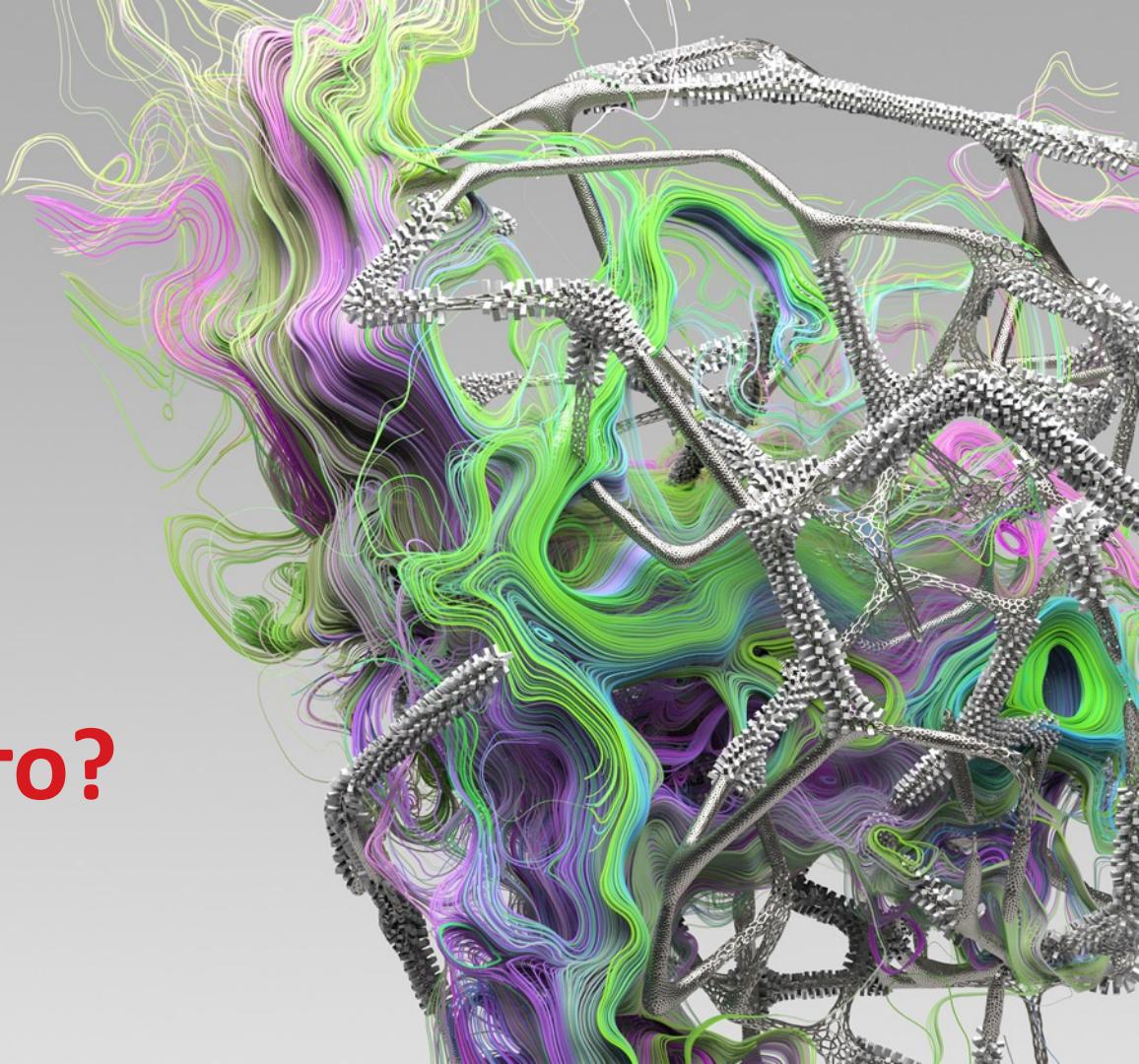




DDEI:ЧТО НОВОГО?

Nurlan Adayev



Возможности DDEI

Predictive Machine Learning

Anti-spam/Graymail

CTD

Threat extraction

Custom Sandbox

Email Reputation Service integration

Password Analyzer

Content filtering

URL Time-of-Click

DLP

Business Email Compromise protection

End-User Quarantine

Integration with other vendor's Products/Services

Sender filtering/Authentication



Режимы работы

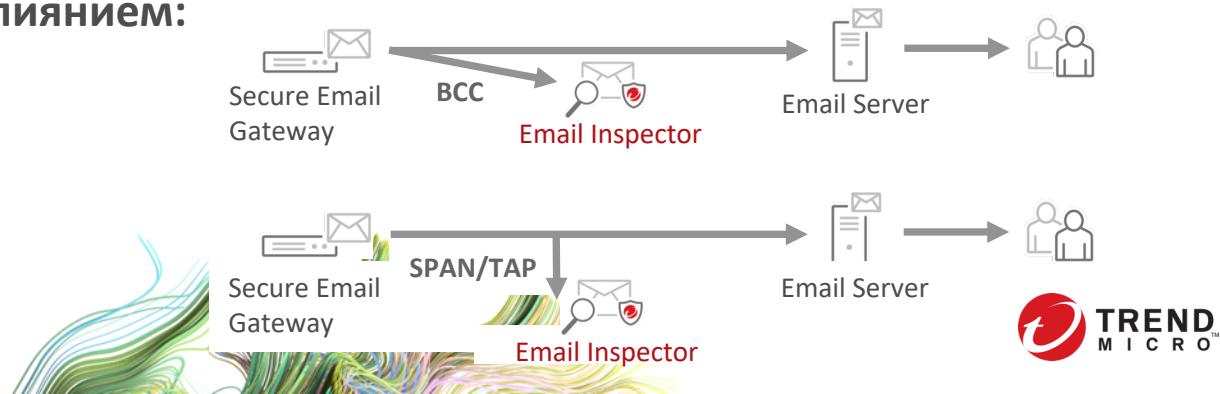


- Блокирует вредоносные письма
- Добавляет расширенную защиту, не влияя на существующие решения по защите электронной почты
- Конфигурация или архитектурные изменения не требуются
- Никаких изменений в политике электронной почты или поведении пользователя

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.

Sender Filtering/Authentication

?

Sender Filtering/Authentication				
Email Reputation	Approved Senders	Blocked Senders	DHA Protection	Bounce Attack Protection
SPF	DKIM Authentication	DKIM Signatures	DMARC	
+ Add Import Export All				
IP Address	Domain/Email Address	Resource Record	Description	Last Updated
<input type="checkbox"/> N/A	"@*.example.com	N/A		2021-03-31 02:51:07
<input type="checkbox"/> N/A	"@example.com	N/A		2021-03-31 02:50:48
<input type="checkbox"/> N/A	"@*	N/A	For all sender	2021-03-31 02:50:24

Records: 1 - 3 / 3 | 10 per page | 1 / 1 < >

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

Import Blocked Senders ×

File: [Select](#)

Merge option:

Merge with current list

Overwrite current list

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

Prevent internal message spoofing

6

Match domain:

Match IP address:

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.

System Settings

Network NIC Teaming Operation Mode Proxy SMTP Time SNMP Session Timeout Certificate Management Connection Security

⚠ Before you disable a security protocol, ensure that the setting does not affect products that integrate with Deep Discovery Email Inspector.

Web console: TLS 1.0 TLS 1.1 TLS 1.2 SSLv3

SMTP: TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3 SSLv3

- DANE/DNSSEC apply to outbound messages

Configure TLS Settings

x

Status:^{*}

Enabled Disabled

Domain:^{*} 

example.com

Description:

Security level:^{*} 

DANE-only

Cipher grade:^{*}

Medium



Difference between DANE-only and DANE:

Security level: [*] i	Opportunistic	▼	
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

Exceptions

Specify the sender-recipient pairs that Deep Discovery Email Inspector excludes from the policy scan.

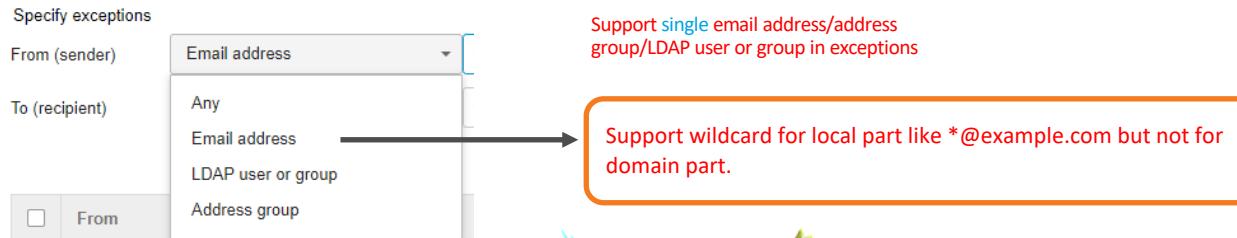
None
 Specify exceptions

From (sender)

To (recipient)

	From	Type (From)	To	Type (To)
<input type="checkbox"/>	test@test.com	Email address	lei_test	LDAP group

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

Actions

Action:

Change recipient

Recipients:

test@test.com

- UI- Message tracking log page

Export								
	Message ID	Recipients	Email Header (To)	Sender	Email Header (From)	Subject	Risk Level	Latest Status
▲	202104071335113822586@ddei2...	lei@ddei2016.com	lei@ddei2016.com	lei@ddei2016.com	lei@ddei2016.com	this is a test mail for DDEI action	⚠	Recipient changed
Message details								
	Source IP:	10.204.168.226	TLS (Upstream):	No TLS				
	Sender IP:	10.204.168.226	TLS (Downstream):	No TLS				
	Direction:	Inbound	DANE verification:	N/A				
Processing history								
	2021-04-07 05:35:39	Received						
	2021-04-07 05:35:39	Recipient changed: test@ddei2016.com						
Action								
	View in Detected Messages							
▲	202104071335113822586@ddei2...	test@ddei2016.com	lei@ddei2016.com	lei@ddei2016.com	lei@ddei2016.com	this is a test mail for DDEI action	⚠	Delivered
Message details								
	Source IP:	10.204.168.226	TLS (Upstream):	No TLS				
	Sender IP:	10.204.168.226	TLS (Downstream):	No TLS				
	Direction:	Inbound	DANE verification:	N/A				
Processing history								
	2021-04-07 05:35:39	Recipient changed						
	2021-04-07 05:46:09	Delivered						
Action								
	View in Detected Messages							

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.**

Actions

Action:	Block and quarantine
BCC:	<input type="text" value="test@ddei2016.com"/> <input type="text" value="test2@ddei.com"/>
Send notification:	None
Insert stamp:	None

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:

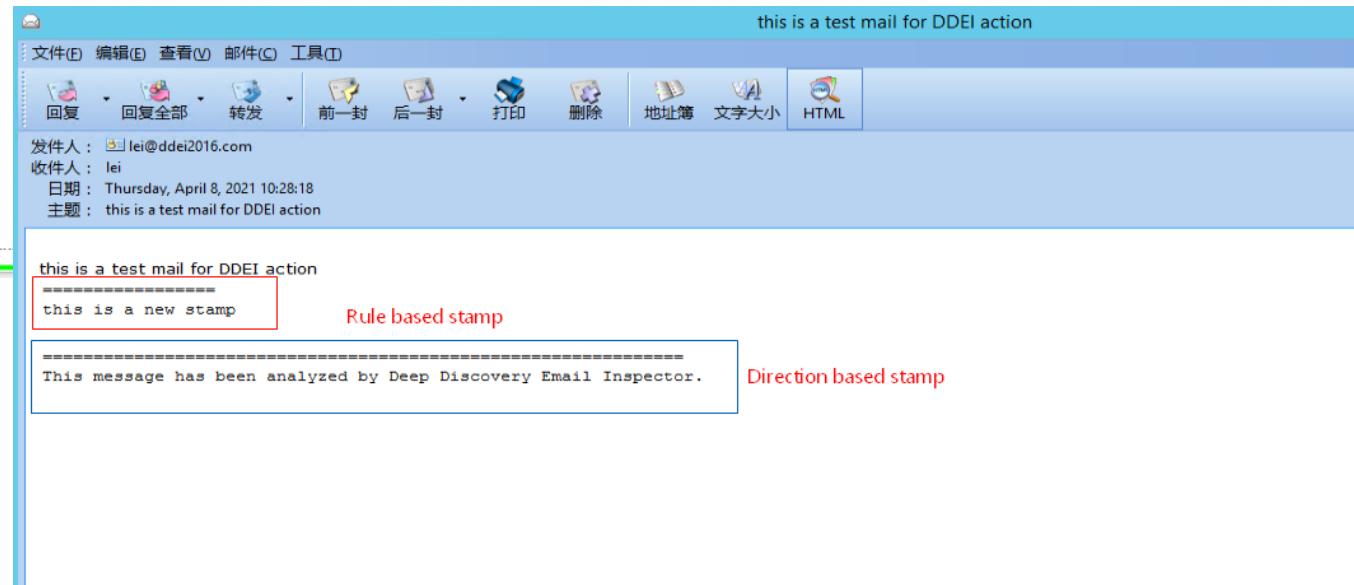
Status: Enabled Disabled

Name:^{*} stamp 1

Insert at: End of message body
 Beginning of message body

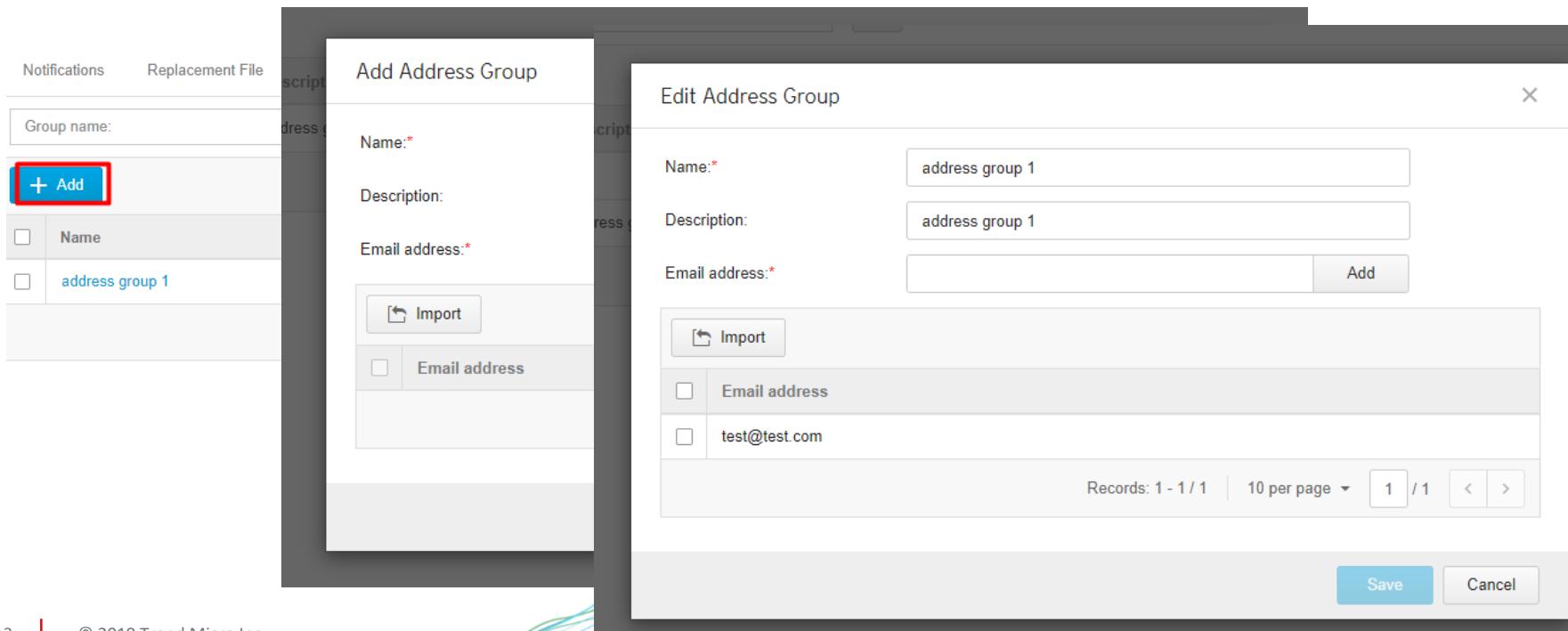
Apply to:

Content:^{*}



Policy enhancement: Configure address group as policy object

- UI
 - Create one address group





THE ART OF CYBERSECURITY

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