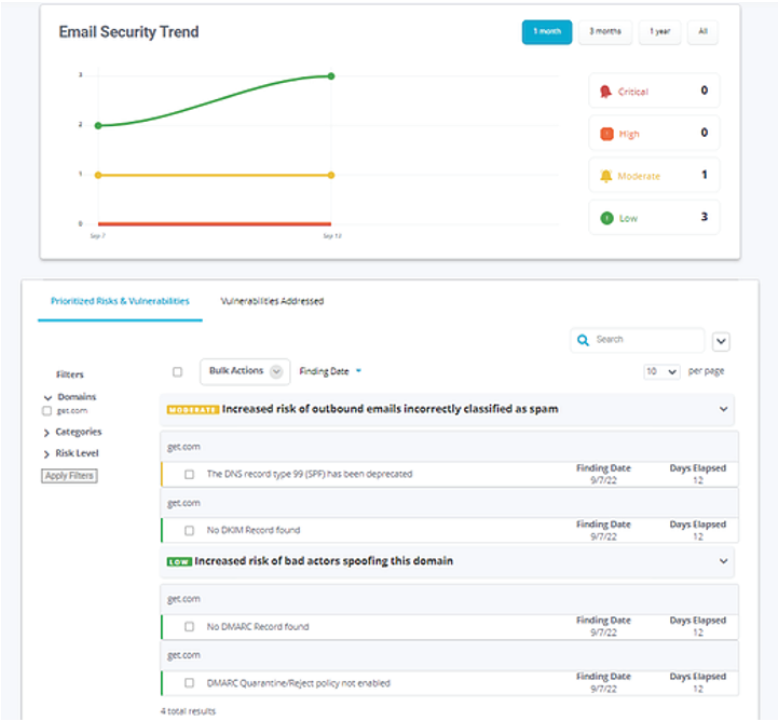
Email Security Monitoring for Enterprise and Third Parties

Email is a favorite vector for threat actors to carry out their phishing and spoofing attacks.

FortifyData can now help you monitor your email security posture related to your DNS TXT records to include assessments for SPF, DKIM and DMARC issues. The results are included in your dashboards and reflect your prioritized risks and score. Let's explore what these are and why they are important to strengthen email security.



SPF – Sender Policy Framework

SPF publishes a DNS record of which servers are allowed to send email from specific domains. As part of scheduled assessments, FortifyData checks the SPF records to ensure the appropriate SPF TXT record exists. Lack of SPF lowers the trustworthiness of emails sent from your domains since this SPF validation check can't be performed against an authenticated originating server.

DKIM - DomainKeys Identified Mail

DKIM provides an encrypted signature on email messages that can be validated via remote server against a DNS TXT record. Encryption is difficult to forge and managed by the sending organization, so a recipient can have a higher sense of confidence that the sent email is authentic. FortifyData checks for encryption signatures in addition to the DNS TXT validation check. Choosing to implement DKIM improves the integrity of your email and decreases the likelihood of your emails being blacklisted.

DMARC – Domain-based Message Authentication, Reporting and Conformance Protocol

DMARC leverages SPF and DKIM to manage verification of sender domains. The DMARC protocol includes reporting that provides visibility into an organization's email policy, and the protocol further specifies actions to take when the underlying SPF and DKIM authentication mechanisms fail. FortifyData's assessments include a check on DMARC and the handling policy to identify inactive DMARC or misconfigurations. Organizations that combine all three have developed a high trust email environment that validates the working DNS TXT record. Using only SPF and DKIM authentication will require different process depending on where messages are sent, whereas incorporating DMARC includes instructions within the email itself for proper handling and standardization.

For Third-Party monitoring use cases, these same checks are applied to the known domains of the vendors that you onboard to the FortifyData platform. As with other services in the FortifyData platform, this information can be shared with specific third parties, assigned tasks, update likelihoods and dispute findings.