SYNOPTIQ
INFOSOLUTIONS

The only place for all “DMARC FAQs”

Alliance Showcase:

PROGIST®

www.synoptiq.biz

WHAT IS DMARC, AND WHY IS IT IMPORTANT?

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance.

It is an email authentication protocol that helps protect email domains from unauthorized use and prevents email-based attacks such as spoofing and phishing.

DMARC is important for organizations because it enhances email security, reduces the risk of email-based fraud, protects brand reputation, and improves email deliverability by reducing the chances of legitimate emails being marked as spam or rejected.

It provides domain owners with greater control and visibility over their email ecosystem, enabling them to take proactive measures against unauthorized email use.

HOW DOES DMARC HELP IN PREVENTING EMAIL SPOOFING AND PHISHING ATTACKS?

DMARC helps prevent email spoofing and phishing attacks by allowing domain owners to set policies that define how receiving mail servers should handle unauthenticated emails claiming to be from their domain.

It enables email authentication through the alignment of DKIM and SPF records, providing a mechanism to verify the integrity of the email sender.

DMARC also provides detailed reports on email authentication results, allowing domain owners to identify and act against malicious emails, thereby reducing the risk of spoofing and phishing attacks.

WHAT ARE THE KEY COMPONENTS OF A DMARC RECORD?

The key components of a DMARC record are:

Policy (p): Specifies the policy to be applied for handling emails that fail DMARC authentication.

Domain (d): Specifies the domain to which the DMARC record applies.

Alignment (alignment): Determines how the emails "From" header domain and DKIM or SPF domain align with each other.

Reporting (rua and ruf): Specifies the email addresses where DMARC reports should be sent.

HOW DO I IMPLEMENT DMARC FOR MY ORGANIZATION'S DOMAIN?

Publish SPF and DKIM records: Ensure that your domain has properly configured SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) records to authenticate outgoing emails.

Create a DMARC record: Create a DNS TXT record for your domain, specifying the DMARC policy, domain, alignment, and reporting addresses (rua and ruf).

Set the DMARC policy: Determine the policy you want to enforce for emails that fail DMARC authentication (none, quarantine, or reject) and specify it in your DMARC record.

Monitor and analyse reports: Monitor the DMARC reports sent to the specified reporting addresses to analyse the authentication status of your emails and identify any unauthorized senders or issues.

Gradually enforce the policy: Start with a "none" policy to monitor the results and gradually enforce stricter policies (quarantine or reject) once you have addressed any legitimate email delivery issues.

Monitor and adjust: Continuously monitor and analyse the DMARC reports, adjust SPF and DKIM records as needed, and fine-tune your DMARC policy to improve email authentication and reduce spoofing or phishing attacks.

CAN DMARC BE IMPLEMENTED FOR SUBDOMAINS AS WELL?

Yes, DMARC can be implemented for subdomains in addition to the main domain.

DMARC provides the flexibility to specify different policies for subdomains, allowing organizations to enforce email authentication and policy enforcement across their entire email ecosystem.

WHAT IS THE IMPACT OF IMPLEMENTING DMARC ON LEGITIMATE EMAIL DELIVERY?

Implementing DMARC can have an impact on legitimate email delivery, especially during the initial stages of enforcement. It is possible that some legitimate emails may be flagged as suspicious or rejected if they fail DMARC authentication.

This can occur if proper SPF and DKIM records are not in place or if email senders have not been aligned with the DMARC policy.

However, with careful implementation and monitoring, the impact on legitimate email delivery can be minimized. By gradually enforcing DMARC policies, organizations can identify and address any delivery issues, update SPF and DKIM records, and ensure proper alignment of authorized senders.

This iterative process allows organizations to strike a balance between improving email authentication and minimizing any negative impact on legitimate email delivery.

HOW DOES DMARC WORK IN CONJUNCTION WITH SPF (SENDER POLICY FRAMEWORK) AND DKIM (DOMAINKEYS IDENTIFIED MAIL)?

DMARC works in conjunction with SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide email authentication and enhance security.

SPF validates the sender's IP address by checking if it is listed as an authorized sender in the DNS records. It helps prevent domain spoofing by verifying that the sending server is authorized to send emails on behalf of the domain.

DKIM adds a digital signature to the email header, ensuring message integrity and confirming that the email content has not been tampered with during transit.

The signature is verified using the public key published in the DNS records. DMARC complements SPF and DKIM by specifying how receiving mail servers should handle emails that fail authentication.

DMARC allows domain owners to set policies and alignment requirements to determine if the "From" domain aligns with SPF or DKIM, and what actions should be taken for failed authentication, such as marking the email as spam, quarantining it, or rejecting it outright.

CAN DMARC PROVIDE INSIGHT INTO WHO IS SENDING EMAILS ON BEHALF OF MY DOMAIN?

Yes, DMARC can provide insight into who is sending emails on behalf of your domain.

By analysing the DMARC reports, you can identify the IP addresses and domains of the senders that are attempting to send emails using your domain.

These reports can help you identify unauthorized senders, detect email spoofing attempts, and take appropriate actions to secure your domain's reputation and prevent abuse.

HOW CAN I MONITOR DMARC AUTHENTICATION AND POLICY RESULTS?

Enable DMARC reporting: In your DMARC record, specify the email addresses (rua) where DMARC reports should be sent. These reports provide information about the authentication status of your emails and any policy actions taken.

Receive and parse DMARC reports: Set up a process to receive and parse the DMARC reports sent to the specified email addresses. There are various tools and services available that can help you automate this process and extract meaningful insights from the reports.

Analyse the reports: Review the DMARC reports to understand the authentication status of your emails, including the percentage of authenticated, unauthenticated, and failed emails. Pay attention to any patterns, such as sources or domains that frequently fail authentication.

Take appropriate actions: Based on the analysis of the reports, take appropriate actions to address any issues.

This may involve updating SPF or DKIM records, aligning senders, or adjusting the DMARC policy.

Iterate and improve: Continuously monitor and analyse the DMARC reports, adjust your authentication setup and policy, and track the progress of email authentication over time. This iterative process will help you improve email deliverability and strengthen the security of your domain.

WHAT ARE THE COMMON CHALLENGES OR ISSUES ENCOUNTERED DURING DMARC IMPLEMENTATION?

During DMARC implementation, some common challenges or issues that organizations may encounter include misconfigured SPF or DKIM records: improper SPF or DKIM records can lead to authentication failures, causing legitimate emails to be flagged as suspicious or rejected.

Lack of email authentication alignment: Ensuring alignment between the "From" domain, SPF, and DKIM is crucial for successful DMARC implementation. If alignment is not properly set up, legitimate emails may fail authentication.

False positives: Initially, DMARC enforcement can result in legitimate emails being mistakenly marked as suspicious or rejected. This can happen if there are authorized senders or email service providers that have not been aligned with the DMARC policy.

Email forwarding issues: When emails are forwarded or relayed through different servers, SPF alignment can break, leading to authentication failures. Organizations need to consider this challenge and properly configure their SPF records.

Lack of awareness or understanding: DMARC implementation requires knowledge and understanding of email authentication protocols. Lack of awareness or expertise in this area can lead to incorrect configuration or challenges in troubleshooting authentication issues.

ARE THERE ANY BEST PRACTICES FOR CONFIGURING DMARC POLICIES?

Yes! Here they are.

Start with a "none" policy: Begin with a "none" policy to monitor the authentication status of your emails without taking immediate action. This allows you to gather data and identify any legitimate email sources that may not be properly aligned with DMARC.

Gradually enforce stricter policies: Once you have identified and addressed any alignment or authentication issues, gradually move towards enforcing stricter policies such as "quarantine" or "reject" to improve email deliverability and mitigate spoofing or phishing attacks.

Specify alignment requirements: Set alignment requirements (either "relaxed" or "strict") to determine how the "From" domain aligns with SPF and DKIM. "Relaxed“ alignment provides flexibility, while "strict" alignment ensures a more precise match.

Monitor DMARC reports: Enable DMARC reporting and regularly analyse the reports to gain insights into the authentication status of your emails, identify sources of failed authentication, and make necessary adjustments.

Utilize subdomain policies: Consider implementing DMARC policies at the subdomain level to gain granular control over email authentication. This allows you to apply different policies for different subdomains based on their specific requirements.

Maintain SPF and DKIM records: Ensure that your SPF and DKIM records are properly maintained and updated to align with your DMARC policy.

Regularly review and update these records as needed.

Implement DMARC record testing: Before deploying a DMARC policy in enforcement mode, conduct thorough testing and monitoring in a controlled environment to identify any potential issues and ensure compatibility with your email infrastructure.

HOW DOES DMARC HANDLE THIRD-PARTY EMAIL SERVICES OR VENDORS THAT SEND EMAILS ON BEHALF OF OUR DOMAIN?

DMARC can handle third-party email services or vendors that send emails on behalf of your domain through the concept of alignment. By properly configuring SPF and DKIM for these third-party services, you can align their sending domains with your DMARC policy.

This alignment ensures that their emails pass DMARC authentication, allowing them to be delivered without issues. It's important to work with your third-party email providers to ensure they have implemented proper SPF and DKIM authentication for your domain to maintain alignment and maintain a consistent DMARC policy for your domain.

CAN DMARC HELP IMPROVE EMAIL DELIVERABILITY AND REDUCE FALSE POSITIVES IN SPAM FILTERS?

Yes, DMARC can help improve email deliverability and reduce false positives in spam filters.

By implementing DMARC and aligning SPF and DKIM records, you provide a stronger authentication framework for your domain’s emails.

This increased authentication helps receiving mail servers verify the legitimacy of your emails, reducing the chances of them being flagged as spam or false positives.

DMARC policies also allow you to specify how receiving servers should handle unauthenticated emails, minimizing the risk of legitimate emails being mistakenly classified as spam. By monitoring DMARC reports and making necessary adjustments, you can optimize email deliverability and reduce false positives in spam filters.

WHAT IS THE DIFFERENCE BETWEEN DMARC QUARANTINE AND REJECT POLICIES?

The difference between DMARC quarantine and reject policies lies in the actions taken by receiving mail servers when an email fails DMARC authentication.

Quarantine: With a quarantine policy, the receiving mail server will typically treat the email as suspicious and place it in the recipient's spam or quarantine folder. The email is still delivered but flagged as potentially problematical.

Reject: A reject policy instructs the receiving mail server to outright reject the email and not deliver it to the recipient’s inbox. The email is discarded, and the sender receives a bounce message indicating that the email failed DMARC authentication.

In summary, a quarantine policy allows the email to be delivered but marked as potentially suspicious, while a reject policy outright refuses delivery of the email. The choice between quarantine and reject depends on the organization's risk tolerance and desired level of email security.

IS IT RECOMMENDED TO IMPLEMENT DMARC FOR ALL DOMAINS IN AN ORGANIZATION?

Yes, it is HIGHLY recommended to implement DMARC for all domains in an organization.

DMARC provides email authentication and helps protect against email spoofing and phishing attacks. By implementing DMARC across all domains, you ensure consistent security measures and enhance the overall email deliverability and trustworthiness of your organization's email communications.

It helps protect not only your organization's reputation but also the recipients from potentially malicious emails.

PROGIST	Security Scorecard	SentinelOne
BUGSBOUNTY.COM	SECURAZE	HYCU
DELL	NUTANIX	Certus Software
ENDPOINT PROTECTOR by CoSoSys	SOPHOS	Microsoft
	Hewlett Packard Enterprise	KnowBe4 Human error. Conquered.
Checkmarx	Bitdefender	COMMVAULT

SYNOPTIQ
INFOSOLUTIONS

Synoptiq Infosolutions

Regd. Office
C303, Balaji Enclave, Akurli Road, Lokhandwala,
Kandivali (East). Mumbai – 400101

Sales Office
#162-164, V Mall, Asha Nagar, Thakur Complex,
Kandivali (East). Mumbai – 400101

contact@synoptiq.biz
www.synoptiq.biz