AREA 1

ANTI-PHISHING EMAIL DEPLOYMENT OPTIONS

In just 10 minutes start catching the phish your defenses miss

Configuring the Area 1 Horizon anti-phishing service is as fast and easy as creating an email address. Deploying and testing new security services can be time-consuming and disruptive for busy IT teams. But not with Area 1 Security. We often quote very brief deployment time estimates for our new customers—as fast as a 5 to 10-minute setup.

The actual configuration is that quick. One email rule or a couple of routing rules are all it takes to speed messages to Area 1 for analysis. This easy deployment enables us to start rendering phishing verdicts in your email flow—inline, out-of-flow via Bcc, or by journaling. See below the simple deployment architecture options and high-level steps for each configuration flow.

The reason Area 1 can be up and running so quickly is that the product is a fully elastic cloud service. There is no hardware or software to install. So, just as easily as setting up a Gmail or Office 365 account, you can configure a routing, Bcc, or journaling rule. Take a few steps in your email admin portal, and you can instantly start catching the phish your current defenses miss.

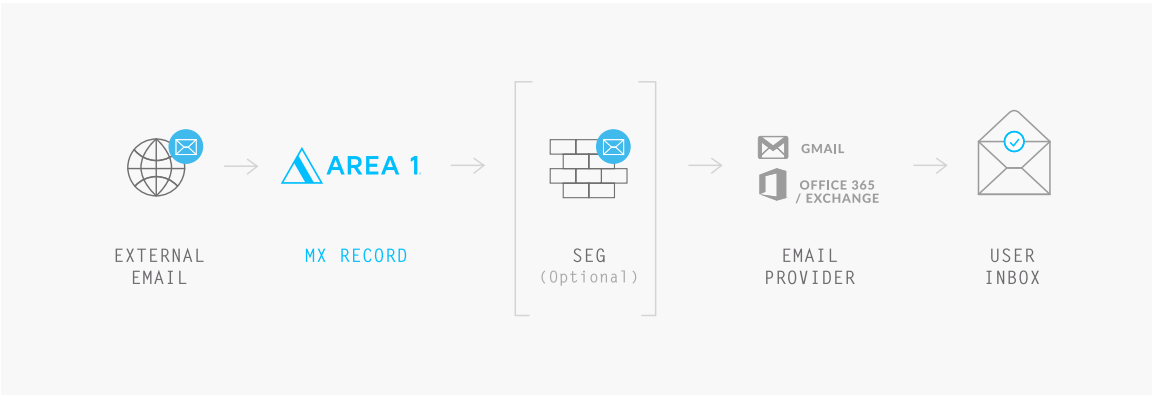
Which deployment configuration will work best for your organization? Area 1 is truly flexible and able to deploy at multiple points in your email flow without disruption. Plus, we have a team of email professionals and engineers with decades of experience, who can work with you to pick the best configuration and setup for your organization. Typically, that starts with a brief email overview and some configuration planning. It ends with full implementation—all in one, under-30-minute call!

EMAIL DEPLOYMENT OPTIONS

MX RECORD

Set-up Steps
- Configure Area 1 to forward mail to the next hop
- Point the email domain to Area 1

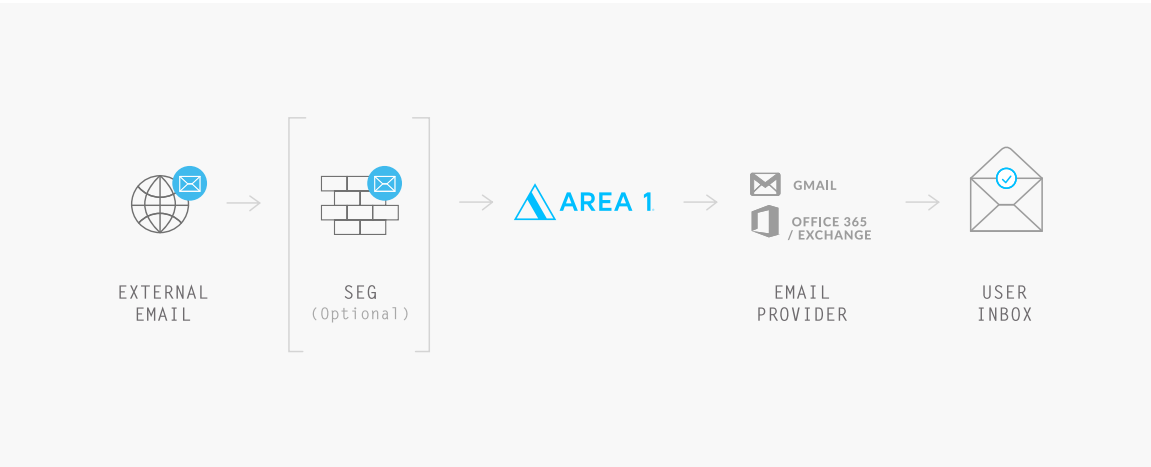
Environments
- Anyone



INLINE (POST SEG)

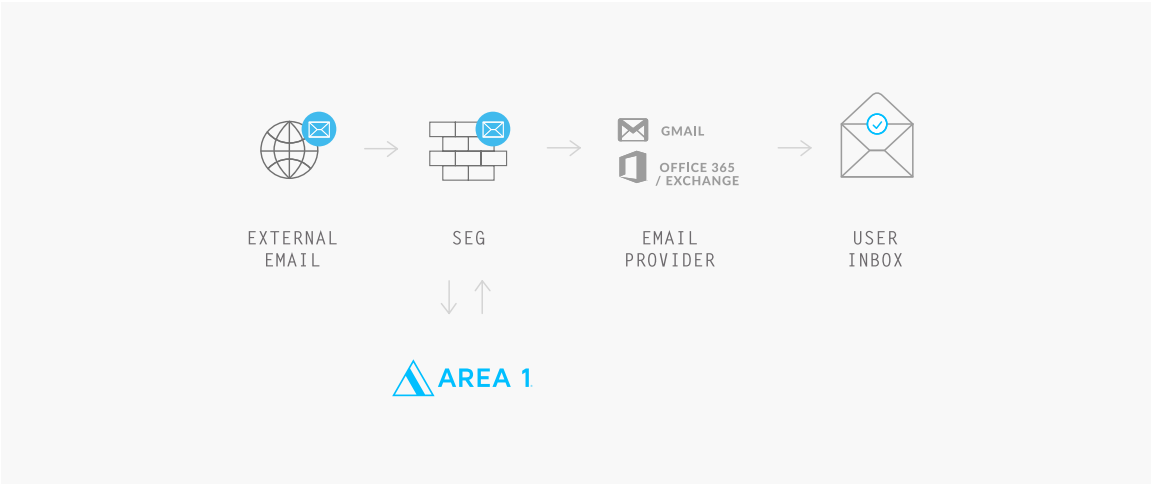
Set-up Steps
- Configure Area 1 to forward mail to the next hop
- Add a rule to SEG to direct mail to Area 1

Environments
- Mimecast
- Proofpoint
- Microsoft Exchange
- Gmail



SEG CONNECTOR

Environments
- Proofpoint
- Mimecast
- Symantec
- Cisco Ironport



EMAIL DEPLOYMENT OPTIONS

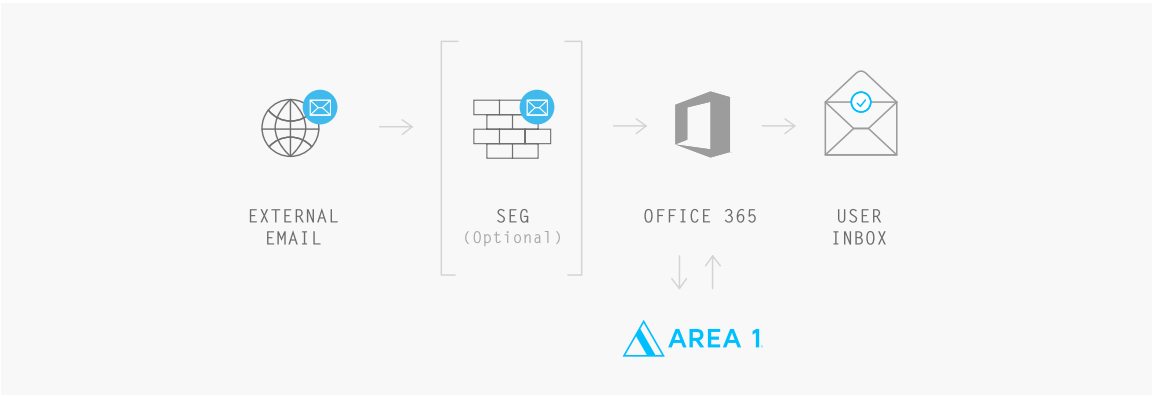
OFFICE 365

Set-up Steps

- Whitelist Area 1 IPs
- Configure where Area 1 should forward mail
- Add a rule to mail provider to direct mail to Area 1

Environments

- Office 365



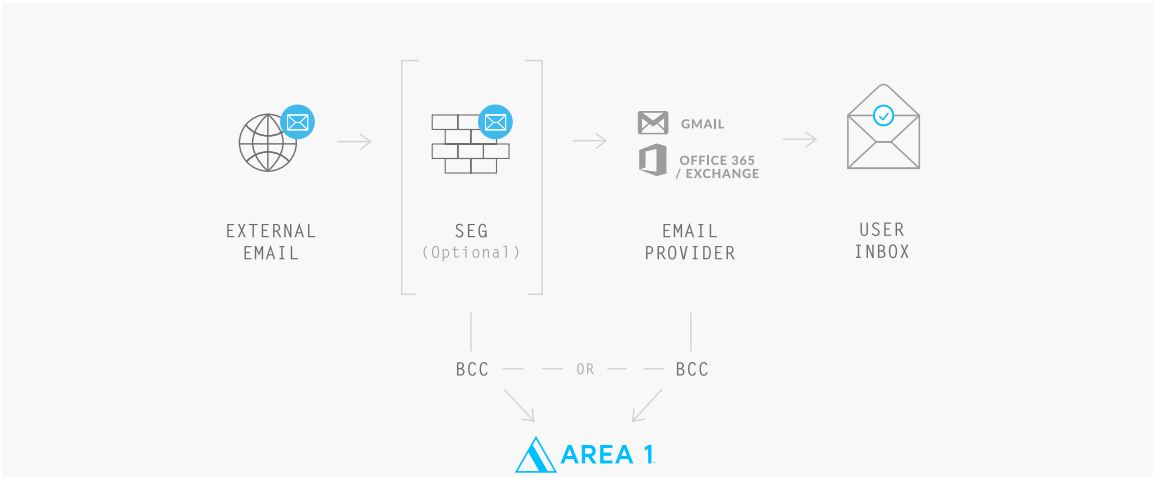
BCC

Set-up Steps

- Add a Bcc rule to forward messages Area 1

Note

- For Evaluation purposes only



JOURNALING

Set-up Steps

- Create a journaling rule and add Area 1 address configuration

Note

- For Evaluation or along with another