IBM Global Technology Services
White Paper de Liderança em Pensamento

Maio de 2011

Selecionando um Provedor de Serviços Gerenciados de Segurança: Os 10 mais importantes critérios a serem considerados

Introdução

As empresas de hoje lutam continuamente para defender-se de ataques online que podem ocorrer a qualquer momento. Sejam ataques de vírus, de negação de serviço ou de acesso não autorizado ao website, se estes atacantes forem bem-sucedidos eles podem gerar caos impactando as operações de negócios e a produtividade da força de trabalho, danificando a infraestrutura ou criando brechas de segurança capazes de prejudicar a reputação de uma empresa. Violações e invasões bem-sucedidas também custam caro em termos de impacto operacional, tanto pelos recursos necessários para remediar as violações quanto pela potencial perda de negócios.

Existe um amplo consenso quanto à necessidade de segurança da informação. Um programa de segurança bem-sucedido exige profundo conhecimento do ambiente atual de ameaças. Exige também uma abordagem estratégica ao gerenciamento do custo e complexidade das tecnologias de segurança necessárias para o gerenciamento de eventos e históricos de segurança, varreduras de vulnerabilidade, segurança de emails e outras atividades. No entanto, com a ampla diversidade de ameaças , as empresas que gerenciam sua própria segurança da informação frequentemente não têm internamente os recursos necessários para proteger sistemas online em modalidade 24 horas por dia7 dias por semana. Práticas avançadas de segurança exigem pessoal altamente qualificado, que pode ser muito caro de recrutar, contratar e manter. Isto é um desafio para empresas com orçamentos limitados de TI. Além disso, implementar e gerenciar soluções de segurança pode desviar recursos de TI de outras iniciativas críticas, incluindo a prevenção do próximo ataque. Ao invés disso, as equipes de TI são forçadas a adotar uma postura reativa, que ignora o papel estratégico mais importante de uma função de segurança de TI.

Para garantir uma postura econômica, abrangente e proativa de segurança, cada vez mais empresas estão seus programas de segurança de TI. Estas empresas tipicamente:

- Não têm internamente as qualificações necessárias para acompanhar o ritmo das mudanças nas demandas de negócio, mandatos de cumprimento e ameaças emergentes de modo a implementar de forma estratégica as novas soluções de segurança de TI.
- Não têm as qualificações para monitorar e gerenciar de forma eficaz a infraestrutura de segurança, garantindo a utilização otimizada dos ativos atuais.
- Têm equipes internas de TI gastando um tempo excessivo em problemas operacionais cotidianos de segurança, ao invés de dedicarem-se a novos projetos estratégicos.
- Dependem de ferramentas e processos de segurança de TI que oferecem uma abordagem reativa, ao invés de proativa, à mitigação de risco e minimização de perda de dados e indisponibilidades.

Terceirizando as operações de segurança para um provedor de serviços gerenciados de segurança (MSSP), as empresas podem tirar proveito das qualificações especializadas, ferramentas e processos oferecidos, e aprimorar significativamente a segurança da empresa sem efetuar um grande investimento em tecnologia e recursos. Os benefícios de terceirizar a segurança são nítidos, mas selecionar o MSSP adequado não é tão fácil.

Este white paper descreve uma abordagem estratégica para a seleção de um MSSP, e estabelece as 10 mais importantes qualificações a serem consideradas na escolha de um provedor. O MSSP adequado pode reduzir o custo e a complexidade da segurança da informação, implementando ao mesmo tempo uma postura de segurança mais robusta.

Os 10 critérios mais importantes a considerar ao selecionar um MSSP

As empresas que não têm os recursos e o orçamento para criar e operar uma infraestrutura de segurança em modalidade 24/7 podem terceirizar isto para um MSSP confiável. Permitir que um MSSP lide com o monitoramento e gerenciamento da segurança no dia a dia fornece às organizações uma oportunidade de designar recursos internos de TI para iniciativas mais estratégicas. Os MSSPs também facilitam a continuidade de negócios, oferecendo inteligência avançada para combater ataques antes que eles causem danos e impactem as operações do mesmo. Esta camada de proteção proativa proporciona uma vantagem competitiva, garantindo que as empresas se mantenham em operação mesmo quando malwaresofisticado estiver se espalhando rapidamente pela Internet.

Os potenciais benefícios da terceirização da segurança só podem ser alcançados selecionando o fornecedor adequado. Para extrair máxima vantagem da terceirização de suas operações de segurança por um MSSP, certifique-se primeiramente de realizar uma avaliação detalhada dos seus requisitos de segurança. Entenda quais medidas de segurança você precisa cumprir e estabeleça um modelo confiável de controle. Entenda também que requisitos de segurança você espera que o MSSP tenha implantados, e esteja preparado para investigar se ele está equipado com as certificações relevantes que demonstrem sua qualificação nestas áreas.

Quando estiver pronto para avaliar MSSPs, considere os 10 critérios a seguir para garantir que o fornecedor que você escolher vai proteger melhor os seus ativos vitais de TI e ajudar você a atender aos requisitos de cumprimento.

1) Amplo portfólio de serviços de segurança

As suas necessidades de segurança estão evoluindo continuamente com a natureza dinâmica do seu ambiente de negócios, o surgimento de novas ameaças e as constantes mudanças da regulamentação. Certifique-se de que o parceiro de serviços gerenciados de segurança ofereça um conjunto abrangente de serviços de avaliação de gerenciamento e vulnerabilidade, capazes de manter você protegido antecipadamente das ameaças, sejam quais forem os seus desafios de segurança. Para atender aos seus requisitos de proteção e de orçamento, escolha um MSSP que ofereça múltiplos níveis de serviço e a capacidade de combinar os serviços. Considere ainda um fornecedor cujas ofertas sejam pré-empacotadas e estruturadas de forma a garantir fornecimento e desempenho consistentes. Através de serviços de classe mundial que lidam com riscos ao longo de cada aspecto da sua empresa, você pode criar uma postura robusta de segurança capaz de reduzir custos, aprimorar o atendimento e gerenciar riscos.

2) Especialistas de pesquisa e inteligência de segurança altamente respeitados

O MSSP que você escolher deve ter recursos internos e externos abrangentes, de alto nível, com conhecimento continuamente atualizado das mais recentes estratégias de ataque, ameaças na rede e vulnerabilidades, incluindo informações atualizadas em tempo real sobre ameaças emergentes e o combate a elas. Grupos globais de operações, robustas equipes de pesquisa e comprovados processos de análise de ameaças e vulnerabilidades são cruciais para manter a sua empresa protegida dos esquemas de ataques em contínua evolução. Quando os fornecedores de MSSP se concentram em identificar e pesquisar vulnerabilidades de segurança, trabalhando com os respectivos fornecedores, seus sistemas serão atualizados e protegidos antes que as ameaças tenham oportunidade de afetá-los.

3) Reputação do MSSP

Você também deve considerar a reputação de um MSSP e seu histórico de satisfação dos clientes. Procure um fornecedor que tenha conseguido reter clientes por vários anos. Pergunte qual a sua rotatividade média de clientes, procurando um fornecedor com clientes de longo prazo operando no mesmo setor de mercado e com necessidades de rede semelhantes às suas. Peça para ver resultados de pesquisas atuais de satisfação de cliente, conduzidas internamente ou por um fornecedor externo. Tire proveito de relatórios de analistas que mencionem o MSSP e o comparem com outros concorrentes, para ter uma avaliação imparcial dos seus serviços e qualificações. Certifique-se ainda de que sua sólida reputação seja acompanhada de uma visão sólida no futuro. Certifique-se de que o fornecedor esteja investindo em seu portfólio de soluções e serviços e que tenha um plano estratégico claramente definido, alinhado com os seus próprios objetivos de segurança.

4) Ferramenta robusta de gerenciamento baseada na web

Embora o MSSP vá fornecer no todo ou em parte o seu programa de segurança , a sua equipe de TI ainda assim precisará ter acesso fácil e uma visão abrangente de toda a sua infraestrutura de segurança. Procure um MSSP que ofereça um gerenciamento consolidado, com a flexibilidade de combinar e misturar por tipo de dispositivo, fornecedor e nível de serviço de modo a atender às suas necessidades específicas de negócio. As melhores ferramentas de gerenciamento baseadas na web permitirão que seus recursos de segurança possam monitorar com facilidade tanto os dispositivos de segurança gerenciados como os não gerenciados.

5) Sofisticada tecnologia de retaguarda

Depois que você estiver seguro de que um MSSP está comprometido com a manutenção de uma inteligência global de segurança contínua, certifique-se de que ele tenha uma tecnologia de retaguarda para alinhar aquela inteligência com a sua infraestrutura de TI e iniciativas de segurança. O sistema de proteção subjacente, acessado através de um portal, deve executar muito mais do que o mero monitoramento de eventos e gerenciamento de dispositivos. A tecnologia de retaguarda também deve ter a capacidade de executar funções avançadas de análise, correlação, agregação, categorização e priorização. Busque uma tecnologia que permita escalada e correção de incidentes, e que tenha um mecanismo sofisticado de alerta - tudo conectado a um enorme banco de dados de ameaças conhecidas, fornecido e continuamente atualizado pelo MSSP. Garanta que seu provedor esteja aproveitando uma plataforma comum em sua base de clientes, ao invés de tentar gerenciar simultaneamente múltiplas plataformas diferentes, o que pode aumentar a possibilidade de variações no fornecimento de serviço.

6) Soluções consolidadas para regulamentações federais, estaduais e de segmento de mercado

Seu MSSP deve ter um entendimento profundo das regulamentações aplicáveis ao seu segmento específico. Portanto, confirme que o seu trabalho está alinhado aos protocolos relevantes de auditoria e segurança padrões do segmento de mercado. Considere buscar serviços de governança, risco e conformidade de um único fornecedor que seja capaz de ajudar a avaliar as suas práticas de segurança no contexto de suas necessidades e objetivos futuros, incluindo considerações técnicas e de negócios, além do cumprimento. Um MSSP com serviços abrangentes que ajudará você a atender a conformidade terá de ter qualificações não apenas para cumprimento de padrões e regulamentações como também para gerenciamento de risco de segurança, projeto e gerenciamento de programa de segurança, privacidade e treinamento de segurança.

7) Ampla experiência de infraestrutura de segurança
Verifique o entendimento, experiência e reputação do fornecedor em termos de infraestrutura e integração de sistemas capaz de suportar seus objetivos de segurança gerenciada. Garanta que o MSSP tenha ampla experiência em infraestrutura, incluindo hardware, software e todos os aspectos dos data centers e da rede, especialmente no que se refere às melhores práticas de segurança. MSSPs que oferecem serviços integrados de tecnologia, como continuidade de negócios, comunicações integradas e serviços de dados e de armazenamento, podem ampliar o valor de sua oferta de serviço de segurança gerenciada. O MSSP deve ter a capacitação para permitir que você cresça além da sua implementação de serviços de segurança gerenciada, ampliando a funcionalidade para áreas adjacentes.

8) Suporte de múltiplos fornecedores para dispositivos de segurança
Além de gerenciar e monitorar a sua postura de segurança 24 horas por dia, 7 dias por semana, seu MSSP deve ter a capacidade e certificação necessárias para proteger o seu equipamento atual. Garanta que o MSSP seja capaz de gerenciar qualquer equipamento que você esteja usando atualmente, para evitar mudanças desnecessárias e custos da implementação de novas tecnologias. Procure por um MSSP que tenha ampla experiência no gerenciamento de diversas tecnologias e plataformas, além de suas próprias linhas de produtos. Peça uma lista de plataformas que o MSSP está certificado para gerenciar. Se a sua plataforma atual não aparecer na lista, verifique com o provedor se eles podem personalizar os seus serviços para atender às suas necessidades. Cuidado, no entanto, com provedores que insistem que podem suportar qualquer ambiente de TI e qualquer necessidade de negócio, considerando o tempo e o custos envolvidos na implementação de um conjunto global de recursos para fornecer serviços especializados, consistentes e confiáveis.

9) Contratos flexíveis baseados nos níveis de serviços
Qualquer provedor de serviços pode dizer que responde de forma rápida e completa. Contudo, o MSSP que você escolher deve oferecer mais do que uma garantia de resposta rápida; deve oferecer também uma garantia de proteção contra ameaças emergentes de Internet. O provedor precisa estar disposto a se comprometer com essas declarações através de um acordo de nível de serviço (SLA). Procure por ofertas estruturadas com escopo e preços fixos que demonstrem a capacidade do provedor fornecer serviços de forma confiável e repetida. Outro fator importante é garantir que o SLA que ele oferece atende às suas necessidades particulares. Depois de adotar o serviço de segurança, valide e teste as capacidades do provedor e garanta que o desempenho esteja alinhado aos acordos contratados.

10) Estabilidade financeira
Um dos critérios mais importantes a serem considerados na avaliação de MSSPs é sua estabilidade financeira. Gerenciar segurança em bases terceirizadas para um grande número de clientes exige investimentos significativos de capital e recursos, de modo a operar uma rede global de centros de operações de segurança, desenvolver novas tecnologias, atrair e reter profissionais capacitados e motivados. Assim como em qualquer decisão de negócios, procure selecionar um MSSP que seja financeiramente estável, com recursos abundantes e um modelo sustentável de negócios.

IBM Managed Security Services

Muitas organizações conscientes que separam um tempo para investigar MSSPs com cuidado escolhem os IBM Managed Security Services para proteger suas empresas. De fato, a IBM é reconhecida no mercado como líder em serviços de segurança gerenciada, tendo recebido o "Prêmio de Liderança de Mercado para Fornecedores de Serviços de Segurança Gerenciada da América do Norte em 2010" da Frost & Sullivan por sua capacidade de aprimorar e manter a maior participação de mercado entre MSSPs.[1]

Em um relatório de 2010 sobre serviços de segurança gerenciados, a empresa de pesquisa independente Forrester Research, Inc., concluiu: "A IBM tem a mais ampla diversidade de MSS de todos os provedores nesse Forrester Wave"2. Forrester observou também que, "Além de ter o conjunto mais amplo de serviços, a IBM também lidera em participação geral de mercado (por aproximadamente 10%), e alcance global (opera em mais de 150 países)".

Os IBM Managed Security Services oferecem soluções avançadas para gerenciamento de segurança em tempo real, incluindo monitoramento e gerenciamento de sistemas e identidades, respostas de emergência e proteção contínua e ininterrupta contra as ameaças mais críticas da Internet. O portfólio de serviços de segurança da IBM ajuda as organizações a minimizar risco, reduzir os crescentes custos de segurança, reduzir complexidade e demonstrar cumprimento. O amplo portfólio de IBM Managed Security Services inclui gerenciamento e monitoramento de dispositivos de segurança, bem como ofertas de Serviços de Segurança de Nuvem.

Gerenciamento e Monitoramento de Dispositivos de Segurança

Os serviços de gerenciamento de dispositivos de segurança da IBM oferecem monitoramento contínuo e ininterrupto de tecnologias de segurança hospedadas no ambiente de TI de uma organização. Através de um de gerenciamento consolidado, as empresas podem visualizar toda a sua infraestrutura de segurança e se manterem ativamente envolvidas com seus programas de segurança da informação, em colaboração com a IBM. Os serviços de IBM Security Device Management incluem:

- **Serviço de firewall gerenciado e monitorado** - Oferecendo gerenciamento contínuo de firewalls em tempo real, esse serviço fornece proteção personalizada com custo menor do que muitas soluções tradicionais. Ele oferece proteção preventiva contra ameaças de segurança conhecidas e emergentes, bem como suporte de múltiplos fornecedores que ajuda a maximizar investimentos existentes em segurança. As empresas são mantidas informadas com relatórios abrangentes e personalizáveis, incluindo opções de relatórios executivos e técnicos.
- **Serviços de identidades gerenciadas** - Essa solução de gerenciamento de ciclo de vida de identidades baseada em nível de serviço ajuda a proteger informações contra usuários não autorizados, fornecendo autorizações de serviço apenas para indivíduos com necessidades válidas de negócio e removendo essas autorizações quando o acesso não é mais necessário.. A solução inclui as melhores práticas de processos de ciclo de vida de identidade e tecnologia pré-configurada baseada no IBM Tivoli Identity Manager.
- **Serviço gerenciado de detecção e prevenção de violações**—Essa é uma oferta multifornecedor que fornece proteção abrangente para a rede e servidores, ajuda a bloquear ameaças e acesso não autorizado de fontes internas e externas. Ele oferece funções especializadas e proativas de detecção de invasores, prevenção de violação e capacidade de resposta a incidentes, bem como resposta e escalada em tempo real para atividades não autorizadas com potencial de ameaçar a empresa.
- **Serviços de proteção gerenciada**—Esses serviços ajudam a fornecer monitoramento especializado, gerenciamento e escalada de incidentes para a infraestrutura de TI de forma contínua e ininterrupta. Os Serviços de Proteção Gerenciada representam a solução de segurança gerenciada mais abrangente da IBM, incluindo os acordos de nível de serviço com a exclusiva garantia de proteção da IBM.
- **Serviços de segurança gerenciada para gerenciamento unificado de ameaças** —Essa é uma solução de segurança abrangente projetada para trabalhar à frente da ameaça, oferece monitoramento e suporte contínuos e ininterruptos para dispositivos unificados de gerenciamento de ameaça de diversos fornecedores, bem como serviços de gerenciamento de mudanças e projetos de políticas de segurança.
- **Gerenciamento seguro de gateway da web** —Esse serviço é projetado para fornecer gerenciamento e monitoramento contínuos para dispositivos seguros de gateway da web, ajudando a fornecer controle e proteção abrangentes para conteúdo web.

Serviços de Segurança em Nuvem

Os IBM Cloud Security Services aproveitam a potência da plataforma IBM Virtual Security Operations Center para oferecer serviços de alto valor que exigem pouco ou nenhum investimento em dispositivos de segurança ou manutenção, tornando o custo total de propriedade muito menor do que o utilizado por empresas que arcam com os custos de executar esses serviços de segurança internamente. As ofertas de serviços de segurança baseados em nuvem da IBM também são complementadas por um portfólio abrangente de segurança gerenciada tradicional e soluções de serviços profissionais. Os serviços de segurança baseados em nuvem dos IBM Managed Security Services incluem:

- ***Serviço de segurança para email*** — Esse serviço é projetado para atuar como a primeira linha de defesa do cliente, fazendo a varredura de emails e eliminando ameaças antes que cheguem à rede. A solução é totalmente hospedada pela IBM e não exige instalação de hardware ou software em locais de clientes.
- ***Serviço de segurança para web***— Projetado para ajudar clientes a proteger seus dados de exposição acidental resultante de malware, roubo de identidade e fraudes de phishing, esse serviço protege a infraestrutura de TI e a continuidade de negócios ao virtualmente eliminar degradação de desempenho e panes de sistema. Ele também reduz a necessidade de soluções adicionais de hardware e software. O serviço pode ajudar a melhorar a produtividade de clientes ao proteger desempenho de desktop, ajuda a evitar acesso a websites inapropriados e ajudar clientes a otimizar a configuração e administração da segurança na web através de uma interface web.
- **Serviço de gerenciamento de log e eventos de segurança** — Esse serviço permite a equipes de TI compilar os arquivos de log e de eventos de aplicativos de rede e sistemas operacionais, bem como de tecnologias de segurança, em uma plataforma otimizada. Ele oferece a capacidade de executar consultas em qualquer destes logs usando uma interface simples. Essa inovação melhora drasticamente a velocidade da condução de investigações de segurança. Além disso, a IBM pode arquivar judicialmente dados de som, admissíveis como evidência em tribunal, por um período de até sete anos.
- **Serviço de gerenciamento de vulnerabilidade** —Oferecendo varredura de infraestrutura interna e externa baseada em nuvem, através de um único portal, esse serviço otimiza requisitos de gerenciamento de cumprimento. Ele oferece suporte para iniciativas de cumprimento ao varrer e classificar vulnerabilidades, fornecendo os dados e passos de correção para gerenciamento de riscos de segurança e redução da exposição a ameaças.
- **Análise de ameaças X-Force**— Fornecendo informações personalizadas sobre uma ampla diversidade de ameaças que podem afetar a segurança de rede, esse serviço de inteligência de segurança ajuda as empresas a proteger proativamente as suas redes com análises detalhadas das condições de ameaças onlines globais.

Por que usar os IBM Managed Security Services?

A IBM tem um longo histórico como especialista confiável de segurança para organizações e governos do mundo inteiro. IBM Managed Security Services - ajudando a definir o padrão de responsabilidade, confiabilidade e proteção em serviços de segurança gerenciados desde 1995 - oferece a capacitação,

ferramentas e infraestrutura que as empresas precisam para proteger seus ativos de informação de ataques da Internet, frequentemente a uma fração do custo de usar recursos internos de segurança.

Experiência de segurança líder de mercado

No núcleo dos IBM Managed Security Services, a equipe de desenvolvimento do relatório IBM X-Force® oferece a base para a abordagem proativa de segurança de Internet que os clientes se acostumaram a esperar da IBM. De fato, a equipe X-Force é um dos grupos de pesquisa de segurança comercial mais conhecidos do mundo. Além disso, a equipe X-Force trabalha como consultor de confiança na área de segurança para o Departamento de Homeland Security dos Estados Unidos, bem como muitas outras organizações governamentais federais, estaduais e locais, ajudando na criação de padrões e iniciativas governamentais de segurança.

A equipe X-force é composta por mais de 15.000 pesquisadores, desenvolvedores, analistas e especialistas em iniciativas de segurança, sendo responsável por 3.000 patentes de gerenciamento de risco e segurança e com mais de 40 anos de sucesso comprovado em segurança.
Esse grupo líder de especialistas em segurança pesquisa e avalia vulnerabilidades e problemas de segurança, desenvolvendo tecnologia de contramedidas e avaliações para produtos da IBM, além de informar o público sobre ameaças emergentes de Internet através de relatórios produzidos durante o ano fornecendo alertas críticos e orientações. A equipe X-Force da IBM mantém o banco de dados mais abrangente do mundo de ameaças e vulnerabilidades, resultado de dezenas de milhares de horas de pesquisa da equipe, e muitos desses dados são usados para impulsionar a proteção preventiva fornecida por produtos IBM.

Os analistas e especialistas de segurança da IBM trabalham em dez centros de operações de segurança (SOCs) globais, onde analisam mais de nove bilhões de eventos de segurança por dia. (ver Imagem 1) (Na imagem está faltando o SOC de Wroclaw, Polônia)

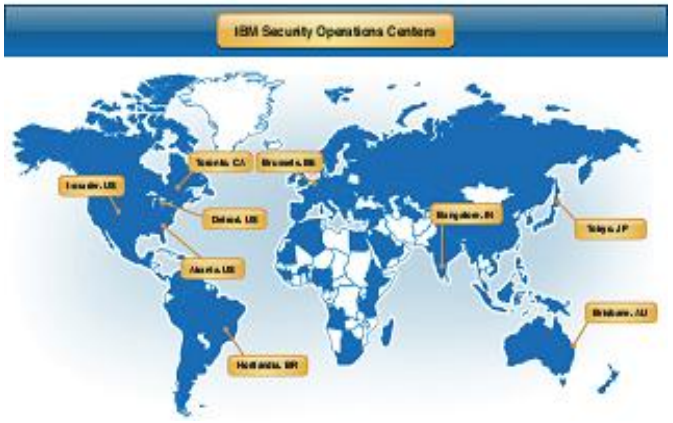

Imagem 1. Centros de Operações de Segurança da IBM.

Tecnologias inovadoras de segurança

Os IBM Managed Security Services, além de utilizar os especialistas de segurança de SOC, são suportados e viabilizados pelo IBM Virtual SOC, uma ferramenta de gerenciamento seguro baseada na web. Aproveitando a combinação de qualificações e inteligência dos SOCs globais, o SOC Virtual oferece uma interface única (mostrada na figura 2) para permitir que gerentes de segurança da empresa monitorem facilmente a segurança da infraestrutura geral de dispositivos de segurança gerenciados e não gerenciados.

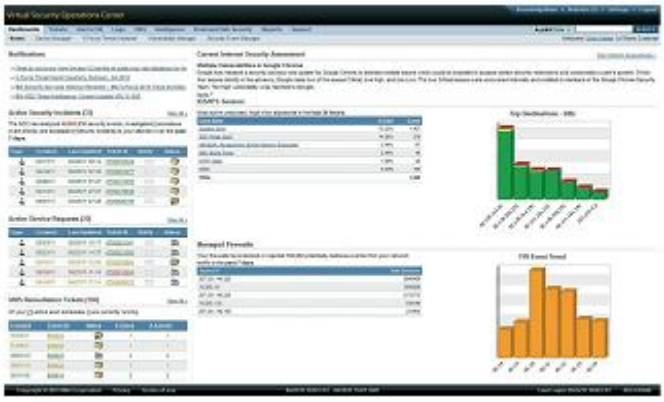

Imagem 2. Portal do IBM Virtual Security Operations Center (SOC).

O portal Virtual SOC combina a pesquisa de segurança X-Force com os dados de nível de serviço de dispositivos em redes corporativas, ajudando equipes de TI a gerenciar vulnerabilidades descobertas em seus sistemas. Os clientes dos IBM Managed Security Services usam o portal Virtual SOC como seu centro de comando e controle para todos os seus IBM Cloud Security Services, bem como para os seus serviços de segurança de gerenciamento de dispositivos. O portal seguro baseado na web oferece a inteligência, ferramentas e capacidade necessárias para tomar decisões em tempo real que melhoram a postura de segurança. Disponível em qualquer lugar, a qualquer momento, o portal Virtual SOC viabiliza colaboração entre organizações e sua equipe de especialistas de segurança da IBM.

O IBM X-Force Protection System é o sistema altamente sofisticado de retaguarda que oferece a inteligência contínua de segurança disponível através do Virtual SOC. A IBM investiu mais de $400 milhões ao longo dos últimos 10 anos no desenvolvimento do Virtual SOC X-Force Protection System.

O X-Force Protection System analisa bilhões de eventos de segurança e logs que os clientes lidam diariamente, de modo a identificar o que precisa de atenção ou de ações adicionais. O sistema agrega informações de segurança de múltiplos conjuntos de dados, independentemente do tipo de dispositivo ou fornecedor ou de ser gerenciado internamente ou pela IBM. O sistema normaliza essas informações e as correlaciona com outros conjuntos de dados relacionados, arquivando os dados brutos de forma judicialmente apropriada para futuras investigações de segurança e cumprimento. Além disso, ele promove a escalada de eventos prioritários, alertando o cliente ou analista de segurança IBM de que precisa agir, além de oferecer orientação individualizada de correção e funcionalidades tais como registro de problema e fluxo de trabalho integrado.

Ao oferecer a clientes uma visão única de operações e gerenciamento de sua infraestrutura completa de segurança - independentemente do tipo de fornecedor ou dispositivo - o X-Force Protection System permite que organizações gerenciem de forma mais eficaz as suas operações de segurança. O sistema é particularmente vantajoso para clientes lidando com múltiplas instalações, tais como corporações multinacionais ouempresas com filiais ou centros de processamento de dados externos.

Os benefícios de escolher os IBM Managed Security Services

Os IBM Managed Security Services permitem a empresas reduzir a necessidade de recursos de segurança internos, ao terceirizar operações ou suplementar equipes existentes de segurança. Ao escolher a IBM para fornecimento de Serviços de Segurança de Nuvem e serviços de gerenciamento de dispositivos de segurança, as organizações podem aprimorar a sua postura e reduzir custos ao mesmo tempo. A IBM oferece a experiência para gerenciar a complexidade do cenário de segurança, fornecendo a experiência de mercado necessária para avaliar a postura de risco de segurança, entregando inovação através de soluções seguras e de ponta a ponta.
Os IBM Managed Security Services permitem que as organizações:

- **Melhorem a postura de segurança** —Conhecimento contínuo sobre ameaças emergentes de Internet e recomendações de correção oferecem proteção aprimorada, garantem a continuidade de negócios, ajudam a unificar gerenciamento de políticas e protegem a imagem da empresa. A equipe IBM X-Force oferece inteligência de segurança profunda e contínua. O portal IBM Virtual SOC oferece a visibilidade, controle e automação necessários, viabilizando gerenciamento de segurança proativo e em tempo real.
- **Reduzam custos** – Os IBM Managed Security Services e o Virtual SOC podem reduzir significativamente os crescentes custos de gerenciamento de segurança. A IBM reduz o custo total de propriedade ao economizar até 55% em custos de gerenciamento de segurança da informação, permitindo que empresas redistribuam recursos para outros objetivos de negócio. As empresas podem eliminar o custo de contratar e treinar recursos adicionais para garantir proteção apropriada de rede. Economias adicionais de custo são obtidas através de redução de indisponibilidade, otimização de infraestrutura, produtividade aprimorada e prevenção da perda de receita que resultaria em violações de segurança e perda de dados.
- **Simplifiquem gerenciamento** - O IBM Virtual SOC oferece um mecanismo sólido para gerenciamento de ponta a ponta para soluções de segurança da IBM e de outros fornecedores, abrangendo também todos os domínios de risco. A IBM ajuda a ampliar eficiências operacionais ao eliminar tarefas de auditoria manual e reduzir o número e complexidade de controles de segurança necessários. Os serviços de segurança da IBM também reduzem gastos redundantes de segurança. As empresas podem consolidar ambientes de múltiplos fornecedores para facilitar o gerenciamento, ao mesmo tempo em que gerenciam com eficácia o volume operacional global.
- **Protejam investimentos em serviços**—Empresas que escolhem os IBM Managed Security Services ganham com SLAs garantidos baseados em desempenho, garantindo proteção 100% confiável e responsável. Serviços padronizados, replicáveis e pré-definidos, bem como fornecimento baseado em ativos aplicando as melhores práticas reconhecidas pelo segmento de mercado, ajudam a otimizar os investimentos em serviços. A proteção adicional resulta de contratos simplificados, precificação previsível e o recebimento de ampla diversidade de serviços flexíveis a partir de um único fornecedor de serviços de TI.

- **Protejam investimentos existentes de TI** — IBM Managed Security Services são baseados em uma abordagem neutra em relação a fornecedor quanto ao gerenciamento de segurança, suportando diversos tipos de dispositivos de vários fornecedores como IBM, CheckPoint, Cisco, Juniper, Symantec, McAfee, TrendMicro, 3com e outros. O fornecimento integrado de serviços permite a integração otimizada de tecnologias de segurança diferentes, e junto com a inteligência de segurança embutida viabiliza tomada de decisões aprimorada e maximização de investimentos em infraestrutura. O gerenciamento aprimorado de segurança ajuda as organizações a ampliar o valor de investimentos em infraestrutura de segurança, ao otimizar seu desempenho.

- **Atingirem e manterem cumprimento** —Através de monitoramento contínuo de segurança e políticas e procedimentos documentados de segurança, os IBM Managed Security Services ajudam as empresas a manter o cumprimento de regulamentos governamentais e do segmento de mercado. A IBM detém certificações para algumas das mais complexas regulamentações de cumprimento do mercado, com a experiência para auxiliar empresas na implementação de controles internos e regulatórios para SOX, PCI, GLBA, HIPAA e outras normas de cumprimento. A IBM viabiliza fornecimento integrado de tecnologias de segurança exigidas por muitas regulamentações, tais como firewalls, sistemas de proteção contra intrusos, gerenciamento de vulnerabilidade, gerenciamento de logs e eventos de segurança.

IBM: Fornecendo confiança, simplicidade e valor

A terceirização da segurança permite que as organizações melhorem seu status de segurança, reduzam custos operacionais e concentrem funcionários importantes de TI nas principais funções de negócios. Um componente central para o sucesso de uma decisão de terceirização de segurança é a escolha do fornecedor certo. As organizações devem buscar um fornecedor com histórico de trabalho confiável e estabilidade financeira, bem como SLAs seguros com proteção garantida. Uma rede global redundante de centros de operações de segurança com especialistas, somada a um conjunto em contínua evolução de serviços, protegerá a empresa e os investimentos feitos.

Com os IBM Managed Security Services, as empresas ganham com a melhoria de eficiências operacionais, financeiras e estratégicas em toda a corporação e, o que é mais importante, podem avançar em suas práticas de gerenciamento de segurança. Como a Forrester reconhece, "As organizações de segurança que precisam de alcance global, conjunto amplo de serviços de segurança e boa inteligência contra ameaças devem considerar a IBM para o fornecimento desses serviços"[2]

As empresas que escolhem a IBM rapidamente ganham *confiança* ao trabalhar em colaboração com a equipe de segurança IBM X-Force de renome global. Elas também apreciam a *simplicidade* oferecida pelo portal IBM Managed Security Services Virtual SOC. Também importante, os dez centros de operações de segurança globais da IBM oferecem serviços gerenciados de segurança consistentes, em nível premium, oferecendo máximo *valor* para empresas que contam com a IBM para suportar seus objetivos de gerenciamento de risco.

Para mais informações

Para saber mais a respeito dos IBM Managed Security Services, contate o seu representante de marketing da IBM ou seu Parceiro de Negócios IBM ou visite o seguinte website: **ibm.com**/services/us/iss

Além disso, as soluções de financiamento da IBM Global Financing podem permitir um gerenciamento efetivo de caixa, proteção contra a obsolescência da tecnologia, melhor custo total de propriedade e retorno do investimento. Nossos Global Asset Recovery Services também ajudam a lidar com as preocupações ambientais, por meio de soluções novas e mais eficientes em relação à energia. Para obter mais informações sobre a IBM Global Financing, visite: **ibm.com**/financing

IBM
Route 100
Somers, NY 10589 E.U.A.

Produzido nos Estados Unidos da América
Maio de 2011

[1] *Frost & Sullivan: Mercado Norte-Americano de Provedores de Serviços Gerenciados de Segurança*, maio de 2010.

[2] *The Forrester Wave: Serviços Gerenciados de Segurança, 3º Trimestre de 2010*, Khalid Kark, para Profissionais de Segurança e Risco, 4 de agosto de 2010.

Por Favor, Reciclável.

SEW03026-USEN-0