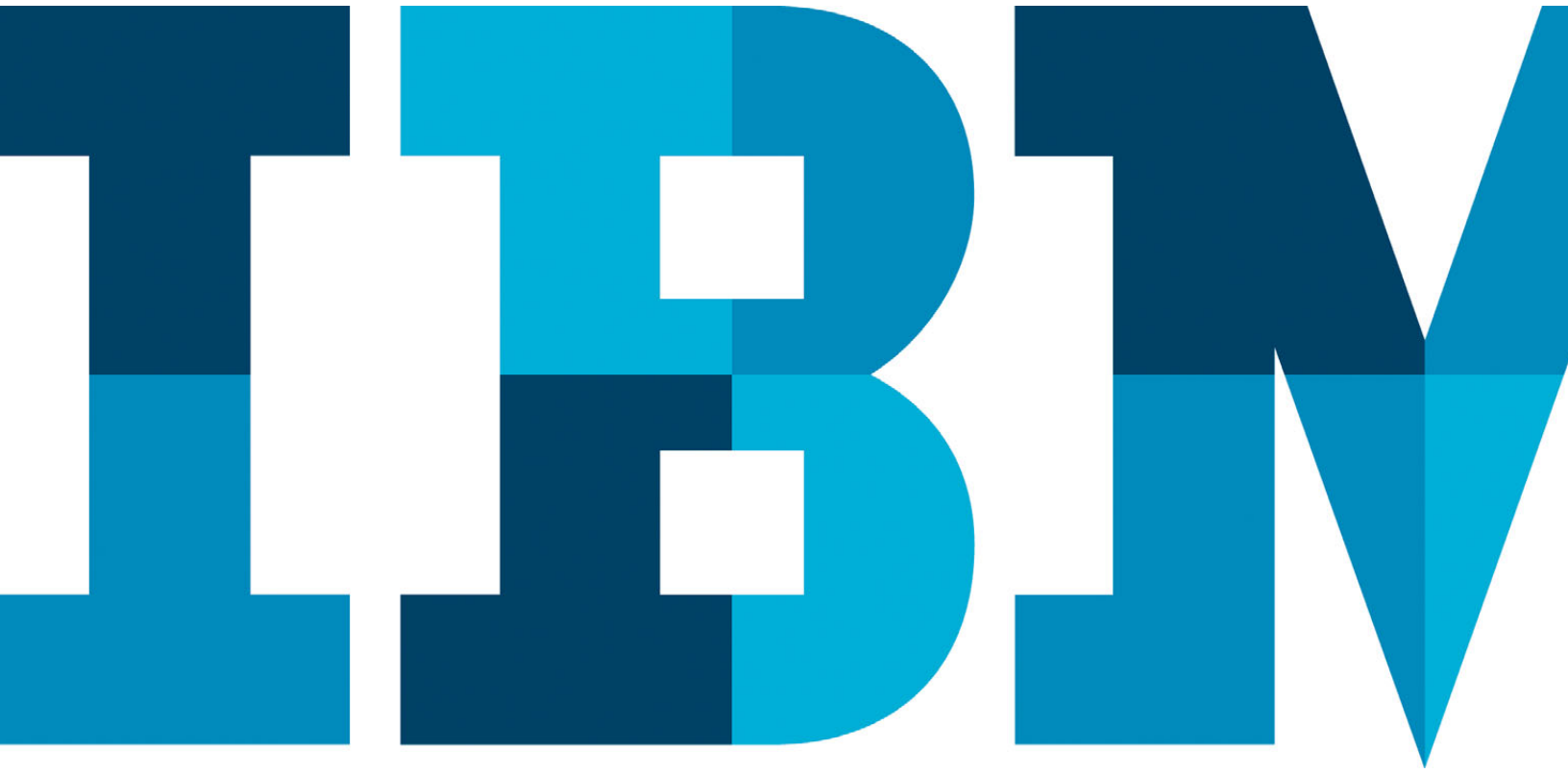
Software IBM
Thought Leadership White Paper

Fevereiro de 2011

Reescrevendo as regras de gerenciamento de patch

O IBM Tivoli Endpoint Manager substitui o paradigma de patching



Índice

Introdução

Os ataques de malwares estão em uma corrida contra o tempo para explorar sistemas de computador vulneráveis, antes que os distribuidores de software publiquem patches e que seus clientes possam aplicá-los. Quando um malware ganha a corrida, as organizações perdem produtividade e há o risco de perda de dados sensíveis, processo judicial potencial e multas regulatórias. A gravidade do problema é alarmante – a batalha em curso entre os hackers e as empresas de software custa à economia norte-americana um valor estimado em US$266 bilhões anuais, de acordo com o Cyber Secure Institute, grupo jurídico com base no distrito federal, Washington.[1]

Para combater esta ameaça, mais e mais distribuidores de software emitem mais e mais patches, em uma tentativa de manter o ritmo das frenéticas explorações dos malwares. Infelizmente, a maioria das organizações não está equipada para lidar com estas investidas de patches, de modo a manter uma relação custo-benefício eficaz. Devido aos processos organizacionais, leva semanas, ou até mesmo, meses para que a maioria dos departamentos de TI implante patches em todo o ambiente. De acordo com algumas estimativas, pode levar até quatro meses para que as organizações atinjam de 90% a 95% de taxa de aderência ao patch. Assim, incontáveis patches adicionais são emitidos, o que significa que as organizações estão permanentemente em risco elevado e fora da aderência – bem como em uma situação que só piora com o passar do tempo.

O gerenciamento de patches sempre foi um caminho desafiador devido à complexidade massiva envolvida. Apesar dos riscos, algumas organizações são relutantes ao patch, devido ao tempo e ao trabalho exigidos, além do potencial de interrupção das operações de negócio. Em uma organização com um ambiente heterogêneo de hardware e software, permanecer no topo de uma multidão de patches – e emiti-los de modo periódico – pode sobrecarregar a equipe de TI e extrapolar os orçamentos. O que é necessário é uma solução de gerenciamento de patch rapidamente implantável, baseada na relação custo-benefício e na política que:

- Funcione para todos os endpoints nas organizações de todos os tamanhos, incluindo as maiores.
- Suporte de múltiplos distribuidores, sistemas operacionais, aplicativos e plataformas.
- Funcione em conexões de baixa velocidade e que suporte dispositivos que funcionam fora da rede organizacional.
- Minimize a demanda da equipe de TI.
- Opera em tempo real, implantando patches em toda a organização, em questão de horas.

O IBM Tivoli Endpoint Manager, incorporado na tecnologia BigFix, combina peças separadas de cada quebra-cabeça de gerenciamento de patches em uma solução inteligente, bem como simplificada que aperfeiçoa e otimiza o processo de pesquisa, avaliação, resolução, confirmação, reforço e emissão de relatórios sobre patches.

O enigma do gerenciamento de patches

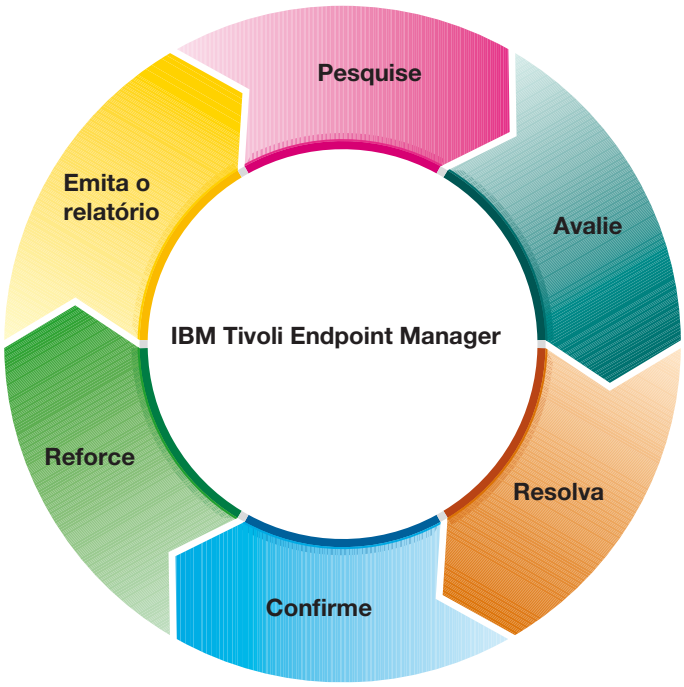
O gerenciamento de patches parece simples e ainda assim é um dos desafios mais complexos e críticos que uma organização enfrenta. As nuances do gerenciamento eficaz de patches vai muito além de simplesmente ter um administrador do sistema que lança patches ou confiar em mecanismos de patch fornecidos por distribuidores, esperando que eles sejam aplicados com sucesso, mas nunca se sabendo ao certo. O enigma de gerenciamento de patches levanta questões que várias organizações podem considerar difíceis – se não impossíveis – de responder. Por exemplo:

- Como uma organização implanta patches críticos “fora de banda” que chegam de modo urgente e fora do cronograma de rotina de patch?
- Como os administradores do sistema podem controlar os patches em um ambiente com centenas ou milhares de endpoints executando uma variedade de sistemas operacionais e aplicativos?
- Como os administradores do sistema pretendem monitorar o estado de laptops remotos e de outros dispositivos móveis?
- Quanto tempo o processo de patching leva, do início ao fim, e como os administradores do sistema confirmam (e comprovam) que cada endpoint, na respectiva infraestrutura, foi adequadamente submetido ao patch – e permanece desta forma?
- Como os administradores do sistema testam, rapidamente, os patches antes de implantá-los e os retiram no caso de problemas?
- Como os patches podem ser implantados sem interferir na experiência do usuário final e na produtividade?

Enquanto pesquisas mostram que o gerenciamento de patch é uma das prioridades de segurança mais importantes para as organizações, estas questões indicam somente as várias barreiras enfrentadas pelas organizações ao implementar práticas eficazes de gerenciamento de patches. Os obstáculos são muitos: entre a falta de visibilidade e de pessoal, impacto potencial ao negócio, limitações de largura de banda da rede, falta de capacidade de gerenciamento, longos intervalos para a resolução, questões de escalabilidade e cobertura para diferentes plataformas, aplicativos de terceiros e endpoints remotos.

Felizmente, estes obstáculos são contornáveis. O Tivoli Endpoint Manager elimina estes obstáculos com uma solução abrangente que é a finalidade para ambientes altamente distribuídos e heterogêneos. Com esta solução, as empresas podem, finalmente, ver a mudança, reforçar e emitir relatórios sobre o estado de aderência do patch em tempo real, em uma escala global, por meio de um único gabinete.

Processo de gerenciamento de patch



Como o Tivoli Endpoint Manager, o gerenciamento de patch se torna um processo completamente unificado, fechado, que ajuda a aprimorar a segurança e a poupar dinheiro.

Mudando o paradigma de gerenciamento de patch

Embora não exista uma melhor prática única e oficial no gerenciamento de patch, a abordagem geral envolve um processo de circuito fechado com seis etapas básicas: pesquise, avalie, resolva, confirme, reforce e emita o relatório. Historicamente, várias destas etapas foram implementadas por meio de tecnologias separadas e não integradas, tornando virtualmente impossível criar um processo de gerenciamento de patch em circuito fechado e em tempo real. O Tivoli Endpoint Manager oferece todas estas etapas como parte de um processo unificado e completamente integrado que ajuda a aprimorar a segurança e a poupar dinheiro e recursos.

Aqui há uma visão antes e depois sobre como esta solução muda as regras para o gerenciamento de patch.

Etapa 1: Pesquise

Antes: A primeira etapa no processo de gerenciamento de patch envolve a descoberta de quais patches estão disponíveis. Isso inclui a pesquisa de disponibilidade de patches por meio de mensagens de e-mail ao distribuidor, notificações de pop-up de aplicativos, sites, blogs e uma variedade de outras fontes. Este processo pode ser semanalmente repetido – ou inclusive diariamente – para centenas de patches, em classificações de distribuidores de sistema operacional, aplicativos e anti-malwares. Uma alternativa – que confia nas atualizações automáticas padrão do distribuidor – pode levar a erros que podem ter consequências negativas, uma vez que a aceitação automática de patches sem testá-los pode colocar as organizações em alto risco, não há um controle na empresa sobre o intervalo e emissão de relatório, bem como confiar nos usuários para aplicar as atualizações apresenta riscos e não é confiável.

Uma abordagem melhor é ter um distribuidor de gerenciamento de patch que oferece um fluxo consolidado dos patches mais comuns, de modo que a organização somente necessita avaliar cada carregamento de patches conforme estes surgem, testá-los quanto à compatibilidade com o ambiente organizacional e, em seguida, implantá-los por meio de políticas altamente granuladas, destinadas a perfis específicos de máquinas, uma vez que isso permite que patches específicos sejam aplicados somente aos endpoints que os necessitam. O problema com esta abordagem é que se não está automatizada, exige tempo e recursos significativos que as organizações não têm.

Depois: A IBM adquire, testa, coloca em pacotes e distribui patches, diretamente ao cliente, provenientes de distribuidores terceirizados de aplicativos comuns, sistemas operacionais e anti-malwares, eliminando uma sobrecarga considerável de pesquisa sobre o gerenciamento de patches. Quando um distribuidor compatível lança um novo patch, a IBM o recebe, realiza análises preliminares e cria políticas de patch, denominadas mensagens IBM Fixlet, que envolvem a atualização com informações de política como dependências de patch, sistemas aplicáveis e nível de importância. As Fixlets são automaticamente enviadas para os servidores do cliente do Tivoli Endpoint Manager. A solução também oferece um processo no qual os clientes podem configurar o produto para download de patches diretamente a partir dos sites dos distribuidores ou armazenar localmente o conteúdo de patch; os clientes também podem criar sua própria Fixlet customizada, com o uso de uma interface inteligente. Este processo funciona, virtualmente, para qualquer atualização, incluindo os patches de aplicativos internos.

Etapa 2: Avalie

Antes: Para cada patch identificado, a organização de TI deve determinar a aplicabilidade e o teor crítico da atualização, identificando quais endpoints precisam executar o patch em toda a organização. No caso de atualizações de segurança, estes dados críticos se traduzem diretamente em riscos, conforme o risco de negócio aumenta com o número de endpoints fora de patch. Várias organizações não têm acesso ao recurso completo e atual, bem como a configuração do conjunto de dados exigida para quantificar o escopo e o impacto dos patches em toda a organização. Há ferramentas que podem ajudar a adquirir estes dados, mas podem exigir dias ou semanas para a coleta e comparação destas informações, por meio de varredura em cada endpoint na rede – e vários endpoints remotos raramente estão conectados à rede – um processo que pode levar dias para conclusão. Esta informação deve estar imediatamente disponível para os administradores do sistema, no momento do lançamento do patch, uma vez que vários patches são críticos em relação ao tempo, bem como o processo de avaliação de risco e a priorização do patch devem ocorrer o mais rápido possível.

Depois: Com o Tivoli Endpoint Manager, um único agente inteligente de software é instalado em todos os endpoints gerenciados para monitorar, continuamente, bem como para emitir relatórios sobre o estado do endpoint, incluindo níveis de patch, para um servidor de gerenciamento. O agente também compara a aderência do endpoint em relação às políticas definidas, como níveis obrigatórios de patch e configurações padrão. Estas informações são especialmente críticas durante os cenários de emergência de patch quando um distribuidor lança um patch altamente crítico e fora de banda, e as organizações devem quantificar, rapidamente, a amplitude geral e o risco de exploração(ões) relacionada(s). Em um exemplo, o cliente que utiliza o Tivoli Endpoint Manager, com agentes instalados em 5.100 endpoints e descobriu que mais de 1.500 (ou 30%) de seus endpoints perderam, no mínimo, um patch crítico. Tomado como um todo, os endpoints em toda a instituição perderam 20.033 patches "críticos" – uma média de 13 patches por endpoint. Uma vez que o número total de patches é mapeado aos endpoints que o necessitam, e o teor crítico do negócio é definido, a organização de TI pode avançar até a etapa de resolução.

Etapa 3: Resolva

Antes: Depois de avaliado um patch e efetuada a determinação de distribuí-lo em toda a organização, ele deve ser colocado em pacotes e testado para garantir que não entrará em conflito com outros patches e com softwares de terceiros instalados em endpoints-alvo. Os pré-requisitos de patch e dependências, como níveis mínimos do pacote de serviço, também devem ser determinados. Isso geralmente é obtido por meio da aplicação e teste de uma atualização em um número selecionado de endpoints antes de um lançamento geral – um processo que pode levar dias ou semanas para ser concluído com o uso de ferramentas manuais. Uma vez que o teste indica que o patch provavelmente é seguro para implantação em toda a organização, ele é aplicado aos endpoints afetados, tipicamente em lotes, estendendo-se ainda à janela de patch. Os longos intervalos para resolução devem-se, primariamente, à incapacidade de confiar na qualidade do patch e, em segundo lugar, devido a mecanismos de distribuição não confiáveis, ambos que resultam em baixas taxas de primeira passagem. A maioria das organizações é, portanto, forçada a avançar lentamente caso um patch provoque um problema imprevisto, bem como para garantir que os links da rede não sejam sobrecarregados pelo processo de distribuição de patch. Como resultado, a resolução é frequentemente difícil de ser rápida e eficazmente obtida em uma escala organizacional.

Outro problema principal é que várias ferramentas de gerenciamento de patch somente funcionam para o Microsoft® Windows® devido a dependências nas ferramentas da Microsoft, como a Windows Server Update Services (WSUS). Várias ferramentas exigem expertise profunda da plataforma e pessoal altamente treinado para operá-las. Várias destas ferramentas não funcionam até que os endpoints estejam conectados a uma rede corporativa de alta velocidade, deixando laptops remotos e outros endpoints móveis fora do ciclo de atualização por longos períodos. Vários não fornecem controles selecionados e baseados na política que os operadores necessitam para implantar, eficazmente, os patches para todos os endpoints afetados na organização. Controles como janelas de intervalo de instalação de patch, se um usuário deve ou não estar presente, opções de reinicialização, método de distribuição (incluindo largura de banda e botões de CPU), tipo de sistema, bem como opções de notificação ao usuário devem estar disponíveis para inserção dentro dos processos automatizados de atualização.

Depois: Quando a IBM publica novas Fixlets de patch por meio do Tivoli Endpoint Manager, a organização pode determinar o escopo da atualização por meio da criação de um relatório em minutos, que mostra quais endpoints devem ser atualizados. As Fixlets de patch incluem instruções de distribuição, incluindo OS, versão e exigências de pré-requisitos, eliminando a necessidade de um "pacote" da equipe de TI e um teste completo do patch. Assim, os operadores podem gastar poucos minutos para determinar quando o patch deve sair, que notificação exibir aos usuários finais (se houver), se deve ser permitido ou não ao usuário adiar a implementação do patch e por quanto tempo, bem como se deve forçar (ou adiar) a reinicialização. Em questão de minutos, o agente de endpoint recebe a nova política e avalia, imediatamente, o endpoint para determinar se o patch é aplicável e, caso seja, seu download e aplicação, relatando o sucesso ou falha dentro de minutos. Esta abordagem, combinada à estrutura de confiança e à capacidade de reagir a dispositivos conectados à internet do Tivoli Endpoint Manager, reduz, significativamente, a carga da rede e melhora as taxas de sucesso na primeira passagem para mais de 95%.

A solução também oferece um mecanismo altamente seguro que emprega identidades criptográficas, garantindo que somente administradores autorizados possam criar e distribuir políticas. Ademais, uma vez que não existe nenhuma dependência de diretório ativo, os administradores do Tivoli Endpoint Manager não precisam ser administradores de domínio de diretório ativo. A solução armazena informações de auditoria que rastreiam quem ordenou que políticas devem ser aplicadas a quais endpoints, e não exige expertise específica em sistemas operacionais para operadores que iniciam o processo de resolução. Qualquer operador do Tivoli Endpoint Manager com algumas horas de treinamento básico pode, de modo seguro e com rapidez, efetuar o patch de sistemas operacionais como Windows, Linux®, UNIX® e Mac, sem conhecimento ou expertise específico de domínio.

Etapa 4: Confirme

Antes: Depois de os patches serem agendados para aplicação, a instalação com sucesso deve ser confirmada, assim a equipe de TI sabe quando o ciclo de patch foi concluído e para confirmar a aderência em efetuar os relatórios de requisitos. Estes dados devem ser comunicados a um sistema central de relatório que atualiza a equipe sobre o processo, incluindo exceções, em tempo real. Entretanto, várias tecnologias de gerenciamento de patch não desempenham, eficazmente, este processo, exigindo semanas para efetuar, novamente, a varredura de todos os endpoints e, inclusive, mais tempo para corrigir exceções. Este atraso apresenta uma incerteza significativa sobre o risco geral do negócio da organização e a postura de aderência.

Vários produtos não oferecem confirmação se os patches foram aplicados – ou se foram, pode levar dias ou, inclusive, semanas para obter um relatório completo da organização. Inclusive pior, algumas ferramentas relatam, de modo incorreto, que os patches foram aplicados, quando, de fato, foi efetuado o download dos arquivos, mas o patch não foi realmente aplicado. Com esta quantidade de atrasos e incertezas, alguns endpoints frequentemente permanecem expostos, deixando uma lacuna significativa de vulnerabilidade.

Depois: Uma vez implantado um patch, o agente do Tivoli Endpoint Manager reavalia, automaticamente e de modo contínuo, o estado do endpoint para confirmar o sucesso da instalação, atualizando, imediatamente, o servidor de gerenciamento em tempo real (ou no caso de dispositivos remotos, na primeira oportunidade). Esta etapa é crítica no suporte de requisitos de aderência, que exigem comprovação definitiva da instalação contínua de patch. Com esta solução, os operadores podem observar o processo de implantação do patch em tempo real por meio de um gabinete centralizado de gerenciamento, recebendo confirmação da instalação do patch em questão de minutos do início do processo de patch. Fechar o circuito de implantação de patch permite às organizações garantir a aderência do patch de modo mais inteligente, mais rápido e muito mais confiável.

Etapa 5: Reforce

Antes: Depois da aplicação inicial, várias atualizações nem sempre "pegam". De modo intencional ou acidentalmente, os usuários desinstalam patches, novos aplicativos ou patches que podem corromper as atualizações existentes, malwares podem deliberadamente eliminar patches ou problemas criados pela atualização podem necessitar de uma recuperação. As tecnologias de gerenciamento de patch devem monitorar, continuamente, as máquinas para garantir a aderência com as políticas de atualização, oferecendo capacidades de desmantelamento rápido e baseado na política, no caso de um problema significativo de patch. Se um patch é retirado em oposição a uma política de segurança, ele deve ser imediatamente reinstalado e, se um patch cria um problema maior depois da aplicação, as organizações também devem ser capazes de emitir rapidamente um desmantelamento em massa. Sem as ferramentas adequadas, esta etapa se torna quase que impossível.

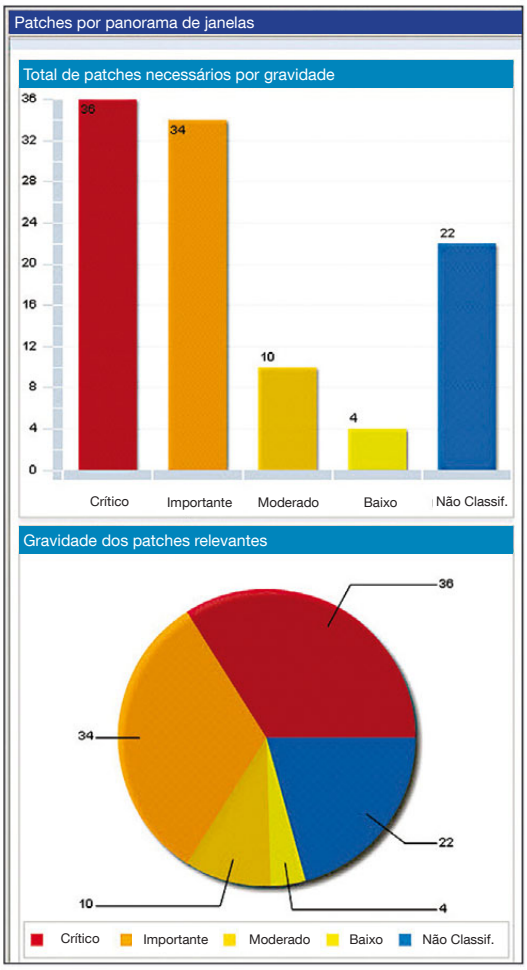
Depois: O agente inteligente do Tivoli Endpoint Manager reforça, continuamente, a aderência à política de patch, garantindo que os endpoints permaneçam atualizados. Se um patch é desinstalado, por qualquer razão, a política pode especificar que o agente deve reaplicá-lo, automaticamente, ao endpoint, conforme necessário. No caso de problemas com um patch, os administradores do Tivoli Endpoint Manager podem, de modo rápido e fácil, emitir um desmantelamento aos endpoints – seja em massa ou selecionando alguns. Por meio do mesmo gabinete centralizado, o estado de aderência ao endpoint é relatado em tempo real, permitindo que os administradores de TI monitorem, facilmente, o estado de todos os endpoints gerenciados na organização.

Os administradores desfrutam de controle total de seus endpoints, permitindo que lidem várias vezes com a quantidade de trabalho de outros produtos que exigem intervenção manual significativa e apresentam atrasos no processo de emissão de relatório.

Etapa 6: Emita o relatório

Antes: Emitir um relatório é um componente crítico do processo de gerenciamento de patches. A aderência e as políticas corporativas exigem painéis altamente detalhados e atualizados, bem como relatórios que indicam a posição de risco da organização e o estado de gerenciamento de patch para uma variedade de clientes, incluindo auditores de aderência, executivos, gerência e, inclusive, usuários finais. Sem uma solução geral, não há um modo claro de efetuar o relatório sobre o estado de patch em toda a organização.

Depois: As capacidades de emissão de relatório, integradas à internet, do Tivoli Endpoint Manager permitem aos usuários finais, administradores, executivos, gerentes e outros uma visão atualizada sobre o momento de painéis e relatórios que indicam quais patches foram implantados, quando, por quem e em quais endpoints. Painéis especiais "por meio de clique" mostram o andamento, em tempo real, do gerenciamento do patch.



Relatórios em painéis no Tivoli Endpoint Manager mostram o andamento, em tempo real, do gerenciamento de patch.

Como funciona

As abordagens tradicionais de gerenciamento de patch utilizam processos manuais e pesados mecanismos baseados em varredura e agrupamento que não são suficientemente rápidos e baratos para atender às exigências de negócio e as exigências regulatórias, levando as organizações a riscos e custos inaceitavelmente elevados. Várias organizações que tentam utilizar ferramentas "gratuitas" ou de baixo custo, como o Windows Server Update Services (WSUS) rapidamente percebem que estas soluções não são para um nível empresarial. Elas estão limitadas a um único distribuidor, que não oferece controle organizacional sobre quais patches vão onde e quando, interrompem o usuário final e oferecem débeis opções de emissão de relatório, o que não reflete o estado em tempo real. O WSUS é um exemplo perfeito de um integrador utilizado para atender somente uma etapa no processo de gerenciamento de patch descrito acima, todavia, é utilizado porque é visualizado como "gratuito".

A Microsoft apresentou ciclos regulares de lançamento de patch, conhecidos como "Patch Tuesdays" que, infelizmente, resultaram em "Hack Wednesdays", dia no qual os criminosos virtuais recebem oportunidades de ouro para explorar os endpoints sem patches, sem ter de trabalhar para descobrir as vulnerabilidades. Os endpoints que não são imediatamente submetidos a patch se tornam uma janela de oportunidades para os criminosos – e a janela para um risco organizacional. Ademais, as organizações devem gerenciar atualizações para uma ampla variedade de produtos de distribuidores e fatores de forma de hardware – não apenas o Windows.

O Tivoli Endpoint Manager lidera o mercado em termos de largura de cobertura, velocidade, automação e relação custo-benefício, oferecendo patches abrangentes de sistema operacional e de aplicativos de terceiros. A solução, que inclui implantação de um agente único, multipropósito, leve e inteligente para todos os endpoints, é compatível com uma ampla variedade de tipos de dispositivos variando de servidores para PCs desktop, laptops "remotos" conectados à internet e equipamento especializado como dispositivos de ponto de venda (PV), ATMs e quiosques de autoatendimento.

Um servidor único de gerenciamento pode atender até 250.000 endpoints, independentemente de sua localização, tipo de conexão e velocidade ou estado, bem como os servidores podem oferecer, virtualmente, escalabilidade ilimitada. Os controles com base em políticas oferecem aos administradores de TI capacidades de gerenciamento de patch, de modo específico e altamente automatizado, bem como relatórios abrangentes que suportam os requisitos de aderência. A aderência à política é continuamente avaliada e reforçada pelo agente inteligente, independentemente da conectividade de endpoint para a rede. Outros produtos são pesados back-end, exigindo quantidades massivas de hardware e equipe para suportar as implantações – em vários casos, dezenas, pontos ou inclusive, centenas de servidores, múltiplos agentes por endpoint e um exército de operadores – para suportar o mesmo ambiente que o Tivoli Endpoint Manager lida com um servidor de gerenciamento, um agente de endpoint e apenas 1/20 da equipe.

Outro aspecto principal da arquitetura é o suporte para endpoints que estão ou não na rede corporativa. Os dispositivos remotos como laptops, por exemplo, podem receber patches por meio de qualquer conexão com a internet, como sem fio ou discada. O processo de gerenciamento de patch é virtualmente transparente ao usuário e as mensagens IBM Fixlet controlam a quantidade total de largura de banda e de CPU consumidos pelo agente de endpoint, que está ciente da localização e da conexão para otimizar o uso da rede.

Aderência contínua

Várias organizações necessitam estabelecer, documentar e comprovar a aderência com os processos de gerenciamento de patch para atender às regulamentações governamentais, contratos em nível de serviço (SLAs) e políticas corporativas. As regulamentações como Sarbanes-Oxley, PCI DSS e HIPAA/HITECH exigem um processo de gerenciamento de patch regular e completamente documentado no local e a comprovação de aderência contínua é necessária para aprovação em auditorias. Infelizmente, várias organizações gastam uma quantidade enorme de tempo e recursos no gerenciamento de patch e ainda assim não conseguem atender aos requisitos de aderência. A capacidade do Tivoli Endpoint Manager em reforçar políticas e emitir relatórios rapidamente sobre a aderência pode ajudar a melhorar a prontidão e as taxas de aprovação da organização em auditorias.

O uso dado pelos clientes

As organizações atendem aos desafios do gerenciamento de patch encabeçado com o uso do Tivoli Endpoint Manager. Para clientes, os resultados incluíram implantação mais rápida, melhor aderência, custos reduzidos de TI e ciclos mais curtos de gerenciamento.

Desafio: Implantar o gerenciamento de patch em dias ou semanas – não em meses ou anos

- O Condado de Albany, NY, consolidou várias ferramentas de gerenciamento de patch e configuração em apenas dois dias.
- O O'Charley's Restaurants implantou patches em mais de 350 restaurantes em apenas quatro dias.
- O SunTrust Banks implementou uma solução para 50.000 endpoints distribuídos em, aproximadamente, 1.800 locais, em três meses, com apenas duas pessoas.
- A International Islamic University Malaysia concluiu uma implantação completa em 7.000 computadores fixos e portáteis em sete campi da universidade com restrição de largura de banda, em apenas seis semanas.

Desafio: atingir a aderência com SLAs, políticas corporativas e regulamentações

- A Purolator atingiu 100% de aderência com um SLA de 24 horas a partir de seu respectivo provedor de serviço gerenciado.
- O SunTrust Banks atingiu 98,5% de aderência de patch em mais de 50.000 endpoints.
- O Concord Hospital aumentou a aderência de patch de 40 a 60% para 93%.
- A Entergy IT, que deve cumprir SLAs que exigem implantação de patch em mais de 22.000 endpoints dentro de um intervalo de 10 dias de lançamento, implantou mais de 4,9 milhões de patches em toda a empresa, desde 2004 – e não perdeu um único SLA durante o período.

Desafio: reduzir os custos de TI

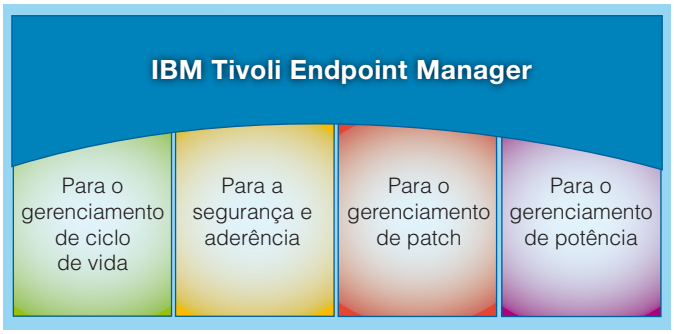
- A BGC Partners eliminou viagens caras a escritórios de filiais de serviço remoto em seis continentes, economizando dezenas de milhares de dólares.
- A Tax Tech reduziu equivalentes integrais de gerenciamento de patch (FTEs) de 20 para 1.
- A Stena Lines atingiu uma proporção de economia de trabalho de 12:1 por meio da redução do tempo de sobrecarga administrativa para processos de patch de 240 horas para 20 horas.
- A Western Federal Credit Union relatou uma redução de 50% nos custos trabalhistas por meio da automação e unificação de gerenciamento de patch.

Desafio: Reduzir os ciclos de gerenciamento de patch

- O Concord Hospital reduziu os ciclos de patch de semanas para apenas 15 minutos.
- O Sun Trust Banks reduziu os ciclos de patch de duas a três semanas para dois ou três dias.
- A Tex Tech automatizou completamente a distribuição noturna de patch para mais de 1.000 locais conectados por meio de VPN.
- O grupo de gerenciamento de desktop e de servidor da Entergy instalou 70.000 patches em toda a empresa, no período de 24 horas.
- A Kronos distribui atualizações, políticas e patches de software para todos os endpoints elegíveis, no período de 15 minutos, em todo o mundo.

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

A IBM oferece capacidades de gerenciamento de patch por meio de um produto autônomo – o IBM Tivoli Endpoint Manager for Patch Management – ou como uma parte integrante de duas das maiores soluções de gerenciamento de endpoint – IBM Tivoli Endpoint Manager for Lifecycle Management e IBM Tivoli Endpoint Manager for Security and Compliance. A família de Tivoli Endpoint Manager opera a partir do mesmo gabinete, servidor de gerenciamento e agente de endpoint, permitindo que as organizações consolidem ferramentas, reduzam o número de agentes de endpoint e reduzam os custos de gerenciamento.



IBM Tivoli Endpoint Manager é uma família de produtos que opera a partir do mesmo gabinete, servidor de gerenciamento e agente inteligente de endpoint.

O Tivoli Endpoint Manager é parte de um portfólio abrangente de segurança da IBM, ajudando as organizações a direcionar os desafios de segurança para os usuários e identidades, dados e informações, aplicativos e processos, redes, servidores e endpoints, bem como infraestruturas físicas. Pelo aprimoramento em tempo real da visibilidade e controle, bem como pelo aprimoramento da segurança e gerenciamento de endpoint, o portfólio da IBM é compatível com a expansão contínua atual, centros de dados mais inteligentes para facilitar as operações instrumentadas, interconectadas e inteligentes de TI de um planeta mais inteligente.

A tecnologia de Tivoli Endpoint Manager oferece:

- **Um agente único de inteligência** – o Tivoli Endpoint Manager utiliza uma abordagem líder do setor que coloca um único agente inteligente em cada endpoint. Este agente realiza múltiplas funções incluindo a autoavaliação contínua e o reforço da política – e ainda tem um impacto mínimo no desempenho do sistema, usando menos de 2% da CPU de endpoint, em média. O agente inicia ações de modo inteligente, enviando mensagens upstream para o servidor de gerenciamento central e reunindo patches, configurações e outras informações para o endpoint, quando necessário, para atender a uma política relevante. Como resultado da inteligência e velocidade do agente, o servidor central de gerenciamento sempre sabe a aderência e o estado de alteração dos endpoints, permitindo uma emissão de relatório de aderência rápida e atualizada.

- **Respostas instantâneas** – seja descobrindo como várias instâncias do Adobe® Acrobat estão instaladas ou validando quais laptops são impactados por um recall do fabricante, o Tivoli Endpoint Manager oferece respostas em questão de minutos – em toda a organização. Graças ao agente inteligente, não há necessidade de esperar por varreduras de longa conclusão, um servidor centralizado confere em detalhes ou milhares de consultas SQL para finalizar a execução antes que os painéis e relatórios sejam gerados. Cada agente avalia a relevância da questão, analisa as informações, relata e, inclusive, toma medidas com base na análise, se necessário.

- **Cobertura para endpoints remotos** – O laptop corporativo foi movimentado para além dos confins de um escritório corporativo. Os usuários se conectam a partir da casa, hotéis, aeroportos e, inclusive, de aviões. Sempre com um passo à frente, o Tivoli Endpoint Manager oferece uma capacidade única para gerenciar endpoints em tempo real – inclusive para dispositivos remotos.

Conclusão

O Tivoli Endpoint Manager direciona desafios principais atualmente enfrentados pelas organizações, oferecendo uma solução de gerenciamento de patch centralizada, em toda a organização, para o servidor, desktop e dispositivo móvel que automatiza e alivia grande parte do processo de teste de patch a partir de TI. O Tivoli Endpoint Manager implantado em dias e um único servidor de gerenciamento suporta até 250.000 endpoints, aumentando drasticamente as taxas de sucesso de patch, aprimorando a aderência regulatória e reduzindo gastos.

Em um mundo onde os segundos contam, o Tivoli Endpoint Manager pode diferenciar entre uma estratégia de gerenciamento de patch de sucesso e uma que leva a organização ao risco.

Para mais informações

Para mais informações sobre o IBM Tivoli Endpoint Manager, entre em contato com seu representante da IBM, com um parceiro de negócios da IBM ou visite:
ibm.com/tivoli/endpoint

Sobre o software Tivoli da IBM

O software Tivoli da IBM ajuda eficientemente às organizações e gerencia, eficazmente, os recursos, tarefas e processos de TI para atender aos requisitos de negócio constante e entrega um gerenciamento de serviço de TI flexível e responsivo, enquanto ajuda a reduzir os custos. O portfólio Tivoli amplia o software quanto à segurança, aderência, armazenamento, desempenho, disponibilidade, configuração, operações e gerenciamento de ciclo de vida em TI, e é respaldado por serviços, suporte e pesquisa mundiais da IBM.

Adicionalmente, as soluções financeiras do IBM Global Financing possibilitam o gerenciamento eficaz da verba, proteção contra a obsolescência da tecnologia, custo total aprimorado da propriedade e retorno do investimento. Ademais, nossos Global Asset Recovery Services ajudam a atender às questões ambientais com soluções novas e mais preocupadas com a relação entre energia e eficiência. Para mais informações sobre o IBM Global Financing, visite:
ibm.com/financing

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo - SP
Brasil

A página inicial da IBM pode ser localizada em:
ibm.com

Por favor, recicle.

O cliente da IBM é responsável por garantir sua própria aderência às exigências legais. É responsabilidade exclusiva de o cliente obter orientação de consultoria jurídica competente para identi,cação e interpretação de qualquer legislação relevante e exigências regulatórias que possam afetar o negócio do cliente e quaisquer ações do cliente que possam necessitar de aderência às referidas legislações. A IBM não oferece aconselhamento jurídico, representação ou garantia de que estes serviços ou produtos garantirão que o cliente esteja em conformidade com qualquer lei ou regulamentação.

[1] http://cybersecureinstitute.org

TIW14065-BRPT-00