MENOR CUSTO

Total de Proteção

KASPERSKY lab

Kaspersky Lab – Proteção Empresarial Consistente Elaborada da Melhor Forma

Em 2009, foi observado um crescimento exponencial na proliferação de malware em todo o mundo. Chegou-se a mais de 30.000 novas ameaças por dia, o que exigiu o lançamento diário de mais de 3.500 novas assinaturas de malware pelas empresas de antimalware. E 2010 não foi diferente. No primeiro trimestre de 2010, houve mais de 327 milhões de tentativas de infecção de mais de 119 milhões de servidores com malware encontrados na Internet. De acordo com a IBM, no primeiro semestre de 2010 houve um pico de 36% nos malwares em comparação ao ano passado, com mais de 10 milhões de novos malwares lançados "em campo".

Desafios para Todas as Organizações

Este cenário de rápida escalada das ameaças, as pressões da tecnologia que muda o tempo todo e a mudança constante da forma de se fazer negócios causam inúmeros problemas para as empresas, independentemente de seu tamanho ou setor:

- **Proteção de Ambientes Descentralizados:** atualmente, os dados são o principal alvo do crime virtual. Porém, os dados não residem mais unicamente no mainframe ou no farm de servidores protegidos. Como resposta, as organizações devem ter proteção premium em todos os lados onde houver dados, o que normalmente resulta em uma sobrecarga no gerenciamento e na utilização de recursos. É necessário proteger os sistemas dentro dos limites do perímetro corporativo, além dos dispositivos móveis, laptops e smartphones que carregam dados de propriedade de empresa. De fato, uma pesquisa da Forrester Research descobriu que a adoção de smartphones e de aplicativos e serviços baseados na Web representam atualmente as duas principais preocupações com a segurança de TI.
- **Gerenciamento de Ambientes Heterogêneos:** devido crescente adoção de sistemas operacionais de software livre ou não da Microsoft na organização de TI, os sistemas operacionais Microsoft Windows deixaram de ser o único alvo dos criminosos virtuais. Hoje em dia, as organizações precisam dar suporte e proteger diversas plataformas: Microsoft, Novell, Linux, Mac e outras. Uma pesquisa recente da Forrester mostrou que 73% das empresas citam a complexidade de seus ambientes de TI como um "desafio importante" para a organização e 45% dizem que outro desafio também é o fato de haver fornecedores de segurança demais para gerenciar. Essa demanda de suporte e proteção pode gerar uma sobrecarga significativa, especialmente se forem necessários vários consoles de gerenciamento.
- **O Alto Custo de uma Proteção Inadequada:** as empresas perdem milhões de dólares a cada ano porque seus fornecedores de antimalware atuais não conseguem identificar e bloquear as ameaças em seus ambientes. De acordo com o FBI, em 2009, esses custos dobraram, atingindo mais de US$ 560 milhões de dólares, e isso inclui apenas os prejuízos relatados. Uma pesquisa recente da RSA descobriu que 88% das empresas Fortune 500 têm computadores comprometidos que executam cavalos de Tróia. O custo de uma proteção inadequada inclui a perda de dados, danos à marca, a contínua reconfiguração do sistema para limpar infecções, a redução na produtividade dos funcionários, entre muitos outros.

- **Deficiências Graves no Suporte:** quando há problemas com as soluções antimalware e ocorrem violações, o suporte fornecido de forma oportuna pode ser crítico. Em várias empresas, os tempos de espera são longos, há promessas de retorno que não são cumpridas e as equipes de suporte terceirizadas e localizadas em outros países não têm experiência suficiente para resolver os problemas. Isso resulta em recursos limitados, gera uma frustração enorme e aumenta o custo do suporte e gerenciamento de sua solução antimalware.
- **Perda da Especialização em Segurança:** conforme aumentam as ameaças de malware, a manutenção do número de recursos treinados de forma adequada para gerenciar as ameaças pode se tornar um desafio real para as organizações de TI. Muitas vezes, as empresas têm poucos recursos e não contam com a especialização em segurança necessária à manutenção de um nível ideal de proteção contra ameaças. A Forrester Research descobriu que 67% das empresas consideram um desafio a falta de recursos em seus departamentos de segurança.
- **Orçamentos Reduzidos:** hoje em dia, é constantemente solicitado que as organizações de TI façam mais com menos, enquanto seus orçamentos são cortados. Os departamentos de TI sofrem pressões de orçamento em relação ao nível dos funcionários, e precisam fornecer níveis mais altos de acessibilidade à rede, continuidade dos negócios e principalmente segurança, a qual não pode ser comprometida, mesmo com recursos limitados. Não é segredo que uma segurança eficiente exige uma defesa em vários níveis, mas a demanda de recursos para gerenciar produtos de diferentes fornecedores para vários pontos podem esmagar os departamentos de TI. Os gastos com a segurança de TI não aumentaram proporcionalmente às ameaças de malware. Portanto, as organizações devem conseguir a melhor proteção possível com o orçamento disponível e, às vezes, durante esse processo, deverão sacrificar a proteção em determinadas áreas para melhorá-la em outras, o que as deixa expostas.

Considerações para a Compra de Segurança de TI

Há muito tempo a proteção contra malwares é considerada uma mercadoria, e seu preço é o principal fator de decisão. Algumas empresas até usam software gratuito de proteção contra malware. Infelizmente, os malwares que esses produtos não conseguem detectar também são gratuitos. Alguns gerentes de TI perguntam: "E todos os fornecedores de antivírus não são iguais?" Outros dizem: "Todos os antivírus são ruins. Você escolhe o menos pior". Embora seja possível entender essa postura, considerando as terríveis experiências de alguns clientes, elas são absolutamente incorretas.

Na verdade, um produto antimalware ineficiente pode gerar custos significativamente maiores que seu preço de compra. Diversos fatores podem elevar o Custo Total de Proteção (TCP, Total Cost of Protection), que respondem tanto pelos 'custos tangíveis' facilmente quantificados quanto pelos 'custos intangíveis' que raramente são considerados ao avaliar propostas de preços dos fornecedores. Esses custos, alguns mais facilmente calculados que outros, crescem rapidamente conforme aumentam as questões relacionadas a detecção, desempenho e suporte. Ao considerar a solução de segurança adequada para a pequena, média ou grande empresa, as organizações devem se fazer as seguintes perguntas para determinar o custo real da proteção e não apenas o custo do produto:

- Qual é o nível de eficiência da proteção da solução antimalware? Uma proteção inadequada pode resultar em custos significativos para uma organização:
  - perda de Propriedade Intelectual da empresa devido a dados roubados
  - perda de produtividade dos funcionários quando os sistemas ficam indisponíveis devido a infecções por malware

  - utilização de recursos de TI ao reconfigurar os sistemas
  - perda de dinheiro de contas bancárias corporativas devido a roubos virtuais
  - danos à reputação da empresa
- **Você sacrifica seu desempenho em função da proteção?** A proteção terá pouca utilidade se impedir o usuário final de executar suas tarefas diárias. Os chamados "bloatware" usam recursos do sistema de tal forma que o funcionário não consegue usá-lo durante a verificação. O baixo desempenho da solução antimalware, que reduz a produtividade dos funcionários, pode aumentar drasticamente o custo da proteção.
- Quantos recursos e quanto tempo são necessários para gerenciar sua segurança antimalware? O console de gerenciamento é um item muito importante na decisão de compra. Se for difícil gerenciar a segurança através de um console de gerenciamento complicado, não intuitivo e que exige muitos recursos, o custo da proteção para sua empresa será maior. O gerenciamento deve ser simples, fácil de usar, porém detalhado e suficientemente potente para atenuar os riscos no seu ambiente.
- **Qual é o custo real do suporte?** Vários fornecedores cobram taxas adicionais pelo suporte, padrão ou premium. Infelizmente, nem sempre os custos adicionais embutidos são calculados ao considerar o valor total. Esses custos incluem tempos de espera muito grandes, um período muito longo até a resolução do problema e a perda de produtividade associada a esses problemas comuns.
- **Qual é o nível de competitividade dos preços?** Os concorrentes do segmento de antimalware se tornaram extremamente agressivos em relação aos preços de suas soluções. Algumas delas são oferecidas gratuitamente. Quando se trata da proteção contra malware, o velho dito ainda é verdadeiro: "você paga, você leva". O custo de uma solução antimalware não se limita ao preço de compra. Você pode escolher o provedor com o preço mais baixo, mas terá altos "custos intangíveis". Ou, você pode escolher o fornecedor com o maior preço e ainda assim não obter a proteção e o desempenho que justifiquem seu investimento. Embora o preço seja muito importante, ele não pode ser o critério decisivo final, pois não considera os custos embutidos da proteção.

Várias empresas estão pagando um preço muito mais alto pela proteção do que imaginam e, em muitos casos, não recebem a proteção necessária.

Proteção Empresarial Elaborada da Melhor Forma

Desde sua fundação em 1997, a Kaspersky Lab está direcionada para uma questão: proteger seus clientes das ameaças de malware. Ao longo desse caminho, vários de seus concorrentes colocaram seu foco além do malware, o que muitas vezes reduziu sua capacidade de fornecer a melhor qualidade em segurança. A Kaspersky Lab, com uma equipe qualificada exclusiva de mais de 700 pesquisadores e engenheiros de antimalware, e mais de 2.000 funcionários em todo o mundo, manteve esse foco de forma incansável, o que a tornou obviamente uma das melhores do mundo em proteger seus clientes contra essas ameaças.

Esse é o foco que conquistou a confiança de nossos clientes. Atualmente, a Kaspersky Lab aparece como a terceira maior empresa de segurança antimalware do mundo, e está crescendo mais rápido que todas as outras, incluindo mais de 50.000

novos clientes por dia; nossos produtos protegem mais de 300 milhões de sistemas em todo o mundo.

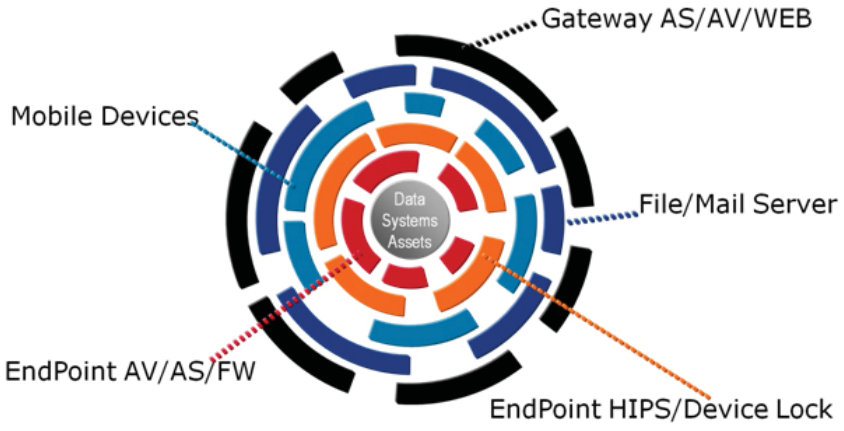
A Kaspersky Lab tem ganhado vários prêmios de empresas de testes independentes por suas tecnologias e soluções de detecção de malware:

- **VB100:** o Kaspersky tem obtido uma das maiores pontuações de RAP (Testes de Detecção Reativa e Proativa) de todos os concorrentes, o que comprova a avançada proteção contra malware que fornecemos.
- **AV Comparatives:** a Kaspersky Lab continua recebendo a melhor classificação, Advanced+, por sua capacidade de detectar e remover ameaças de malware.
- **Anti-Malware Test Lab:** a Kaspersky é o único fornecedor a receber o prêmio GOLD em todas as categorias testadas, o que demonstra o alto nível de nossa proteção total contra ameaças. Também somos o único fornecedor que não foi reprovado em nenhuma categoria de teste.
- **AV-Test.Org:** de acordo com o AV-Test.Org, o Kaspersky tem a resposta mais rápida a novas ameaças, respondendo em menos de duas horas e reduzindo significativamente a janela de exposição de nossos clientes.

O Kaspersky tem obtido pontuações maiores que a concorrência em proteção total de forma consistente, devido ao nosso foco sobre todas os vetores de ameaças de malware, que incluem:

- Proteção Antimalware
- Proteção Antispam
- Proteção Antiphishing
- Heurística de "Dia Zero"
- Proteção contra Rootkits
- Proteção contra Worms/Bots/Cavalos de Tróia/Vírus Polimórficos
- Proteção contra Invasão de Hosts
- Sólida Proteção de Firewall Pessoal
- Proteção de Emails e da Web contra Malware
- Controle de Aplicativos e de Dispositivos

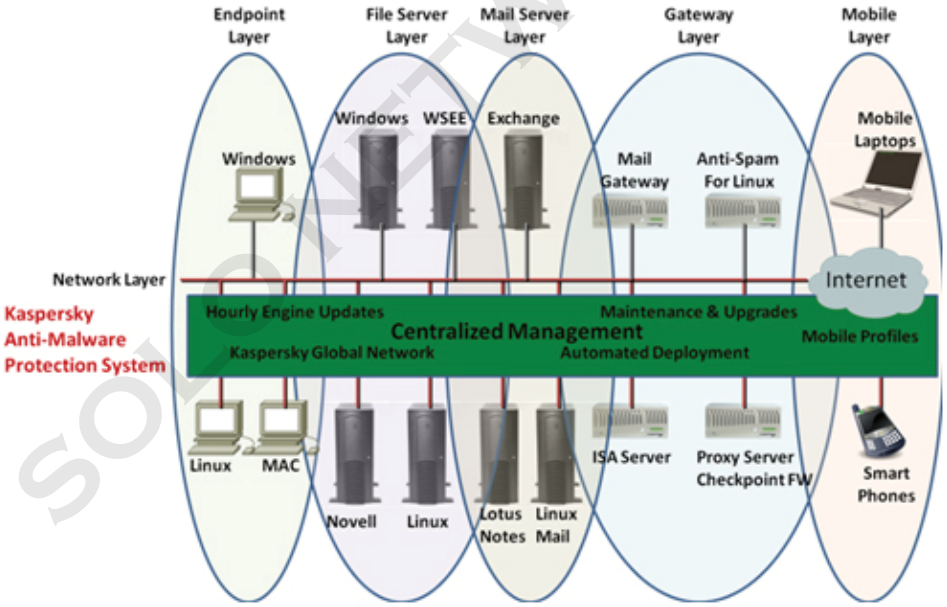
Essa extraordinária base de proteção sobre a qual todos os produtos da Kaspersky são construídos e que é o centro da metodologia de proteção em camadas protege da mesma forma pequenas e grandes empresas. Nós a chamamos de Sistema de Proteção Antimalware da Kaspersky.



O Sistema de Proteção Antimalware da Kaspersky

O crescente cenário de ameaças e a necessidade de proteger um ambiente cada vez mais complexo causam problemas reais para as organizações de TI em todas as instâncias. A Kaspersky Lab está respondendo com soluções extremamente avançadas para combatê-los. Nossa visão e nossa estratégia transcendem o porte organizacional, fornecendo opções exclusivas da melhor e mais ampla proteção contra malware.

Atualmente, a expansão do crime virtual aproveita todos os vetores possíveis para disseminar conteúdo malicioso: emails, conteúdo da Web, redes sociais, vulnerabilidades de aplicativos de terceiros, entre muitos outros. Por isso, as empresas devem considerar todos os vetores de ameaças e implementar uma proteção real em todos os níveis da organização. Raramente se considera uma estratégia de proteção contra malware em camadas. Hoje em dia, várias empresas pensam na proteção antimalware como uma simples mercadoria, uma tecnologia de segurança exigida para fins de conformidade e, na melhor das condições, uma compra a ser feita pelo menor preço possível.



Para dificultar o crime virtual, é necessário vigiar cada camada e não simplesmente o endpoint ou o perímetro. O diagrama acima ilustra a maior proteção criada por uma estratégia de proteção contra malware em camadas. Do ponto de vista holístico, não existe uma segurança 100%, mas a segurança em camadas coloca a organização no nível mais próximo possível dos 100%.

Então, a questão é qual a melhor abordagem a ser utilizada na segurança em camadas de toda a organização. Componentes de segurança em camadas com uma integração inadequada criam uma desvantagem desde o início. Essas soluções limitam a visibilidade dos riscos de malware em toda a empresa, dificultando o gerenciamento da proteção e, em última instância, dificultando também a rápida resposta a ameaças conforme elas surgem.

O Sistema de Proteção Antimalware da Kaspersky é um conjunto proprietário premiado de tecnologias de proteção integradas que forma o pilar do sucesso da proteção real contra malware em camadas. Esse Sistema de Proteção se estende de todos os endpoints (laptops, estações de trabalho, dispositivos móveis) até a nuvem e além, garantindo a melhor proteção possível em todos os níveis da empresa.

Cada produto do sistema usa a mesma tecnologia antimalware proprietária premiada que unifica a melhor proteção em todos os nós da rede. Um console de gerenciamento centralizado fornece uma visão completa de todos os riscos de malware em toda a empresa e possibilita a implementação automatizada, a manutenção e a atualização dos componentes do sistema de proteção simplificadas. Todos esses componentes antimalware funcionam perfeitamente em conjunto para garantir a proteção de ponta a ponta mais coesa possível, conforme ilustrado a seguir.

A camada de proteção antimalware do Kaspersky oferece o melhor valor de proteção, com visibilidade imediata de todos os espaços da empresa e um nível de resposta não encontrado em outras abordagens antimalware.

Proteção Premium contra Malware

A estratégia da Kaspersky Lab consiste em oferecer um conjunto unificado de produtos criados sobre um único mecanismo antimalware de qualidade superior que se estende a todos os níveis da empresa, do endpoint à nuvem. Não se trata de um conjunto de produtos diversos integrados de forma inadequada que exige vários agentes e vários consoles de gerenciamento. Um único mecanismo proprietário da melhor qualidade alimenta todas as nossas soluções tecnológicas, estações de trabalho, laptops, dispositivos móveis, servidores de arquivos, servidores de email, gateways e soluções em nuvem. Desde 2009 e novamente no final de 2010, o Kaspersky chegou muito mais perto de fornecer um único núcleo de tecnologias premium de proteção antimalware para proteger ambientes de TI heterogêneos de todos os tamanhos.

- O mecanismo único do Kaspersky usado em toda a empresa representa a melhor proteção disponível de todos os vetores de ataque, garantindo uma proteção premium contra malware.
- O mecanismo único do Kaspersky usado em todos os produtos simplifica o gerenciamento e a atualização, permitindo a consistência em todos os níveis da empresa.
- Devido à sua superfície reduzida e ao uso mínimo de recursos do sistema, o mecanismo antimalware do Kaspersky garante o melhor desempenho em todas as plataformas, em todas as empresas.

Stanley Mierzwa, Diretor de TI do The Population Council, testemunhou a diferença que o Kaspersky faz em termos de proteção:

"Nós percebemos o impacto do carregamento do Kaspersky imediatamente. Tivemos menos infecções, o que afetou nossas operações de forma muito positiva, tornando nossa empresa muito mais eficiente."

Desempenho Superior

O Kaspersky fornece os melhores níveis de desempenho de forma consistente, garantindo a produtividade e a proteção contínua dos funcionários. O Sistema de Proteção Antimalware da Kaspersky colabora para essa alta taxa de desempenho através de atualizações de assinaturas constantes. Alguns outros produtos antimalware atualizam seus bancos de dados de assinaturas uma vez por dia. O Kaspersky mantém seu mecanismo antimalware premium atualizado a cada hora, fornecendo a proteção mais imediata disponível. Dois motivos tornam isso extremamente importante:

- O maior número de atualizações significa que elas são menores, o que minimiza o impacto sobre os recursos do sistema e mantém a produtividade dos funcionários. Com a criação de mais de 3.500 assinaturas por dia, uma única atualização pode afetar drasticamente o desempenho do sistema.
- Com as atualizações mais rápidas, você obtém a proteção do computador conforme ela fica disponível e não no final do dia. O Kaspersky é atualizado 22 vezes por dia, enquanto outros sistemas são atualizados 2 ou 3 vezes ou menos; isso reduz significativamente a janela de exposição de nossos clientes.

O Kaspersky tem atualmente uma das menores superfícies do setor e usa menos memória e recursos de CPU, deixando os preciosos recursos do sistema disponíveis para manter a produtividade dos funcionários. Isso é especialmente importante na economia atual, em que várias empresas tiveram de adiar a atualização de seus computadores. Na Conferência Mundial de Parceiros da Microsoft 2010, realizada em Washington, D.C., a vice-presidente corporativa para o Microsoft Windows, Tammi Reller, declarou que 74% dos computadores corporativos ainda executam o Windows XP. Ela também disse que a idade média dos computadores é agora de 4,4 anos, o maior valor observado pela Microsoft em mais de uma década. A proteção dos recursos dos sistemas nunca foi tão importante.

Na Great Batch, Inc., Mike Ciura, Analista de segurança e Oracle, observou uma diferença imediatamente após o carregamento do Kaspersky:

"As pessoas que usam produtos de CAD e que exigem muitos recursos do sistema não tiveram nenhum problema. Eu recebi vários elogios, dizendo que ele é mais rápido e funciona em segundo plano, sem incomodar".

Proteção Abrangente

O Kaspersky oferece cobertura abrangente para ambientes multiplataforma heterogêneos. Nosso suporte inclui todas as versões de produtos Microsoft Windows para endpoints e servidores.

O Kaspersky também dá suporte a redes Novell, incluindo os Netware herdados, que vários concorrentes abandonaram, e os atuais produtos para servidores Novell. Além disso, o Kaspersky dá suporte para sistemas operacionais Linux e MAC, cuja participação de mercado cresceu a ponto de agora serem um alvo do crime virtual. O Kaspersky também dá suporte a aplicativos de email, tanto Microsoft Exchange quanto Lotus Notes. Todos esses ambientes são gerenciados de forma central, por meio de um único console de gerenciamento com uma visualização única.

As fronteiras entre os ambientes pessoais e corporativos estão de desfazendo. Os usuários corporativos esperam um acesso mais fácil e rápido a suas redes corporativas e aplicativos de negócios em qualquer dispositivo. Está aumentando a demanda por mais dispositivos móveis menores ou até mesmo dispositivos para o consumidor, com a expectativa de que a organização de TI dê suporte a eles. Além disso, os sites de redes sociais para consumidores, como Facebook e Twitter, entraram rapidamente no ambiente empresarial, criando um risco de perda de dados e um novo canal para a distribuição de malware. O número crescente de usuários móveis e remotos está criando um local de trabalho distribuído complexo. A proliferação de dispositivos pessoais que podem acessar e armazenar dados corporativos representa um perigo óbvio para as empresas que devem obedecer a normas e proteger dados corporativos confidenciais. De fato, a pesquisa da Forrester descobriu que a adoção de smartphones e de aplicativos e serviços baseados na Web representam as duas principais preocupações com a segurança de TI.

O portfólio da Kaspersky inclui suporte a várias versões de smartphones, com compatibilidade e suporte adicionais para smartphones prometidas para o próximo ano.

De acordo com Jeff Smith, Gerente de Serviços de Experiência em Computação da Universidade de Northern Brunswick, a qualidade do suporte dos produtos da Kaspersky fez toda a diferença:

"O suporte a Novell foi um fator chave. Nosso fornecedor atual não dava suporte ao Netware herdado, apesar de dizerem que sim. Também precisávamos de uma solução para endpoints em diversos sistemas operacionais, incluindo Windows, MAC e Linux."

O Kaspersky realmente fornece a cobertura mais abrangente para a proteção contra malware nesses diferentes ambientes de TI.

Implementação Facilitada

Muitas vezes, os clientes se dão conta que precisam de proteção e desempenho melhores em seus ambientes; porém, devido ao receio de trocar de fornecedor, decidem não mudar. Nessa situação, eles mantêm um ambiente de segurança inadequado e aceitam o risco para evitar o medo da mudança.

O Kaspersky reduziu drasticamente esse receio através da automatização completa do processo de remoção, instalação e configuração. Os "assistentes" de gerenciamento do Kaspersky, incorporados ao console de gerenciamento, encontram e removem automaticamente todos os softwares incompatíveis, e instalam o Kaspersky, incluindo a configuração detalhada de políticas. O processo é concluído com uma reinicialização configurável no final. A instalação remota nunca foi tão fácil, a implementação em um ambiente complexo e disperso é instantânea.

Tim Pemberton, Diretor de TI do Hospital Markham Stouffville, descreve a implementação do Kaspersky em 1.200 sistemas em apenas dois dias da seguinte maneira:

"Nós implementamos primeiro nos PCs. Com a ajuda de nosso parceiro, a instalação foi surpreendentemente tranquila. Foi mais fácil atualizar para o Kaspersky do que seria atualizar para a nova versão do nosso fornecedor atual. Não foi nada de especial."

Gerenciamento Simplificado

Vários agentes e vários consoles de gerenciamento podem sobrecarregar recursos já extenuados e reduzir a eficiência do gerenciamento da estratégia antimalware geral. A abordagem do Kaspersky consiste em minimizar a utilização de recursos e maximizar o gerenciamento de riscos de malware através de um console de gerenciamento que compreende todos os produtos da Kaspersky, do endpoint à nuvem, incluindo dispositivos remotos e móveis. Nossos produtos podem ser gerenciados em uma visualização central, o Kaspersky Security Center. Independentemente da plataforma ou do nível de complexidade, você tem uma visão da segurança para identificar e atenuar os riscos de malware.

George Thornton, Gerente de Operações de Rede da Montgomery Independent School District, teve uma experiência com a economia em "custos intangíveis" que a Kaspersky Lab oferece:

"Nosso fornecedor anterior exigia diversos consoles. Com o Kaspersky, o gerenciamento é centralizado em um console. Sua automatização é ótima. Nós levávamos de um a dois dias por semana gerenciando nossa solução antivírus. Agora, gastamos apenas alguns minutos por semana."

Suporte de Qualidade Superior

Como todas as tecnologias do Sistema de Proteção Antimalware da Kaspersky foram desenvolvidas pela própria empresa, é possível fornecer o melhor suporte, com uma resposta rápida. A Kaspersky acredita que o suporte deve ser estabelecido localmente, altamente responsivo e excepcionalmente eficiente. Todas as equipes de suporte se encontram no país; fornecem suporte no seu idioma e compreendem as peculiaridades locais. A Kaspersky apresenta o menor tempo de espera do setor, inferior a cinco minutos, o que reduz o tempo necessário para chegar a uma solução. Suas equipes de suporte são constantemente treinadas, o que resulta em mais de 90% dos problemas resolvidos na primeira ligação. Tudo isso significa que, quando precisar, você terá um suporte rápido e eficiente.

Victor Andreev, Administrador de Sistemas do Centre for Education & Training, tinha uma experiência diferente com seu fornecedor atual:

"Era um pesadelo ligar para o helpdesk deles. Depois de muito esperar, eles diziam que retornariam a chamada, mas nunca o faziam. Quando ligávamos novamente, éramos atendidos por outro técnico de suporte que não tinha registros da chamada anterior, então tínhamos de repassar os problemas novamente. O que realmente nos impressionou foi o suporte que recebemos da Kaspersky. Tivemos alguns problemas e precisamos ligar para o Helpdesk da Kaspersky. Nossa experiência foi muito boa. A linha de comunicação entre o Helpdesk e o grupo de desenvolvimento foi ótima e recebemos as DLLs que resolveram nosso problema no mesmo dia."

Custo Total de Proteção (TCP) Minimizado

A proteção real, como a fornecida pelo Sistema de Proteção Antimalware da Kaspersky, não precisa acabar com seu orçamento. E você também não precisa perder em desempenho e gerenciabilidade. Descrevemos anteriormente as considerações de compra necessárias para garantir o melhor Custo Total de Proteção. Como disseram os clientes da Kaspersky, a empresa empenhou todos os esforços para fornecer o melhor Custo Total de Proteção geral do setor, em todas as categorias:

- Detecção Premium de Malware: o Kaspersky fornece proteção premium contra malware, reduzindo drasticamente o Custo Total de Proteção com a minimização da ameaça.
- Desempenho Superior: a tecnologia proprietária da Kaspersky reduz significativamente o impacto sobre os recursos e a superfície do sistema, mantendo a produtividade e a proteção dos funcionários. Um desempenho baixo pode aumentar o custo da proteção. O Kaspersky minimiza o impacto sobre o desempenho, reduzindo o Custo Total de Proteção.
- Gerenciamento Simplificado: a estratégia do Kaspersky consiste em ter todos os produtos gerenciados em um único console de gerenciamento simples, intuitivo e avançado, reduzindo o tempo e os recursos necessários para gerenciar até mesmo as maiores corporações, permitindo identificar e gerenciar riscos em toda a empresa, inclusive dispositivos remotos e móveis. Assim, o Custo Total de Proteção é drasticamente reduzido.
- Suporte de Qualidade Superior: o suporte padrão da Kaspersky é gratuito e conta com o menor tempo de espera do setor, inferior a cinco minutos. Nossa taxa de resolução na primeira chamada é superior a 90%, ou seja, seus problemas são solucionados mais rapidamente, com um tempo mínimo gasto por seus recursos de TI. O Kaspersky reduz o Custo Total de Proteção através do suporte padrão local, oportuno e eficiente que é fornecido sem custos adicionais.
- Preços Competitivos: o Kaspersky oferece o melhor Custo Total de Proteção disponível, por um preço bastante competitivo.

Muitas vezes, as organizações consideram que preço e valor são a mesma coisa. Como mostramos, o valor real pode se encontrar na proteção do custo do investimento em soluções de segurança através do fornecimento de uma proteção real, um desempenho que mantenha a produtividade, um gerenciamento que reduza a utilização de recursos e um suporte rápido e gratuito. O Sistema de Proteção Antimalware da Kaspersky fornece a melhor proteção contra malware e oferece o menor Custo Total de Proteção disponível no momento.

Kaspersky Lab – Sempre à Frente

A Kaspersky Lab planeja o futuro por meio do aprimoramento contínuo do desempenho e da funcionalidade de nossos produtos. Também adicionamos novos recursos que auxiliam na proteção e no gerenciamento de dados, para que possamos fornecer uma estratégia de proteção de dados mais holística.

O principal negócio da Kaspersky Lab é entender as principais tendências e oportunidades do setor, e os riscos que elas apresentam, além de fornecer soluções para as ameaças atuais e que também antecipem as prováveis ameaças futuras. O Laboratório de Análise de Vírus da Kaspersky Lab, que se estende ao redor do mundo com centenas de especialistas em pesquisa de vírus, é o centro da experiência sempre atualizada com os desenvolvimentos em ameaças de malware. Essa rede global de especialistas internacionais oferece entradas constantes sobre desenvolvimentos e tendências regionais para assegurar que os mais de 300 milhões de sistemas protegidos pelo Kaspersky

continuem sempre seguros.

As estratégias da Kaspersky Lab para lidar com as principais tendências do setor são as seguintes:

1. **Mudando para Modelos de Computação em Nuvem**
   - A detecção baseada em nuvem do Kaspersky Security Network (KSN) beneficia todos os produtos atuais da Kaspersky Lab. As informações de malware são coletadas na nuvem do Kaspersky a partir de instalações de vários milhões de consumidores. O laboratório de vírus cria atualizações de assinaturas de malware para usuários corporativos e domésticos com uma frequência de duas vezes por hora, com base nesse enorme recurso em nuvem que é os olhos e ouvidos da empresa no cenário global de ameaças imediato.
   - A Kaspersky está lançando os serviços de filtragem de email Hosted Mail & Web, com os quais as empresas obtêm filtragem antimalware e antispam em nuvem antes que o tráfego chegue ao sistema de email cliente
   - A Kaspersky está lançando os Serviços Gerenciados, em que o Kaspersky Management Security Center reside nas instalações do Provedor de Serviços e gerencia a segurança de seus clientes.
   - Desenvolvimentos futuros: o Kaspersky Endpoint 8.0, programado para ser lançado no final de 2011, incluirá a opção de conexão com a nuvem do KSN. A detecção/reputação em nuvem do KSN será adicionada às futuras versões dos produtos da Kaspersky para email e Web, por exemplo, a fim de bloquear links em que residem malwares, tudo em tempo real.
2. **Mudando para a Virtualização**
   - A Kaspersky já possui a certificação VMWare Ready para seus principais produtos. Esse é o primeiro estágio para ativar a proteção antimalware nas arquiteturas virtualizadas.
   - No caso do ESXi, não há necessidade de proteger o sistema operacional host do VMWare (a própria plataforma de virtualização), pois o sistema operacional do hipervisor e host é pequeno, monolítico e assinado digitalmente.
   - No caso do Hyper-V, o sistema operacional host é o sistema operacional Windows padrão, de forma que um produto antimalware da Kaspersky seria instalado no sistema operacional host, assim como em todos os computadores convidados. O produto WSEE da Kaspersky Lab dá suporte ao modo Core (recomendado pela Microsoft para implementações do Hyper-V) e oferece proteção perfeita ao Hyper-V
   - Os testes de compatibilidade do Microsoft Hyper-V fazem parte do programa de certificação referente ao logotipo Certified for Windows Server 2008 R2. A Kaspersky Lab pretende receber esse logotipo para o WSEE 8.0.
   - A Kaspersky criará pequenos produtos compatíveis com o ambiente virtualizado, ou seja, atualizações de bancos de dados de antivírus do Offline Image, verificações do Offline Image, relatórios, interoperabilidade com sistemas como o VMWare (vCenter/ vSphere) e o Microsoft System Center Virtual Machine Manager, distribuição de desempenho e carga inteligente, NAC Virtual e Equipamentos Virtuais
3. **O Kaspersky terá maior foco na Prevenção de Perda de Dados (DLP, Data Loss Prevention)**
   - A Kaspersky Lab pretende incluir políticas avançadas de controle de dispositivos em seu produto para endpoints em 2011 a fim de reduzir o risco de perda de dados, por exemplo, através de pendrives.
   - A Kaspersky pretende lançar a proteção a dados de criptografia em 2011
   - A Kaspersky Lab pretende adicionar a funcionalidade DLP a seu produto de proteção do Microsoft Exchange em 2011/12

4. **A Kaspersky Lab desenvolverá um novo cliente para endpoints, incluindo:**
   - Avaliação de Vulnerabilidades
   - Gerenciamento de Patches
   - Controle de Aplicativos Avançado
   - Controle de Dispositivos Avançado
   - Outras tecnologias: criptografia, DLP, NAC, serviços de reputação baseados em nuvem
5. **A Kaspersky desenvolverá outras tecnologias para plataformas móveis**
   - Adição do suporte a Blackberry e Android, além do Symbian e Windows Mobile.
6. **O Kaspersky terá maior foco no Gerenciamento de Acesso a Identidades**
   - O Kaspersky Lab Administration Kit faz relatórios usando nomes de host e endereços IP, além de usar informações de domínio/usuário em eventos de detecção de vírus, o que acrescenta a dimensão do "usuário". Pretendemos estender o Kaspersky Lab Management Security Center para resolver logins em nomes reais através da integração com o Microsoft Active Directory

Resumo

O Kaspersky realmente oferece proteção premium contra malware, para hoje e amanhã! O Sistema de Proteção Antimalware da Kaspersky fornece a melhor proteção e o melhor desempenho totais para todas as empresas, pequenas ou grandes, e tudo isso com o melhor Custo Total de Proteção disponível atualmente.

Porém, não estamos satisfeitos com a proteção contra as ameaças de hoje. Estamos nos planejando para o futuro, ampliando nosso portfólio e investindo na tecnologia que protegerá os clientes das ameaças de amanhã.

Esta é a Kaspersky Lab – Proteção Empresarial Consistente Elaborada da Melhor Forma!

500 Unicorn Park
Woburn, MA 01801
866.563.3099
smbsales@kaspersky.com

www.kaspersky.com
www.threatpost.com