

Metadefender Email Security

최신 랜섬웨어, 신종 및 변종
악성코드 차단을 위한 효과적인
이메일 보안 방안

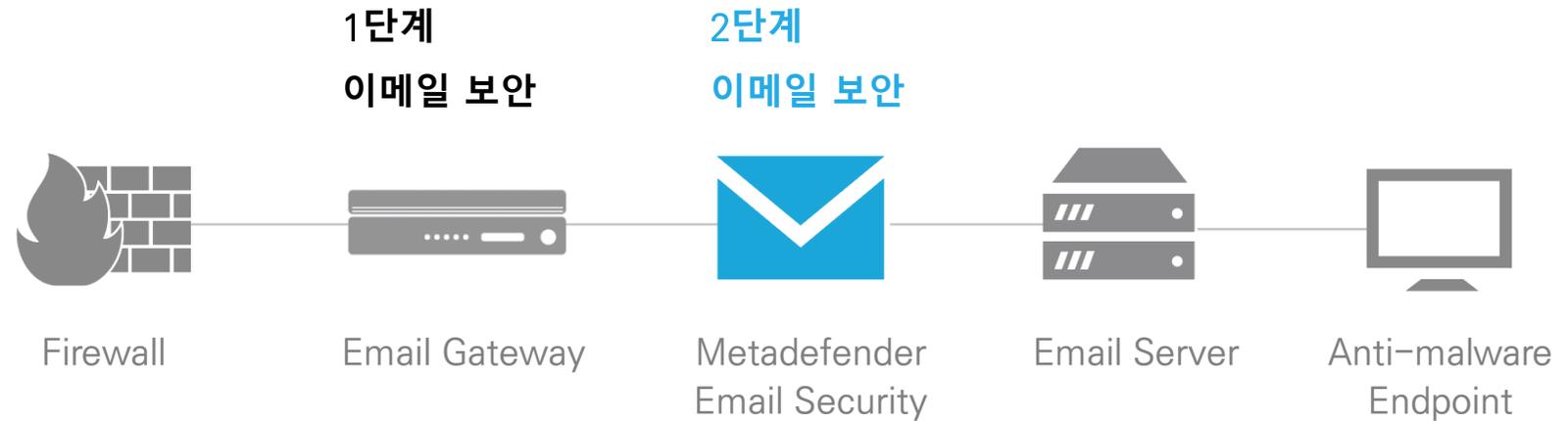
Metadefender Email Security

1단계 보안

- 스팸 차단 보안 게이트웨이

2단계 보안

- Metadefender



Multi-scanning

높은 악성코드 탐지율 제공
over 30+ anti-malware engines

Data Sanitization

데이터 살균 [문서파일에 삽입된 악성코드 제거]
90+ data sanitization engines



Metadefender Email Security

멀티 스캐닝 : 최대 30개 이상의 스캔 엔진 제공으로 높은 탐지율 제공

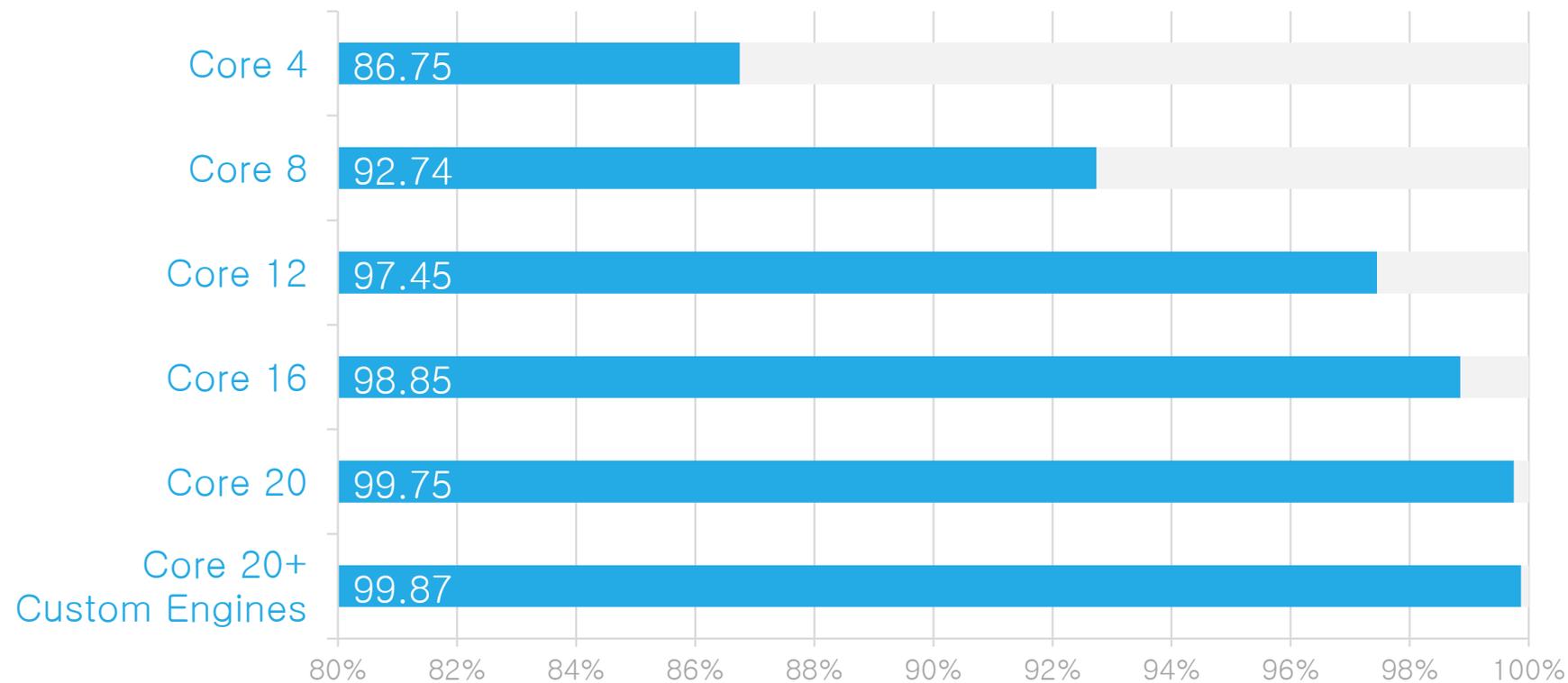
-  For Windows
-  For Linux
-  Windows Custom Engines



Metadefender Email Security

멀티 스캐닝 : 최대 30개 이상의 스캔 엔진 제공으로 높은 탐지율 제공

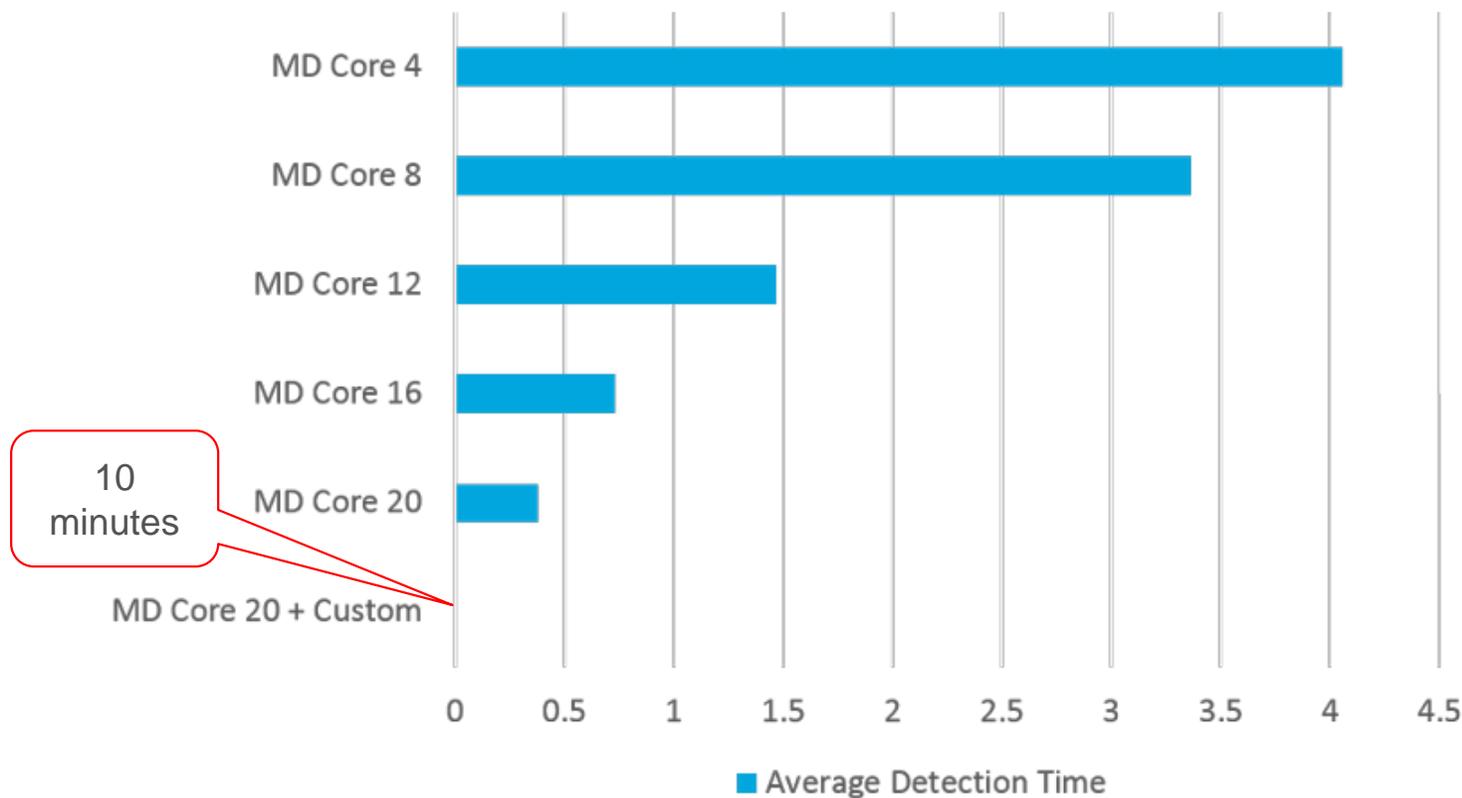
Detection of top 10,000 threats



Metadefender Email Security

멀티 스캐닝 : 평균 탐지 시간

Outbreak Detection (In Days)



Metadefender 16개 이상 엔진 사용시
위협 탐지 1일 미만

Metadefender 20개 이상 엔진 사용시
위협 탐지 10분 미만

Metadefender Email Security

멀티 스캐닝 : 탐지 로그 분석

OPSWAT[™]
Metadefender[™]
CORE

Dashboard Configuration Sources Quarantine Logs Licenses Documentati

File Log Email History Email Event Log Application Log Windows Event Log Configuration Download

All time Search name Showing 20 of 21763 Quick Filters: Allowed Blocked Refresh Clear Logs

FILE NAME	REASON	WORKFLOW APPLIED	SOURCE	SCAN TIME	START TIME
eicar.com	Infected	Web Scan	localhost	1809 ms	2016/10/17 4:23:54 PM
Metadefender Client.exe	Infected	Metadefender Client	WindowsDemo	2531 ms	2016/10/18 9:24:51 AM
heurscn2.qvd	Infected	Metadefender Client	WindowsDemo	5553 ms	2016/10/18 9:24:54 AM
PowerISO6-x64.exe	Filtered	Mail Agent	fe80::acbf:d18b:3a0c:d9e8%11	0 ms	2016/10/19 10:32:45 AM
eicar_com.zip	Infected	Mail Agent	fe80::acbf:d18b:3a0c:d9e8%11	1201 ms	2016/10/19 11:09:54 AM
PowerISO6-x64.exe	Infected	Mail Agent	fe80::acbf:d18b:3a0c:d9e8%11	5459 ms	2016/10/19 11:10:09 AM
eicar_com.zip	Infected	Mail Agent	fe80::acbf:d18b:3a0c:d9e8%11	78 ms	2016/10/19 11:10:24 AM
export	Mismatch	Mail Agent	fe80::acbf:d18b:3a0c:d9e8%11	0 ms	2016/10/20 9:36:07 AM

Metadefender Email Security

멀티 스캐닝 : 이메일 감염 메시지

Metadefender Core notification: Email infected



aschulman@opswat.com

To: www@caffeine.andymillar.co.uk; Demo DU. User; ♪

Metadefender Core has detected an infection in the following email:

Date : 11/08/2016 01:33:09

From : "Apache, andymillar.co.uk" <andy@andymillar.co.uk>

To : "demouser@napswitch.com" <demouser@napswitch.com>

Subject: EICAR Virus Test Email

Result : EICAR_Test_File

Infected

1/21
engines found a threat
Infected
OPSWAT
Metadefender

Metadefender Client (2).exe

Reason	Infected	Source	aschulman-l8e
File Type	Generic Win/DOS Executable	Start Time	2016/11/03 12:31:06 PM
Workflow	Metadefender Client	Size	10.28 MB
User Agent	-		

Hashes

MD5	E4816D02C7F66E19E1A2B5E2BC87086A
SHA1	CA018D7AE792534EC72DA5E9669CF8B345A0BA6C
SHA256	35B1E22356369F5BDD29E661C0D2923CFE6C40A1FC1148DE2077EE0D1D2D096E

ENGINE	SCAN TIME	DEFINITION TIME	RESULT
Ahnlab	1341 ms	2016-10-27	✓
AVG	1263 ms	2016-11-02	✓
Avira	124 ms	2016-11-02	TR/Dropper.Gen ✗
BitDefender	1778 ms	2016-11-02	✓
ClamAV	2152 ms	2016-11-02	✓

Metadefender Email Security

Data Sanitization:
데이터 살균
첨부파일에서 위협요소 제거

- 기 알려지지 않는 악성코드
- 신종 / 변종 악성코드
- 문서파일 기반 악성코드 대응 방안



Sanitization Rules

<input checked="" type="checkbox"/> Sanitize Allowed Files	Enable	Original Format:	Sanitized Format:
Adobe Files			
<input checked="" type="checkbox"/>		Portable Document Format (.pdf)	pdf
Microsoft Office Files			
<input checked="" type="checkbox"/>		Word Document (2003 and earlier) (.doc)	doc
<input checked="" type="checkbox"/>		Excel Spreadsheet (2003 and earlier) (.xls)	xls
<input checked="" type="checkbox"/>		PowerPoint Presentation (2003 and earlier) (.ppt)	ppt
<input checked="" type="checkbox"/>		Word Document (2007 and later) (.docx)	docx
<input checked="" type="checkbox"/>		Excel Spreadsheet (2007 and later) (.xlsx)	xlsx
<input checked="" type="checkbox"/>		PowerPoint Presentation (2007 and later) (.pptx)	pptx
Other Documents			
<input checked="" type="checkbox"/>		Rich Text Format (.rtf)	rtf
<input checked="" type="checkbox"/>		Hypertext Markup Language (.htm/html)	pdf
Image Files			
<input checked="" type="checkbox"/>		Joint Photographic Experts Group (.jpg)	bmp
<input checked="" type="checkbox"/>		Bitmap Image File (.bmp)	eps
<input checked="" type="checkbox"/>		Portable Network Graphics (.png)	bmp
<input checked="" type="checkbox"/>		Tagged Image File Format (.tiff)	tiff
<input checked="" type="checkbox"/>		Scalable Vector Image Format (.svg)	bmp
<input checked="" type="checkbox"/>		Graphics Interchange Format (.gif)	bmp
<input type="checkbox"/>		Sanitize Blocked Files	

Unknown Malware
Ransomware 차단

16종류 원본형식을 100개 이상의
변환형식으로 변경 (.hwp 지원)

이메일 보안을 위한 연동 제품



이메일 보안을 위한 연동 제품군

Secure email gateway와 간단한 연동 구성



proofpoint

Email Protection



CISCO

Email Security Appliance



FireEye

Ex Series



FORCEPOINT
POWERED BY Raytheon

TRITON AP-EMAIL



Symantec

Messaging Gateway



Barracuda

Email Security Gateway



SOPHOS

Email Appliance



clearswift

SECURE Email Gateway

이메일 보안을 위한 연동 제품군

Secure email gateway와 간단한 연동 구성



Terrace Mail Suite



Spam Email Gateway



Spam Email Gateway



Secure Email Gateway



McAfee Email Gateway



Spam Email Gateway



Spam Email Gateway



Secure Email Gateway

이메일 보안을 위한 연동 제품

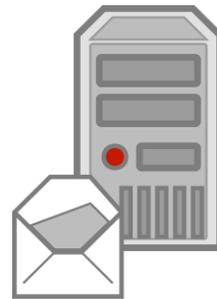
메일서버, 익스체인지, 클라우드
호스팅 메일 솔루션들과의 간편한
연동 구성

On-Premises

Cloud & Hosted

On-Premises

Cloud & Hosted



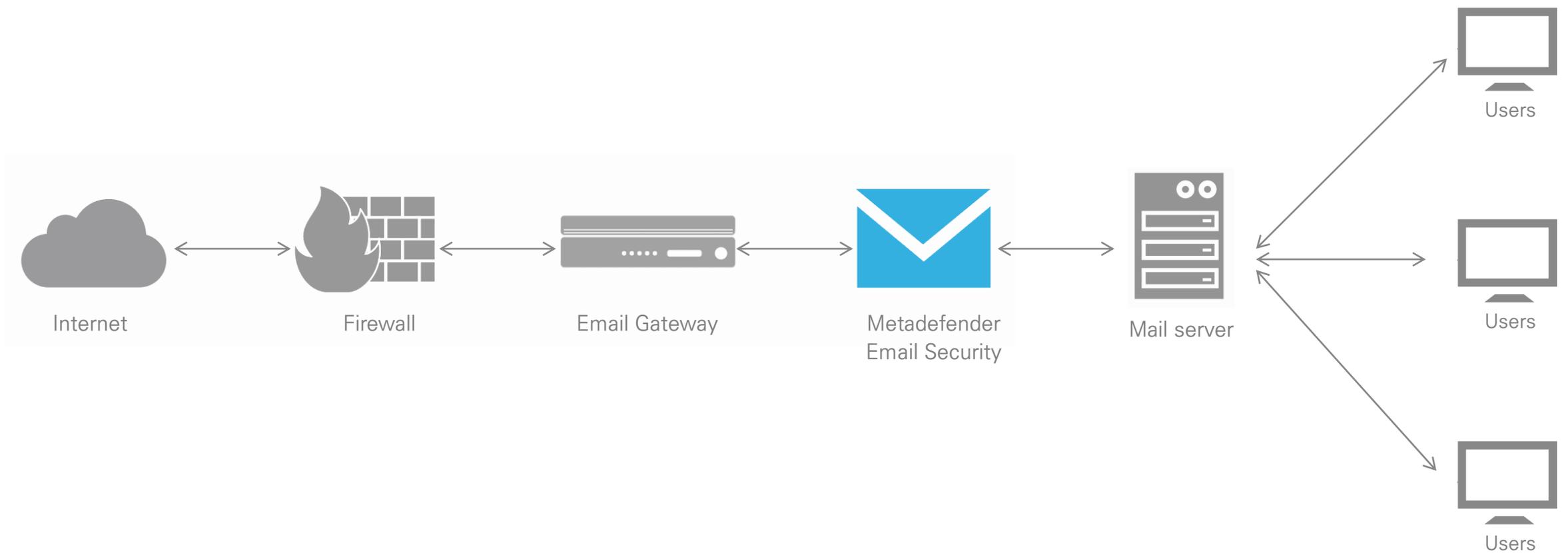
G Suite

 Microsoft
Hosted Exchange

 Office 365

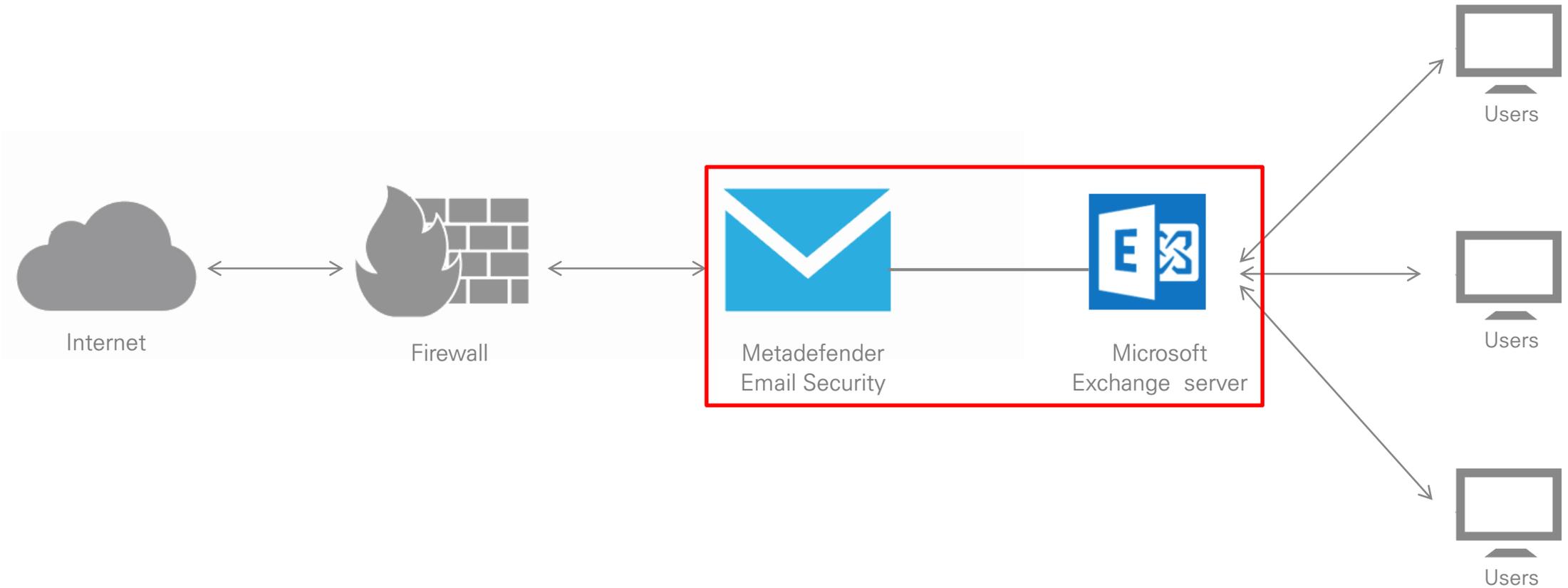
이메일 보안 구성 1

Email Gateway와 Metadefender 연동 구성



이메일 보안 구성 2

Exchange 메일 서버 보안을 위한 Metadefender Email Security



이메일 보안 구성 3

Cloud 호스팅 메일솔루션

