E-BOOK

Proteja seu site WordPress com as melhores

Práticas de segurança

Sumário

Visão geral

Aprenda sobre a importância da segurança digital na Via Agência Digital e como proteger seu site WordPress contra ameaças cibernéticas sofisticadas. Descubra as ferramentas e práticas essenciais para manter sua presença online segura e confiável.

Introdução e Compromisso com a Segurança

Na Via Agência Digital, a segurança dos websites é uma prioridade absoluta desde o início de nossa trajetória. **Com mais de 19 anos de experiência em desenvolvimento web, estamos plenamente cientes das ameaças cibernéticas que podem comprometer a integridade de um site.**

Entendemos que garantir a segurança de um site WordPress vai muito além da simples seleção de plugins e temas; é necessário efetuar a configuração correta, integrar com precisão e aderir estritamente às melhores práticas de desenvolvimento. Nosso compromisso com a segurança é perceptível em cada etapa do processo.

Para assegurar a segurança dos websites desenvolvidos por nós, utilizamos exclusivamente plugins e temas premium, previamente avaliados meticulosamente. Além disso, não realizamos alterações no core do WordPress, nos temas originais ou nos plugins instalados, visando manter a estabilidade e a segurança dos sites em primeiro plano.

Ao escolher nossos serviços, você efetua uma parceria que valoriza a segurança e busca a excelência em cada etapa do desenvolvimento. Nosso compromisso é garantir que seu site WordPress estará sempre resguardado contra as mais sofisticadas ameaças cibernéticas, oferecendo a segurança e a estabilidade que você merece.

Suíte de Segurança da Via Agência Digital

Na Via Agência Digital, a segurança dos sites dos clientes é uma prioridade. A Suíte de Segurança oferecida é uma solução completa e integrada, projetada para proteger os sites WordPress de forma eficaz contra ameaças cibernéticas. Esta suíte combina tecnologia avançada e práticas recomendadas de segurança para garantir tranquilidade e desempenho superior aos usuários.

Funcionalidades da Suíte de Segurança:

1. **Detecção de Malware em Tempo Real (Solid Security):** Monitora constantemente o site, identificando e removendo ameaças de malware assim que surgem, garantindo a integridade do site.
2. **Firewall e Proteção DDoS (Cloudflare):** Oferece um Web Application Firewall (WAF) para bloquear tráfego malicioso e protege contra ataques DDoS, injeções de SQL e outras ameaças cibernéticas.
3. **Gerenciamento Detalhado de Permissões (Solid Security):** Permite controle preciso sobre as permissões de usuários, limitando o acesso a áreas sensíveis do site e prevenindo violações de segurança.
4. **Autenticação Multifator (Solid Security):** Protege as contas dos usuários com uma camada extra de segurança, exigindo múltiplos fatores de autenticação para acesso administrativo.
5. **Backups Automáticos e Sob Demanda (Cloudways e ManageWP):** Garante backups regulares do site, permitindo restaurações rápidas e fáceis em caso de incidentes de segurança.
6. **Gerenciamento de Atualizações e Patches (ManageWP):** Automatiza a aplicação de atualizações e patches de segurança para WordPress, plugins e temas, garantindo que o site esteja sempre atualizado e protegido contra vulnerabilidades.
7. **Content Delivery Network (CDN) (Cloudflare):** Melhora o desempenho do site, reduzindo o tempo de carregamento das páginas e oferecendo uma experiência de navegação mais rápida e segura para os usuários.

Benefícios da Suíte de Segurança:

1. **Proteção Completa Contra Ameaças Cibernéticas:** Combinação de detecção de malware, firewall, proteção DDoS e autenticação multifator para defender o site contra uma ampla gama de ameaças.

2. **Alta Disponibilidade e Confiabilidade:** O uso do Cloudflare e dos backups automáticos do Cloudways assegura que o site esteja sempre acessível, mesmo em caso de ataques ou falhas de segurança.

3. **Gestão Eficiente e Simplificada:** O ManageWP facilita o gerenciamento de atualizações, backups e segurança em um único painel centralizado, economizando tempo e recursos.

4. **Experiência de Navegação Rápida e Segura:** A integração com o Cloudflare CDN otimiza o desempenho do site, proporcionando uma experiência de usuário mais fluida e protegida.

5. **Redução de Riscos Operacionais:** A detecção proativa de malware e a capacidade de restaurar rapidamente o site em caso de incidentes minimizam o risco de perda de dados e interrupção dos negócios.

Solid Security

O Solid Security oferece uma solução de segurança robusta para proteger seu site WordPress contra uma ampla gama de ataques, como tentativas de força bruta, injeções XSS, injeções de SQL e outras ameaças cibernéticas comuns. Com varreduras automáticas e frequentes, ele identifica e corrige vulnerabilidades, garantindo que seu site esteja sempre protegido e funcionando com segurança.

Funcionalidades do Solid Security:

1. **Análise em Tempo Real de Malware:** Fornece monitoramento contínuo para identificar, analisar e neutralizar malwares antes que eles possam causar danos aos sistemas.

2. **Controle de Acesso:** Implementa autenticação multifator (MFA) para garantir que apenas usuários autorizados acessem os sistemas, além de limitar tentativas de login para evitar ataques de força bruta.

3. **Proteção Avançada de Firewall:** Oferece regras de firewall personalizadas para criar camadas adicionais de proteção, bloqueando tráfego malicioso e acessos não autorizados.

4. **Monitoramento de Integridade de Arquivos:** Verifica alterações em arquivos críticos do sistema para identificar atividades suspeitas que possam comprometer a segurança.

5. **Detecção de Comportamento Anômalo:** Utiliza algoritmos avançados para identificar e responder rapidamente a comportamentos anômalos, prevenindo possíveis incidentes de segurança.

6. **Prevenção contra Ransomware:** Bloqueia tentativas de criptografia não autorizada de dados, garantindo que informações críticas não sejam sequestradas por ataques de ransomware.

7. **Segurança de Rede:** Monitora o tráfego da rede em tempo real para detectar padrões de ataque e evitar invasões ou comprometimentos.

Continuação...

8 **Proteção contra Phishing:** Identifica e bloqueia tentativas de phishing, protegendo os usuários contra ataques que tentam roubar credenciais ou informações confidenciais.

9 **Isolamento de Aplicações:** Segrega aplicativos críticos em ambientes isolados, minimizando o impacto de possíveis ataques ou falhas.

10 **Relatórios e Alertas em Tempo Real:** Gera relatórios detalhados e envia alertas em tempo real sobre qualquer atividade suspeita ou tentativa de violação de segurança.

Voltar ao índice

Voltar ao índice

Cloudflare

O Cloudflare proporciona uma proteção completa ao seu site por meio de sua rede global de Content Delivery Network (CDN), melhorando significativamente a velocidade, a segurança e o desempenho. Além de otimizar o carregamento das páginas, a plataforma oferece defesa robusta contra ataques DDoS e outras ameaças cibernéticas.

Funcionalidades do Cloudflare:

1. **Criptografia SSL/TLS:** Garante a segurança na transmissão de dados entre o servidor e o usuário.
2. **Proteção contra Ataques DDoS:** Defende contra ataques de negação de serviço distribuída, assegurando a continuidade do site.
3. **Firewall de Aplicações Web (WAF):** Protege contra vulnerabilidades comuns como injeção de SQL e cross-site scripting (XSS).
4. **Otimização Automática de Imagens:** Reduz o tamanho das imagens para melhorar o tempo de carregamento do site.
5. **Minificação de Código:** Diminui o tamanho de arquivos HTML, CSS e JavaScript, acelerando o carregamento.
6. **Balanceamento de Carga:** Distribui o tráfego entre múltiplos servidores, garantindo maior performance e resiliência.
7. **Cache Dinâmico e Estático:** Armazena conteúdos nas bordas da rede, acelerando a resposta do site aos usuários.

Continuação...

8. **Rate Limiting:** Limita o número de requisições a um site, prevenindo ataques de força bruta e abusos.

9. **DNSSEC:** Protege contra ataques de envenenamento de cache e assegura a integridade das respostas DNS.

10. **Proteção contra Bots:** Detecta e bloqueia tráfego de bots maliciosos, evitando fraudes e abusos.

11. **Gerenciamento de Tráfego:** Direciona os visitantes ao servidor mais próximo para reduzir latência.

12. **Argo Smart Routing:** Otimiza o roteamento de dados através da rede para reduzir a latência.

13. **Page Rules:** Personaliza o comportamento do site para URLs específicas, melhorando a entrega de conteúdo.

14. **Magic Transit:** Protege redes corporativas contra ataques DDoS ao nível de rede.

15. **Workers:** Executa código sem servidor na borda da rede, facilitando o desenvolvimento de aplicações mais rápidas e seguras.

Voltar ao índice

Voltar ao índice

Cloudways

O Cloudways facilita o gerenciamento de servidores e a hospedagem de sites WordPress, oferecendo uma plataforma intuitiva que simplifica a configuração, o monitoramento e a manutenção dos servidores. Com funcionalidades avançadas e automação integrada, garante desempenho otimizado e controle total, sem a complexidade típica da administração de servidores.

Principais Características do Cloudways:

1. **Facilidade de Configuração:** Simplifica o processo de configuração dos servidores, permitindo que os usuários iniciem seus projetos rapidamente, sem complicações técnicas.

2. **Backups Automáticos e Sob Demanda:** Oferece backups automáticos diários, com a opção de realizar backups sob demanda, garantindo a proteção contínua dos dados.

3. **Segurança Avançada:** Implementa patches de segurança regulares, firewalls dedicados e monitoramento 24/7 para proteger servidores contra ameaças.

4. **Monitoramento de Servidores em Tempo Real:** Oferece análise detalhada e monitoramento em tempo real para identificar problemas de desempenho e segurança.

5. **Suporte para Várias Aplicações:** Suporta diversos CMS (WordPress, Magento, etc.), permitindo a instalação de várias aplicações em um único servidor.

6. **Migração Gratuita:** Facilita a migração de sites para a plataforma Cloudways sem custos adicionais.

7. **Escalabilidade Sob Demanda:** Permite aumentar ou diminuir os recursos do servidor de acordo com a necessidade do projeto, garantindo flexibilidade.

Continuação...

8 **Firewalls Dedicados:** Protege os servidores contra acessos não autorizados e ataques de força bruta, utilizando firewalls dedicados.

9 **Integração com CDNs:** Facilita a integração com Content Delivery Networks (CDN), melhorando a performance do site em diferentes regiões geográficas.

10 **Ambiente de Staging:** Oferece um ambiente de testes separado para realizar alterações e atualizações sem afetar o site ao vivo.

11 **Gerenciamento de Equipes:** Permite a adição de membros da equipe com diferentes níveis de acesso, facilitando a colaboração.

12 **Suporte 24/7:** Disponibiliza suporte técnico 24 horas por dia, garantindo ajuda sempre que necessário.

Voltar ao índice

ManagerWP

O ManageWP oferece uma solução completa para a gestão de sites WordPress, permitindo que seus sites estejam sempre atualizados, seguros e com desempenho otimizado. Com ferramentas centralizadas de monitoramento, backups automáticos e gestão de atualizações, ele facilita a administração eficiente de múltiplos sites em um único painel.

Funcionalidades do ManagerWP:

1. **Gerenciamento Centralizado:** Permite gerenciar vários sites WordPress a partir de um único painel de controle, facilitando a administração.

2. **Backups Automáticos e Sob Demanda:** Oferece backups automáticos diários e a opção de realizar backups sob demanda para garantir a segurança dos dados.

3. **Monitoramento de Uptime:** Verifica continuamente se os sites estão online, notificando em tempo real caso algum fique fora do ar.

4. **Verificação de Segurança:** Realiza escaneamentos de segurança regulares para identificar vulnerabilidades e proteger os sites contra malwares e ataques.

5. **Atualizações em Massa:** Facilita a atualização de plugins, temas e versões do WordPress em todos os sites gerenciados, tudo com um clique.

6. **Relatórios de Desempenho:** Gera relatórios detalhados sobre o desempenho, tráfego e atualizações dos sites, personalizáveis e enviados regularmente para os clientes.

7. **Monitoramento de Desempenho:** Avalia a velocidade e o desempenho dos sites, identificando possíveis problemas que possam afetar a experiência do usuário.

Continuação...

8 **Clonagem e Migração de Sites:** Permite clonar ou migrar sites facilmente, sem a necessidade de processos técnicos complicados.

9 **Escaneamento de Vulnerabilidades:** Detecta potenciais falhas de segurança em temas e plugins, garantindo que as correções sejam aplicadas rapidamente.

10 **Gerenciamento de Equipes:** Permite a criação de diferentes níveis de acesso para equipes, facilitando a colaboração em projetos de manutenção.

11 **Otimização de Banco de Dados:** Limpa e otimiza os bancos de dados do WordPress para melhorar o desempenho do site.

12 **Verificação de Links Quebrados:** Disponibiliza suporte técnico 24 horas por dia, garantindo ajuda sempre que necessário.

13 **Verificação de Links Quebrados:** Identifica links quebrados nos sites gerenciados, ajudando a manter uma boa experiência de navegação e SEO.

14 **Suporte a Google Analytics:** Integra-se com o Google Analytics para fornecer dados de tráfego diretamente no painel de controle do ManageWP.

15 **Relatórios Mensais para Clientes:** Gera relatórios mensais sobre a manutenção dos sites, ideal para agências que precisam enviar atualizações aos clientes.

Ataques Comuns e Vulnerabilidades do WordPress

Voltar ao índice

Ataques Comuns ao WordPress:

1. **Ataques de Força Bruta (Brute Force):** Tentativas automatizadas de adivinhar senhas de login por meio de combinações de palavras ou senhas comuns. Esse tipo de ataque visa quebrar as credenciais de acesso administrativo.

2. **Cross-Site Scripting (XSS):** Envolve a injeção de scripts maliciosos em páginas da web, que são executados nos navegadores dos usuários. Esses scripts podem roubar dados, manipular sessões ou redirecionar os usuários para sites maliciosos.

3. **Injeção de SQL (SQL Injection - SQLi):** Os invasores inserem comandos SQL maliciosos nos campos de entrada do site para acessar, alterar ou excluir dados no banco de dados, comprometendo a integridade das informações armazenadas.

4. **Ataques DDoS (Distributed Denial of Service):** Consistem no envio massivo de tráfego malicioso para sobrecarregar o servidor, tornando o site inacessível para usuários legítimos.

5. **Phishing:** Técnica em que os invasores disfarçam-se como fontes confiáveis para enganar os usuários e induzi-los a fornecer informações confidenciais, como senhas ou dados financeiros.

6. **Malware e Injeção de Backdoors:** Os invasores inserem malware ou backdoors em temas e plugins vulneráveis, permitindo acesso contínuo e não autorizado ao site, mesmo após correções de segurança.

7. **Ataques de Upload de Arquivos Maliciosos:** Invasores utilizam formulários de upload para enviar arquivos infectados que, se executados no servidor, podem comprometer a segurança do site.

8. **Cross-Site Request Forgery (CSRF):** Força usuários autenticados a executar ações indesejadas no site, como a alteração de senhas ou o envio de formulários, sem o seu consentimento.

Vulnerabilidades do WordPress:

1. **Versões Desatualizadas:** A falta de atualizações deixa o site vulnerável a ataques baseados em falhas conhecidas. O ManageWP facilita a atualização em massa de diversas instalações do WordPress, garantindo que o core, plugins e temas estejam sempre na versão mais recente, reduzindo riscos.

2. **Backdoors:** Códigos maliciosos inseridos em temas, plugins ou arquivos principais permitem acesso não autorizado ao site. O Solid Security realiza varreduras profundas e contínuas para detectar e eliminar backdoors, garantindo a integridade dos arquivos do site.

3. **Plugins e Temas Vulneráveis:** Plugins ou temas desatualizados ou mal codificados são alvos fáceis para invasores. O ManageWP gerencia atualizações automáticas de plugins e temas, enquanto o Solid Security monitora a segurança e identifica vulnerabilidades, oferecendo proteção em tempo real.

4. **Permissões Inadequadas de Arquivos:** Configurações incorretas de permissões de arquivos e pastas podem permitir modificações não autorizadas. O Cloudways gerencia permissões com firewalls avançados e controles de segurança, garantindo que arquivos sensíveis estejam devidamente protegidos.

5. **Cross-Site Scripting (XSS):** Scripts maliciosos injetados em páginas da web podem comprometer a segurança dos usuários. O Cloudflare utiliza seu Web Application Firewall (WAF) para bloquear requisições maliciosas e proteger o site contra ataques XSS.

6. **Injeção de SQL (SQLi):** Inserção de comandos SQL maliciosos em campos de entrada para obter acesso ao banco de dados. O WAF do Cloudflare bloqueia essas tentativas, protegendo a integridade e segurança dos dados armazenados no banco de dados do site.

7. **Falta de Autenticação Forte:** Senhas fracas ou a ausência de autenticação multifator tornam o site vulnerável a ataques de força bruta. O Solid Security oferece proteção com autenticação multifator (MFA) e contra ataques de força bruta, enquanto o Cloudflare aplica técnicas de rate limiting e firewalls para proteger páginas de login.

8. **Upload de Arquivos Não Seguros:** A permissão para upload de arquivos sem verificação adequada pode permitir a introdução de arquivos maliciosos no servidor. O Solid Security monitora e analisa os arquivos enviados, bloqueando conteúdos perigosos, enquanto o Cloudways restringe os tipos de arquivos permitidos para upload, oferecendo maior controle e segurança.

AGÊNCIA DIGITAL

Voltar ao índice

Conclusão e Escolha da Via Agência Digital

Ao escolher a Via Agência Digital, **você está garantindo mais do que um site; está investindo em uma parceria que coloca a segurança e o desempenho em primeiro lugar.** Com mais de duas décadas de experiência e uma abordagem focada na inovação, a Via oferece soluções de ponta para proteger seu site contra as ameaças mais sofisticadas do ambiente digital.

Cada detalhe do desenvolvimento é cuidadosamente planejado para garantir não apenas a segurança contínua, mas também uma performance impecável. O resultado é um site visualmente impactante, funcional e, acima de tudo, seguro — proporcionando tranquilidade para que você possa se concentrar no crescimento do seu negócio.

Com a Via Agência Digital, sua empresa estará protegida por uma equipe comprometida com a excelência, garantindo que seu ambiente online seja confiável, eficiente e preparado para o futuro. Escolher a Via é optar por uma solução completa, que combina segurança robusta, tecnologia avançada e um atendimento dedicado às suas necessidades.