



DATA SHEET

PRINCIPAIS BENEFÍCIOS

Inteligência inigualável em segurança

O Managed Intrusion Prevention Service maximiza a VeriSign Intelligence para garantir inteligência às operações dentro da empresa, entre empresas e na Internet. A VeriSign, por gerenciar serviços importantes de infra-estrutura de Internet, como o Sistema de Nomes de Domínio (DNS), tem uma visibilidade única sobre ameaças de segurança na Internet.

Os melhores acordos de nível de serviço (SLAs) do mercado

A VeriSign fornece o serviço de mais alta qualidade do setor com o respaldo de SLAs rigorosos.

Serviços de implementação abrangente

Os gerentes de programa e engenheiros de segurança da VeriSign asseguram que os dispositivos de prevenção contra intrusão sejam preparados e amplamente testados antes da implementação.

Gerenciamento de todo o ciclo de vida

A VeriSign fornece um gerenciamento de ciclo de vida verdadeiramente contínuo.

VeriSign® Managed Intrusion Prevention Services

A crescente sofisticação dos ataques na Internet e a velocidade na qual se propagam exigem um tipo mais inteligente de tecnologia com mais capacidade para evitar intrusões. As empresas não podem mais depender de produtos que somente notificam ataques. Elas necessitam de uma tecnologia que possa barrar potenciais brechas de segurança antes de haver algum impacto negativo em seus negócios. Como resposta, os fornecedores de segurança incluíram tecnologias de prevenção contra intrusão em seus produtos existentes, além de criar uma nova linha de dispositivos para manter suas redes seguras. Hoje, as tecnologias de prevenção contra intrusão utilizam uma grande variedade de técnicas, inclusive correspondência de assinatura, além de detecção de anomalias de protocolo e tráfego, para monitorar e bloquear o tráfego malicioso com eficiência.

A adoção de tecnologias de prevenção contra intrusão criou um desafio singular para os profissionais de segurança. A criação e a manutenção de diretivas eficientes para dispositivos demandam amplo conhecimento sobre segurança e tempo. Se as diretivas forem incorretamente adaptadas ao ambiente do cliente e não forem atualizadas com regularidade, o tráfego malicioso poderá ser autorizado e o tráfego benigno, bloqueado. Além de gerenciar políticas de prevenção contra intrusão, os profissionais de segurança devem monitorar continuamente os eventos gerados pelos dispositivos, bem como os próprios dispositivos. Como essas tecnologias são muitas vezes implementadas por meio de dispositivos em série, a interrupção das operações pode fazer com que todo o tráfego seja bloqueado ou o tráfego malicioso seja permitido no ambiente do cliente.

+ A abordagem

O VeriSign® Managed Intrusion Prevention Service (MIPS - Serviço de prevenção a intrusões gerenciado) é um componente do aclamado conjunto MSS (Managed Security Services). Com esse serviço, as empresas podem maximizar o retorno do investimento em tecnologias de prevenção de intrusão ao mesmo tempo em que reduzem custos operacionais e de capital. A equipe de especialistas em segurança da VeriSign gerencia e monitora o dispositivo permanentemente, controlando eventos que ameaçam sua integridade e violações de segurança provocadas por ataques originados dentro ou fora da rede. Os acordos de nível de serviço (SLAs) líderes de mercado da VeriSign garantem que os clientes sejam rapidamente notificados sobre questões de segurança e integridade a fim de poderem agir a tempo para minimizar o risco.



Where it all comes together.™

Monitoramento de segurança e gerenciamento de riscos

Os eventos de segurança, monitorados permanentemente, são capturados, analisados e correlacionados em tempo real. Eventos suspeitos e maliciosos são, dessa forma, identificados proativamente, reduzindo o potencial de risco de uma organização. Junto com os serviços de consultoria da VeriSign, os especialistas em segurança da empresa imediatamente executam os planos de reparo.

+ Descrição

O VeriSign Managed Intrusion Prevention Service oferece gerenciamento e monitoramento 24 horas de uma ampla gama de tecnologias de prevenção contra intrusão. A criação e manutenção de diretivas eficientes são o aspecto mais desafiador do gerenciamento dessas tecnologias. Devido à nossa ampla experiência no assunto e à incomparável inteligência de segurança do Managed Intrusion Prevention Service, a VeriSign está em uma posição exclusiva de criar uma política apropriada para o ambiente do cliente.

Durante o período de adaptação inicial, a VeriSign faz simulações das diretivas e trabalha com os clientes para determinar o tráfego que deverá ser bloqueado. Após ampla adaptação e aprovação do cliente, o bloqueio ativo é habilitado e as diretivas são ampliadas conforme os fornecedores lançam atualizações e novas ameaças surgem. O status da integridade do dispositivo, assim como todas as tentativas de intrusão, são registrados e reportados no Portal de recursos do cliente da VeriSign. Os clientes são notificados sobre as principais questões de segurança e integridade por telefone, e-mail ou pager. Além disso, a VeriSign atualiza e corrige todos os dispositivos gerenciados.

+ Recursos do serviço

O VeriSign Managed Intrusion Prevention Service executa os seguintes serviços:

- Configuração e provisionamento de dispositivos
- Criação de diretivas iniciais, atualizações e adequações permanentes
- Monitoramento e relatório de integridade e eventos de segurança 24 horas
- Relatório de todos os eventos de segurança no Portal de recursos do cliente (as opções de relatório são flexíveis)
- Notificação aos clientes de questões importantes sobre segurança e integridade
- Atualizações e correções de dispositivos

Esse serviço ainda oferece integração total com a equipe VeriSign Incident Response and Forensics.

+ Centros de operações de segurança

Os centros de operações de segurança (SOCs) da VeriSign são ambientes seguros e altamente disponíveis que fornecem monitoramento e gerenciamento 24 horas de infra-estruturas de segurança para grandes empresas. Construção em estilo bunker, acesso biométrico em camadas a áreas sensíveis e vigilância por vídeo são recursos especiais do controle de segurança física, enquanto um gerador reserva, uma fonte de alimentação condicionada (UPS) e sistemas de ponta para controle de incêndios garantem disponibilidade 24 horas. Todos os sistemas fundamentais, da eletricidade aos links de telecomunicações e processamento de dados, são totalmente redundantes, eliminando, dessa forma, qualquer ponto único de falha.

+ TeraGuard®

A arquitetura de gerenciamento de informações da VeriSign, o TeraGuard™, coleta uma grande variedade de dados de fontes diferentes por meio do SDA (Security Defense Appliance). O SDA fica localizado nas instalações do cliente e converte os dados dos dispositivos de rede e segurança em um único fluxo normalizado de eventos relacionados à segurança. O TeraGuard então analisa e prioriza esses eventos usando um processo de correlação em camadas. Com essa função, a VeriSign pode eliminar rapidamente falsos positivos, encontrar ameaças reais e tomar as providências necessárias.

+ O diferencial da VeriSign

- **Escala global e Intelligence and Control** – a VeriSign oferece a seus clientes a vantagem de um sistema de aviso antecipado que maximiza sua ampla base de dados sobre ameaças disponíveis com os serviços Intelligence and Control™. Com uma base de clientes mundial e milhares de dispositivos de segurança de rede sob seu gerenciamento, a VeriSign possui uma visão mais ampla e profunda das atividades na Internet e, por isso, pode identificar e alertar proativamente seus clientes sobre as tendências de ataque.

- **Compromisso com a excelência** – a VeriSign dedica-se ao crescimento e ao aprimoramento constantes dos MSS (Managed Security Services) e investe continuamente em seus centros de operações de segurança especializados, infra-estruturas inigualáveis e inteligência e correlação avançadas.
- **Monitoramento de integridade e desempenho** – o monitoramento 24 horas de integridade e desempenho de dispositivos permite à VeriSign lidar proativamente com problemas operacionais antes das falhas de serviço ocorrerem.
- **Resposta imediata garantida** – a VeriSign inicia um procedimento de dimensionamento específico para o cliente assim que o problema é detectado e então age rapidamente para identificar a origem.
- **Canal de comunicação/gerenciamento confiável** – o VeriSign SDA patenteado é um canal de gerenciamento e comunicação tolerante a falhas e seguro. O SDA, executado por trás do firewall do cliente, oferece recursos seguros de armazenamento e encaminhamento de eventos por meio de uma conexão criptografada com o centro de operações de segurança da VeriSign. Apesar de não ser obrigatória, a implantação do SDA é altamente recomendada.
- **Portal permanente de recursos do cliente** – o Portal de recursos do cliente oferece uma visão detalhada dos dispositivos de segurança que são gerenciados pela VeriSign. Isso inclui vários relatórios por tipo de dispositivo e acesso a um mecanismo de consulta ad hoc para análises sofisticadas de eventos de segurança em diversos locais e plataformas. O acesso ao sistema é protegido por autenticação com token e criptografia SSL (Secure Sockets Layer - camada de soquetes de segurança).
- **Suporte, monitoramento e gerenciamento 24 horas** – a equipe de analistas de segurança especializados da VeriSign está permanentemente disponível. Os serviços da empresa são criados para serem altamente redundantes e oferecer suporte e disponibilidade ininterruptos 24 horas.
- **O melhor suporte do mercado para dispositivos de terceiros** – a VeriSign não recomenda um fornecedor especificamente e garante compatibilidade com uma grande variedade dos melhores produtos de segurança do mercado. A empresa desenvolve e implementa soluções de segurança baseadas nas necessidades e nos requisitos específicos de seus clientes e regularmente avalia e aprimora seus produtos e os produtos de segurança compatíveis de outras empresas.
- **Parceiro de confiança** – a VeriSign tem uma forte tradição no gerenciamento de serviços de segurança confiáveis e milhares de organizações beneficiam-se dessa tradição todos os dias. Juntamente com autenticação forte, segurança de aplicativo e de comércio eletrônico, os VeriSign Managed Security Services representam um compromisso incomparável com o fornecimento dos Intelligent Infrastructure Services, que permitem às empresas dedicarem-se a comércio eletrônico, comunicações e computação colaborativa de maneira confiável.
- **Profissionais treinados e dedicados** – a VeriSign possui uma ampla equipe de profissionais de segurança certificados, especialmente treinados para gerenciar produtos de segurança dos principais fornecedores do mercado.
- **Custo total de propriedade (TCO) mais baixo** – o VeriSign Managed Intrusion Prevention Service economiza tempo e dinheiro das organizações ao reduzir gastos com equipes, treinamento, manutenção e investimento inicial.

+ Comece hoje

Para obter mais informações sobre os serviços de consultoria e MSS da VeriSign, ligue para (0) XX 11 5853-2900 ou envie um e-mail para faleconosco@verisign.com.

Visite www.verisign.com.br para obter mais informações.

Nota: Gartner Inc. (NYSE: IT e ITB) posicionou a VeriSign no quadrante líder do relatório 1H04 Managed Security Services Provider (MSSP) Magic Quadrant para a América do Norte. A versão completa deste relatório está disponível em www.verisign.com/cgi-bin/lga.cgi?a=068050192724827000.

© 2006 VeriSign Brasil. Todos os direitos reservados. VeriSign, o logotipo da VeriSign, TeraGuard, "Intelligence and Control", "Where it all comes together" e outras marcas comerciais, marcas de serviço e logotipos são marcas registradas ou não-registradas da VeriSign e de suas subsidiárias nos Estados Unidos e em outros países.