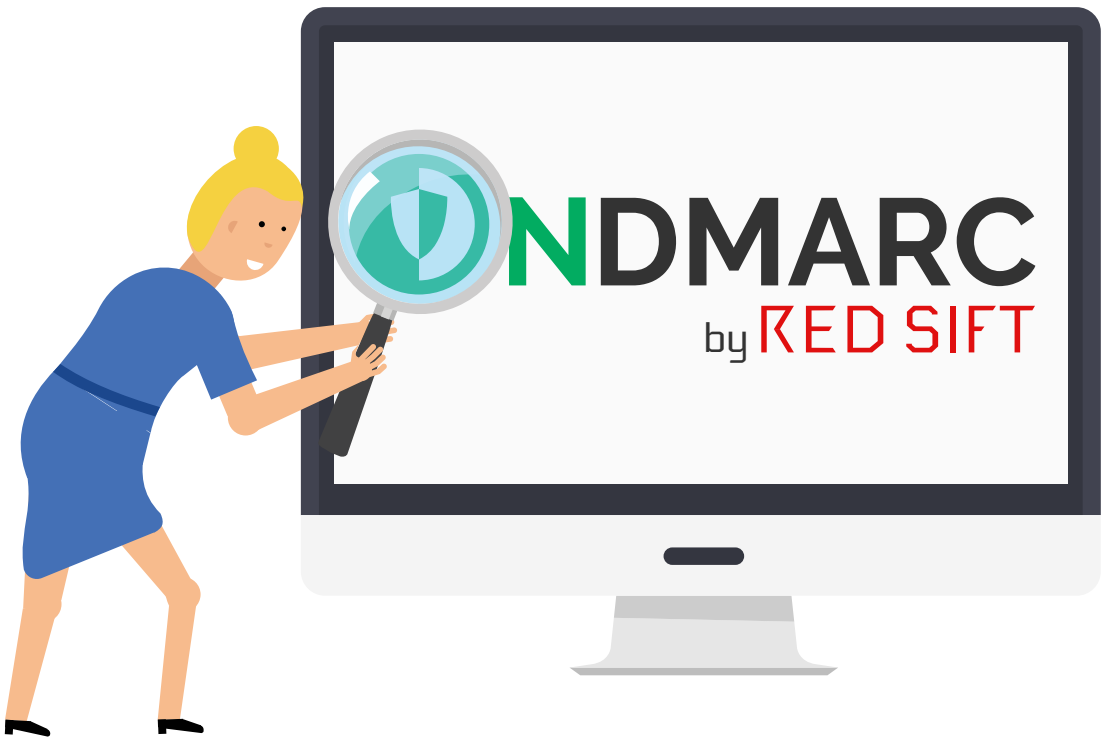
Achando seu provedor DMARC ideal

Aqui está tudo que você precisa saber sobre os aspectos chave e facilidades de um provedor DMARC.



Conteúdo

Perdeu a parte um "**DMARC: O que é e por que deveria ser a sua próxima prioridade?**" desta série? Não se preocupe, você pode encontrar *aqui* e obter a informação básica sobre o DMARC.

Parece um bom negócio obter uma cobertura básica à um preço baixo, porém isso não te trará benefício nenhum se seu fornecedor não prover bons relatórios e não te direcionar em como corrigir os problemas que eles identificarem. Aqui estão algumas informações referentes as inovações únicas, planejamento do design e algumas informações extras que te ajudarão na sua jornada com o DMARC.

1. Verificando um provedor

- **Quais são as credenciais de segurança do provedor?** É importante verificar se o provedor do DMARC tem as credenciais apropriadas de segurança. Verifique se eles são certificados na ISO27001 ou se tem Cyber Essentials.

- **Eles estão usando a política de configuração p=reject dentro da própria empresa?** Para confiar que um provedor pode implementar o DMARC efetivamente dentro de sua organização, você deve verificar se eles foram capazes de implementar o DMARC corretamente dentro da sua própria organização. Você pode verificar isso facilmente com ferramentas online gratuitas.

- **O que os atuais clientes pensam?** Se possível, tente falar com um dos atuais clientes saber mais informações sobre os produtos e serviços do provedor.

- **Que projetos estão por vir?** Você pode estar comprando um produto pelo que ele oferece hoje, mas considere também que outras inovações estão sendo desenvolvidas que deva ser de seu interesse no futuro.

- **Como é o suporte de serviço deles?** Sem o conhecimento interno de TI do provedor, DMARC pode parecer complexo de implementar em pequenas organizações ou de implantar em grandes e complexas organizações. O serviço de suporte do provedor deve então ser uma parte integral para agilizar efetivamente a implementação do DMARC. A equipe de suporte será também útil em implementações vigentes e em ajustes de configurações DMARC existentes.

2. Verificação do produto

O que você deve buscar na sua solução DMARC

O básico

- **Relatório e painéis de visualização:** Você deve ser capaz de visualizar todas as validações de e-mail que ocorrem em seu domínio. As melhores ferramentas irão simplificar os relatórios complexos XML do DMARC para que você possa rapidamente ter uma visão geral de conformidade do DMARC nos seus e-mails. Painéis de visualização simples irão te possibilitar facilmente identificar qualquer configuração inapropriada, além de visualizar a escala e frequência de ataques de personificação (*spoofing*). Para aqueles buscando conhecer a fundo seus ataques *phishing*, relatórios forenses proveem mais detalhes de como o domínio da organização está sendo explorado.

- **Configuração:** Uma vez que você tenha usado o DMARC para entender a segurança de seu domínio, Você pode implementar uma solução que irá te possibilitar configurar suas políticas de SPF e DKIM para garantir que a identidade de sua organização só possa ser usada por usuários legítimos. Uma estrutura clara de soluções é importante para organizações que não possuem um especialista em DMARC e/ou possuem recursos limitados. A solução deve te auxiliar a seguir confiantemente pelos vários estágios de implementação do DMARC até que a organização alcance a política p=reject.

- **Proteção contínua:** Conforme sua organização cresce e muda, você sem dúvida terá que atualizar sua configuração DMARC para garantir que seu domínio continue protegido e que a entrega de e-mails não seja afetada. Uma boa solução de DMARC irá te permitir facilmente atualizar e manter sua configuração SPF e DKIM, além de prover alertas quando algum deles parar de funcionar. Uma solução como ***OnDMARC*** irá ressaltar qualquer mudança que precise de sua atenção e prover instruções claras de como resolver rapidamente.

3. Informações extras

Pesquise essas informações extras de alguns provedores

- **SPF Dinâmico:** O protocolo SPF é limitado a 10 DNS lookups. Isso é constantemente um problema para organizações com uma infraestrutura complexa de e-mails ou para aquele que usam diversos serviços Cloud pois eles facilmente atingirão esse limite. Quando esse limite é atingido, e-mails legítimos podem falhar a autenticação SPF. A funcionalidade de SPF Dinâmico, que está disponível no ***OnDMARC***, supera esse problema permitindo que uma organização use somente 1 SPF lookup para conectar-se ao sistema OnDMARC, de onde ele terá lookups ilimitados.

- **Acesso à API:** A possibilidade de integrar os dados do DMARC em um único Painel de Visualização da sua solução de segurança atual é uma forma útil de ter as informações de segurança do seu e-mail em um só lugar para análise.

- **Single-Sign-On (SSO):** Alguns provedores, incluindo o ***OnDMARC***, possibilitam uma organização integrar o DMARC com outros sistemas de TI fundamentais, como o Okta, para que se possa ter acesso com um único login às configurações de segurança da organização.

- **ChatBot:** O ChatBot pode ser de grande valor quando uma organização o utiliza para receber e tomar decisões em alertas do DMARC diretamente no Slack. Isso significa que você não precisa verificar o a aplicação DMARC regularmente.

- **Verificação DMARC:** Geralmente quando você faz uma mudança no DNS, você tem que esperar pelo primeiro relatório agregado chegar para poder verificar o impacto das mudanças. Isso pode levar até 24 horas. Com o ***OnDMARC***, a ferramenta de inspeção '*Investigate*' te possibilita verificar imediatamente os resultados das mudanças feitas na configuração de 5 sinais essenciais: DMARC, SPF, DKIM, FCrDNS e TLS descritos em um Painel de visualização.

- **Forense:** Relatórios forenses para e-mails que falharam na validação DMARC proveem informações uteis e compreensivas sobre cada e-mail individual. Verifique se o provedor é capaz de fazer isso depois que eles editarem o corpo do e-mail.

- **Perfil de seguranca do e-mail:** Ser capaz de comparar a configuração do seu e-mail com um padrão de indústria é uma grande forma de garantir que você atende as necessidades de qualquer regulamentação vigente. Provedores como o ***OnDMARC*** te possibilitam comparar sua conformidade com os requerimentos de diferentes perfis como os do Reino Unido (*Minimum Security Standards*) e o dos EUA (*Binding Operational Directive 18:01*).

4. Garantindo sucesso com o DMARC

- **Implementação:** Um pacote de implementação pode ajudar a colocar a proteção DMARC em efeito mais rapidamente, diminuindo a chance de ataques de personificação. O serviço incluído deve te possibilitar identificar fontes validas de e-mails dentro de sua organização, configure-as corretamente então coloca o DMARC em modo *quarantine* ou *reject*.

- **Serviços Gerenciáveis:** O benefício em ter o serviço gerenciado por uma pessoa é que você assegura acesso a uma equipe de especialistas que estão disponíveis todo o tempo. Esses especialistas podem te notificar de algum alerta de incidente e sugerir resoluções, liberando sua equipe para focar em outras atividades.

- **Suporte:** Suporte técnico é uma boa maneira de tratar problemas específicos ou obter ajuda utilizando a ferramenta DMARC. Algumas soluções, como o ***OnDMARC*** incorporam a função chat dentro do portal DMARC, para que somente com um clique de um botão você possa se conectar a um agente pronto para te ajudar a resolver sua dúvida.

- Além disso, verifique se seu provedor possui uma base de conhecimentos, incluindo respostas para perguntas mais frequentes e dicas úteis que irão te ajudar a otimizar sua implementação do DMARC e gerenciamento como um todo.

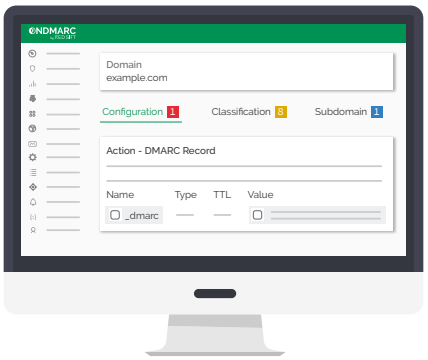
5. Qual o próximo passo?

Nós esperamos que você esteja confiante agora sobre o que esperar de um provedor DMARC confiável. Se você tiver algum dúvida, simplesmente entre em contato com alguém de nossa equipe no e-mail contato@managerone.com.br - nós teremos prazer em ajudá-lo!

Agora que você leu a Parte 2, não deixe de ver a Parte 3 dessa série útil sobre o DMARC chamada Fazendo o DMARC Funcionar na Sua Organização para um melhor entendimento de como o DMARC pode funcionar dentro de sua organização.

Quer ver o DMARC em ação?

Um provedor DMARC fácil de usar, como o ***OnDMARC***, irá te ajudar a alcançar o modo de proteção total mais rapidamente. Dê uma olhada e veja o quão simples é navegar e ter uma visão panorâmica do seu e-mail e dê o primeiro passo para assegurar o seu domínio contra personificação recebendo um diagnóstico grátis em: https://www.managerone.com.br/avaliacao.



Cuidem-se,

Equipe OnDMARC

Referências

1. http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf
2. https://techcrunch.com/2018/11/01/half-fortune-500-dmarc-email-security/
3. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
4. http://www.newsweek.com/origins-nigerias-notorious-419-scams-456701
5. https://enterprise.verizon.com/resources/reports/dbir/
6. https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda
7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf
8. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Inicie sua conversa sobre o DMARC hoje!

www.ondmarc.com.br

ONDMARC

O Red Sift Open Cloud é uma plataforma de análise de dados desenvolvida especificamente para os desafios da segurança cibernética. Ao aproveitar o poder da IA, podemos coletar, computar e visualizar dados de milhares de sinais individuais com segurança para ajudar as organizações a otimizar sua segurança cibernética. Nosso primeiro produto na plataforma Red Sift é o OnDMARC, um produto SaaS que ajuda a implementar e manter o DMARC. Este protocolo de autenticação de e-mail bloqueia efetivamente ataques de phishing e aumenta a capacidade de entrega de e-mails genuínos.

www.ondmarc.com.br
contato@managerone.com.br