativo.

Etapa 2: Avaliação

Antes: Para cada correção identificada, a organização de TI deve determinar a aplicabilidade e o grau de gravidade da atualização, identificando quais terminais precisam de correção na organização. No caso de atualizações de segurança, esses dados críticos são convertidos diretamente em risco, conforme o risco de negócio aumenta com o número de terminais não corrigidos. Muitas organizações não têm acesso ao recurso completo e atual e ao conjunto de dados de configuração necessários para quantificar o escopo e o impacto das correções na organização. Há ferramentas que podem ajudar a adquirir esses dados, mas muitas precisam de dias ou semanas para coletar e intercalar essas informações, varrendo cada terminal na rede – e muitos terminais móveis raramente estão conectados à rede – um processo que pode levar dias para ser concluído. Essas informações devem estar imediatamente disponíveis para os administradores do sistema no momento da liberação da correção, pois muitas correções são críticas quanto ao tempo, e o processo de avaliação de risco e a priorização de correção devem acontecer o mais rapidamente possível.

Depois: Com o Tivoli Endpoint Manager, um agente único de software inteligente é instalado em todos os terminais gerenciados para monitorar e relatar continuamente o estado do terminal, incluindo níveis de correção, para um servidor de gerenciamento. O agente também compara a conformidade do terminal com relação às políticas definidas, tais como níveis de correção obrigatórios e configurações padrão. Estas informações são especialmente críticas durante cenários de correção de emergência quando um fornecedor libera uma correção altamente crítica e fora da banda e as organizações devem quantificar rapidamente a magnitude geral e o risco da(s) exploração(ões) relatada(s). Em um exemplo, um cliente usando os agentes instalados do Tivoli Endpoint Manager em 5.100 terminais descobriu que em mais de 1.500 (30 por cento) dos seus terminais faltava pelo menos uma correção crítica. Considerando como um todo, os terminais por toda a instituição estavam sem 20.033 correções "críticas" – uma média de 13 correções por terminal. Uma vez mapeado o número total de correções para os terminais que precisam delas e definido o grau de gravidade para os negócios, a organização de TI pode continuar com a etapa de correção.

Etapa 3: Correção

Antes: Após uma correção ser avaliada e ser feita uma determinação para distribuí-la por toda a organização, ela deve ser empacotada e testada para garantir que não causará conflito com outras correções e software de terceiros instalados nos terminais de destino. Os pré-requisitos de correção e as dependências, tais como níveis mínimos de pacote de serviços, também devem ser determinados. Isso normalmente é realizado aplicando e testando a atualização em um número selecionado de terminais antes de uma liberação geral - um processo que pode levar dias ou semanas para ser concluído usando ferramentas manuais. Uma vez que o teste indica que a correção é provavelmente segura para a implementação na organização toda, ela é aplicada para afetar terminais, tipicamente em lote, ampliando ainda mais a janela de correção. As longas horas de correção se devem, primeiro, à incapacidade de confiar na qualidade da correção e, segundo, aos mecanismos de distribuição não confiáveis, ambos resultam em baixas taxas correção de primeira passagem. A maioria das organizações é, portanto, forçada a continuar lentamente no caso de uma correção causar um problema não previsto, assim como a garantir que os links da rede não sejam esmagados pelo processo de distribuição da correção. Como resultado, a correção é geralmente difícil de ser realizada rápida e efetivamente em uma escala organizacional.

Outro grande problema é o fato de que muitas ferramentas de gerenciamento de correções funcionam apenas para o Microsoft® Windows® devido às dependências de ferramentas da Microsoft, como o Windows Server Update Services (WSUS). Muitas ferramentas também requerem profundo conhecimento da plataforma e equipes altamente treinadas para operá-las. Muitas dessas ferramentas não funcionam até que os terminais estejam conectados a uma rede corporativa de alta velocidade, deixando laptops e outros terminais móveis fora do ciclo de atualização por longos períodos. Muitas não fornecem os controles de baixa granularidade baseados em políticas que os operadores precisam para implementar efetivamente as correções em todos os terminais afetados na organização. Controles como o espaço de tempo de instalação de correção, se um usuário deve ou não estar presente, opções de reinicialização, o método de distribuição (incluindo a largura da banda e reguladores de CPU), tipo de sistema e opções de notificação de usuário devem ser entradas disponíveis nos processos de atualização automatizada.

Depois: Quando a IBM publica novos Fixlets de correção por meio do Tivoli Endpoint Manager, as organizações podem determinar o escopo da atualização criando, em minutos, um relatório que mostra quais terminais precisam da atualização. Os Fixlets de correção incluem instruções de distribuição, incluindo SO, versão e requisitos de pré-requisito, eliminando a necessidade de TI para "empacotar" e testar completamente a correção. Os operadores podem passar poucos minutos determinando quando a correção deve sair, qual notificação exibir aos usuários finais (se houver alguma), se permitir ou não que os usuários atrasem uma implementação de correção e por quanto tempo e se forçar (ou atrasar) reinicializações. Em minutos, o agente de terminal recebe a nova política e imediatamente avalia o terminal para determinar se a correção é aplicável, e, se for, ele transfere por download e aplica a correção, relatando o seu sucesso ou falha em minutos. Essa abordagem, combinada com a estrutura de retransmissão e a habilidade de alcançar dispositivos conectados à Internet do Tivoli Endpoint Manager, reduz significativamente a carga na rede e melhora as taxas de sucesso de primeira passagem em mais de 95 por cento.

A solução também fornece um mecanismo altamente seguro que emprega identidades criptográficas, garantindo que apenas administradores autorizados possam criar e distribuir políticas. Além disso, como não existe nenhuma dependência do Active Directory, os administradores do Tivoli Endpoint Manager não precisam ser administradores do domínio do Active Directory. A solução armazena informações de auditoria que controlam quem ordenou quais políticas a serem aplicadas em quais terminais e não requer conhecimento específico do sistema operacional para os operadores que iniciarem o processo de correção. Qualquer operador do Tivoli Endpoint Manager com poucas horas de treinamento básico pode corrigir rapidamente e com segurança sistemas operacionais Windows, Linux®, UNIX® e Mac sem nenhum conhecimento específico do domínio.

Etapa 4: Confirmação

Antes: Após as correções serem planejadas para aplicação, a instalação bem sucedida deve ser confirmada, assim TI saberá quando o ciclo da correção está completo, e para suportar requisitos de relatório de conformidade. Esses dados devem ser comunicados a um sistema de relatório central que atualiza a equipe sobre o processo, incluindo exceções, em tempo real. Entretanto, muitas tecnologias de gerenciamento de correções não executam efetivamente esse processo, precisando de semanas para varrer novamente todos os terminais e até mais para corrigir as exceções. Essa discrepância traz uma incerteza significativa sobre o risco de negócio geral da organização e a variação de conformidade.

Muitos produtos não fornecem confirmação de que as correções são aplicadas – ou, se o fazem, obter um relatório da organização toda pode levar dias ou até semanas. Ainda pior, algumas ferramentas relatam incorretamente que as correções foram aplicadas quando, na verdade,os arquivos foram transferidos por download, mas a correção não foi de fato aplicada. Com essa quantidade de atrasos e incertezas, alguns terminais são frequentemente deixados expostos, deixando uma significante janela de vulnerabilidade.

Depois: Uma vez que uma correção é implementada, o agente do Tivoli Endpoint Manager reavalia automática e continuamente o status do terminal para confirmar o sucesso da instalação, atualizando imediatamente o servidor de gerenciamento em tempo real (ou, no caso de dispositivos móveis, na primeira oportunidade). Essa etapa é crítica no suporte aos requisitos de conformidade, o que requer uma prova definitiva de instalação de correção contínua. Com esta solução, os operadores podem assistir ao processo de implementação da correção em tempo real por meio de um console de gerenciamento centralizado, recebendo a confirmação da instalação da correção em minutos após o início do processo de correção. Fechar o circuito da implementação de correção permite que as organizações garantam a conformidade de correção de um modo mais inteligente, rápido e muito mais confiável.

Etapa 5: Aplicação

Antes: Após o aplicativo inicial, muitas atualizações nem sempre "permanecem". Os usuários desinstalam, intencional ou acidentalmente, correções, novos aplicativos ou as correções podem corromper atualizações existentes, malware pode remover correções deliberadamente, ou os problemas criados pela atualização podem precisar de retrocesso. As tecnologias de gerenciamento de patches devem monitorar continuamente as máquinas para garantir conformidade com as políticas de atualização, fornecendo recursos rápidos de retrocesso com base em política no caso de um problema grave de correção. Se uma correção for removida contrariando a política de segurança, ela deverá ser reinstalada imediatamente e, se uma correção criar um problema grave após a sua aplicação, as organizações também deverão ser capazes de emitir um rápido retrocesso em massa. Sem dispor das ferramentas adequadas, essa etapa se torna quase impossível.

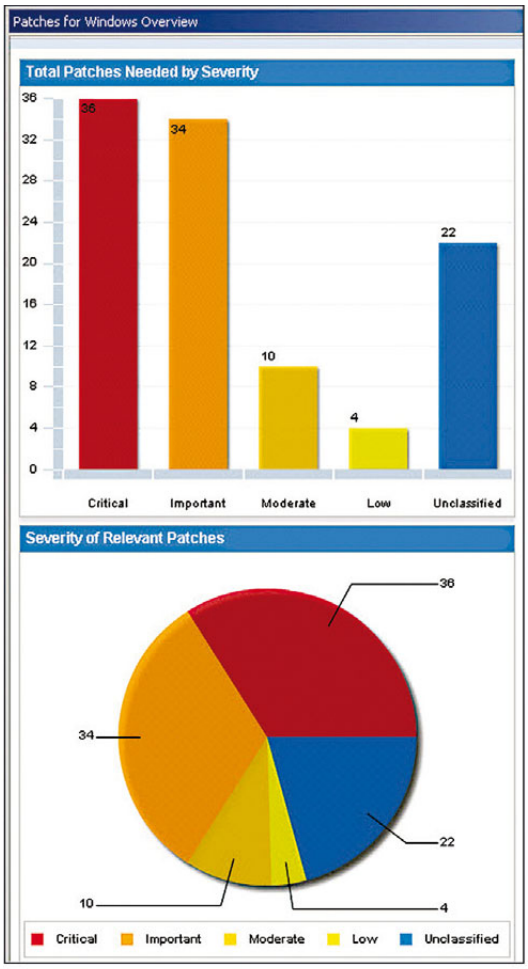
Depois: O agente inteligente do Tivoli Endpoint Manager aplica continuamente uma conformidade de política de correção, garantindo que os terminais permaneçam atualizados. Se uma correção for desinstalada por alguma razão, a política pode especificar que o agente deve reaplicá-la automaticamente no terminal, conforme necessário. Em caso de problemas com uma correção, os administradores do Tivoli Endpoint Manager podem emitir, de forma rápida e fácil, um retrocesso para os terminais – em massa ou para um grupo seleto. Por meio do mesmo console centralizado, o status de conformidade do terminal é relatado em tempo real, permitindo que os administradores de TI monitorem com facilidade o estado de todos os terminais gerenciados na organização.

Os administradores desfrutam do controle total de seus terminais, o que permite a eles manipular muitas vezes a quantidade de trabalho de outros produtos que requerem uma intervenção manual significativa e introduzem discrepâncias significativas no processo de geração de relatório.

Etapa 6: Geração de Relatório

Antes: A Geração de Relatório é um componente crítico do processo de gerenciamento de patches. As políticas de conformidade e da empresa requerem painéis e relatórios altamente detalhados e atualizados que indiquem a posição de risco da organização e o status do gerenciamento de correção para consumidores variados, incluindo auditores de conformidade, executivos, gerenciamento e até mesmo usuários finais. Sem uma solução global, não há maneira clara de gerar relatório sobre o status da correção da organização toda.

Depois: Os recursos de relatório da Web integrados do Tivoli Endpoint Manager permitem que os usuários finais, administradores, executivos, gerenciamento e outros visualizem painéis e relatórios minuto a minuto que indicam quais correções foram implementadas, quando elas foram implementadas, quem as implementou e em quais terminais. Painéis especiais "click through" mostram o progresso do gerenciamento de correção em tempo real.



Os relatórios de painel presentes no Tivoli Endpoint Manager mostram o progresso do gerenciamento de correção em tempo real.

Por que isso funciona

As tradicionais abordagens de gerenciamento de patchesutilizando processos manuais e complicados mecanismos baseados em varredura e em pesquisa já não são rápidas nem possuem custo reduzido suficiente para atender aos requisitos regulamentares e de negócios, deixando as organizações com riscos e custos inaceitavelmente elevados. Muitas organizações que tentam utilizar ferramentas de fornecedor que são "gratuitas" ou de baixo custo, como o Windows Server Update Services (WSUS), percebem rapidamente que essas soluções não são voltadas para a classe empresarial. Elas estão limitadas a um único fornecedor, não fornecem controle organizacional sobre quais correções cabem onde e quando, causam incômodos ao usuário final e oferecem uma geração de relatórios incompletos que não refletem o status em tempo real. O WSUS é um exemplo perfeito de um produto de ponto usado para realizar apenas uma etapa no processo de gerenciamento de correção descrito acima; porém, ele é usado, pois é visto como sendo "gratuito".

A Microsoft introduziu ciclos regulares de liberação de correção, conhecidos como "Patch Tuesdays", o que, infelizmente, também gerou as "Hack Wednesdays", durante as quais os cibercriminosos têm oportunidades de ouro para explorar terminais sem correções sem precisar se dar ao trabalho de descobrir novas vulnerabilidades. Os terminais que não são corrigidos imediatamente se tornam uma janela de oportunidades para criminosos – e uma janela de risco para a organização. Além disso, as organizações precisam gerenciar atualizações para uma grande variedade de produtos de fornecedores e fatores de forma de hardware – não apenas o Windows.

O Tivoli Endpoint Manager é líder no mercado em termos de amplitude de cobertura, velocidade, automação e efetividade em custo, fornecendo correções abrangentes a sistemas operacionais e aplicativos de terceiros. A solução, que inclui a implementação de um agente único, multi-uso, leve e inteligente para todos os terminais, suporta uma grande variedade de tipos de dispositivos, que vai desde servidores a computadores desktop, laptops "móveis" conectados à Internet e equipamento especializado, como dispositivos de ponto de venda (PDV), ATMs e quiosques de autoatendimento.

Um servidor de gerenciamento único pode suportar até 250.000 terminais, independentemente da localização, do tipo de conexão, da velocidade ou do status, e os servidores adicionais podem fornecer escalabilidade praticamente ilimitada. Os controles baseados em política fornecem aos administradores de TI recursos de gerenciamento de correção com baixa granularidade e altamente automatizados, e relatórios abrangentes suportam requisitos de conformidade. A conformidade com a política é continuamente avaliada e aplicada pelo agente inteligente, independentemente da conectividade do terminal à rede. Outros produtos possuem backends pesados e requerem grandes quantidades de hardware e equipe para suportar as implementações – em muitos casos, dezenas ou até centenas de servidores, diversos agentes por terminal e um exército de operadores – para suportar o mesmo ambiente que o Tivoli Endpoint Manager trata com um servidor de gerenciamento, um agente de terminal e apenas 1/20 da equipe.

Um outro aspecto chave da arquitetura é o suporte para terminais que estão ligados e desligados da rede corporativa. Dispositivos móveis como laptops, por exemplo, podem receber correções por qualquer conexão com a Internet, como Wi-Fi ou até mesmo conexão discada. O processo de gerenciamento de patches é praticamente transparente para o usuário, e as mensagens do IBM Fixlet controlam a quantidade total de largura da banda e de CPU consumida pelo agente de terminal, o que é informado com relação à localização e à conexão para otimizar o uso da rede.

Conformidade contínua

Muitas organizações precisam estabelecer, documentar e provar conformidade com os processos de gerenciamento de correção para cumprirem os regulamentos governamentais, acordos de nível de serviço (SLAs) e políticas corporativas. Regulamentos como Sarbanes-Oxley, PCI DSS e HIPAA/HITECH requerem que um processo regular de gerenciamento de patchescompletamente documentado esteja em vigor, e é necessária uma prova de conformidade contínua para passarem por auditorias. Infelizmente, muitas organizações gastam uma enorme quantidade de tempo e recursos no gerenciamento de correção e, ainda assim, não conseguem atender aos requisitos de conformidade. A capacidade do Tivoli Endpoint Manager de aplicar políticas e gerar relatório rapidamente sobre conformidade pode ajudar a melhorar a disponibilidade de auditoria de uma organização e as taxas de aprovação.

Como os clientes estão usando

As organizações estão enfrentando os desafios do gerenciamento de patches de cabeça erguida usando Tivoli Endpoint Manager. Para os clientes, os resultados incluem implementação mais rápida, melhor conformidade, custos reduzidos de TI e ciclos menores de gerenciamento.

Desafio: Implementar o gerenciamento de patches em dias ou semanas – não em meses ou anos

- A Albany County, NY, consolidou diversas ferramentas de gerenciamento de patches e de configuração em apenas dois dias.
- A rede O'Charley's Restaurants implementou patches em mais de 350 restaurantes em apenas quatro dias.
- Os SunTrust Banks implementaram uma solução em 50.000 terminais espalhados por aproximadamente 1.800 locais em três meses com o trabalho de apenas duas pessoas.
- A International Islamic University Malaysia completou uma implementação total em 7.000 computadores fixos e móveis entre sete campus universitários com largura de banda limitada em apenas seis semanas.

Desafio: Alcançar a conformidade com SLAs, políticas corporativas e regulamentos

- A Purolator atingiu 100 por cento de conformidade com um SLA em 24 horas a partir de seu fornecedor de serviço gerenciado.
- Os SunTrust Banks atingiram 98,5 por cento de conformidade de correção em 50.000 terminais.
- O Concord Hospital aumentou a conformidade de correção que era de 40 a 60 por cento para 93 por cento.
- A Entergy IT, que deve estar em conformidade com SLAs que requerem a implementação de correção em mais de 22.000 terminais dentro de uma janela de liberação de 10 dias, implementou mais de 4,9 milhões de correções pela empresa desde 2004 – e não perdeu um único SLA durante este período.

Desafio: Reduzir custos de TI

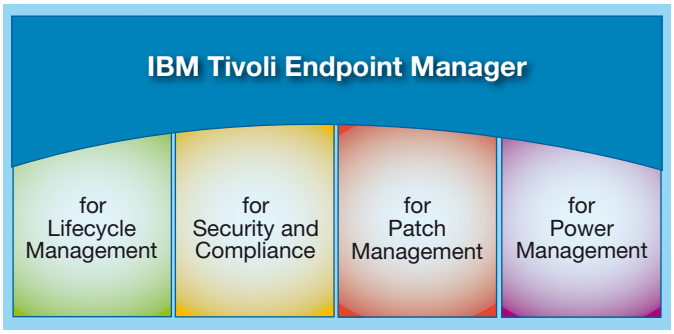
- A BGC Partners eliminou viagens caras para execução de serviço remoto em filiais localizadas em seis continentes, economizando dezenas de milhares de dólares.
- A Tax Tech reduziu Full-Time Equivalents (FTEs) do gerenciamento de patches de 20 para um.
- A Stena Lines atingiu uma proporção de economia de mão de obra de 12:1, reduzindo de 240 horas para 20 horas o tempo de gasto adicional administrativo para processos de correção.
- A Western Federal Credit Union relatou uma redução de 50 por cento nos custos com mão de obra por meio da automação e do gerenciamento de patches unificado.

Desafio: Reduzir os ciclos de gerenciamento de correção

- O Concord Hospital reduziu os ciclos de correção de semanas para apenas 15 minutos.
- Os SunTrust Banks reduziram os ciclos de correção de duas a três semanas para dois a três dias.
- A Tax Tech automatizou completamente a distribuição de correção durante o período noturno para mais de 1.000 locais conectados por meio de VPN.
- O grupo de gerenciamento de servidor e desktop da Entergy instalou 70.000 correções por toda a empresa em 24 horas.
- A Kronos distribui atualizações de software, políticas e correções para todos os terminais elegíveis dentro de 15 minutos por todo o mundo.

Um portfólio abrangente de soluções de gerenciamento de terminais e de segurança

A IBM oferece recursos de gerenciamento de patches por meio de um produto independente – o IBM Tivoli Endpoint Manager for Patch Management – ou como uma parte integral de duas soluções maiores de gerenciamento de terminais – o IBM Tivoli Endpoint Manager for Lifecycle Management e o IBM Tivoli Endpoint Manager for Security and Compliance. Toda a família Tivoli Endpoint Manager opera a partir do mesmo console, servidor de gerenciamento e agente de terminal, permitindo que as organizações consolidem ferramentas, reduzam o número de agentes terminais e baixem os custos de gerenciamento.



O IBM Tivoli Endpoint Manager é uma família de produtos totalmente operados a partir do mesmo console, servidor de gerenciamento e agente de terminal inteligente.

O Tivoli Endpoint Manager é parte de um portfólio abrangente de segurança da IBM, ajudando as organizações a resolverem desafios de segurança para usuários e identidades, dados e informações, aplicativos e processos, redes, servidores, terminais e infraestruturas físicas. Ao aprimorar o controle e a visibilidade em tempo real e melhorar a segurança e o gerenciamento de terminais, o portfólio da IBM suporta os datacenters mais inteligentes em expansão hoje, para facilitar as operações de TI interconectadas, instrumentadas e inteligentes de um planeta mais inteligente.

A tecnologia do Tivoli Endpoint Manager fornece:

- **Um único agente inteligente** – o Tivoli Endpoint Manager utiliza uma abordagem líder no segmento de mercado que coloca um único agente inteligente em cada terminal. Esse agente executa diversas funções, incluindo autoavaliação contínua e cumprimento de política – e ainda causa um impacto mínimo no desempenho do sistema, usando, em média, menos de dois por cento da CPU do terminal. O agente inicia as ações de um modo inteligente, enviando mensagens de envio de dados ao servidor de gerenciamento central e extraindo correções, configurações ou outras informações para o terminal, quando necessário, para cumprir com uma política relevante. Como resultado da inteligência e da velocidade do agente, o servidor de gerenciamento central sempre tem conhecimento da conformidade e da mudança de status dos terminais, possibilitando uma geração rápida e atualizada de relatório de conformidade.

- **Respostas Instantâneas** – Seja descobrindo quantas instâncias do Adobe® Acrobat estão instaladas ou seja validando quais laptops são impactados por um recall do fabricante, o Tivoli Endpoint Manager fornece as respostas em minutos – em toda a organização. Graças ao agente inteligente, não há necessidade de esperar pela conclusão de longas varreduras, nem pela produção de detalhes em massa feita por um servidor centralizado, tampouco pela conclusão da execução de milhares de consultas SQL antes da geração de painéis e relatórios. Cada agente avalia a relevância da questão, analisa as informações, gera relatórios de volta e pode até mesmo tomar ações com base nas análises, se desejado.
- **Cobertura para terminais móveis** – O laptop de propriedade da empresa é movido para além das dependências de um escritório da empresa. Os usuários estão se conectando de suas casas, de hotéis, aeroportos e até mesmo aviões. Permanecendo sempre um passo à frente, o Tivoli Endpoint Manager fornece a exclusiva capacidade de gerenciar terminais em tempo real – mesmo para dispositivos móveis.

Conclusão

O Tivoli Endpoint Manager trata dos principais desafios que muitas organizações enfrentam atualmente, fornecendo uma solução de gerenciamento de patches centralizada para servidores em toda a organização, desktop e dispositivo remoto que automatiza e alivia muito o processo de teste de correção de TI. O Tivoli Endpoint Manager é implementado em dias, e um único servidor de gerenciamento suporta até 250.000 terminais, aumentando drasticamente as taxas de sucesso de correção, melhorando a conformidade regulamentar e reduzindo gastos.

Em um mundo em que cada segundo é importante, o Tivoli Endpoint Manager pode ser a diferença entre uma estratégia de gerenciamento de correção bem-sucedida e uma que deixa a organização em perigo.

Para mais informações

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

Sobre o software Tivoli IBM

O software Tivoli da IBM ajuda organizações a gerenciar recursos, tarefas e processos de TI de modo eficiente e eficaz para atender a requisitos de negócios em contínua mudança e a entregar gerenciamento flexível e responsivo de serviço de TI, enquanto ajuda a reduzir custos. O portfólio Tivoli abrange software para segurança, conformidade, armazenamento, desempenho, disponibilidade, configuração, operações e gerenciamento de ciclo de vida de TI e tem o apoio de serviços, suporte e pesquisa da IBM de nível mundial.

Além disso, as soluções de financiamento do IBM Global Financing podem permitir gerenciamento efetivo de dinheiro, proteção contra defasagem de tecnologia, melhora do custo total de propriedade e retorno sobre investimento. Nossos Global Asset Recovery Services também ajudam a tratar de interesses ambientais com soluções novas e com maior eficiência energética. Para obter mais informações sobre o IBM Global Financing, visite: **ibm.com**/financing

IBM Corporation Software Group
Route 100
Somers, NY 10589
EUA

Produzido nos Estados Unidos da América
Fevereiro de 2011

Por favor, recicle

O cliente é responsável por assegurar a conformidade com os requisitos legais. É responsabilidade total do cliente obter informações dos conselhos legais competentes como identificação e interpretação de qualquer lei relevante ou requisitos regulamentares que podem afetar os negócios dos clientes e qualquer ação que o leitor possa ter de tomar para estar de acordo com essas leis. A IBM não fornece aconselhamento jurídico, nem representa ou garante que os seus serviços ou produtos garantirão que o cliente esteja em conformidade com qualquer lei ou regulamentação.

[1] http://cybersecureinstitute.org