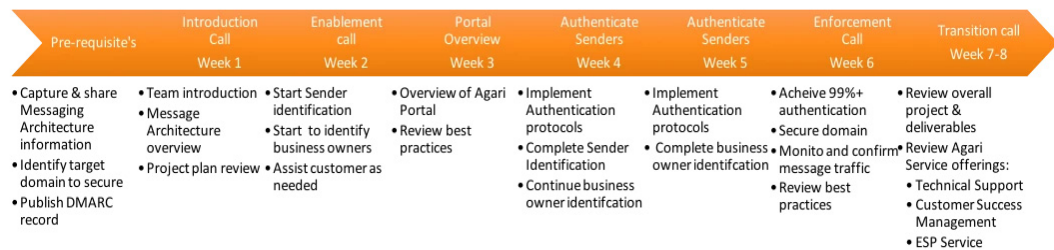# Cisco Domain Protection: Implementation Process

Published Date: June 22, 2018

Deploying Cisco is a straightforward, well-defined process. The process has been refined based on years of experience supporting large organizations with their email security initiatives. Two primary project elements include: 1) Cisco and 2) Organization's DNS.

These goals will be achieved:

- Deployment of DMARC records
- Authentication of message streams including Third-Party Senders
- One Domain secured with DMARC

	Introduction Call	Enablement call	Portal Overview	Authenticate Senders	Authenticate Senders	Enforcement Call	Transition call
Pre-requisite's	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7-8

- • Capture & share Messaging Architecture information
- • Identify target domain to secure
- • Publish DMARC record

- • Team introduction
- • Message Architecture overview
- • Project plan review

- • Start Sender identification
- • Start to identify business owners
- • Assist customer as needed

- • Overview of Agari Portal
- • Review best practices

- • Implement Authentication protocols
- • Complete Sender Identification
- • Continue business owner identifcation

- • Implement Authentication protocols
- • Complete business owner identifcation

- • Acheive 99%+ authentication
- • Secure domain
- • Monito and confirm message traffic
- • Review best practices

- • Review overall project & deliverables
- • Review Agari Service offerings:
  - • Technical Support
  - • Customer Success Management
  - • ESP Service

Additional discrete steps are detailed.

Primary Project Tasks

The primary On boarding tasks consist of:

- Publish DMARC Monitor records for domains in scope. Enabling full visibility to the organization's outbound mail stream.
- Authenticate Senders Implementing DMARC authentication protocols.
- Achieve 99%+ Message Authentication Proving validity and trustworthiness of message streams to external email receivers.

- Secure domain with DMARC.
- Protecting customers and partners from email spoofing your domains.