GUIA PRÁTICO

SEJA VOCÊ QUEM COLOCA A SEGURANÇA EM PAUTA

Recomendações para ajudar a alinhar a segurança de TI com seus objetivos de negócios

Proteja seus negócios com a segurança
kaspersky.com/business
#securebiz

KASPERSKY lab

ÍNDICE

COLOQUE A SEGURANÇA EM PAUTA

PROMOVENDO NOVOS RENDIMENTOS

No atual ambiente corporativo, que muda tão rapidamente, as empresas que são rápidas em adotar novas tecnologias conseguem estabelecer uma vantagem significativa sobre a concorrência. Os desenvolvimentos mais recentes da TI, juntamente com o aprimoramento contínuo dos aplicativos de negócios, podem ajudar empresas de todos os tamanhos a:

- Incrementar a eficiência de seus processos de negócios diários.
- Melhorar seus níveis de atendimento ao cliente.
- Acelerar o tempo de colocação no mercado.
- Trabalhar mais de perto com fornecedores e parceiros de negócios.
- Adaptar-se às mudanças de requisitos em seus mercados-alvo.

... tudo gastando menos.

Por outro lado, talvez as empresas que demoram para aproveitar o potencial oferecido pelos novos processos de negócios – proporcionados pelas novas tecnologias – descubram que ficam sempre para trás das outras em termos de eficiência... e isso pode ter um impacto muito negativo sobre suas margens de lucro.

GARANTINDO QUE AS NOVAS TECNOLOGIAS NÃO TRAGAM NOVOS RISCOS

Em particular, as empresas se beneficiam de tecnologias que permitem maior mobilidade – incluindo iniciativas “Traga seu próprio dispositivo” (BYOD) – e de programas de virtualização de servidores e desktops. No entanto, da mesma forma que qualquer mudança empresarial, as novas tecnologias também podem introduzir novos desafios, inclusive riscos de segurança com potencial para causar danos graves para a empresa.

Há soluções avançadas de segurança disponíveis para proteger todos os elementos da rede corporativa de TI, mas apenas se a empresa investir o tempo necessário para selecionar a solução certa para cada possível problema de segurança. Além disso, é necessário ter o cuidado de selecionar somente produtos de segurança eficientes, que oferecem proteção abrangente sem colocar uma carga excessiva sobre os sistemas de TI e a equipe de administração de TI... ou reduzir a agilidade dos negócios.

Se a segurança não está na pauta de cada novo projeto de tecnologia de sua empresa, há uma possibilidade real de que posteriormente ela tenha que lidar com a perda de dados importantes, “vazamento” de informações confidenciais de clientes, interrupção de processos críticos para os negócios, problemas de conformidade, sanções financeiras, danos à reputação e muito mais.

ESTE É MAX, O DESTEMIDO ESPECIALISTA EM TI E SEGURANÇA

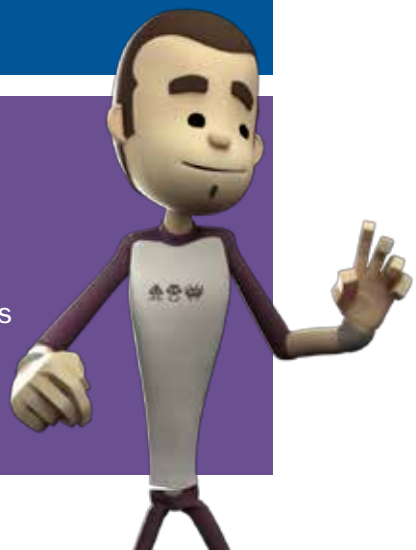
Gerente de TI de uma empresa com 150 funcionários, Max dedica sua vida profissional ao gerenciamento de tudo o que diz respeito aos sistemas e serviços de TI da empresa – físicos, virtuais e móveis. Ele também é responsável por manter todos os servidores, desktops e dispositivos móveis – além da segurança e proteção dos dados corporativos sigilosos.

Max precisa fazer malabarismos para realizar tantas tarefas e ainda ater-se às restrições orçamentárias. Por isso, está sempre à procura de soluções de TI que simplifiquem o suporte, automatizem as tarefas diárias e ajudem a controlar os custos.

Os superiores de Max não se dão conta dos desafios que ele enfrenta no dia a dia – eles só sabem que tudo tem que funcionar sem problemas. No entanto, eles também percebem que o sucesso da empresa depende cada vez mais da TI. A capacidade de Max de introduzir novas tecnologias e novos serviços de TI para melhorar os processos de negócios é crucial, e ele ainda precisa continuar com seu trabalho do dia a dia e garantir que as informações valiosas da empresa estejam protegidas.

UMA MENSAGEM DE MAX

"Infelizmente, pela experiência... Eu sei que as novas tecnologias podem introduzir novos riscos de segurança. Eu aprendi a considerar a segurança no início de cada projeto. Dessa forma, podemos avaliar os riscos, examinar se as tecnologias de segurança existentes são adequadas e, se necessário, fazer a adaptação de nossas políticas de segurança."



CAPACITANDO A EMPRESA SEM IMPOSSIBILITAR OS NEGÓCIOS

Mais do que nunca, a 'agilidade dos negócios' é essencial para o sucesso contínuo da empresa. Hoje, muitos dos fatores que podem afetar diretamente a rentabilidade de uma empresa estão sujeitos a mudanças mais rápidas do que era normal até poucos anos atrás, incluindo:

- Mudanças no comportamento e nas necessidades dos clientes.
- Alterações nos níveis de serviço que a concorrência oferece e que os clientes começam a exigir.

Empresas da área de manufatura sofrem pressão para lançar novos produtos rapidamente, enquanto os varejistas e empresas de serviços tentam constantemente encontrar formas de reduzir os custos operacionais a fim de se manterem competitivas.

Obviamente, é fundamental manter-se a par das novas tecnologias que podem ajudar a empresa a vencer esses desafios. Contudo, embora provavelmente a TI tenha um papel central na viabilização dos principais processos e no aumento da eficiência, vale a pena lembrar que a finalidade da rede corporativa de TI é atender à empresa. Todas as tecnologias que afetam negativamente as operações de negócios diárias ou atrasam a introdução de novos processos eficientes não estão servindo à empresa tão bem quanto deveriam.

Ocorre exatamente o mesmo com a segurança de TI. Embora seja extremamente importante proteger seus sistemas e os dados confidenciais armazenados neles, produtos de segurança complexos e com uma integração inadequada já não são adequados para empresas modernas, ágeis e eficientes.

A equipe de segurança de TI precisa cuidar da proteção sem 'impossibilitar' a agilidade dos negócios devido à:

- Lentidão dos processos essenciais.
- Limitação da capacidade da empresa de introduzir novas tecnologias que permitam novos processos.
- Incapacidade de um dimensionamento adequado conforme o crescimento da empresa.

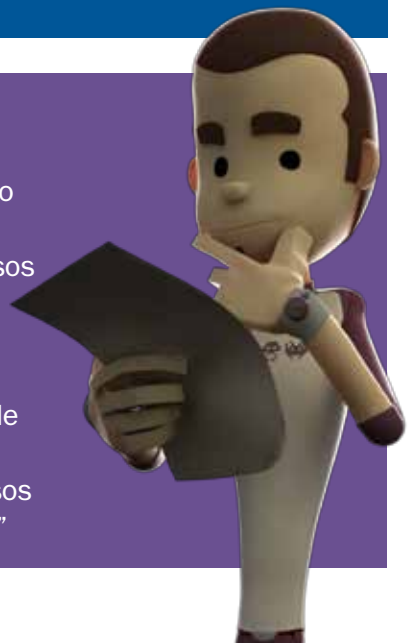
"A variedade dos produtos de segurança instalados em um único dispositivo tornou-se complicada de adquirir e gerenciar, além de serem caros. Em resposta a isso, muitas organizações agora compram um único produto capaz de lidar com vários requisitos de segurança. Os pacotes/as plataformas de segurança têm a vantagem de ser mais fáceis de instalar e gerenciar do que vários aplicativos, desde que possam ser gerenciados em um único console."

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS (ANÁLISE DE FORNECEDORES DE SEGURANÇA CORPORATIVA DE ENDPOINTS NA EUROPA OCIDENTAL 2012)
JANEIRO DE 2013, IDC #IS01V, VOLUME: 1

UMA MENSAGEM DE MAX

"No passado, eu passei muito tempo tentando trabalhar com produtos de segurança sem flexibilidade que nos obrigam a 'adaptar' nossos processos de negócios para adequá-los às limitações próprias do produto."

"No decorrer dos anos, cheguei à conclusão de que o melhor software de segurança é aquele capaz de 'envolver' nossos principais processos de negócios com suas camadas de proteção."



MUDANÇAS QUE ESTÃO TOTALMENTE FORA DE SEU CONTROLE

Embora a TI possa ser positiva no sentido de possibilitar mudanças para aumentar a eficiência e as margens de lucro, também está ocorrendo uma mudança menos desejável no ambiente dos negócios. O volume e a sofisticação dos malwares e ataques direcionados estão acelerando, e os criminosos virtuais estão se tornando mais organizados e profissionais em suas tentativas de roubar dinheiro, ter acesso a informações valiosas ou causar perturbações.

Os custos diretos para a recuperação de um ataque, incluindo sanções normativas, podem ser substanciais. No entanto, os custos indiretos, que incluem danos à reputação, ações judiciais de clientes e fornecedores cujas informações confidenciais foram acessadas sem autorização, perda de propriedade intelectual que davam à empresa uma vantagem competitiva e outros, podem ser ainda mais significativos.

PRINCIPAIS CONSIDERAÇÕES NA ESCOLHA DE UMA SOLUÇÃO DE SEGURANÇA EFICIENTE

O ANTIMALWARE É O PRIMEIRO PASSO ESSENCIAL EM SUAS DEFESAS

O software antimalware ainda é um elemento extremamente importante das defesas de TI de uma empresa. As boas soluções antimalware não contam apenas com a proteção baseada em assinaturas, mas também incluem:

- Análise heurística.
- Fornecimento em tempo real de dados baseados em nuvem sobre ameaças novas e emergentes.

A proteção baseada em assinaturas depende dos fornecedores de segurança analisarem cada novo programa de malware descoberto e fornecerem atualizações dos bancos de dados de malware para os dispositivos de endpoint. Porém, há um período durante o qual sua rede corporativa de TI pode ficar altamente vulnerável. Mesmo que o período entre o lançamento do novo programa de malware e a disponibilidade da nova atualização de assinaturas seja de apenas algumas horas, seus sistemas ainda ficam vulneráveis... a menos que o software de segurança inclua tecnologias adicionais de proteção.

A análise heurística fornece uma resposta mais proativa ao surgimento de novos malwares. Na ausência de uma assinatura de malware, a análise heurística pode detectar muitos itens de malware desconhecidos ou novas variações de uma ameaça existente.

O terceiro elemento essencial da proteção antimalware moderna é o fornecimento em nuvem. Com a adição de serviços baseados em nuvem, que fornecem dados em tempo real sobre novos malwares e outras ameaças, os fornecedores de segurança podem melhorar consideravelmente a capacidade da rede corporativa de TI de combater os ataques de malware mais recentes.

MAS SERÁ QUE O ANTIMALWARE É SUFICIENTE CONTRA AMEAÇAS NOVAS E COMPLEXAS?

Embora o antimalware seja um componente extremamente importante em suas defesas, e as soluções que combinam tecnologias baseadas em assinaturas, heurísticas e assistidas em nuvem forneçam níveis mais elevados de proteção do que as soluções anteriores, não é nada sensato confiar apenas no antimalware para proteger sua empresa e sua reputação.

Infelizmente, com as técnicas mais sofisticadas usadas pelos criminosos virtuais para comprometer a segurança corporativa, o antimalware não é mais suficiente para garantir a segurança de seus sistemas e seus dados.

Contra as ameaças de hoje, é essencial usar um produto de segurança que ofereça um sistema de tecnologias de segurança em vários níveis, incluindo:

- Antimalware
- Controle de Aplicativos com listas brancas dinâmicas
- Controle de Dispositivos
- Controle da Web
- Avaliação de Vulnerabilidades
- Gerenciamento de Correções
- Criptografia de Dados

... além de tecnologias de segurança especializadas para proteger dispositivos móveis, ambientes virtualizados e outros.

"A segurança de endpoints tradicional é sinônimo de antimalware. Não é segredo que as tecnologias antimalware baseadas em assinaturas não são tão eficientes contra os malwares modernos. Como resultado, a TI corporativa está deixando de lado as tecnologias antimalware pontuais e passando a implementar a defesa em camadas, com um conjunto de medidas que incluem não apenas o antimalware, mas também um firewall/IPS baseado em host, controles de aplicativos, controles de dispositivos e de mídia, e criptografia de endpoints."

THE FORRESTER WAVE™:
ENDPOINT SECURITY, Q1 2013
ENDPOINT SECURITY SUITES TAKE CENTER STAGE IN THE ENTERPRISE (OS PACOTES DE SEGURANÇA DE ENDPOINTS OCUPAM UM PAPEL CENTRAL NA EMPRESA)
FORRESTER RESEARCH, INC
4 DE JANEIRO DE 2013

UMA MENSAGEM DE MAX

"Além de prejudicar a empresa, as violações da segurança também podem resultar em sanções para a equipe administrativa sênior."

"Em muitas regiões, as agências normativas podem aplicar uma série de penalidades, que incluem multas e/ou detenção, aos diretores de qualquer empresa que tenha sido negligente em relação às medidas de segurança."

CONTROLES – PROTEGENDO SUA EMPRESA CONTRA ERROS DE SEGURANÇA DOS USUÁRIOS

CONTROLE DE APLICATIVOS E LISTAS BRANCAS DINÂMICAS

Aplicativos não autorizados podem surgir em sua rede corporativa de diversas formas, e alguns desses aplicativos indesejados podem representar um risco de segurança:

- Os usuários podem deliberadamente baixar aplicativos da Internet.
- Os usuários podem baixar aplicativos em seus desktops usando dispositivos removíveis de armazenamento.

Naturalmente, se você não tem a oportunidade de verificar e aprovar esses aplicativos, como pode ter certeza de que eles não contêm malware... e como pode garantir que sua presença na rede não gera problemas de licenciamento?

Os fornecedores de segurança desenvolveram recursos de Controle de Aplicativos que tornam mais fácil controlar quais aplicativos têm permissão para serem executados na rede. As ferramentas de Controle de Aplicativos podem possibilitar o gerenciamento de:

- Quais aplicativos podem ser executados (listas brancas).
- Quais aplicativos são bloqueados (listas negras).
- Qual é o comportamento dos aplicativos autorizados permitido durante sua execução (Controle de Privilégios de Aplicativos).

A maioria das ferramentas de Controle de Aplicativos permite escolher entre políticas do tipo Permissão Padrão ou Negação Padrão:

- Permissão Padrão – escolha essa opção para permitir que todos os aplicativos sejam executados, exceto aqueles incluídos na lista negra de programas que serão bloqueados.
- Negação Padrão – escolha essa política para certificar-se de que seja bloqueada a execução de todos os aplicativos, exceto aqueles incluídos na lista branca de programas seguros que têm permissão para ser executados.

A opção de negação Padrão pode ser especialmente útil para ajudar a evitar a execução de malware e também impedir que os usuários executem aplicativos que não são relevantes para seu trabalho. No entanto, é muito mais fácil aplicar uma política de Negação Padrão, caso seu fornecedor de segurança ajude na avaliação da segurança de aplicativos comuns por meio da análise de programas em seu próprio 'laboratório de listas brancas'.

"A proteção contra ataques altamente direcionados, novos e de baixo volume requer uma abordagem mais proativa baseada em processos sólidos de gerenciamento de operações, como funcionalidades de análise de vulnerabilidades, gerenciamento de correções e controle de aplicativos. Em particular, o controle de aplicativos, que restringe a execução de aplicativos reconhecidamente íntegros, está se mostrando eficaz em ambientes de segurança exigentes, sendo especialmente eficiente em combinação com o suporte a alterações confiáveis e complementado com serviços de reputação de arquivos baseados em nuvem."

QUADRANTE MÁGICO PARA PLATAFORMAS DE PROTEÇÃO DE ENDPOINTS

CONTROLE DE DISPOSITIVOS

Os dispositivos removíveis de armazenamento, que incluem unidades flash USB, cartões SD e discos rígidos externos, podem ser usados para roubar dados confidenciais ou baixar malware na rede corporativa. Assim, seu uso deve ser bem controlado.

Os recursos de Controle de Dispositivos podem facilitar a identificação dos dispositivos que têm autorização de uso na rede corporativa e daqueles não autorizados, usados por funcionários ou prestadores de serviços para se conectar a seus sistemas. Além disso, o Controle de Dispositivos permite:

- Bloquear tipos específicos de dispositivos; por exemplo, todos os armazenamentos removíveis.
- Bloquear todos os dispositivos que usam um tipo específico de barramento; por exemplo, todos os dispositivos USB.
- Bloquear dispositivos individuais de acordo com seus identificadores exclusivos.
- Impor a criptografia ao copiar arquivos para um dispositivo removível.
- Configurar restrições de dispositivos em horários específicos do dia.

OS DISPOSITIVOS USB AJUDAM A POSSIBILITAR ATAQUES DE GRANDE VISIBILIDADE

Acredita-se que um dos ataques mais conhecidos contra o proprietário de uma infraestrutura crítica tenha sido executado usando uma simples unidade flash USB. É provável que o Stuxnet, um worm de sabotagem virtual, tenha sido baixado de um dispositivo USB para os sistemas de uma instalação nuclear.

CONTROLE DA WEB

O acesso descontrolado dos funcionários à Internet pode afetar a segurança e a produtividade de sua empresa.

Mesmo que seus funcionários visitem apenas sites legítimos enquanto cumprem suas tarefas diárias, como você pode ter certeza de que esses sites são seguros? Há muitos casos de criminosos virtuais que invadem sites autênticos, e os visitantes inocentes ficam sujeitos a “execuções por download”, em que o malware é baixado automaticamente para o dispositivo do usuário. Obviamente, isso cria uma oportunidade para o malware se espalhar por toda sua rede corporativa de TI.

Um pouco além dos riscos de segurança que a Internet pode representar, a navegação na Web também pode ser uma grande distração e afetar a produtividade dos funcionários.

Algumas soluções de segurança incluem recursos flexíveis de Controle da Web que permitem:

- Bloquear completamente o acesso a sites específicos ou categorias de sites; por exemplo, sites de jogos ou com conteúdo para adultos.
- Bloquear completamente o acesso a sites que possibilitam downloads ilegais ou não autorizados, inclusive de aplicativos sem licença.
- Limitar o acesso a sites de redes sociais; por exemplo, permitindo o acesso apenas durante o intervalo de almoço.
- Usar as informações mais recentes fornecidas em tempo real a partir da nuvem a fim de alertar os usuários sobre sites infectados ou perigosos e ajudar a impedir infecções executadas por download.

IMPEDINDO A EXPLORAÇÃO DE VULNERABILIDADES

Uma das maneiras mais comuns em que os criminosos virtuais conseguem acessar computadores e dispositivos móveis é usando vulnerabilidades nos sistemas operacionais ou aplicativos. Essas vulnerabilidades surgem normalmente de 'bugs' no código do aplicativo ou sistema operacional. Assim que a comunidade de hackers identifica um novo bug e trabalha para explorá-la, a notícia sobre a vulnerabilidade se espalha rapidamente, e pode ser desencadeado um número crescente de novos ataques.

Como as empresas mais modernas dependem de uma grande variedade de aplicativos de software e, possivelmente, de várias versões diferentes de um sistema operacional, pode ser muito difícil para os departamentos de TI acompanhar as vulnerabilidades mais recentes e descobrir se os desenvolvedores de software já lançaram correções ou patches para elas. Além disso, não é fácil priorizar a distribuição das correções necessárias e depois implementá-las.

AVALIAÇÃO DE VULNERABILIDADES

Embora normalmente a Avaliação de Vulnerabilidades seja associada ao gerenciamento de sistemas e não à segurança, ela é fundamental para ajudar na proteção da rede corporativa de TI contra ataques. Por isso, é essencial escolher uma solução de segurança ou de gerenciamento de sistemas que verifique automaticamente as vulnerabilidades da rede.

GERENCIAMENTO DE CORREÇÕES

Obviamente, a identificação das vulnerabilidades do sistema operacional e de aplicativos presentes na rede corporativa é apenas a primeira fase. Depois, você precisa priorizar e implementar as correções e atualizações de software mais recentes. Novamente, essa pode ser considerada uma atividade de gerenciamento de sistemas, mas é uma tarefa capaz de melhorar significativamente sua segurança. Os bons softwares de segurança ou de gerenciamento de sistemas podem ajudar a automatizá-la.

UMA MENSAGEM DE MAX

"Com o amadurecimento dos mercados de segurança de TI e de software de gerenciamento de TI, começaram a surgir soluções de segurança e de gerenciamento de sistemas totalmente integrados. Felizmente, foi-se o tempo de usar 'soluções pontuais' de diferentes fornecedores e tentar fazê-las funcionarem juntas!"

"No entanto, vale a pena conferir a realidade por trás das afirmações sobre integração dos fornecedores. Se um fornecedor 'incorpora' uma nova funcionalidade simplesmente por meio da compra da solução de outro fornecedor, talvez possa haver problemas. Tente confirmar se há algo além de uma 'integração aparente' que simplesmente oculta uma série de problemas operacionais."

CRIPTOGRAFIA DE DADOS

Se um funcionário perder um laptop, uma unidade flash USB ou um disco rígido removível, dados empresariais sigilosos poderão cair em mãos erradas, o que pode sair muito caro. No entanto, se os dados foram criptografados, a perda do dispositivo não necessariamente leva à perda dos dados confidenciais que estão em formato legível. Depois de criptografados, os dados só podem ser 'decodificados' de imediato para um formato legível usando o algoritmo de descriptografia necessário.

Apesar de estar disponível há muitos anos, a criptografia de dados não é usada por todas as empresas. Isso se deve em parte pela não facilidade de uso de alguns produtos de criptografia disponíveis no mercado. Muitos se mostram complexos demais de configurar e gerenciar, ou afetam negativamente o desempenho da TI.

No passado, isso levou muitas empresas a abandonar o uso da criptografia em favor do desempenho e da produtividade. No entanto, os fornecedores de segurança responderam à demanda de soluções mais eficientes e agora é possível comprar produtos de criptografia fáceis de usar.

A MOBILIDADE TRAZ AINDA MAIS RISCOS

Os dispositivos móveis revolucionaram a forma como empresas e trabalhadores remotos podem interagir e obter mais de seu dia de trabalho.

Os smartphones são muito mais do que simples telefones. Como são computadores poderosos capazes de armazenar uma grande quantidade de dados corporativos confidenciais, juntamente com códigos de acesso e senhas de sua rede corporativa, você precisa protegê-los da mesma maneira que protege seus desktops e servidores.

No entanto, a portabilidade dos smartphones, tablets e laptops também introduz riscos de segurança adicionais. Todos esses dispositivos estão fora do seu perímetro de segurança tradicional. Eles podem ser facilmente perdidos ou roubados, o que resultaria no acesso de usuários não autorizados a sua rede corporativa.

AS INICIATIVAS BYOD ACRESCENTAM MAIS COMPLICAÇÕES

As iniciativas do tipo Traga Seu Próprio Dispositivo (BYOD) oferecem muitos benefícios para empresas e funcionários. No entanto, o fato dos funcionários usarem dispositivos que contêm informações confidenciais corporativas e dados pessoais do usuário pode apresentar riscos.

Além disso, se os funcionários tiverem a liberdade de usar praticamente qualquer dispositivo móvel, a tarefa de gerenciar as permissões de acesso aos sistemas corporativos e garantir que todos tenham softwares de segurança eficientes instalados pode ser particularmente complicada.

É fundamental escolher uma solução de segurança móvel que inclua recursos abrangentes de gerenciamento de dispositivos móveis (MDM).

OS AMBIENTES VIRTUALIZADOS TAMBÉM SÃO VULNERÁVEIS

Os ambientes virtualizados de servidor e desktop podem ajudar as empresas a controlar os custos de aquisição de hardware e reduzir os custos de manutenção, energia e licenciamento. Além disso, como é possível implementar as máquinas virtuais rapidamente, a virtualização pode aumentar a agilidade dos negócios, garantindo o fornecimento de novos serviços de TI à empresa sem atrasos desnecessários.

Apesar do mito comum de que as máquinas virtuais são de algum modo mais seguras do que os servidores e desktops físicos, todas as máquinas virtuais precisam ser protegidas da mesma forma que o hardware físico. No entanto, as tecnologias de segurança usadas para proteger os ambientes virtuais podem ser bastante diferentes dos produtos de segurança que defendem a infraestrutura de TI física.

A execução de uma solução tradicional de segurança baseada em agentes em cada máquina virtual limitará bastante a taxa de consolidação que se pode alcançar, o que significa que seu projeto de virtualização terá um retorno menor sobre o investimento. Em vez disso, é melhor escolher uma solução de segurança otimizada para ambientes virtuais. Isso pode eliminar a necessidade de ter bancos de dados antimalware e agentes de segurança idênticos em cada máquina virtual.

SAIBA MAIS...

... sobre os desafios de proteger ambientes virtualizados.

Obtenha o último relatório da Kaspersky Lab:

Guia prático – Segurança para virtualização

Dicas para ajudá-lo a proteger seus sistemas e dados corporativos sigilosos.

QUANDO A SEGURANÇA ESTÁ FORTEMENTE INTEGRADA COM O GERENCIAMENTO DE SISTEMAS

Como os recursos de avaliação de vulnerabilidades e gerenciamento de correções bem executados podem ter um efeito bastante positivo sobre a segurança geral dos seus sistemas, há um forte argumento para a escolha de uma solução de segurança que inclua essas e outras funções de gerenciamento de sistemas.

Muitas empresas executam pacotes de software de segurança e de gerenciamento de sistemas separados, de fornecedores diferentes. Porém, isso pode tornar o gerenciamento da segurança dos sistemas mais complexo de configurar e controlar, e também:

- Aumentar a sobrecarga sobre a administração de TI.
- Criar lacunas na segurança corporativa.

Por outro lado, uma solução que combina funcionalidades de segurança e gerenciamento de sistemas em um único produto, desenvolvido por um único fornecedor pode simplificar os dois conjuntos de tarefas.

Algumas soluções combinadas de segurança e gerenciamento de sistemas também têm um console de gerenciamento unificado para todas as tarefas. Isso pode proporcionar grandes benefícios para os administradores de TI:

- Há apenas um conjunto de recursos para aprender.
- Não há necessidade de alternar entre diferentes consoles para o gerenciamento da segurança e dos sistemas.
- É possível implementar políticas únicas para englobar problemas de segurança e de gerenciamento de sistemas.

UMA MENSAGEM DE MAX

"À primeira vista, a necessidade de usar dois ou três consoles diferentes para gerenciar as tecnologias individuais de segurança e gerenciamento de diferentes fornecedores pode parecer uma tarefa trivial para um administrador profissional de TI."

"No entanto, na prática, ela é surpreendentemente demorada e pode facilmente gerar erros, especialmente quando você está sob pressão para reagir rapidamente a um problema de segurança."

COMO A KASPERSKY LAB PODE AJUDAR... SEGURANÇA E GERENCIAMENTO DE SISTEMAS INTEGRADOS

A Kaspersky Lab integrou ao premiado antimalware, além das tecnologias flexíveis de controle, criptografia de dados, segurança móvel e segurança para virtualização, tecnologias de gerenciamento de sistemas e gerenciamento de dispositivos móveis (MDM)... para que você possa gerenciar a segurança e a infraestrutura de TI em um único produto e um único console de gerenciamento.

"A mais recente plataforma Kaspersky Endpoint Security for Business (KESB) demonstra a capacidade da empresa para desenvolver ofertas baseadas nos problemas que desafiam as complexidades de recursos, gerenciamento e custos dessa categoria. O IDC posiciona a Kaspersky Lab como Líder no Western Europe Endpoint Security Software IDC MarketScape (IDC MarketScape de software de segurança de endpoints na Europa ocidental)."

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS (ANÁLISE DE FORNECEDORES DE SEGURANÇA CORPORATIVA DE ENDPOINTS NA EUROPA OCIDENTAL 2012)
JANEIRO DE 2013, IDC #IS01V, VOLUME: 1

A Kaspersky Lab é reconhecida como "Líder" no Quadrante Mágico do Gartner para Plataformas de Proteção de Endpoints.

QUADRANTE MÁGICO PARA PLATAFORMAS DE PROTEÇÃO DE ENDPOINTS
8 DE JANEIRO DE 2014
GARTNER, INC.

PROTEÇÃO ANTIMALWARE AVANÇADA

As tecnologias antimalware mais recentes da Kaspersky Lab oferecem uma poderosa combinação de:

- Proteção baseada em assinaturas.
- Tecnologias proativas.
- Fornecimento assistido em nuvem da proteção contra novos malwares.

... para plataformas Mac, Linux e Windows, além de uma ampla gama de dispositivos móveis, incluindo Android, iOS, Windows Phone, Windows Mobile, BlackBerry e Symbian.

Com a atualização contínua do banco de dados do Sistema de Detecção Urgente Kaspersky com informações sobre novas descobertas de malware, as avançadas tecnologias antimalware da Kaspersky Lab protegem as empresas contra as ameaças e os ataques mais recentes, até mesmo antes do lançamento da assinatura do novo malware.

Além disso, a tecnologia Inspetor do Sistema da Kaspersky monitora o comportamento dos aplicativos executados em seus endpoints. Quando o Inspetor do Sistema detecta comportamentos suspeitos, o aplicativo é bloqueado e as mudanças maliciosas são revertidas automaticamente.

A Kaspersky Lab continua a inovar com a introdução de novas tecnologias antimalware, incluindo a Prevenção Automática contra Exploits (AEP), que monitora os sistemas para identificar comportamentos comumente executados por malwares que tentam explorar vulnerabilidades do sistema operacional ou dos aplicativos. A AEP bloqueia efetivamente os exploits para proteger os sistemas contra exploits de dia zero.

FERRAMENTAS FLEXÍVEIS DE CONTROLE

CONTROLE DE APLICATIVOS

As ferramentas de Controle de Aplicativos da Kaspersky Lab fornecem controle granular sobre as permissões de execução de aplicativos na rede corporativa; assim, você pode facilmente implementar políticas de Negação Padrão ou Permissão Padrão:

- A Negação Padrão permite bloquear todos os programas, exceto aqueles que se encontram na lista branca.
- A Permissão Padrão bloqueia apenas os aplicativos contidos na lista negra e permite que todos os outros programas sejam executados.

LISTAS BRANCAS DINÂMICAS

A Kaspersky Lab é o único fornecedor de segurança que conta com um laboratório de listas brancas próprio, onde os aplicativos mais utilizados são avaliados e verificados em relação a riscos de segurança. As atualizações da lista branca dinâmica de aplicativos da Kaspersky Lab são baixadas automaticamente da Kaspersky Security Network baseada em nuvem para facilitar a aplicação de uma política de Negação Padrão, usando informações atualizadas sobre os aplicativos.

Enquanto alguns fornecedores atualizam sua lista branca de aplicativos de forma não muito frequente, as listas brancas dinâmicas da Kaspersky Lab oferecem proteção superior.

CONTROLE DE DISPOSITIVOS

Os recursos de Controle de Dispositivos da Kaspersky Lab ajudam a controlar o uso de dispositivos removíveis para que você possa se proteger contra os riscos de segurança introduzidos por dispositivos não autorizados. Com eles, é fácil:

- Controlar privilégios de acesso de tipos específicos de dispositivos, um barramento específico ou um dispositivo individual.
- Definir períodos em que suas políticas de Controle de Dispositivos são aplicadas; por exemplo, para impedir que dispositivos acessem a rede corporativa fora do horário normal de expediente.

CONTROLE DA WEB

As ferramentas de Controle da Web simplificam a tarefa de monitorar e filtrar o uso da Web por cada funcionário. A Kaspersky Lab torna rápido e simples gerenciar controles que permitem, proíbem, limitam ou auditam o acesso dos usuários a sites específicos ou categorias de sites, incluindo sites de jogos, jogos de azar ou redes sociais.

A Kaspersky Lab também avalia a reputação de sites e fornece avisos em tempo real a partir da nuvem para ajudar os usuários a evitar sites perigosos e infecções automatizadas.

"Por causa da extensiva potência de sua segurança e seu preço atraente, esperamos que muitas organizações cheguem à Kaspersky Lab ao considerar um produto de segurança de endpoints."

THE FORRESTER WAVE™: ENDPOINT SECURITY, Q1 2013
ENDPOINT SECURITY SUITES TAKE CENTER STAGE IN THE ENTERPRISE (OS PACOTES DE SEGURANÇA DE ENDPOINTS OCUPAM UM PAPEL CENTRAL NA EMPRESA)
FORRESTER RESEARCH, INC
4 DE JANEIRO DE 2013

VERIFICAÇÃO DE VULNERABILIDADES E GERENCIAMENTO DE CORREÇÕES

O aplicativo Gerenciamento de Sistemas Kaspersky inclui a verificação automática de vulnerabilidades, além da funcionalidade de distribuição de correções, para ajudar a manter a estabilidade e a segurança de sua rede corporativa

VERIFICAÇÃO DE VULNERABILIDADES

As tecnologias da Kaspersky Lab verificam seus endpoints para localizar vulnerabilidades de segurança produzidas por sistemas operacionais e aplicativos sem correções. Além do banco de dados de vulnerabilidades da própria Kaspersky Lab, a verificação também utiliza os bancos de dados da Secunia e da Microsoft.

AUTOMATIZANDO A DISTRIBUIÇÃO DE CORREÇÕES

Todas as vulnerabilidades identificadas durante uma verificação são "codificadas com cores" para ajudá-lo a decidir as prioridades das correções. As tecnologias da Kaspersky Lab podem distribuir automaticamente as correções urgentes por toda a rede, e você pode programar atualizações de software não urgentes para fora do horário de expediente normal.

CRIPTOGRAFIA DE DADOS FÁCIL DE USAR

As ferramentas de criptografia da Kaspersky Lab fornecem:

- Criptografia Total do Disco (FDE) – que opera nos setores físicos do disco para uma estratégia "criptografar tudo de uma vez".
- Criptografia em Nível de Arquivos (FLE) – que criptografa arquivos ou pastas individuais para permitir o compartilhamento seguro de dados entre funcionários e parceiros de confiança.

Embora um algoritmo de criptografia AES com comprimento de chave de 256 bits forneça criptografia forte, todos os processos de criptografia e descriptografia são totalmente transparentes para seus usuários. Em vez disso, os administradores de TI configuram políticas simples que controlam quais arquivos e discos são criptografados automaticamente. Além disso, os processos de criptografia e descriptografia não têm impacto significativo sobre o desempenho da TI.

Para a criptografia de dispositivos móveis, o Kaspersky permite gerenciar as instalações de criptografia residentes em muitas plataformas móveis comuns.

SEGURANÇA E GERENCIAMENTO DE DISPOSITIVOS MÓVEIS

A Kaspersky Lab foi um dos primeiros fabricantes a oferecer soluções antivírus para dispositivos móveis. Hoje, a empresa é líder no fornecimento de agentes antimalware avançados e funcionalidades eficientes de Gerenciamento de Dispositivos Móveis (MDM) em uma única solução integrada.

As tecnologias de segurança móvel da Kaspersky Lab protegem uma grande variedade de plataformas móveis, que incluem Android, iOS, Windows Phone, Windows Mobile, BlackBerry e Symbian, contra as mais recentes ameaças de malware. Como a Kaspersky Lab combina proteção baseada em assinaturas, defesas proativas e tecnologias baseadas em nuvem, os dispositivos móveis tiram proveito do antimalware em vários níveis.

FERRAMENTAS DE CONTROLE

O Controle de Aplicativos também facilita o gerenciamento dos aplicativos que têm permissão para ser executados em dispositivos móveis. É fácil implementar uma política "negação padrão" que só permite a execução de aplicativos da lista branca ou uma política "negação padrão" que bloqueia apenas os aplicativos da lista negra.

As ferramentas de Controle da Web permitem bloquear sites maliciosos e sites que não estão de acordo com suas políticas corporativas de segurança ou de uso da Internet.

SEPARANDO DADOS CORPORATIVOS E DADOS PESSOAIS PARA INICIATIVAS BYOD MAIS SEGURAS

A tecnologia de conteinerização da Kaspersky Lab facilita a separação de dados corporativos e informações pessoais no dispositivo móvel do usuário.

Um contêiner especial mantém os aplicativos corporativos, e você pode ativar a criptografia dos dados corporativos. Se um funcionário sair da empresa, você poderá executar remotamente um procedimento de limpeza seletiva que exclui todos os dados corporativos do dispositivo móvel dele.

LIDANDO COM DISPOSITIVOS MÓVEIS PERDIDOS OU ROUBADOS

Se um dispositivo móvel for perdido ou roubado, os recursos Kaspersky operados remotamente permitem:

- Travar o dispositivo móvel.
- Excluir dados corporativos ou todos os dados do dispositivo.
- Encontrar a localização aproximada do dispositivo.

Mesmo que um ladrão troque o chip do dispositivo, a tecnologia Verificação do Chip da Kaspersky Lab enviará o novo número do telefone para você. Assim, será possível acessar os recursos remotos de bloqueio, localização e limpeza de dados.

SIMPLIFICANDO O GERENCIAMENTO MÓVEL

As abrangentes funcionalidades de gerenciamento de dispositivos móveis (MDM) simplificam a implementação do agente de segurança móvel da Kaspersky Lab e de todos os outros aplicativos que você deseja distribuir, seja por conexão sem fio (OTA) ou usando um cabo, e incluem suporte para o Microsoft Exchange Active Sync e o Apple MDM Server.

UMA OPÇÃO DE TECNOLOGIA DE SEGURANÇA PARA VIRTUALIZAÇÃO

Com soluções de segurança para uma ampla gama de ambientes virtuais, incluindo VMware, Citrix e Microsoft, o Kaspersky Security for Virtualization permite escolher entre duas abordagens de segurança para virtualização, desenvolvidas para ajudar a minimizar o impacto sobre as taxas de consolidação e aumentar o retorno sobre o investimento.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Em ambientes virtuais baseados em VMware, o Kaspersky Security for Virtualization | Agentless opera por meio do VMware vShield, possibilitando a proteção de todas as máquinas virtuais em um host virtual com a instalação de uma única máquina virtual dedicada à segurança (dispositivo virtual de segurança ou VSA).
Além de oferecer proteção antimalware em nível de arquivos e em nível de rede, por meio da tecnologia Bloqueador de Ataques de Rede da Kaspersky Lab, o Kaspersky Security for Virtualization | Agentless também tira proveito dos dados em tempo real sobre ameaças da Kaspersky Security Network.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Com um dispositivo virtual de segurança dedicado instalado no host e um pequeno agente de software, chamado de agente leve, instalado em cada máquina virtual convidada, o Kaspersky Security for Virtualization | Light Agent oferece um nível mais alto de segurança do que as soluções de virtualização sem agentes. No entanto, ele ainda usa muito menos poder de processamento e capacidade de armazenamento do que é necessário para executar um produto de segurança tradicional baseado em agentes, por descarregar as tarefas antimalware e o banco de dados de definições de malware no dispositivo virtual de segurança.

Além da avançada proteção antimalware e da proteção em nível de rede, o Kaspersky Security for Virtualization | Light Agent também inclui ferramentas de Controle de Aplicativos, Controle de Dispositivos e Controle da Web.

ALTAS TAXAS DE CONSOLIDAÇÃO E ALTA DISPONIBILIDADE

Quer você escolha o Kaspersky Security for Virtualization | Agentless ou o Kaspersky Security for Virtualization | Light Agent, não é necessário reiniciar nenhum computador, nem colocar o servidor em modo de manutenção para implementar a solução de segurança Kaspersky.
Isso é de vital importância em qualquer central de dados ou empresa que precisa alcançar 99,999% de tempo de atividade.

COMBINANDO A SEGURANÇA E O GERENCIAMENTO DE SISTEMAS

GERENCIANDO O HARDWARE, O SOFTWARE E AS LICENÇAS

Com a descoberta automática de todo o hardware e software na rede corporativa de TI e o registro de todos os itens nos inventários de hardware e software, o Kaspersky oferece visibilidade detalhada de todos os seus recursos de TI. Isso ajuda a:

- Monitorar o status de segurança de seus sistemas.
- Aplicar as configurações de segurança necessárias.
- Identificar violações das condições das licenças.

IMPLEMENTAÇÃO DO SISTEMA OPERACIONAL

O Kaspersky ajuda a otimizar a implementação de sistemas operacionais, fornecendo recursos automáticos para a criação e clonagem de imagens de computador que podem ser armazenadas em um inventário específico, pronto para ser acessado durante a implementação.

PROVISIONAMENTO DE APLICATIVOS

O Kaspersky ajuda a simplificar a distribuição de aplicativos, facilitando a implementação de software por comandos ou de acordo com sua programação.

IMPLEMENTAÇÃO REMOTA DE SOFTWARE... E SOLUÇÃO DE PROBLEMAS

Sempre que você precisa instalar um software em um escritório remoto, o Kaspersky permite usar uma estação de trabalho local como agente de atualização para todo o site remoto. Além disso, o acesso remoto ajuda a simplificar a solução de problemas.

CONTROLE DE ACESSO À REDE:

Com tecnologias para descobrir automaticamente todos os dispositivos na rede corporativa, o Kaspersky torna mais fácil:

- Quais dispositivos têm permissão de acessar a rede.
- Verificar se cada dispositivo está em conformidade com suas políticas corporativas de segurança.
- Bloquear o acesso à rede de dispositivos que não têm o software de segurança necessário em execução.

UM ÚNICO CONSOLE DE GERENCIAMENTO UNIFICADO

As tecnologias de segurança e a funcionalidade de gerenciamento de sistemas da Kaspersky Lab podem ser configuradas e controladas em um único console de gerenciamento que fornece aos administradores de TI uma "exibição única". Eliminando a necessidade de executar vários consoles diferentes e incompatíveis, o Kaspersky Security Center reduz a complexidade e economiza o tempo de seu departamento de TI.

Assim, uma grande variedade de tarefas de administração e segurança são simplificadas em ambientes físicos, móveis e virtuais e você tira proveito:

- Da maior visibilidade de todos os endpoints da rede corporativa de TI.
- De uma interface simples com os recursos de segurança, MDM e gerenciamento de sistemas da Kaspersky Lab.
- Do controle detalhado sobre as atividades dos usuários, incluindo a forma como eles usam os aplicativos, os dispositivos e a Web.

HISTÓRICO COMPROVADO DE INOVAÇÕES E REALIZAÇÕES DA KASPERSKY LAB

Dentre muitos prêmios, elogios e reconhecimentos, a Kaspersky Lab recebeu o prêmio Product of the Year Award 2013 do laboratório de testes independentes AV-Comparatives depois que a solução de segurança de Internet da empresa demonstrou sistematicamente os melhores resultados nos testes durante todo o ano de 2013.

O programa de testes da AV-Comparatives é considerado o mais completo do setor e o prêmio Product of the Year baseia-se na classificação geral durante um ano de testes. O Kaspersky Lab Internet Security foi escolhido porque o produto mostrou uma liderança sólida em todos os testes aos quais foi submetido. A Kaspersky também recebeu o prêmio Product of the Year da AV-Comparatives em 2011 e ficou empatada no primeiro lugar em 2012.

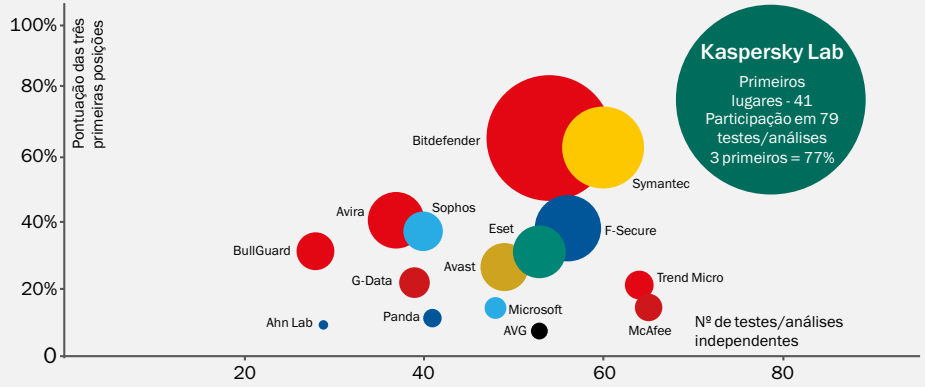
Como o Kaspersky Endpoint Security for Business emprega as mesmas tecnologias centrais de proteção antimalware usadas no Kaspersky Internet Security, sua empresa pode se beneficiar da premiada proteção da Kaspersky Lab.

Outros prêmios e realizações incluem:

- Prêmio 'Information Security Vendor of the Year' (Fornecedor do ano de segurança de informações) – Prêmios da SC Magazine Europa 2013.
- Prêmio 'Information Security Team of the Year' (Equipe de segurança de informações do ano) – Prêmios da SC Magazine Europa 2013.
- Vencedor do Excellence Award (Prêmio de excelência) – Prêmios da SC Magazine 2013.
- O Kaspersky Endpoint Security for Windows recebeu o maior prêmio em proteção antivírus corporativa do teste de abril–junho de 2013 da Dennis Technology Labs.
- O maior número de prêmios Gold e Platinum – em todas as categorias de teste – do laboratório terceirizado Anti-Malware Test Lab, desde 2004.
- Mais de 50 pontuações de aprovação no rigoroso sistema de testes da VB100, desde 2000.
- Prêmio Checkmark Platinum Product Award da West Coast Labs.

MAIS POSIÇÕES ENTRE AS TRÊS PRIMEIRAS DO QUE QUALQUER OUTRO FORNECEDOR

Em 2013, os produtos da Kaspersky Lab participaram de 79 testes e análises independentes. Nossos produtos foram premiados com 41 primeiros lugares e ficaram 61 vezes entre os três primeiros.



Observações:

- De acordo com o resumo de resultados dos testes independentes de 2013 para produtos corporativos, para o consumidor e dispositivos móveis.
- O resumo inclui testes realizados pelos seguintes laboratórios de testes independentes e revistas:
  Laboratórios de testes: Anti-Malware.ru, AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, TollyGroup, VB100.
  Revistas: CHIP Online, ComputerBild, Micro Hebdo, PC Magazine, PCWorld, PC Welt.
- No gráfico acima, o tamanho de cada círculo está relacionado com o número de primeiros lugares obtidos.

DICAS DE ESTRATÉGIA DE MAX PARA COLOCAR SEGURANÇA NA PAUTA

"Com o crescimento contínuo do volume e da sofisticação dos malwares e de outras ameaças, a segurança deve estar na pauta da estratégia de TI de todas as empresas."

- 'Dê um passo atrás' em sua rotina diária de TI e dedique algum tempo à avaliação das suas medidas de segurança de TI atuais. Avalie se elas são adequadas para enfrentar os desafios de hoje.
- Escolha a solução de segurança de TI mais flexível e escalonável possível, e evite usar produtos que limitem a agilidade dos negócios.
- Lembre-se de que a segurança de TI engloba muito mais do que apenas um antimalware. Procure soluções de segurança que oferecem proteção adicional, incluindo Controle de Aplicativos, Controle de Dispositivos, Controle da Web, criptografia de dados e outros recursos.
- Com a crescente utilização de dispositivos móveis, não se esqueça que os smartphones e tablets são capazes de armazenar grandes quantidades de dados corporativos confidenciais. Certifique-se de que todos os dispositivos móveis que acessam a rede corporativa e informações de negócios tenham um software de segurança adequado. Implemente o Gerenciamento de Dispositivos Móveis (MDM) para ajudar a monitorar e controlar os dispositivos móveis em sua rede.
- Antes de lançar uma iniciativa do tipo Traga Seu Próprio Dispositivo (BYOD), avalie como ela afetaria a segurança da empresa. Considere tecnologias de segurança que permitam separar dados corporativos e dados pessoais do usuário nos dispositivos móveis.
- Os ambientes virtualizados não são mais seguros do que os servidores e desktops físicos; todos eles precisam de proteção. No entanto, cuidado com a escolha de produtos de segurança para sua infraestrutura virtual. Uma tecnologia de segurança inadequada pode afetar negativamente as taxas de consolidação.
- Como as vulnerabilidades de software são uma das maneiras mais comuns usadas pelos malwares e criminosos virtuais para acessar computadores e redes, verifique se o seu software de gerenciamento de sistemas inclui funcionalidades de avaliação de vulnerabilidades e distribuição de correções. Embora essas funções estejam relacionadas ao gerenciamento de sistemas, elas podem afetar drasticamente a segurança.
- A escolha de um produto que combina segurança e gerenciamento de sistemas pode simplificar as tarefas e permitir a definição de políticas integradas... e isso pode representar uma grande economia de tempo.
- Em relação aos softwares de segurança de TI e de gerenciamento de sistemas, a facilidade de uso é muito mais do que apenas uma conveniência. Se o seu software de segurança e gerenciamento de sistemas é complexo e difícil de administrar, há um risco muito maior de erros e falhas de segurança.

"A Kaspersky Lab se concentra naquilo que faz muito bem: a segurança de endpoints. O alto nível de capacidade e os critérios estratégicos reconhecem o desenvolvimento orgânico da empresa que garante, sempre que possível, que os diversos componentes para estações de trabalho, laptops, e-mail, servidores de colaboração e gateways de Internet utilizem a mesma base de código para facilitar a atualização e a continuidade no caso de uma falha do produto."

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS (ANÁLISE DE FORNECEDORES DE SEGURANÇA CORPORATIVA DE ENDPOINTS NA EUROPA OCIDENTAL 2012)
JANEIRO DE 2013, IDC #IS01V, VOLUME: 1

SOBRE A KASPERSKY LAB

A Kaspersky Lab é o maior fornecedor privado de soluções de proteção de endpoints do mundo. A empresa está classificada entre os quatro principais fornecedores de soluções de segurança para usuários de endpoints do mundo*. Durante os seus mais de 16 anos de história, a Kaspersky Lab continua sendo inovadora em segurança de TI e fornece soluções de segurança digital eficientes para consumidores, pequenas e médias empresas e grandes corporações. Com sua empresa matriz registrada no Reino Unido, atualmente a Kaspersky Lab opera em quase 200 países e territórios ao redor do globo, fornecendo proteção para mais de 300 milhões de usuários em todo o mundo.

Saiba mais em kaspersky.com.br

*A empresa ficou na quarta posição na classificação da IDC de Worldwide Endpoint Security Revenue by Vendor. (Receita em segurança de endpoints no mundo por fornecedor), 2012. Essa classificação foi publicada no relatório da IDC "Worldwide Endpoint Security 2013-2017 Forecast and 2012 Vendor Shares (Previsão de 2013-2017 de segurança de endpoints em todo o mundo e participações de fornecedores em 2012) (IDC #242618, agosto de 2013). O relatório classificou os fornecedores de software de acordo com as receitas de vendas de soluções de segurança de endpoints em 2012.