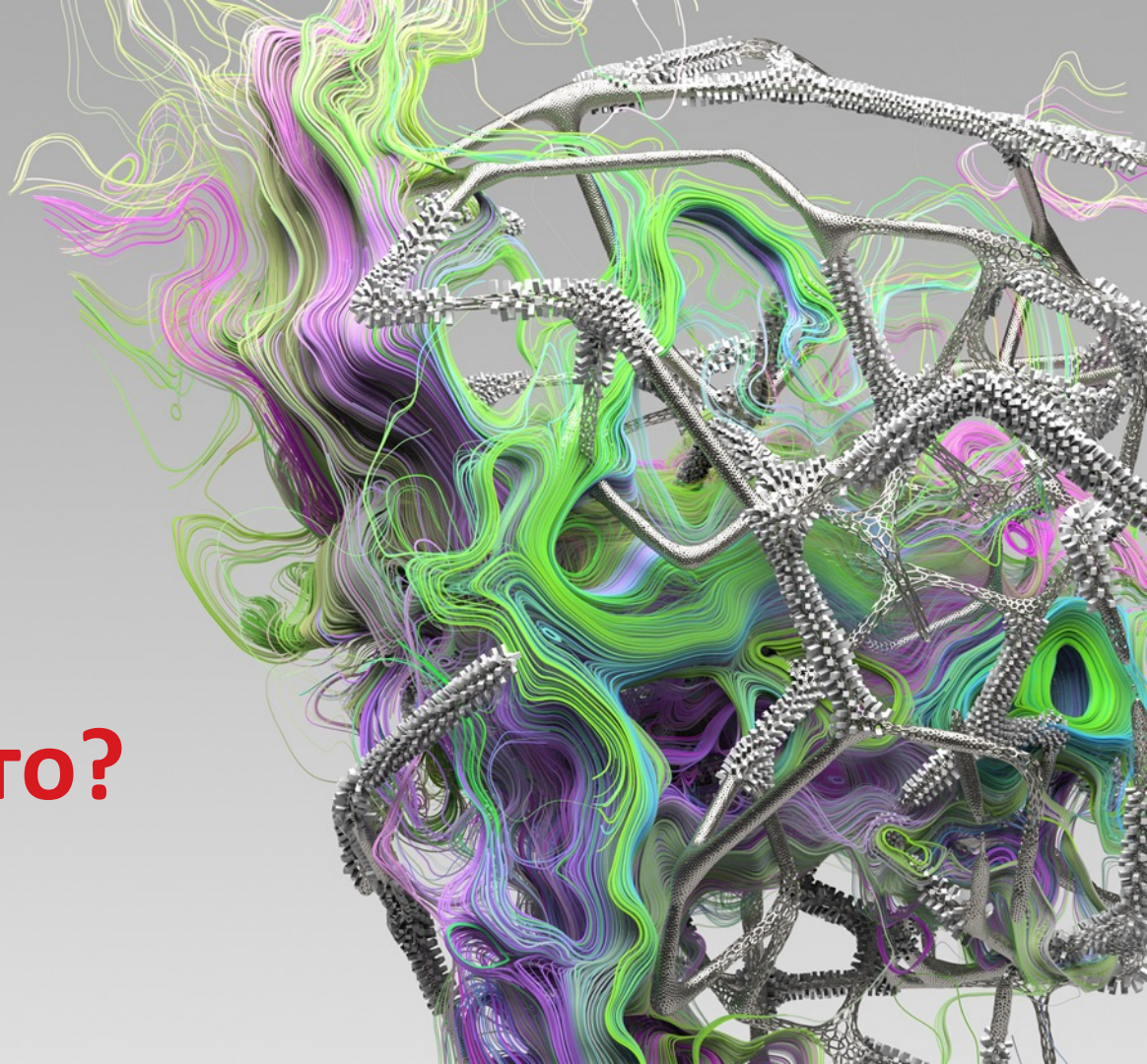
TREND MICRO™



DDEI:что нового?

Nurlan Adayev

Возможности DDEI

Predictive Machine Learning

Anti-spam/Graymail

CTD

Threat extraction

Custom Sandbox

Email Reputation Service integration

Content filtering

Password Analyzer

URL Time-of-Click

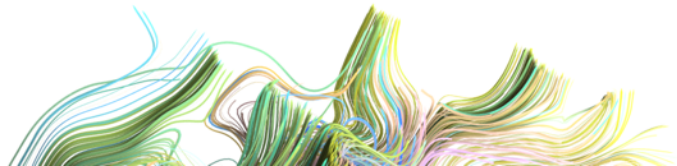
DLP

Business Email Compromise protection

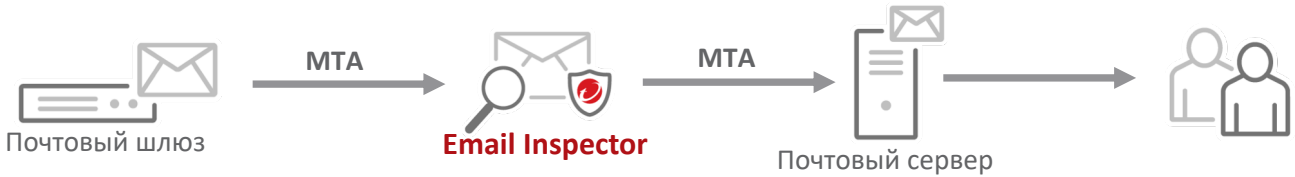
End-User Quarantine

Integration with other vendor’s Products/Services

Sender filtering/Authentication



Режимы работы

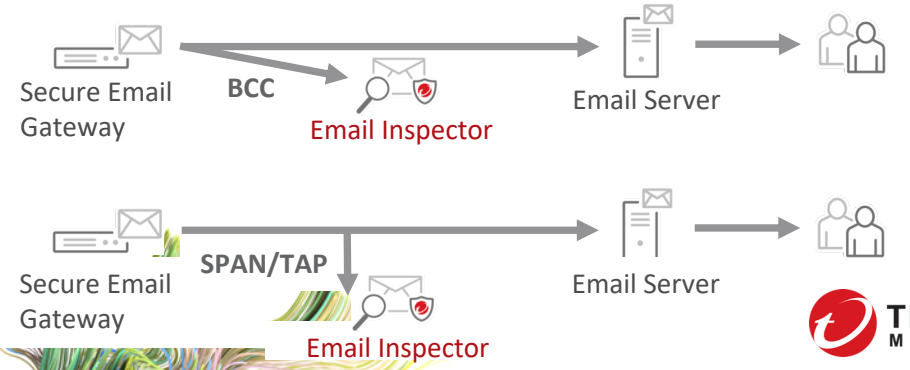


- Блокирует вредоносные письма
- Добавляет расширенную защиту, не влияя на существующие решения по защите электронной почты
- Конфигурация или архитектурные изменения не требуются
- Никаких изменений в политике электронной почты или поведении пользователя

Тестирование с нулевым влиянием:

BCC или SPAN/TAP режимы:

- Слушает почтовый трафик
- Обеспечивает анализ угроз и оповещения
- Только режим мониторинга



What’s new

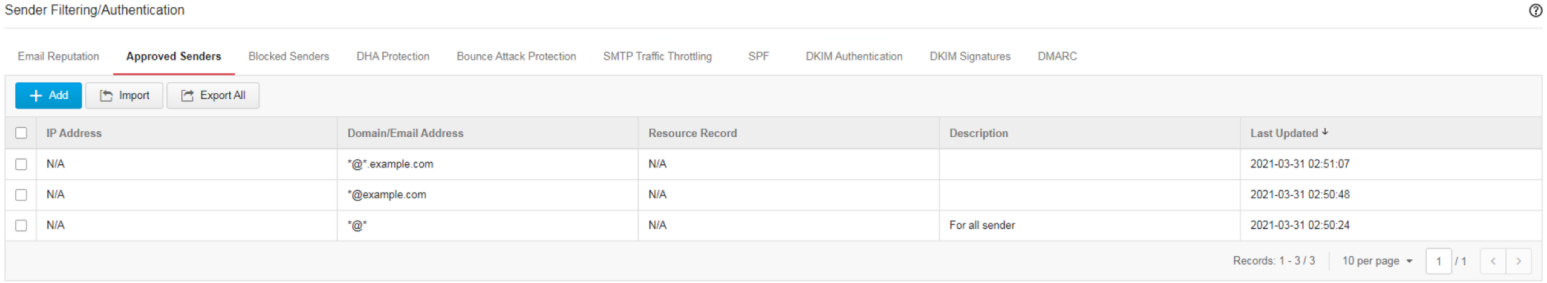
Support Gateway Module License only

- DDEI 5.1 support Gateway license only scenario, until now, DDEI can support 3 license model in total:
  - Advanced Threat Protection only. (existing)
  - Advanced Threat Protection + Gateway Module. (existing)
  - Gateway Module only (new in this release)

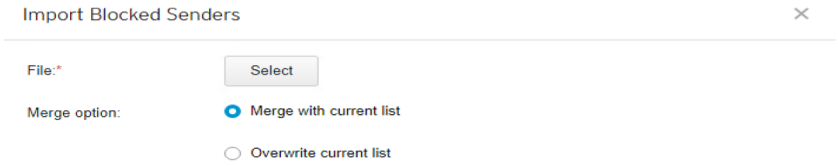
Feature	All-in-one	ATP license only	GW license only
Internal VA	Yes	Yes	No
Password Analyzer	Yes	Yes	No
YARA detection	Yes	Yes	No
Sender Filtering/Authentication	Yes	No	Yes
Content Filtering	Yes	No	Yes
Anti-spam/EUQ	Yes	No	Yes
DLP	Yes	No	Yes
Encryption	Yes	No	Yes
All Others	Yes	Yes	Yes

Detection Improvement

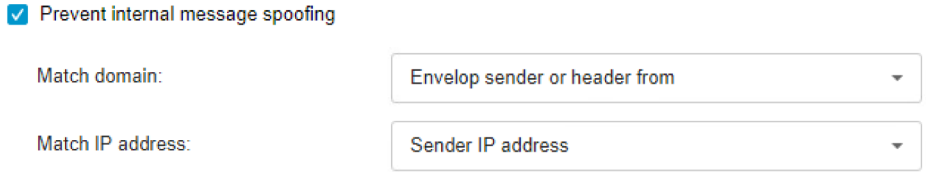
- Support wildcard for local part & subdomain part in approved/blocked sender.
  - such as, *@*, *@example.com, *@*.example.com.



- Support to import/export user-defined approved/blocked sender list



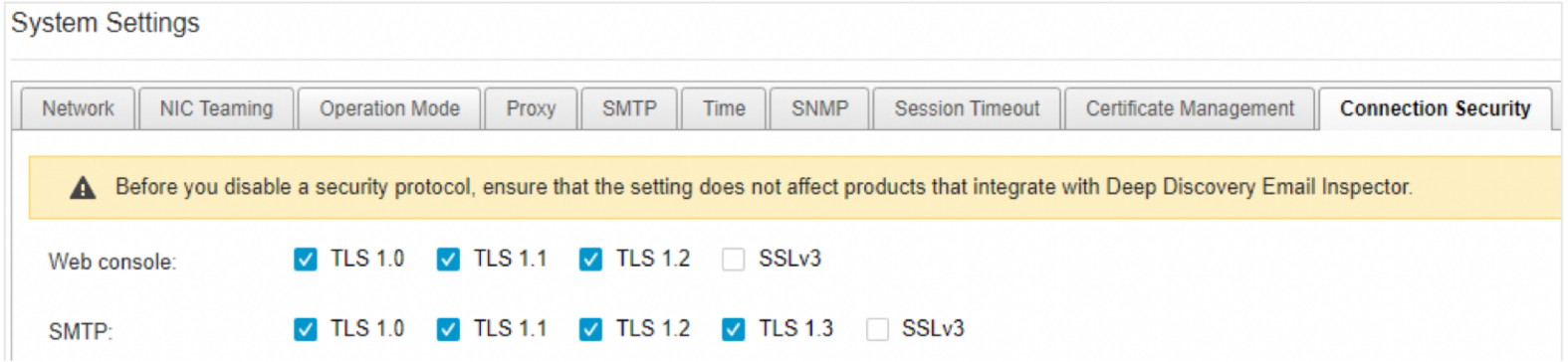
- Rely on new scan criteria in content filtering to prevent internal message spoofing



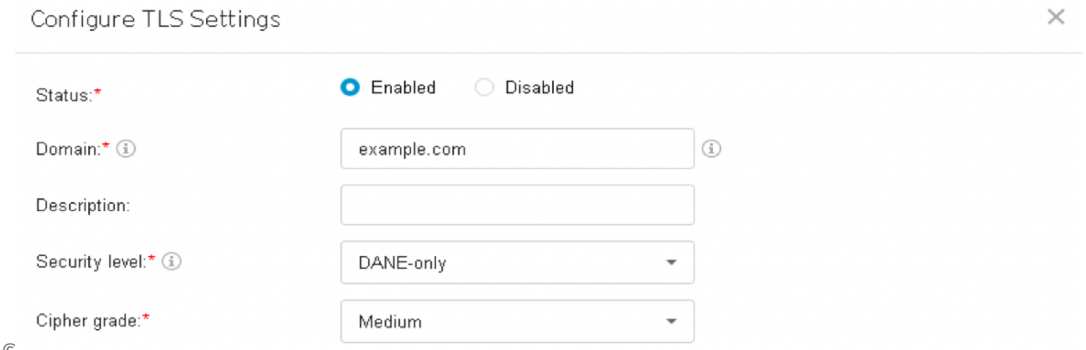
TREND MICRO

Provide more secure controls on mail traffic:

- Support TLS v1.3
  - Only SMTP/mail traffic can support TLS up to v1.3, the web console still only supports up to v1.2.



- DANE/DNSSEC apply to outbound messages



Difference between DANE-only and DANE:

Security level:* Opportunistic

Cipher grade:*

Examples:

Never: Deep Discovery Email Inspector does not use TLS for the specified domain.

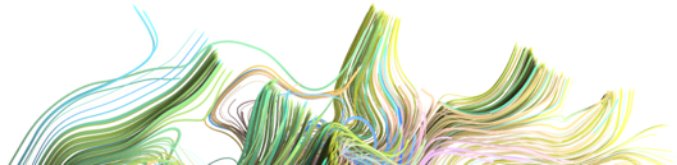
Opportunistic: Deep Discovery Email Inspector declares support for TLS for the specified domain. The mail server can choose whether to start a TLS connection.

Must: Deep Discovery Email Inspector requires TLS for communication for the specified domain. Communication between Deep Discovery Email Inspector and the mail server is encrypted.

Verify: Deep Discovery Email Inspector starts a TLS connection with the mail server for the specified domain. Deep Discovery Email Inspector gets the certificate from the mail server for server identification.

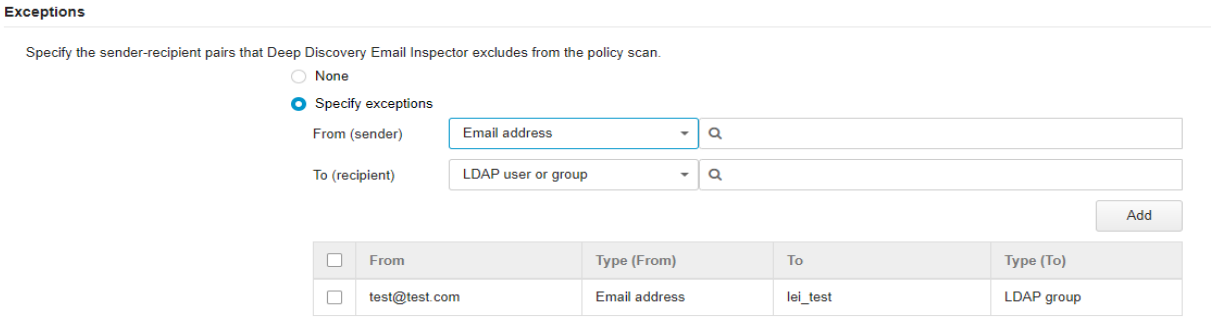
DANE: DDEI uses DANE for email message verification. If DANE verification is unsuccessful, DDEI performs one of the following based on the error condition: revert to using opportunistic TLS for secured connections, add the message to the deferred queue, or reject the message.

DANE-only: DDEI uses DANE for email message verification. If DANE verification is unsuccessful, DDEI adds the message to the deferred queue or rejects the message, depending on the error condition.

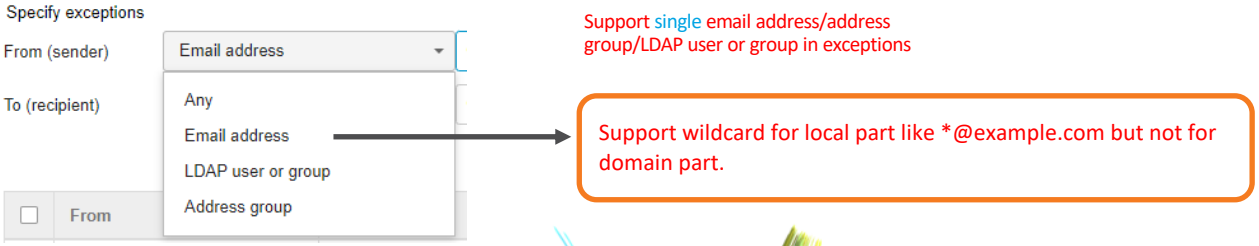


Policy enhancement: sender & recipient pair exception

- Support policy-based sender & recipient pair exception

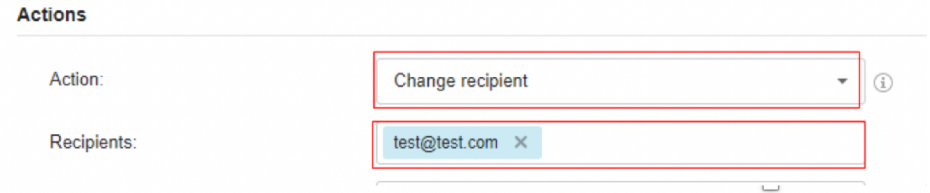


Under **Exceptions**, you can configure Deep Discovery Email Inspector to bypass policy scanning for messages with the specified sender-recipient address pair.

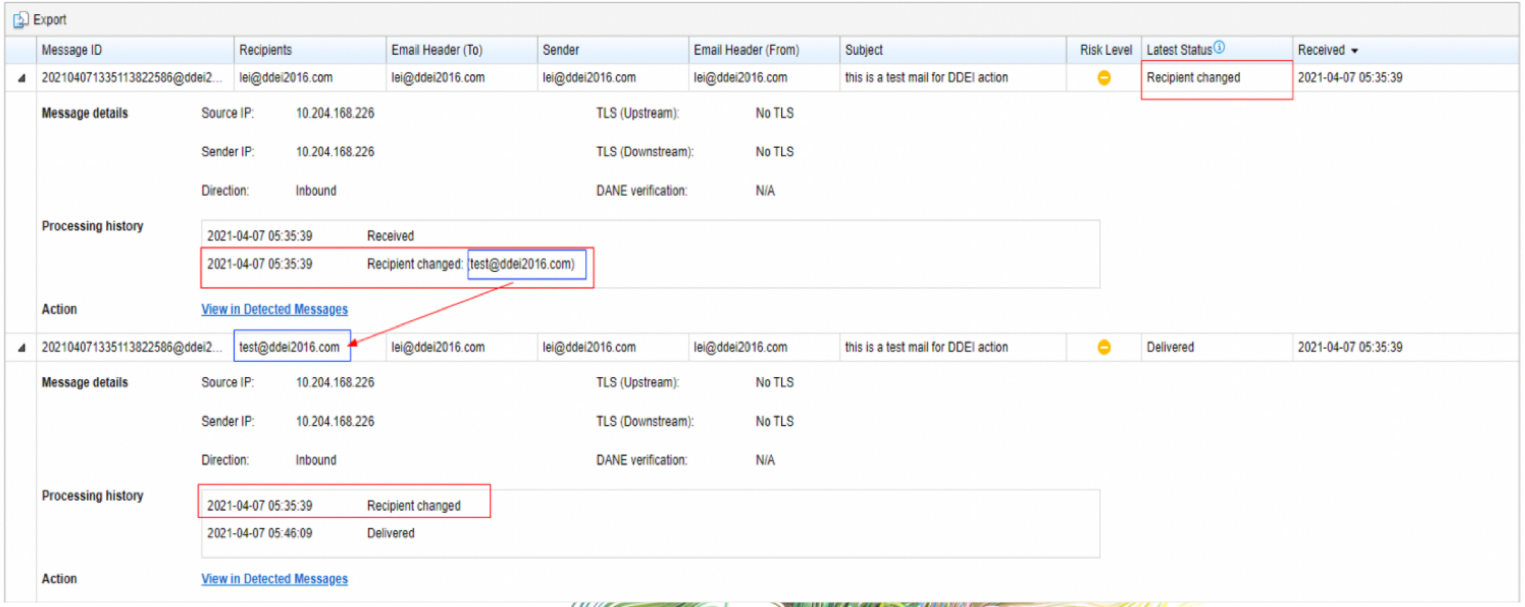


Policy enhancement: “Change Recipient” action

- Support rule-based “Change Recipient” action

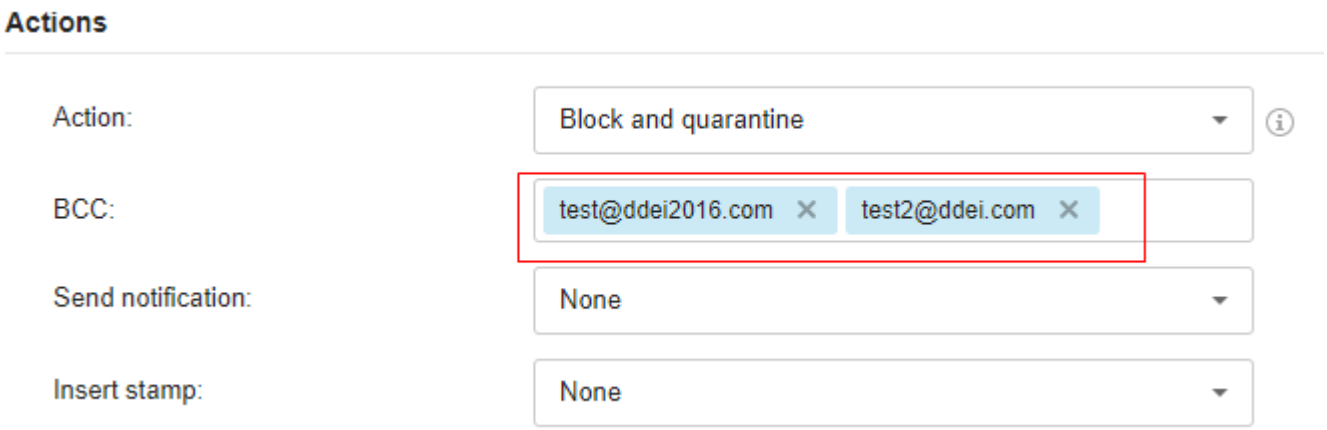


- UI- Message tracking log page



Policy enhancement: “BCC” action

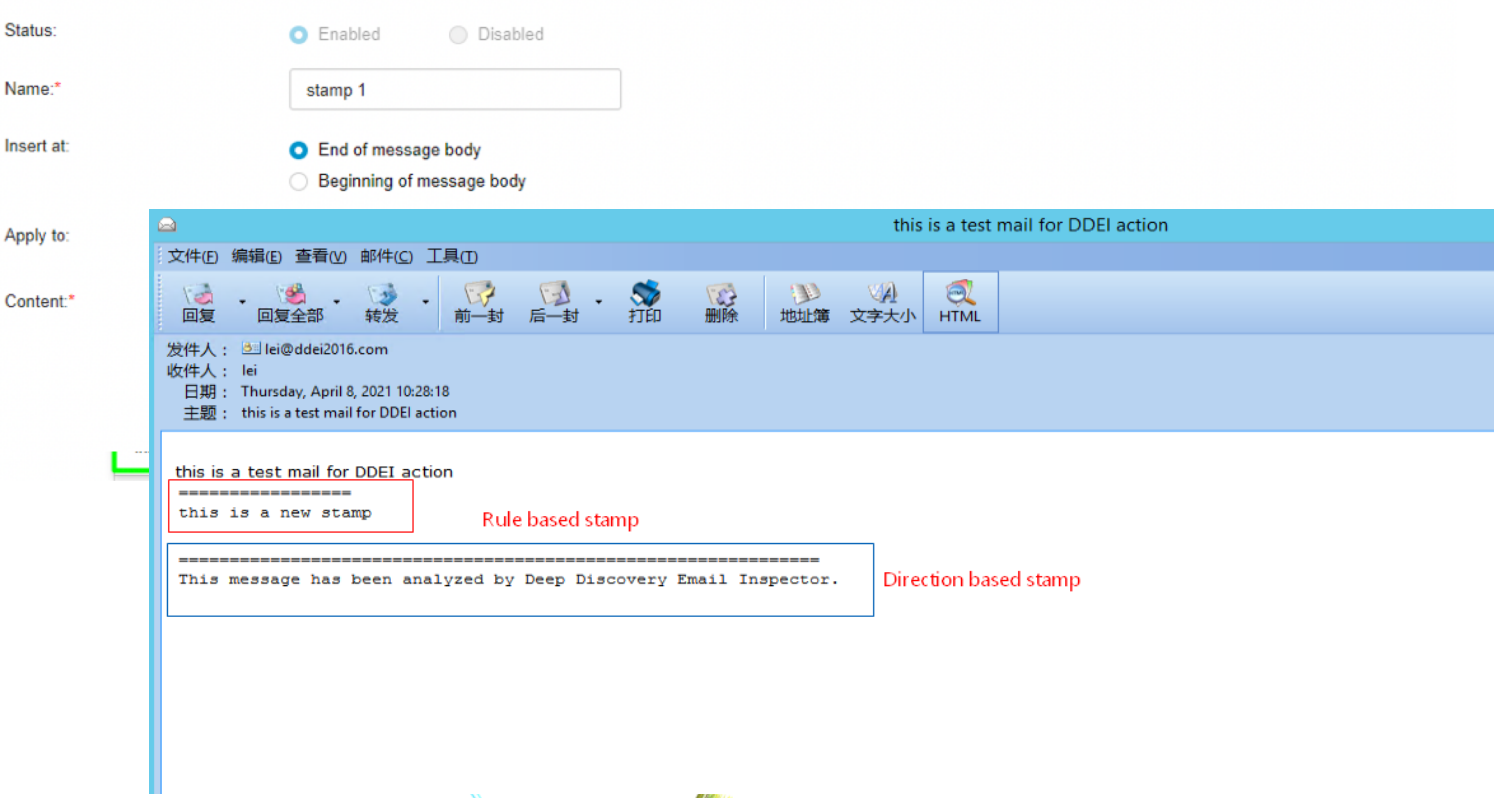
- UI- Content/DLP/Spam Rule page
  - Add or edit rule page, input email addresses into ‘BCC’ item. Max 50 email addresses.



Support for all types of policy rule.
BCC action can co-exist with any other action. It’s a non-terminal action, it cannot be configured alone and always comes with other action together.
It only worked on MTA mode.

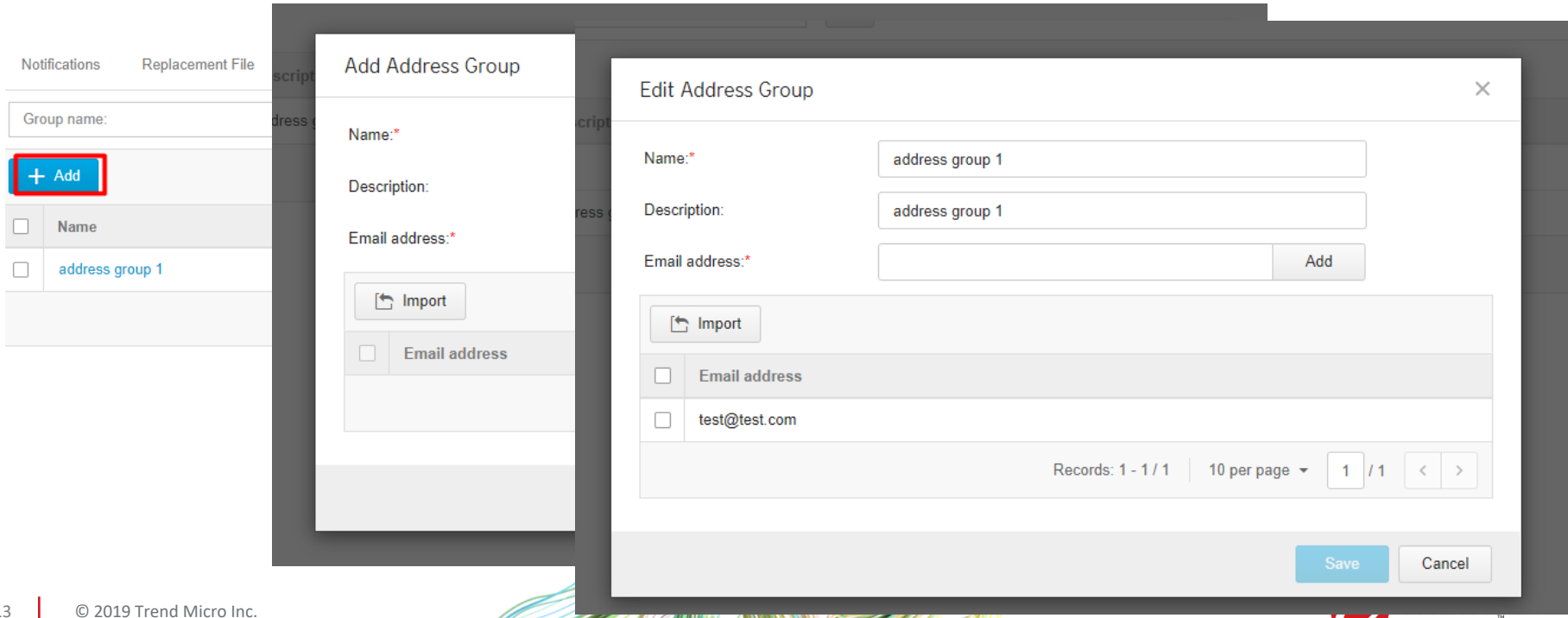
Policy enhancement: rule-based “Stamp” action

Sample:



Policy enhancement: Configure address group as policy object

- UI
  - Create one address group



TREND MICRO™

THE ART OF CYBERSECURITY

Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**