



Belnet – Advanced Mail Security

FortiMail overview – Information Session

Presenters: Steven Versonnen & Johan Van Gestel

Date: 07 May 2020

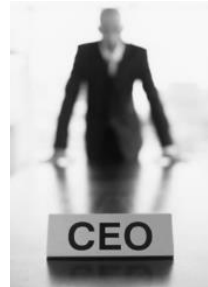
Email is **THE** critical threat vector

Malware



- Targets unskilled users therefore often volumetric attacks
- Use of social engineering techniques to get users to open email and execute malware
- Some zero day, mostly a numbers game
- 92.4% of malware is delivered via the email vector*

Phishing



- Targets an interest group, organization or individuals (spear phishing) within the organization
- Customised content based on user interests or role
- Often targeted at C-levels (whaling)
- Zero-day malware or social engineering to divulge financial or credential information
- 4% users click on malicious attachments or links in such mails*

Compliance & Data Loss



- Sending of Personally Identifiable Information (PII) via Email
- Sending of corporate confidential information out of the organization
- Corporate espionage
- Failure to encrypt sensitive emails
- Failure to backup/save/archive emails to comply with corporate standards
 - IRS – 7 years
 - PCI – 1 year
 - State depts – 3 years
 - HIPPA – 6 years

Email Based Threats

* Source: Verizon 2018 Data Breach Investigations Report

Le Monde | [HOME](#) | [ACTUALITÉS](#) | [ÉCONOMIE](#) | [VIDÉOS](#) | [OPINIONS](#) | [CULTURE](#) | [M LE MAG](#) | [SERVICES](#)

PIXELS

Les autorités mettent en garde contre une arnaque « massive » par e-mail

Une enquête sur cette arnaque est menée depuis l'été 2018, mais plusieurs centaines de cas ont été signalés au cours des dernières semaines.

Le Monde avec AFP · Publié le 04 février 2019 à 22h21 - Mis à jour le 04 février 2019 à 22h21

BANK INFO SECURITY® **BETTER.**

Topics | News | Training | Resources | Events | Jobs

TRENDING: Live Webinar | Fraud Prevention for Banks: Top 10 Tech Requirements to Evaluate | Risk & Resp

Business Email Compromise (BEC), Fraud Management & Cybercrime, Governance

FBI: Global Business Email Compromise

Mattel nearly loses \$3M to a classic phishing scam
 by BRYAN CLARK — 5 months ago in INSIDER

CYBERANGRIFFE

Infizierte E-Mails greifen Medien an

Deutsche Medienunternehmen und Organisationen in der Chemiewaffenforschung sind Ziel eines professionellen Cyberangriffs geworden. Zwei Datenbanken, die jetzt mit Namen bekannt sind...

CSO | Mobile Security | Data Protection | Identity & Access | SecurityWatch | CSO Lead

CEO fired after 'fake CEO' email scam

Liam Tung (CSO Online) on 26 May, 2016 09:29

5 Comments

threatpost | Cloud Security / Malware / Vulnerabilities / Privacy

Podcast: Breaking Down the COSCO Ransomware Attack

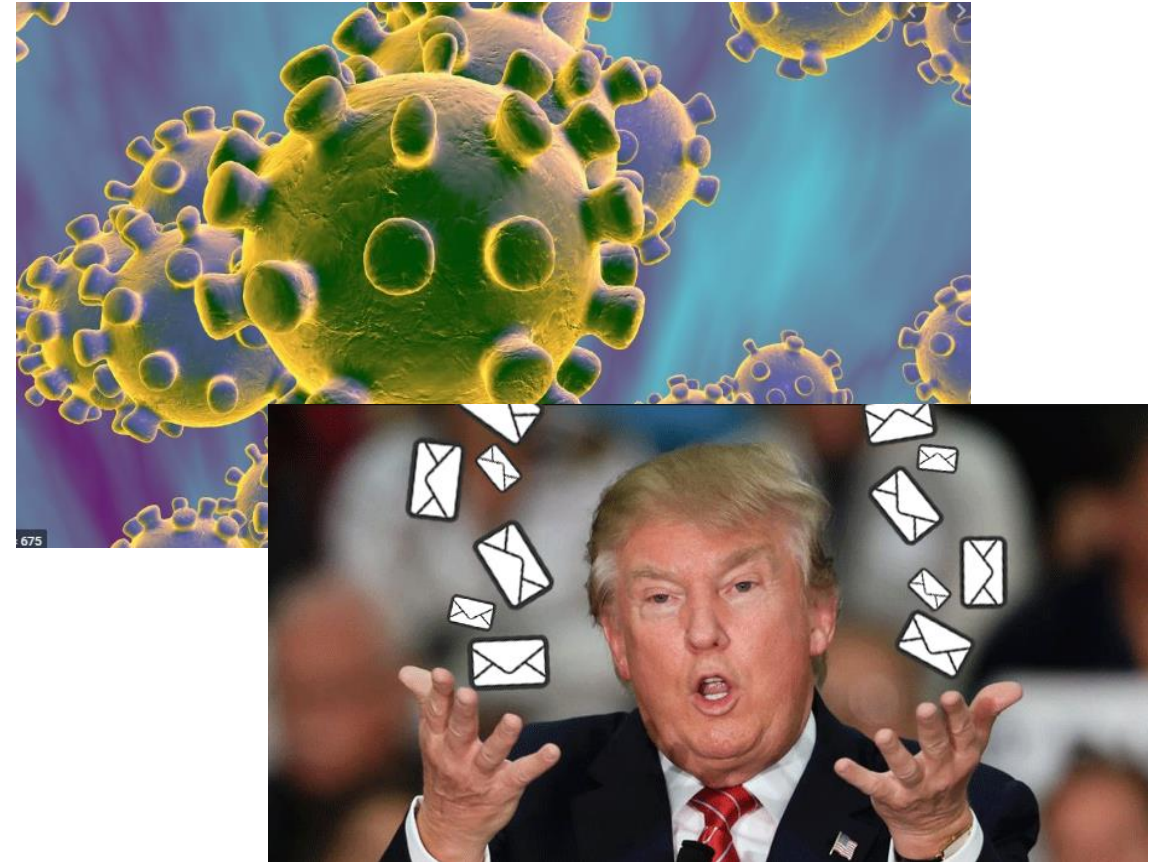
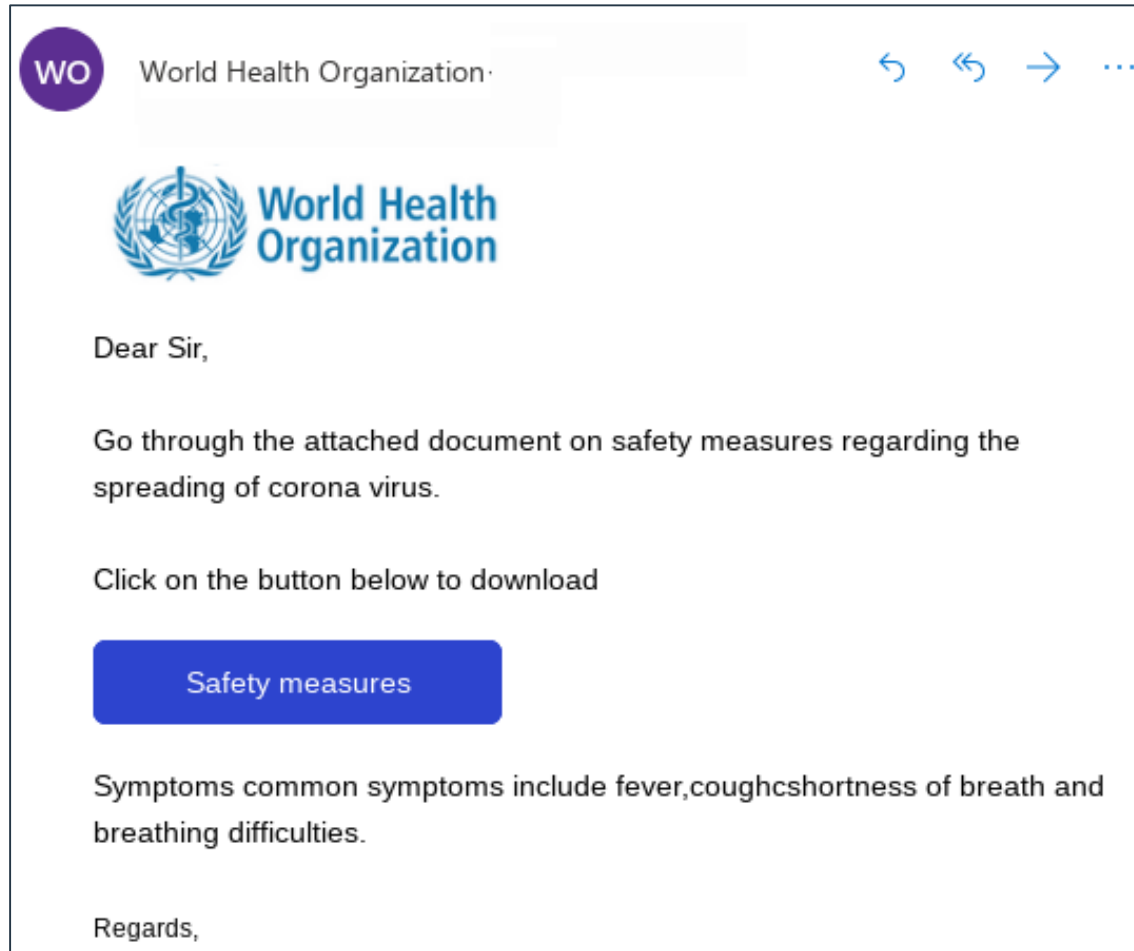
Phishing Campaign Steals Money From Industrial Companies

Author: Lindsey O'Donnell
 August 2, 2018 / 12:46 pm
 3 minute read

It's about your ...

- Money
- Reputation
- Productivity
- Confidential data
- Identity

Spam – Exploiting headlines and fear



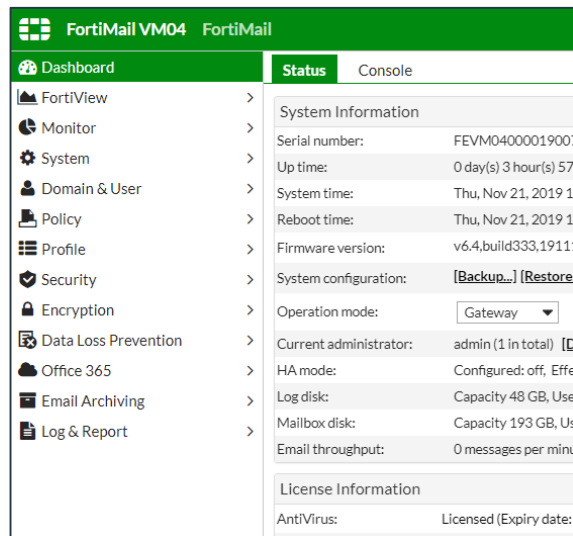
<https://fortiguard.com/resources/threat-brief/2020/02/07/fortiguard-threat-intelligence-brief-february-07-2020>

FortiMail

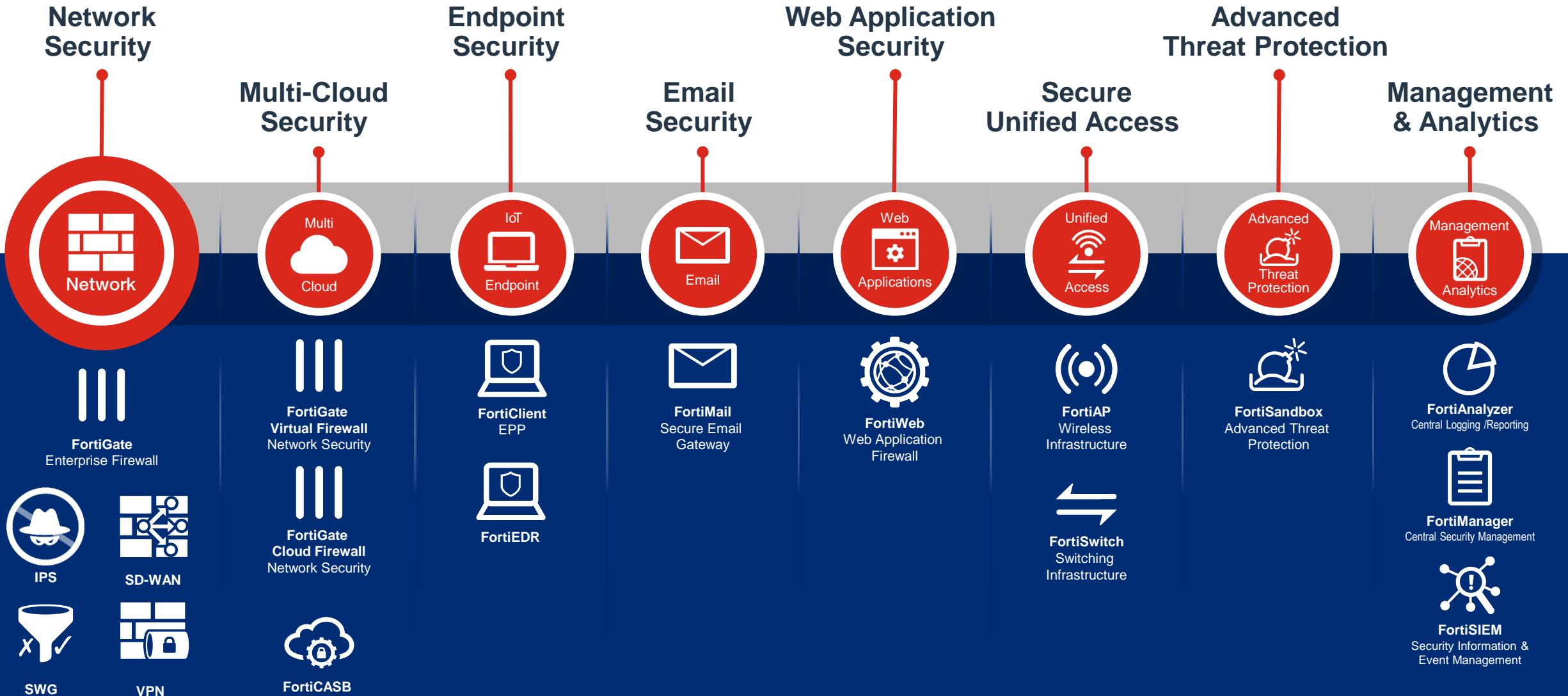
Overview

FortiMail Overview

- **Consolidated email security platform to prevent threats and data loss in a single high performance appliance**
 - Top-rated email threat prevention
 - Enterprise class anti-virus and anti-spam solution
 - Advanced threat prevention integration with **FortiSandbox**
 - **FortiGuard** Labs security services
 - Advanced features such as Identity Based Encryption, Content Protection and Archiving
 - Intuitive



FortiMail : part of a complete Network Security Solution



Protection from Email-based Threats

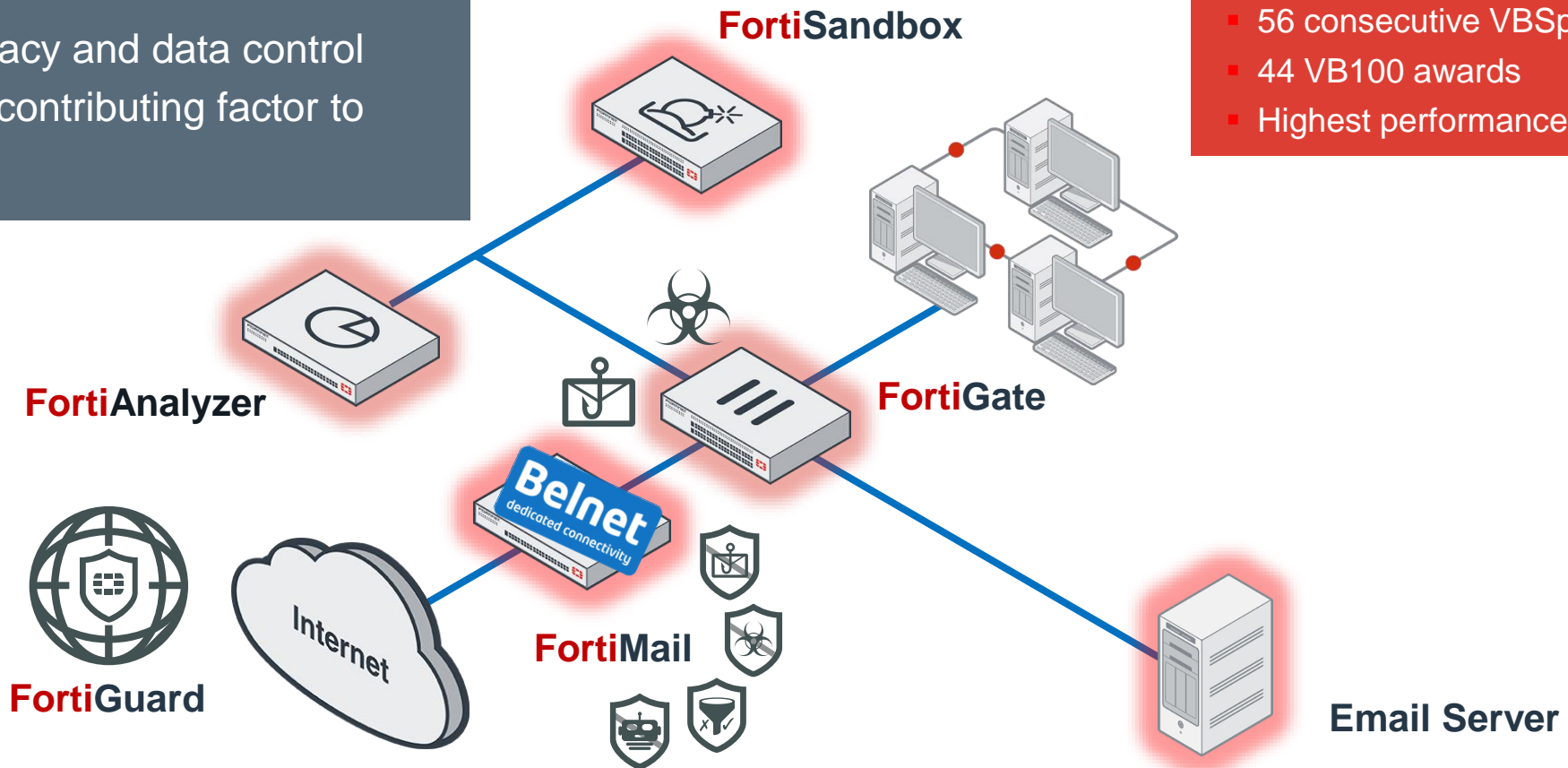
Primary Challenges

Email common entry point for attackers

- Spam, attachments, phishing
- Targeted attacks

Compliance, privacy and data control

Users are major contributing factor to risk



Solution

FortiMail Email Security

- Inbound and outbound threat protection
- Content protection and encryption
- FortiSandbox integration

Advantages

- 56 consecutive VBSpam awards
- 44 VB100 awards
- Highest performance in industry

FortiMail is Rigorously Tested



Recent update:
<https://selabs.uk/download/enterprise/essp/2020/mar-2020-essp.pdf>

Fortinet FortiMail

SC rate: 99.98%

FP rate: 0.00%

Final score: 99.98

Project Honey Pot SC rate: 100.00%

Abusix SC rate: 99.96%

Newsletters FP rate: 0.0%

Malware SC rate: 100.00%

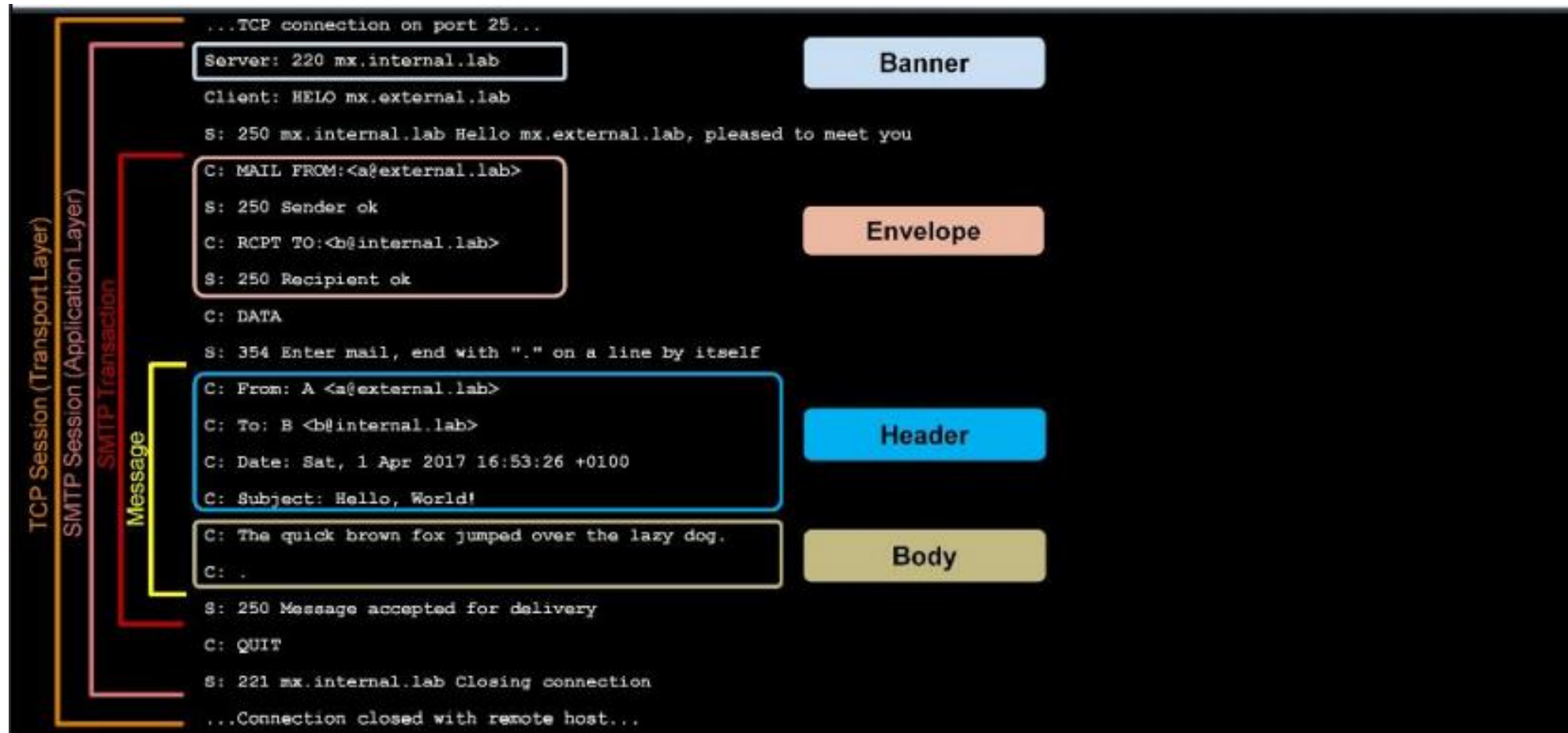
Speed:



Product	Block Rate	NSS-Tested Throughput	3-Year TCO (US\$)				
Fortinet Advanced Threat Protection (FortiSandbox Cloud with FortiGate 600D v5.6.1, FortiMail Virtual Appliance v5.4.0 and FortiClient ATP Agent v5.6.1.1112)	99.6%	2,692 Mbps	\$20,430				
	Drive-by Exploits	Social Exploits	HTTP Malware	Email Malware	Offline Infections	False Positives	Evasions ¹
Block Rate	100.0%	93.3%	99.3%	99.0%	100.0%	0.00%	88.6%
Additionally Detected	0.0%	6.7%	0.5%	1.0%	0.0%	0.00%	NA

Product	Breach Detection Rate ¹	NSS-Tested Throughput	3-Year TCO (US\$)		
Fortinet FortiSandbox-2000E v.3.0.0 & FortiClient (ATP Agent) v.5.6.6.1167	99.0%	8,667 Mbps	\$130,405		
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware (Executables)	HTTP Malware (Docs & Scripts)	SMTP Malware
0.93%	100.0%	100.0%	99.9%	100.0%	99.9%
Offline Infections	Stability & Reliability	Evasions Detected			
100.0%	PASS	370/374			

Multi-level Anti-spam filtering



FortiMail combines more than a dozen antispam technologies that act at the connection, header and content level of email messages in order to identify spam, phishing, newsletters and more with high accuracy.

Basic Features

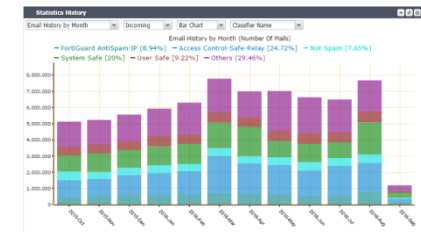
Anti-Spam/Anti-Phishing

- **FortiGuard Reputation Databases**

- Cloud database query to identify know spam IP and content
 - FortiGuard Antivirus, Anti-Spam and URL Filtering
 - FortiGuard IP Reputation including Botnets
- Removes volumetric spam at low cost

- **Advanced Filtering Techniques**

- Detects new Spam campaigns using a variety of dynamic techniques
 - Header Analysis
 - Dynamic Heuristics
 - Sender Reputation
 - Suspicious Newsletter
 - DKIM / SPF / DMARC
 - Greyware Scanning



Fortinet FortiMail contd.

Final score: 99.997

Project Honey Pot SC rate: 99.995%

Abusix SC rate: 99.999%

Newsletters FP rate: 0.0%



Basic Features

Data Protection and Compliance

• Data Loss- & Content Protection

- Preset HIPAA, GLBA, SOX, PCI dictionaries for easy compliance policy creation
- Detailed content detection and protection techniques

• Helping with GDPR Compliancy

- Role-based access to queues and quarantine for better delegation granularity
- Detailed log audit:
 - Admin content changes
 - Configuration changes
 - Search terms
 - Archive retention

• Per Mailbox Policy-based Archiving

- Sender/recipient, Subject/body/attachment filename keywords
- Archive to remote system
- Microsoft Exchange Journal Archiving



Basic Features

Quarantine, End User Digest, Newsletter detection

- **Self-service personal quarantine digest**

- Sender and subject
- Release or delete links

- **Central quarantine**

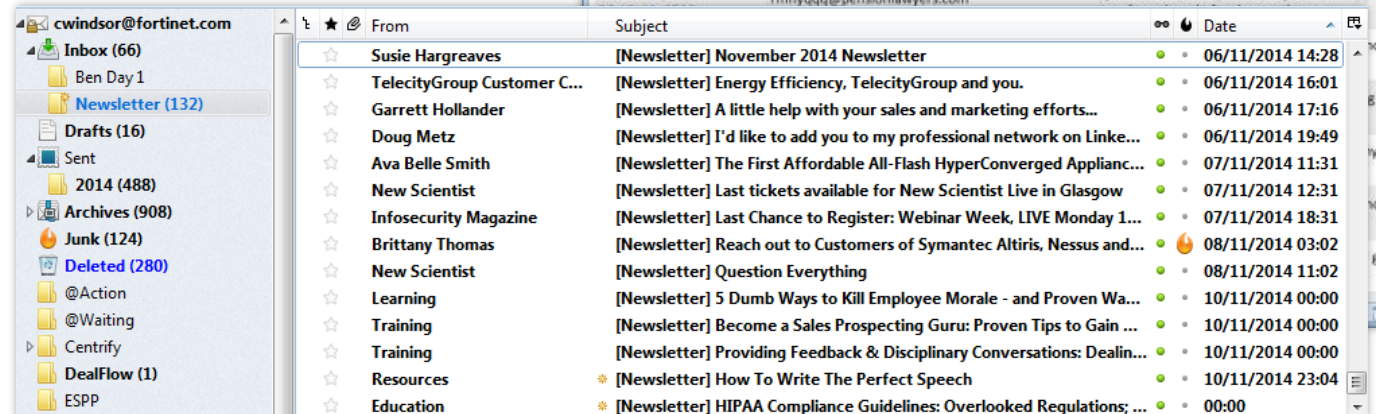
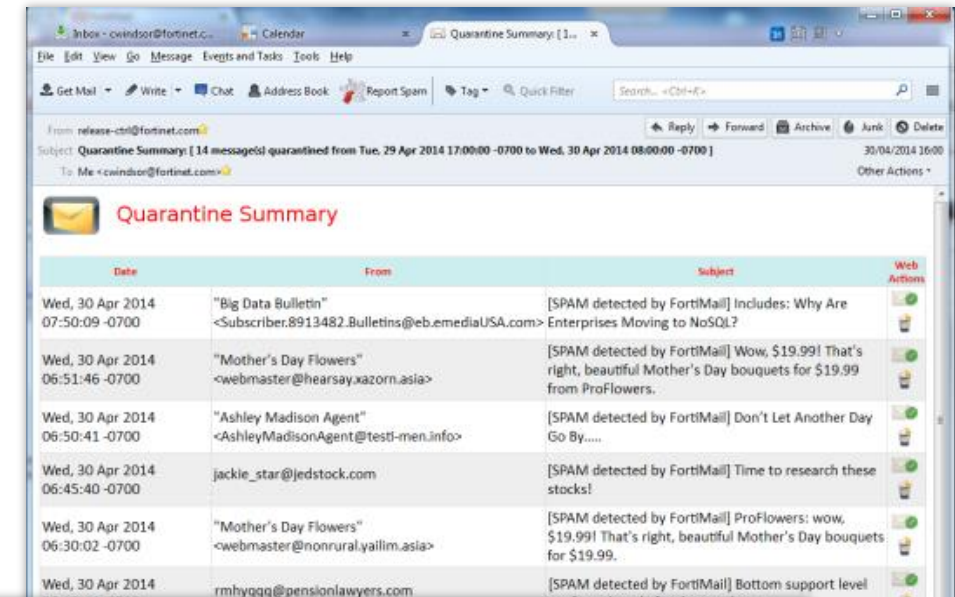
- Easy administration
- Can be consolidated across devices

- **Newsletter detection**

- Both regular and suspicious

- **Content modification**

- Automatic tagging and delivery
- Header insertion
- ...



Advanced protection

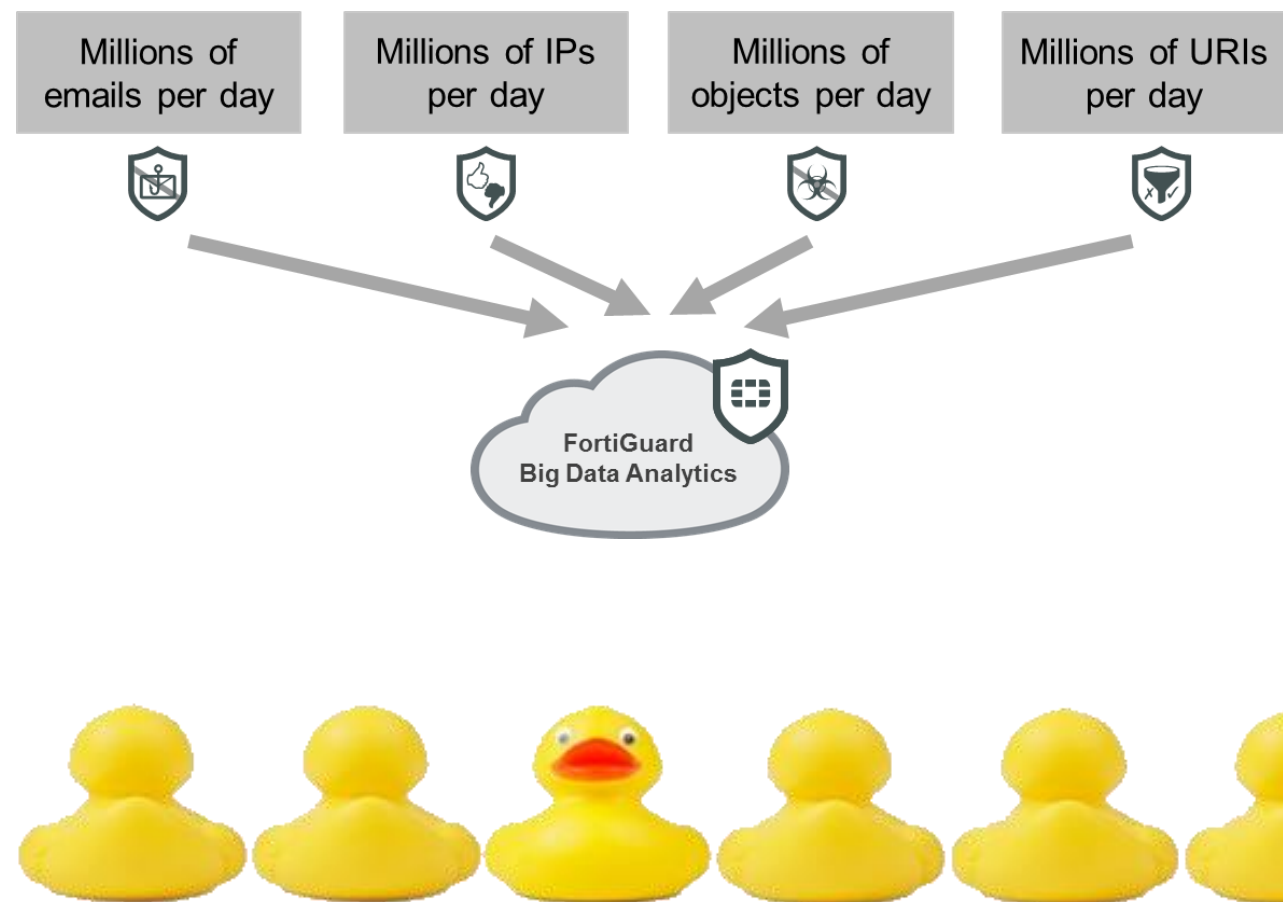
Defending Against Emerging Threats

- **Outbreak Protection**

- **Spam** : Suspicious attachments detected in known spam can be blocked until full evaluation by FortiGuard Labs.
- **Virus** : Cyberthreat Alliance, FortiSandbox Cloud Collaboration, FortiGuard Pre-Signature hashes

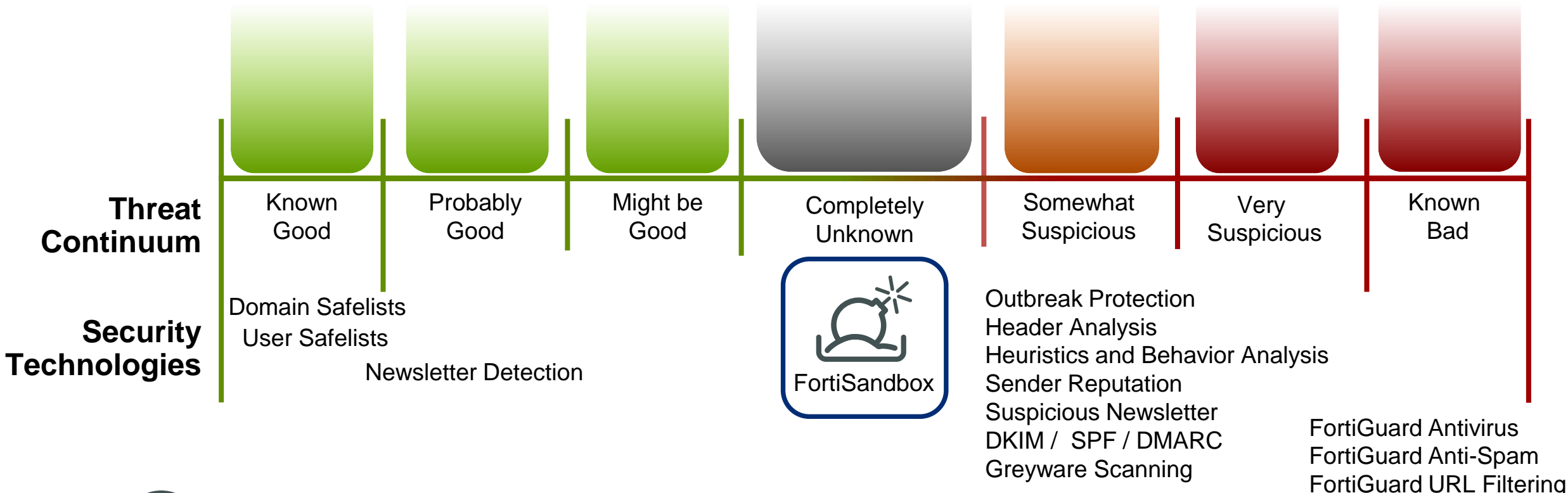
- **Behavioural Analysis**

- Machine learning engine based on previous detections
- Is behaviour similar to recent signature based detections? If it walks like a duck.....



Behavior-based Detection of the Unknown

“99% of malware hashes are seen for only 58 seconds or less. This reflects how quickly hackers are modifying their code to avoid detection.” *



← FortiGuard IP Reputation →

* Source: Verizon 2016 Data Breach Investigations Report

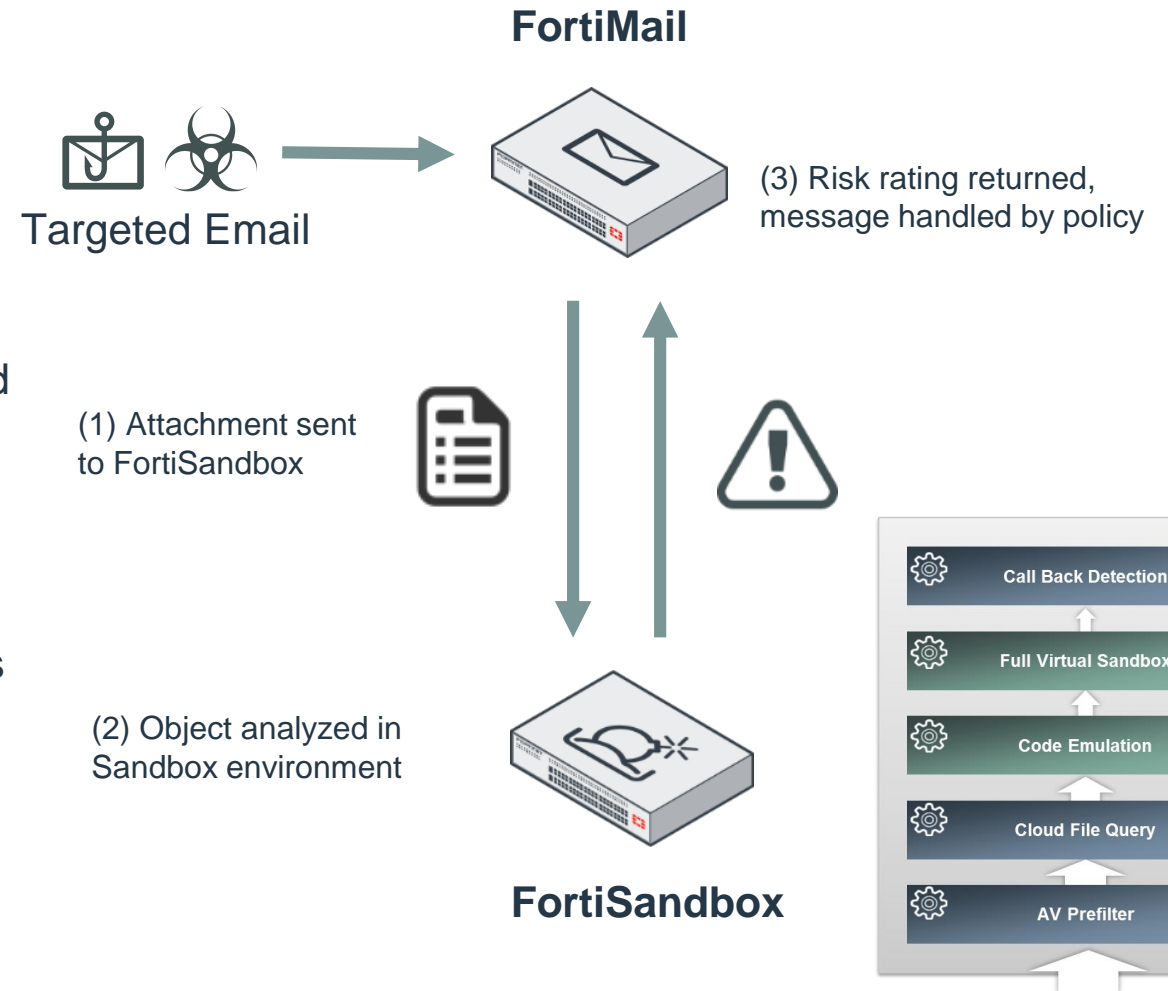
Sandboxing – Analyzing unknown threats

Most efficient Zero-day prevention

FortiSandbox Threat Analysis

FortiMail queues email and submits files and URLs to FortiSandbox for analysis

- AV Pre-filtering
- Cloud results lookup - is sample already known bad
- Analyze objects in a virtual sandbox environment
- Callback detection – does sample try to call home for instructions
- Assign and return a rating for the submission
- FortiMail maintains a cache of FortiSandbox results



* Optional but a core part of an ATP solution

FORTINET

Enhanced Visibility - Monitoring

- **Monitoring**

- Quarantine / Greylisting / ...

- **FortiView**

- Mail Statistics
- Threats
- Top users
- Session view

FortiMail VM01 FML_CLOUD_VM-126_GW

Mail Queue Spam Outbreak Virus Outbreak FortiSandbox Dead Mail

Records per page: 50

Client IP	Envelope From	Envelope To	Subject	Session ID	Received
209.87.240.248	test@fortinet.com	carl@tryptichconsulting.com,feqa@tryptic...	Samuel Yang, Best_R_A_T_E's @ easy RE-FL...	w2GBspe9024657...	Fri, Mar 16, 201
209.87.240.248	test@fortinet.com	carl@tryptichconsulting.com,feqa@tryptic...	Select All	w2GBv3Ak024939...	Fri, Mar 16, 201
209.87.240.248	test@fortinet.com	carl@tryptichconsulting.com,feqa@tryptic...	Clear Selection	w2GBukFA024782...	Fri, Mar 16, 201
209.87.240.248	test@fortinet.com	carl@tryptichconsulting.com,feqa@tryptic...	Do	w2GBug6x024832...	Fri, Mar 16, 201

FortiMail VM01 FML_CLOUD_VM-126_GW

Threat Statistics FortiSandbox Statistics

Statistics Summary (Today)

- Total (3519, 100%)
- Virus (8, 0.2%)
- Spam (3511, 99.8%)

Count, By Hour

Attachment Filter (99.51%) FortiSandbox (0.25%) SMTP Auth Failure (0.22%) Access Control-Relay Denied (0.01%) Not Spam (0.01%)

FortiMail VM01 FML_CLOUD_VM-126_GW

Top Recipient Top Sender

Domain: --All-- Period: Today Category: By Message Count

Top Recipient	Top Sender
carl@tryptichconsulting.com	1697
feqa@tryptichconsulting.com	1697

FortiMail VM01 FML_CLOUD_VM-126_GW

By Count By Size

Count, By Minute

Count, By Hour

Attachment as Spam (0.1%) Attachment Filter (13.79%) Content Monitor and Filter (2.52%) Data Loss Prevention (1.92%) DMARC Failure (0.35%) Domain Block (0.35%) FortiSandbox (0.36%) Header Analysis (17.48%) Heuristic (0.07%) Image Spam (0.28%) Newsletter (0.07%) SPF Failure (0.19%) Virus Signature (0.29%) Virus Delivery (1.34%) Delivery Control (0.51%) Disclaimer (43.45%) Domain Safe (0.83%) Not Spam (0.61%) Policy Match (0.54%) Safelist Word (0.17%)

Count, By Day
Count, By Month
Count, By Year

Enhanced Visibility - Log and message tracking

■ Millisecond Log Timestamp

2018-04-16	05:59:28.892
2018-04-16	05:59:28.892
2018-04-16	05:59:28.924
2018-04-16	05:59:28.934
2018-04-16	05:59:28.962
2018-04-16	05:59:28.997

Mail Queue Spam Outbreak Virus Outbreak FortiSandbox Dead Mail

List View Delete Send Download Search... Clear

Records per page: 50

Client IP	Envelope From	Envelope To	Subject	Session ID	Received
217.206.228.170	PurchasingPF2@wickhill.co.uk	po_germany@fortinet.com	Wick Hill Ltd Purchase Order 1190342	w0BG87aN012353-w0BG87aO012353	Thu, Jan 11, 2018 08:08:0...
40.107.1.101	Order_se@exclusive-networks.com	sweden-sales@fortinet.com	PO180145 - Xite	w0BG7WOF011833-w0BG7WOH01183...	Thu, Jan 11, 2018 08:07:3...
217.206.228.170	PurchasingPF2@wickhill.co.uk	po_germany@fortinet.com	Wick Hill Ltd Purchase Order 1190339	w0BG7KNQ011705-w0BG7KNR011705	Select All Clear Selection Message Tracking

System Quarantine

Back View Delete Release...

Records per page: 50 Filter: Unreleased

Subject	From	To	Rcpt To	Received
Fwd: Any support/restrict file typ...	Simon Yu <simonyu@fortinet.com>	"zarif@fortinet.com" <zarif@forti...	zarif@fortinet.com	View
Subject: Quote For 1000T Slop Ta...	"China Marine Bunker(Petro Chi...	undisclosed-recipients;;	hkim@fortinet.com	Select All Clear Selection Message Tracking Delete
RE:PV OIL JUPITER / JVL Agro// ...	"SHINJUNG-TMS CO., LTD" <spar...	undisclosed-recipients;;	virus_suspicious@ott-fo	

Cross Search Logs from Mail Queues and Quarantine

Mail Queue Spam Outbreak Virus Outbreak FortiSandbox Dead Mail Message Tracking result: w0BG7KNQ011705-w0BG7KNR011705

Records per page: 100 View Download

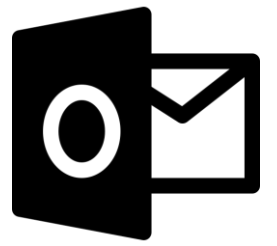
Log Type	Date	Time	Classifier	Dispositi...	From	Header F...	To	Subject	Client	Message
History	2018-01-...	08:09:01	User Safe	Accept;D...	Purchasin...	purchasin...	po_germa...	Wick Hill ...	mail.wick...	
Mail Event	2018-01-...	08:07:23								from=<PurchasingPF2@wickhill.co.uk>, size=224580, clas
Mail Event	2018-01-...	08:09:01								to=<archive2pnc> stat=Sent
Mail Event	2018-01-...	08:09:03								to=archive@mailarchiva.corp.fortinet.com, delay=00:00:02
Mail Event	2018-01-...	08:09:06								to=po_germany@fortinet.com, delay=00:00:05, xdelay=00
AntiSpam	2018-01-...	08:07:23			Purchasin...		po_germa...	Wick Hill ...	mail.wick...	po_germany@fortinet.com Personal safe list: purchasing@v
AntiSpam	2018-01-...	08:09:01			Purchasin...		po_germa...	Wick Hill ...	mail.wick...	po_germany@fortinet.com Personal safe list: purchasing@v

Log Cross Search

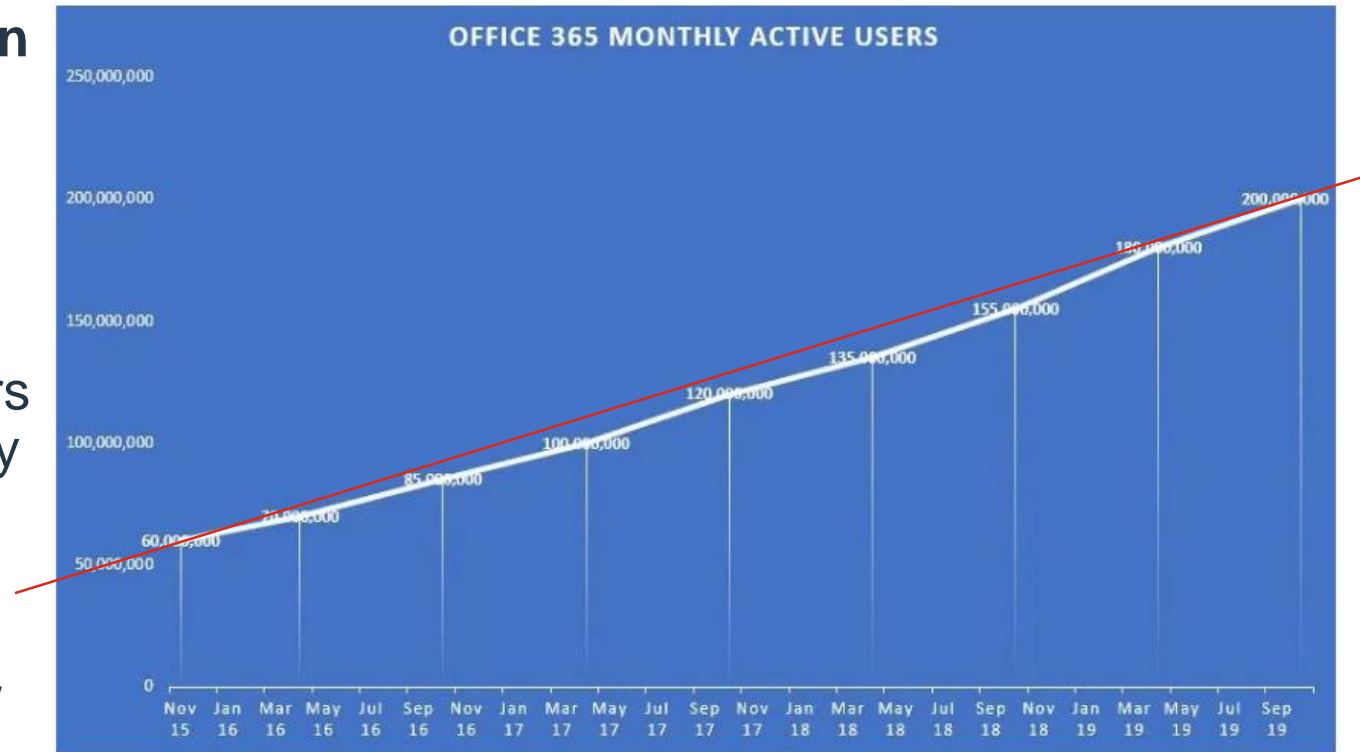
FortiMail

What about Office 365?

Office 365



- **E-mail is driving the Office365 migration**
 - Adoption is ever-increasing
- **Integrated security could be better**
 - More than 50% of Office365 customers use third party Secure E-mail Gateway solutions (according to Gartner)
- **FortiMail protecting Office365 can offer**
 - Better security and visibility
 - Remediation features



Office 365 - Customer's feedback

"Spam Filtering From Microsoft Should Be The Best!But It Is Far From It."

Submitted: November 26, 2018

0 of 1 found this review helpful.

☆☆☆☆ Overall User Rating

Product(s): Microsoft Exchange Online Protection (EOP)

Overall Comment: "I feel that a spam filter from a company like Microsoft should be the best of the best, but ever since switching it has been a headache. The "new" console is unreliable and always freezes or doesn't show all of your information. You have to constantly refresh the screen to make sure you aren't missing anything. Things like simply adding a domain to the global safe sender list have to be done multiple times and double checked to make sure it works. The reporting console is also unreliable and often dies on you. I also don't feel that the reporting product has a lot of potential, but it falls short in many areas."

Office 365 Advanced Threat Protection

☆☆☆☆

Nov 6, 2019

Reviewer Role
R&D/Product Development

Good but need more security

— Software Developer in the Services Industry

Overall a good product but many malicious emails are still getting through to the organization.....

- Difficulty in addressing Spam and Phishing issues
- Complex Web UI and reportedly not always reliable console

Office 365 - Exchange Online Protection

- Customers report **poor recognition of phishing attempts**, including attacks that impersonate Microsoft Outlook and SharePoint which contain links leading to dangerous payloads
- **No concept of System Quarantine.** The default EOP configuration move malicious content (including viruses) to users Junk folder who can easily release messages.
- Threat Reports in the security and compliance center focus on malware and spam but ignore other non malware based attached including credential phishing and email fraud.
- **Limited Quarantine handling** and report frequency

Office 365 - Perceived strengths and weaknesses

Strengths	Weaknesses
<ul style="list-style-type: none">▪ Native Office365 integration for email security▪ Ease of use, scalability, and integration with Office365▪ EOP has a large number of deployments, making it a popular choice (155 million)	<ul style="list-style-type: none">▪ Complex licensing structure - many different plans at different price points. Difficult for customers to understand exactly what security features they are getting with what plans▪ Expensive: ATP-1 \$24, ATP-2 \$60 and Office365 Enterprise E5 \$420 /year/user▪ Challenges with Hybrid Cloud implementation▪ Features and functionalities are accessed and managed through different consoles▪ Customers still report high degrees of spam, malware and other forms of attacks▪ High False Positive rate▪ Capability to block phishing is poor. Customers need to create custom rules▪ Multiple OEM AV Engines▪ Sandbox has limited file type support with limited reporting







Independent Testing

Fortinet FortiMail (5 out of 5)




Microsoft (1 out of 5)




Fortinet Result	Test	Microsoft
 99.97%	<i>Virus Bulletin VBSpam</i>	DNP
 99.6%	<i>ICSA Labs ATD Email</i>	DNP
 97.8%	<i>NSS Labs Breach Prevention</i>	DNP
 99.0%	<i>NSS Labs Breach Detection</i>	DNP
 AAA Rating 93%	<i>SE Labs Email Security Services</i>	B Rating- 35% Accuracy 

- Symantec Email Security .cloud with ATP
- Proofpoint Essentials Advanced
- Fortinet FortiMail Cloud - Gateway Premium



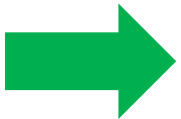
- Microsoft Office 365 Advanced Threat Protection



EXECUTIVE SUMMARY			
Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Symantec Email Security .cloud with ATP	97%	100%	98%
Proofpoint Essentials Advanced	98%	97%	98%
Fortinet FortiMail Cloud - Gateway Premium	92%	100%	93%
Microsoft Office 365 Advanced Threat Protection	20%	95%	35%
Microsoft Office 365	-15%	100%	8%

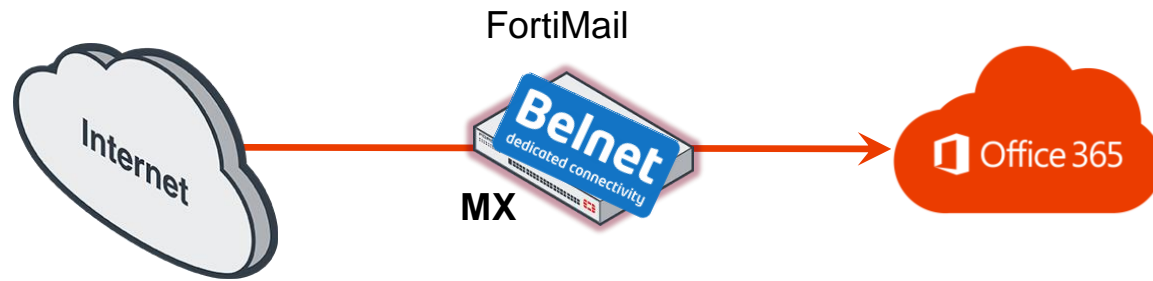
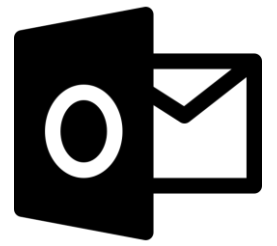
SE Labs Summary - March 2020

EXECUTIVE SUMMARY				
Product	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)
Perception-Point	2,603	700	3,303	94%
Fortinet FortiMail	2,525	640	3,165	90%
Mimecast Secure Email Gateway	2,412	700	3,112	89%
Kaspersky Security for Office 365	1,681	550	2,231	64%
Google G Suite Enterprise	956	505	1,461	42%
Google G Suite Business	825	535	1,360	39%
Microsoft Office 365	463	550	1,013	29%
Microsoft Office 365 Advanced Threat Protection	426	550	976	28%

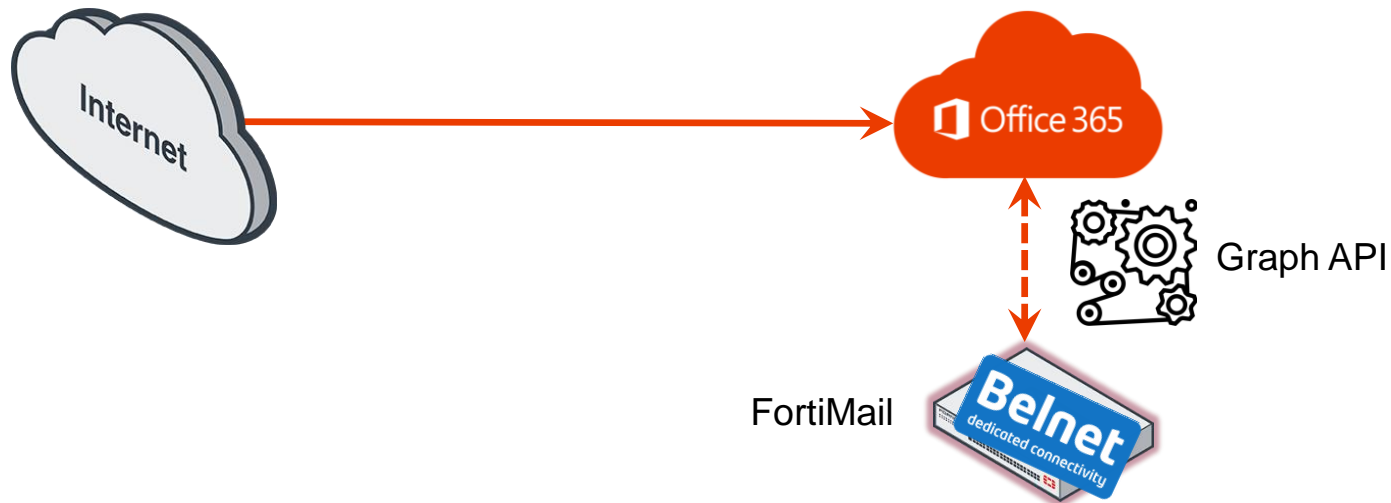


Products highlighted in green were the most accurate, scoring 40 per cent or more for Total Accuracy. Those in orange scored between 20 to 40 per cent. Any products shown in red scored less than 20 per cent.

FortiMail with Office 365 architectures



Inline Mode

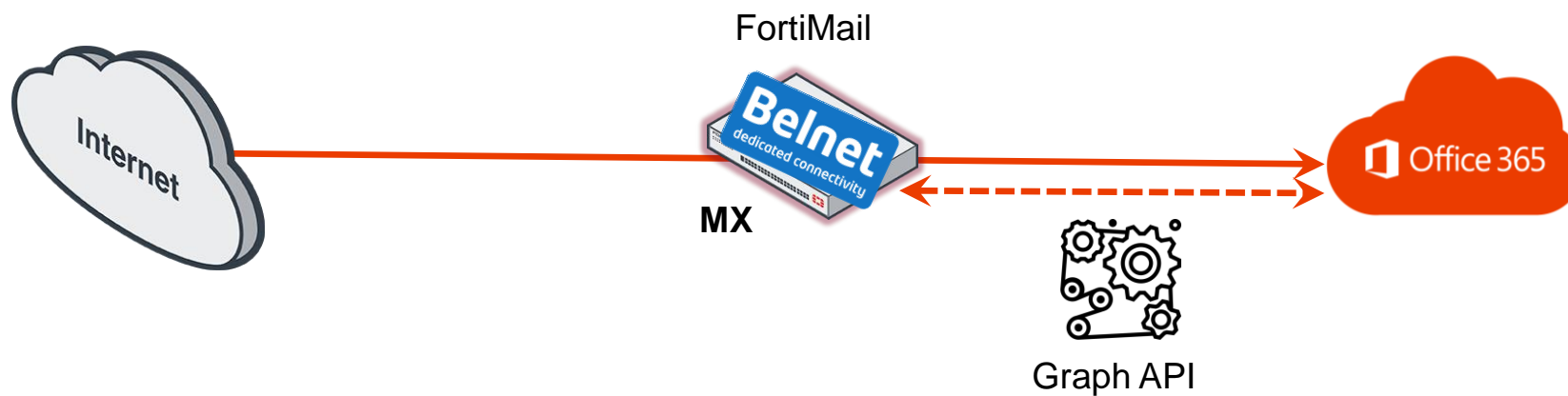


Off Path Mode

FortiMail with Office 365 architectures



Mixed Mode (Inline + API)



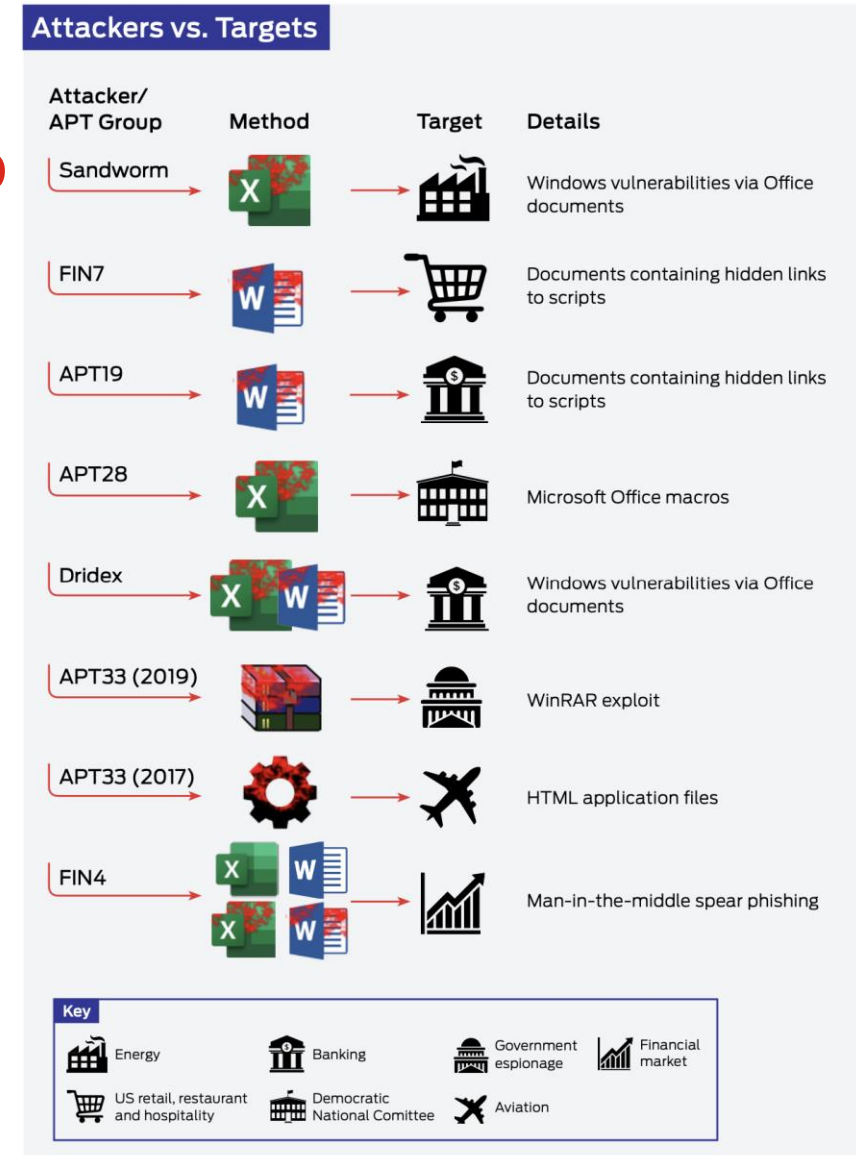
FortiMail

Key Features

Aligning with Market Needs and Recommendations

Making sure new techniques are relevant to today's evolving threat landscape:

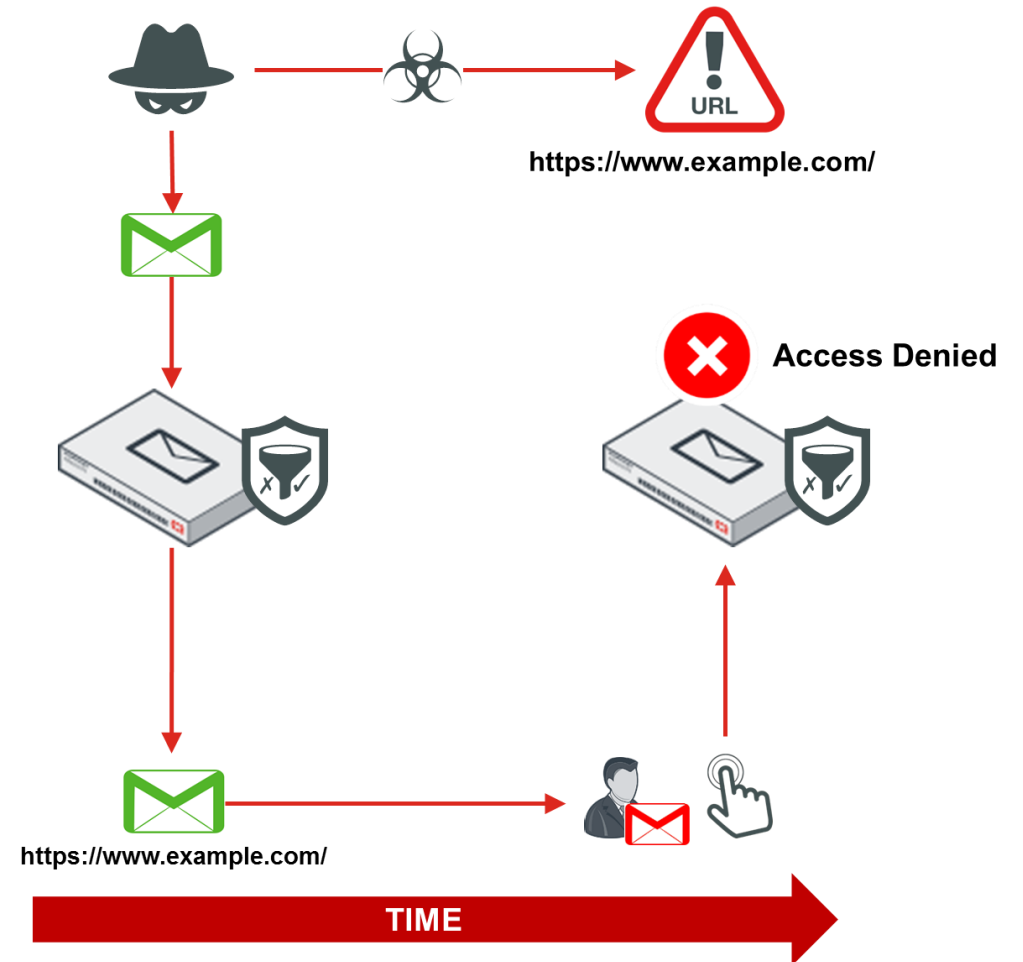
- Time-of-Click and URL Removal
- Content Disarm and Reconstruction
- Business Email Compromise
- Geo-IP capabilities
- Identity Based Encryption



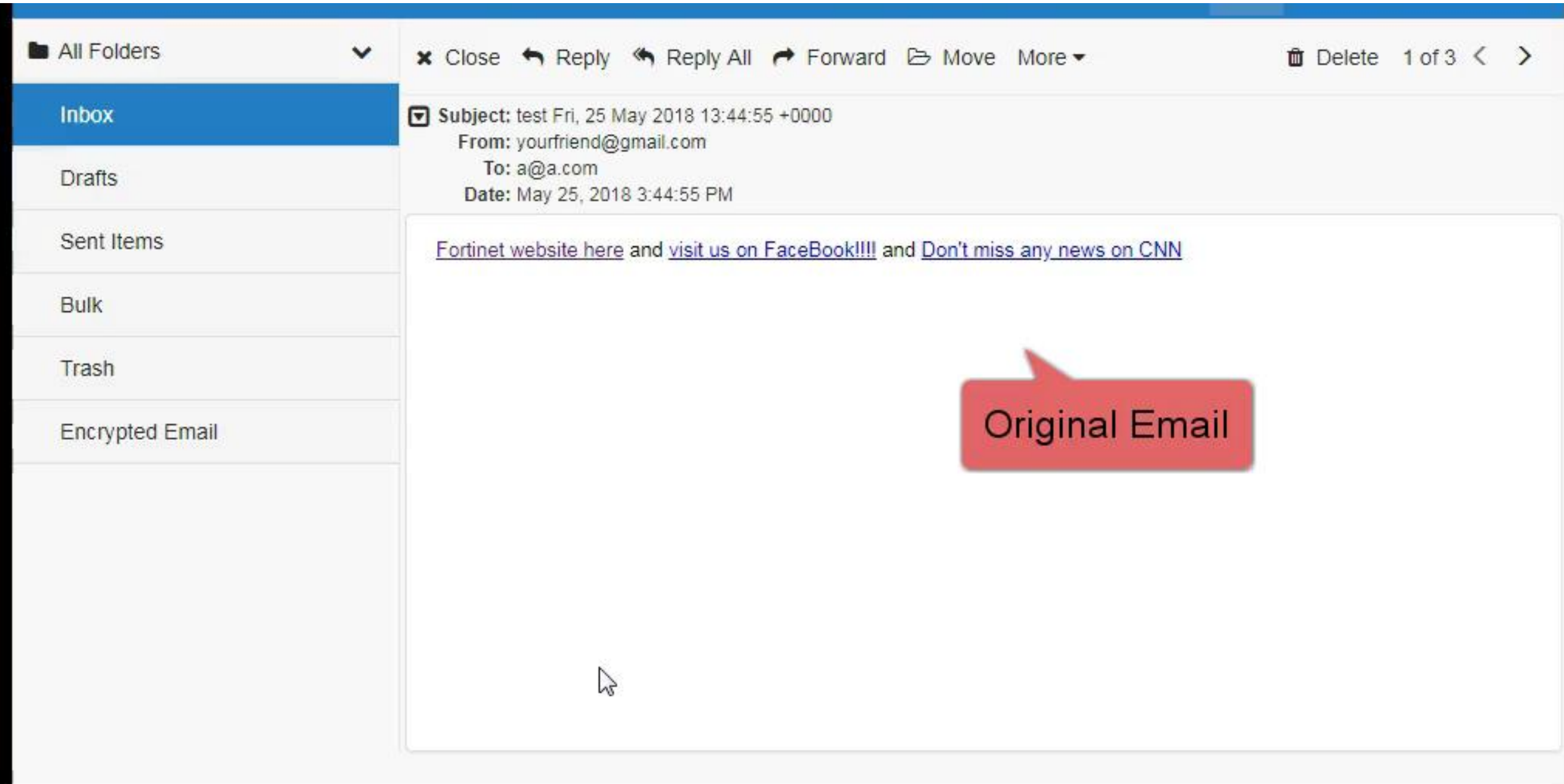
(view of some of some attacks used in SE Labs independent testing)

Time-of-Click Protection

- URL's are rewritten to point at FortiMail
- FortiMail rescans when links are clicked to detect status change since first rating



Time-of-Click Protection - Demo



The screenshot displays an email client interface. On the left, a sidebar lists folders: All Folders, Inbox (selected), Drafts, Sent Items, Bulk, Trash, and Encrypted Email. The main area shows an email with the following details:

- Subject: test Fri, 25 May 2018 13:44:55 +0000
- From: yourfriend@gmail.com
- To: a@a.com
- Date: May 25, 2018 3:44:55 PM

The email body contains the text: [Fortinet website here](#) and [visit us on FaceBook!!!!](#) and [Don't miss any news on CNN](#). A red callout box with the text "Original Email" is positioned over the main content area, pointing to the email body.

Time-of-Click Protection: logs

Log Type	Date	Time ▲	Classifier	Dispositi...	From	Header F...	To	Subject	Client IP	Client Na...	Source	Message
Mail Event	2018-10-01	11:50:31.854										from=<yourfriend@gmail.com>, size=861, class=0, nrcpts=1, msgid=...
AntiSpam	2018-10-01	11:50:32.190			yourfrien...		a@a.com	test Mon, ...	10.0.0.66			Detected by Attachment Filter. Content disarm
History	2018-10-01	11:50:32.191	Attachme...	Modify S...	yourfrien...	yourfrien...	a@a.com	test Mon, ...	10.0.0.66		External	
Mail Event	2018-10-01	11:50:32.226										STARTTLS=client, relay=a.com., version=TLSv1.2, verify=OK, cipher...
Mail Event	2018-10-01	11:50:32.568										to=<a@a.com>, delay=00:00:01, xdelay=00:00:00, mailer=esmtpl, pri...
AntiSpam	2018-10-01	12:07:08.043					a@a.com			10.0.0.1		URI Protect Passed: received at Mon, 01 Oct 2018, received categor...
AntiSpam	2018-10-01	12:09:47.317					a@a.com			10.0.0.1		URI Protect Blocked: received at Mon, 01 Oct 2018, category: 37, cli...
AntiSpam	2018-10-01	12:10:01.653					a@a.com			10.0.0.1		URI Protect Passed: received at Mon, 01 Oct 2018, received categor...

Date=2018-10-01

Time=12:10:01.653

To=a@a.com

Client Name=10.0.0.1

Message=URI Protect Passed: received at Mon, 01 Oct 2018, received category: 36, clicked category: 36, http://www.cnn.com

Session ID=w919oV12004663-w919oV13004663

Content Disarm and Reconstruction

- General Observation:
 - Sandboxing can possibly impact real-time business flows (introducing delay)
- Complementing Solution:
 - Incoming E-mail will be
 - disarmed (harmful content is disabled)
 - reconstructed
 - forwarded
 - Original attachment can be delivered to user quarantine
- CDR considered an essential complement to Sandboxing in ATP



Content Disarm and Reconstruction

Remove macros

Content Profile

Domain:

Profile name:

Action: + New... Edit...

- + Attachment Scan Rules
- + Scan Options
- Content Disarm and Reconstruction**
 - Action:
 - HTML content ⓘ
 - Text content
 - MS Office ⓘ
 - PDF ⓘ
- + Archive Handling
- + File Password Decryption Options
- + Content Monitor and Filtering

example.docm - Microsoft Word

File Home Insert Page Layout References Mailings Review View Developer

Pages Tables Illustrations Links Header & Footer Text Symbols

DOCM test file

Purpose: Provide example of this file type
Document file type: DOCM
Version: 1.0
Remark:

Example content: <https://www.playboy.com>

Test Data:	
1	
1	
2	
3	
4	

The names "John Doe" for males, "Jane Doe" or "Jane Roe" for females, or "Jonnie Doe" and "Janie Doe" for children, or just "Doe" non-gender-specifically are used as placeholder names for a party whose true identity is unknown or must be withheld in a legal action, case, or discussion. The names are also used to refer to a corpse or hospital patient whose identity is unknown. This practice is widely used in the United States and Canada, but is rarely used in other English-speaking countries including the United Kingdom itself, from where the use of "John Doe" in a legal context originates. The names Joe Bloggs or John Smith are used in the UK instead, as well as in Australia and New Zealand.



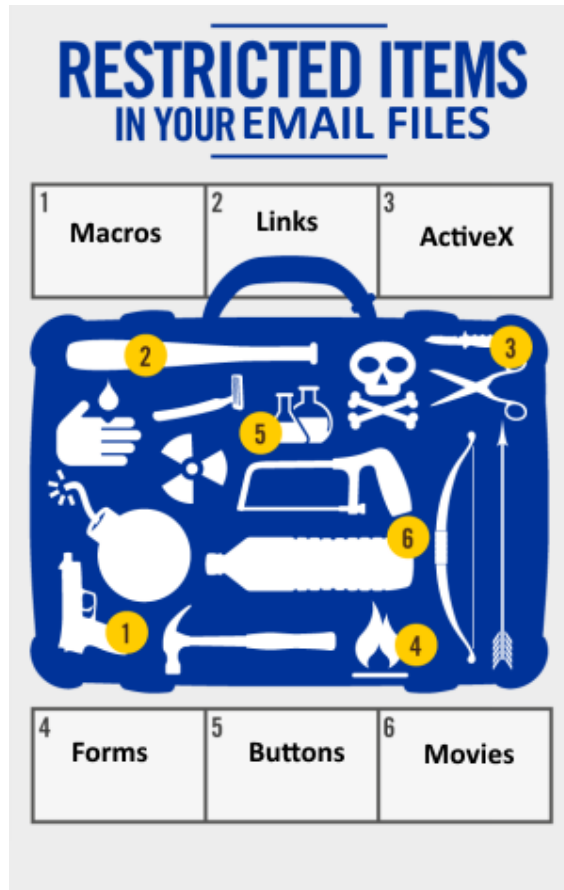
Neutralize URLs



Remove embedded content

Content Disarm and Reconstruction

- Formats and Active Functions can be selected



```
config file content-disarm-reconstruct
set component-type-options ?
end
```

```
...
office-dde                strip Dynamic Data Exchange fields in Microsoft Office documents
office-embedded-object    strip embedded objects in Microsoft Office documents
office-hyperlink          strip hyperlinks in Microsoft Office documents
office-linked-object      strip linked objects in Microsoft Office documents
office-macro              strip macros in Microsoft Office documents
pdf-action-form           strip actions that submit data to other targets in PDF documents
pdf-action-gotor         strip links to other PDF documents in
...
```

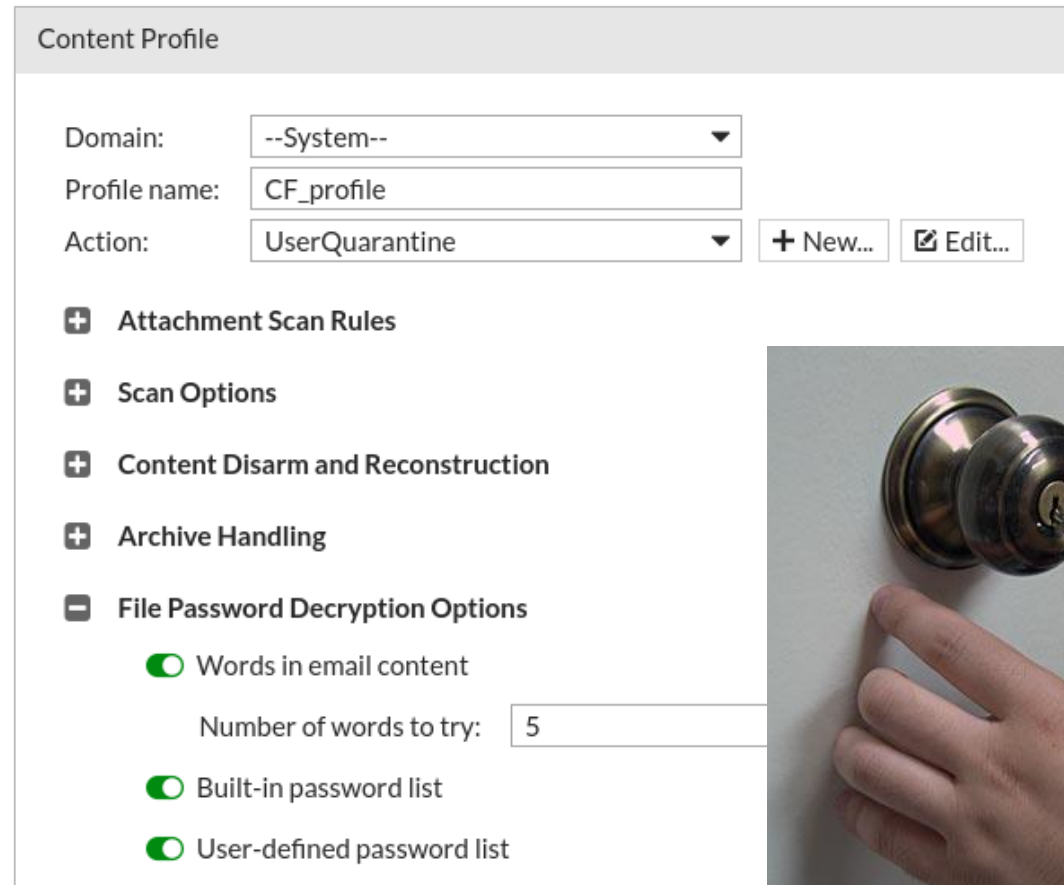

Password Protected and/or Encrypted Attachments

FortiMail can be made capable of giving visibility on password protected/encrypted attachments:

- PDF
- Archive
- Office files

Using keywords from:

- mail body
- built-in password list
- user-defined password list



Content Profile

Domain: --System--

Profile name: CF_profile

Action: UserQuarantine + New... Edit...

- + Attachment Scan Rules
- + Scan Options
- + Content Disarm and Reconstruction
- + Archive Handling
- File Password Decryption Options
 - Words in email content
 - Number of words to try: 5
 - Built-in password list
 - User-defined password list

Business Email Compromise

Detect spoofing of C-Level Emails (whaling attacks)

- » Identify normal Display Name/Header Address matches
- » Detect inbound email spoofing
- » Warn recipient with Subject Tag or Body Header



Mail From : Ken Xie <kxie@fortinet.com>
To : CFO@fortinet.com

Warning: Suspected Impersonation



Impersonation

Profile name:

Domain:

Impersonation Entry

[+ New...](#) [Edit...](#) [Delete](#)

[Refresh](#) [Previous](#) [Next](#) / [Next](#) [Last](#) Records per page: Selected: 1 / 1

Display Name Pattern	Pattern Type	Email Address
Ken Xie	Wildcard	ken.xie@fortinet.com

AntiSpam Profile

Domain:

Profile name:

Default action: [+ New...](#) [Edit...](#)

Scan Configurations

- FortiGuard Action:
- Greylist
- SPF check Action:
- DMARC check Action:
- Behavior analysis Action:
- Header analysis Action:
- Impersonation analysis Action:
Impersonation profile: [+ New...](#) [Edit...](#)
- Heuristic Action:
- SURBL [[Configuration...](#)] Action:
- DNSBL [[Configuration...](#)] Action:
- Banned word [[Configuration...](#)] Action:

FortiGuard Geo-IP database



- Policies based on Country Groups instead of IP
- Support custom Geo-IP to handle exceptions

GeoIP Group

Group name: CH_FR_DZ

Comment:

Country/Region: Available: (250)

Members: (3)

Members list: Switzerland, France, Algeria

Country/Region list: Afghanistan, Aland Islands, Albania, American Samoa, Andorra, Angola, Anguilla

Access Control Rule

Enabled:

Sender: User Defined

Recipient: User Defined

Source: GeoIP Group

CH_FR_DZ

+ New... Edit...

IP Based Policy

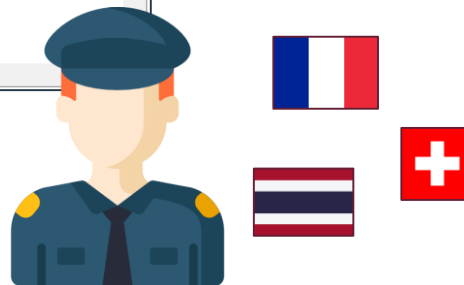
Enable:

Source: GeoIP Group CH_FR_DZ

Destination: IP/Netmask 0.0.0.0 / 0

Action: Scan

Comment:



Geo-IP capable wherever you need it

	Client IP	Location	Clier
x499fR8...	20.0.0.66	US	
-x496ok...	20.0.0.66		

FortiGuard AntiSpam Query

Query input:

Query result:

Type: IP

Location: Japan

Score: 2, Spam

Sender Reputation		Authentication Reputation
<input type="button" value="Refresh"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="text" value="1"/> / <input type="text" value="1"/> <input type="button" value="Previous"/> <input type="button" value="Next"/> Records per page: <input type="text" value="50"/>		
IP	Location	Score
1.1.111.3	JP (Japan)	16
62.192.1.1	CH (Switzerland)	10
222.165.195.75	ID (Indonesia)	0

History Log Search

Keyword:

Subject:

From:

Header From:

To:

Session ID:

Client location:

Client name/IP:

Classifier:

Disposition:

Match condition:

Start time:

End time:

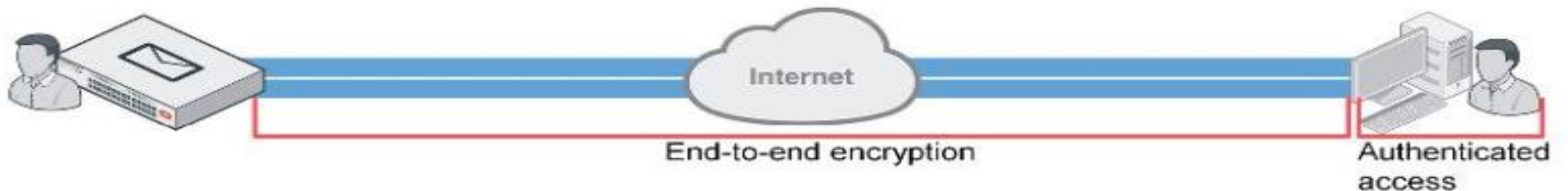
- Afghanistan (AF)
- Aland Islands (AX)
- Albania (AL)
- Algeria (DZ)**
- American Samoa (AS)
- Andorra (AD)
- Angola (AO)
- Anguilla (AI)
- Antarctica (AQ)
- Antigua and Barbuda (AG)
- Argentina (AR)
- Armenia (AM)
- Aruba (AW)
- Australia (AU)

Identity Based Encryption (IBE)

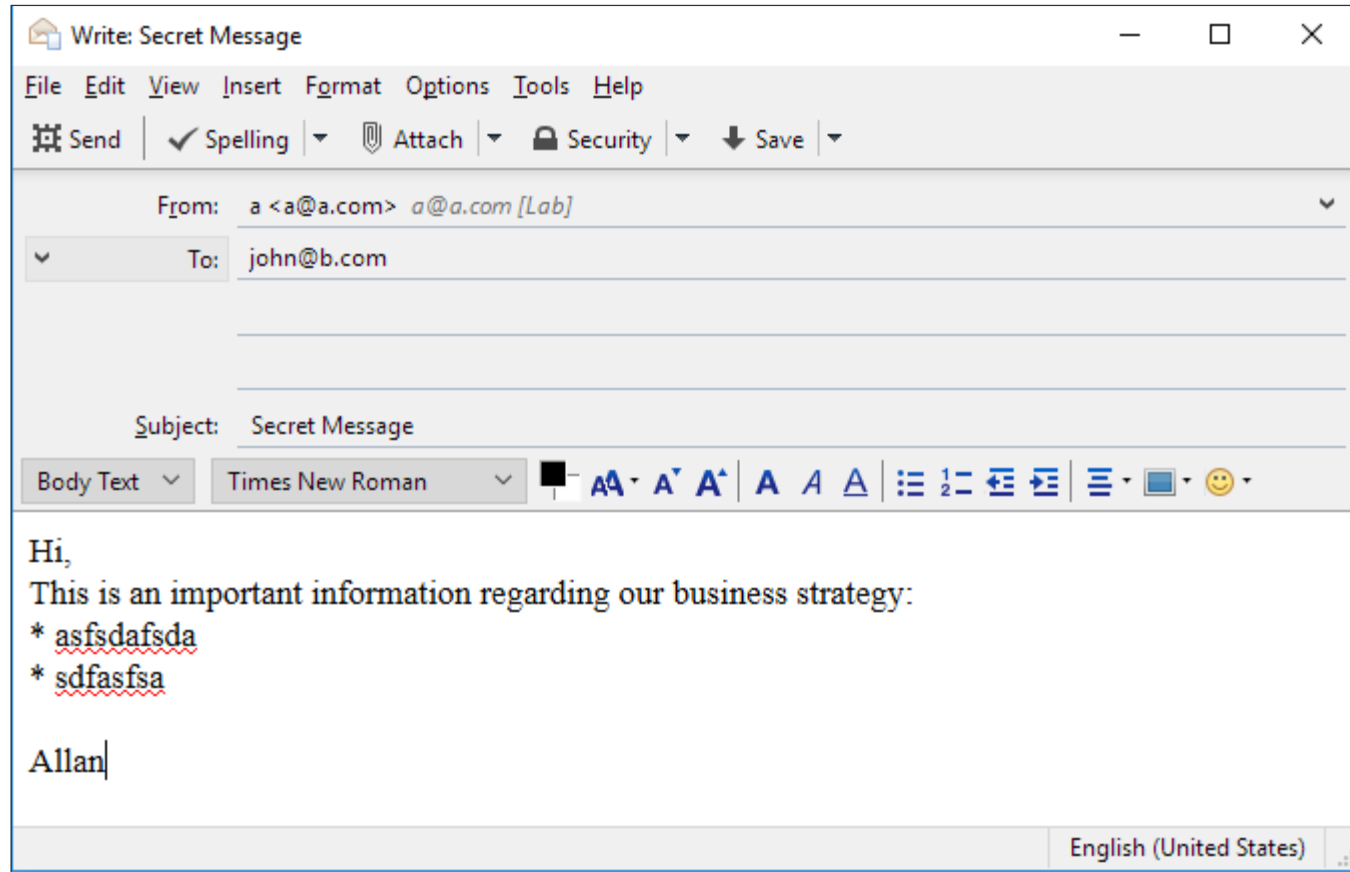
FortiMail provides Identity-Based Encryption (IBE), in addition to S/MIME and TLS/SSL, as email encryption options to enforce policy-based encryption for secure content delivery.

Benefits:

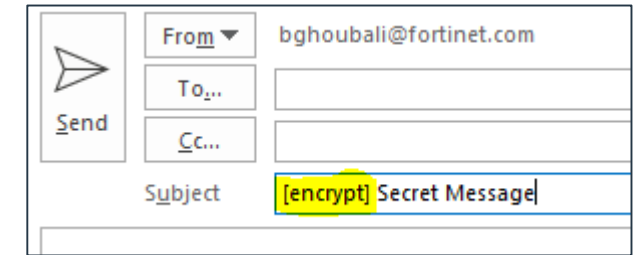
- **Security** – an extra layer of email protection and confidentiality
- **Ease of use** – as easy to use as a standard email. No need of certificate and key management for end-users and no need to install additional hardware or software.
- **Flexibility** – both Push and Pull delivery options, delivering encrypted emails directly to your users, or storing them on the FortiMail platform for retrieval, or a combination of the two options.



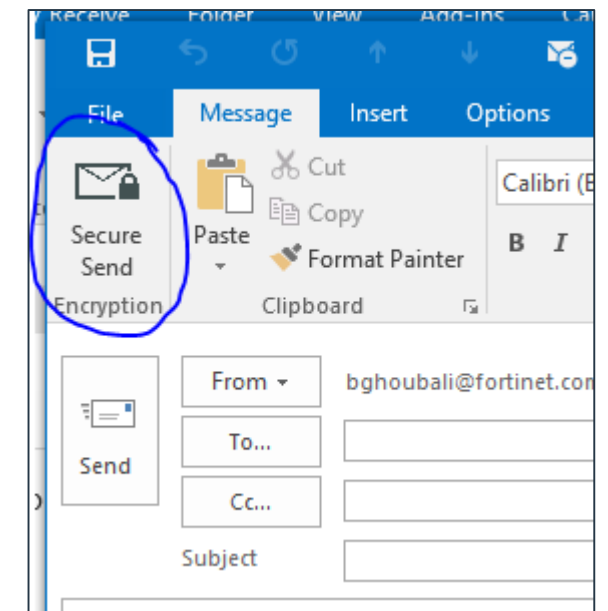
IBE Example: Client experience



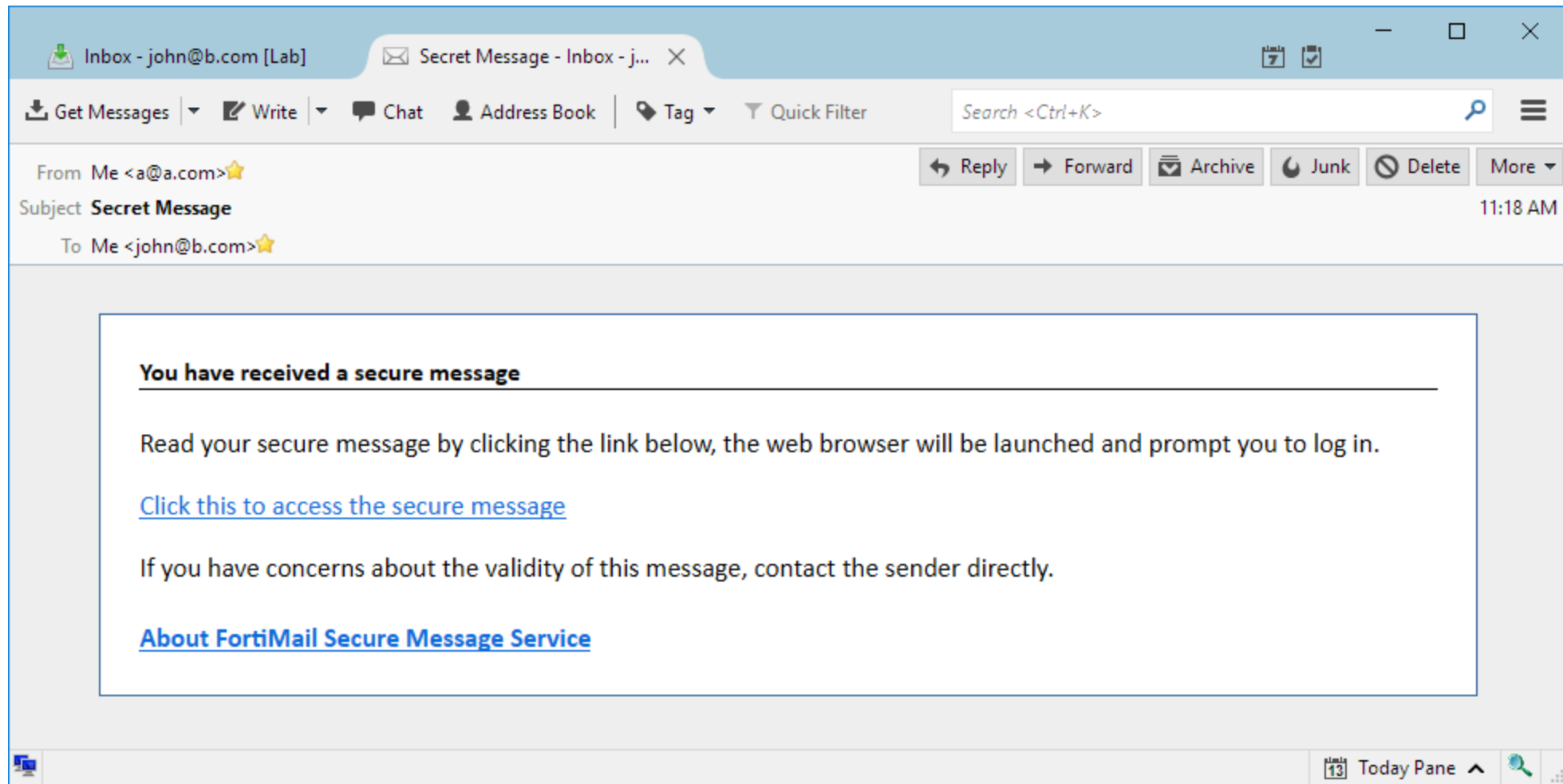
keyword

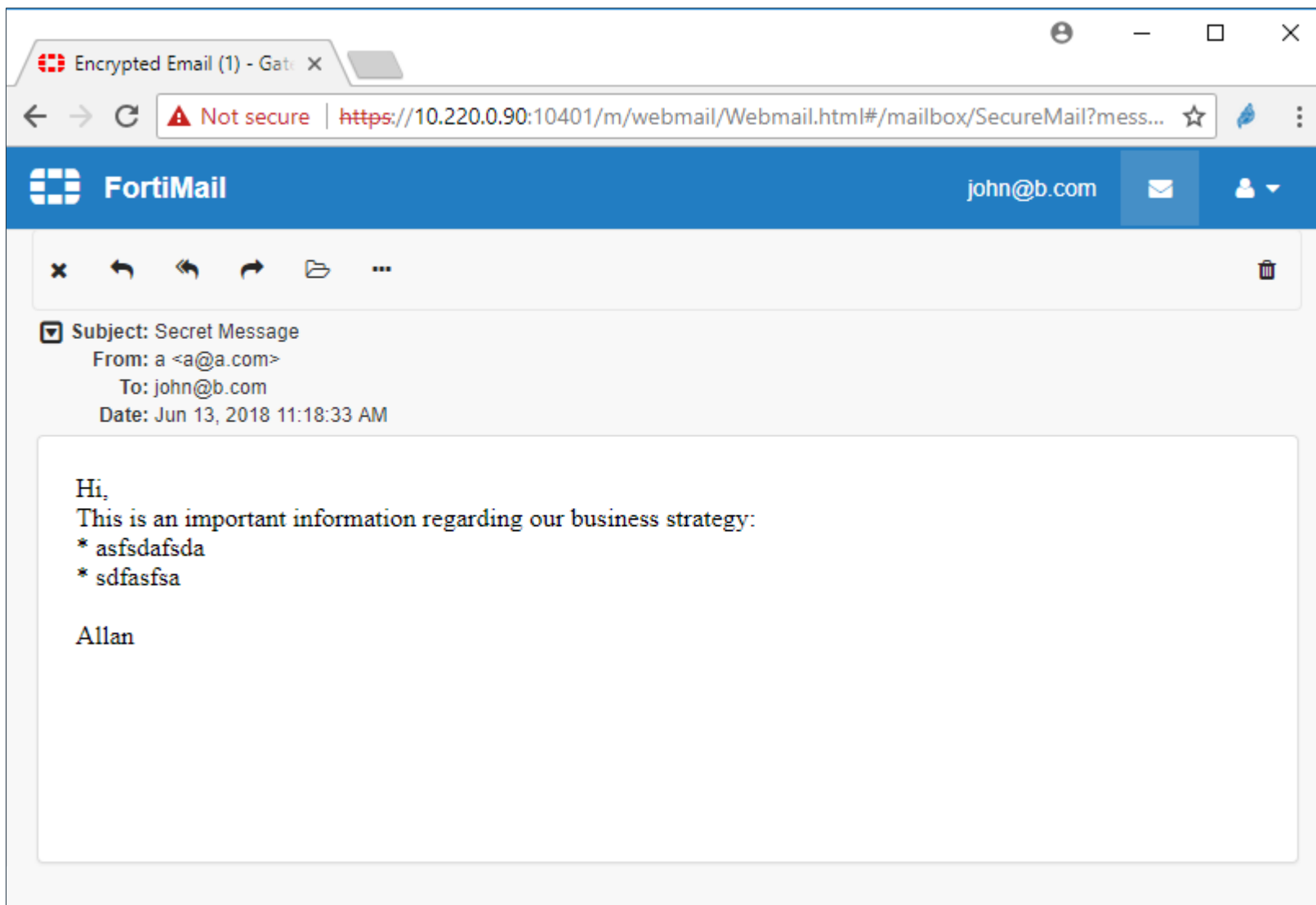


Plugin



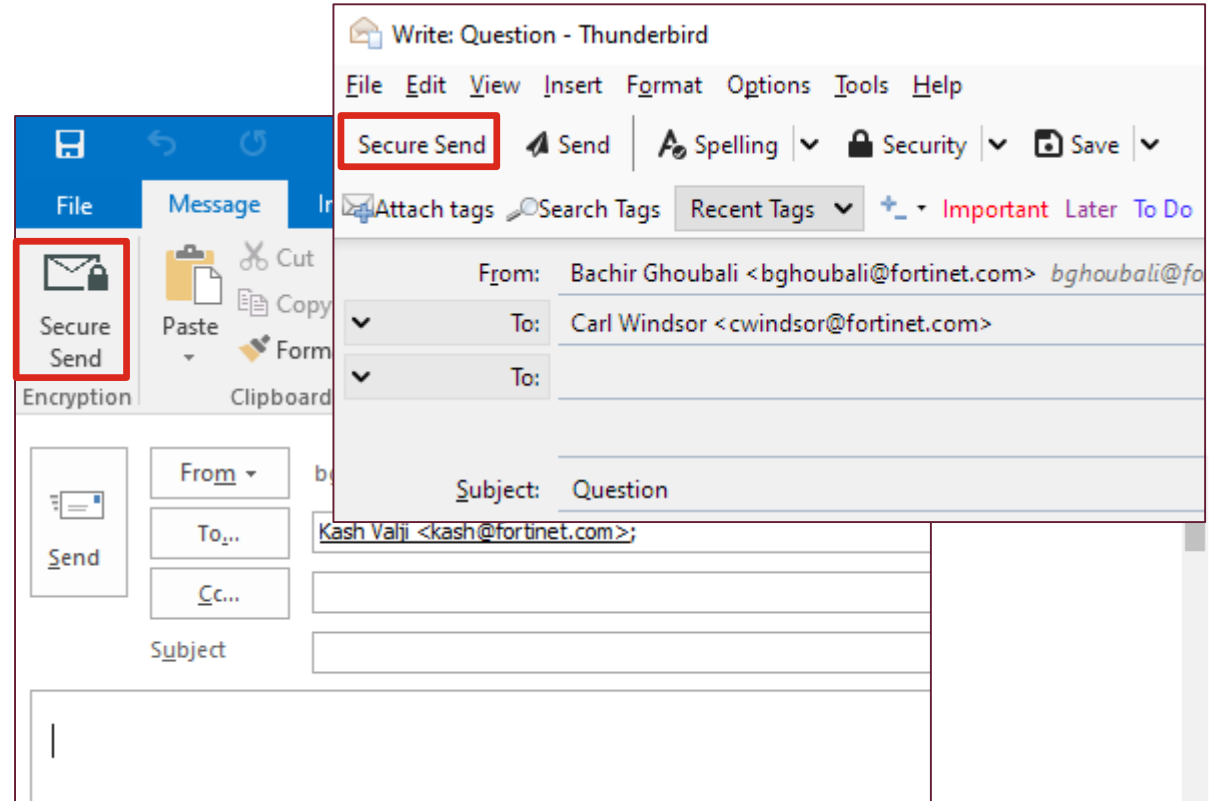
IBE Example : received email





IBE Plugin for secure e-mail sending

- Compatible with
 - Outlook 2013 / 2016
 - Thunderbird
- Sets header to trigger IBE on FortiMail



X-Mailer: Microsoft Outlook 16.0
Thread-Index: AdRgHYcBGOhPZmmjSwmHwUq41EXbpQ==
Content-Language: en-gb
x-fe-sensitivity: confidential
X-FEAS-AUTH-USER: cwindsor@fortinet.com
X-FE-BYPASS-SCAN-ON-AUTH:
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; d=fortinet.com; s=dkim; c=relaxed/relaxed;
h=from:to:subject:date:message-id:mime-version:content-type;
bh=uVPOKaQkUlfw+hdeO4taLPBe8/HcC9hQgHfQIHgjf/g=;
b=S4eudAYPHM/yobowYAnz4RbFEcaN0cAbOEtLlqiuYeaQl p0uKv727/57YH0vbrffibAYuPfd

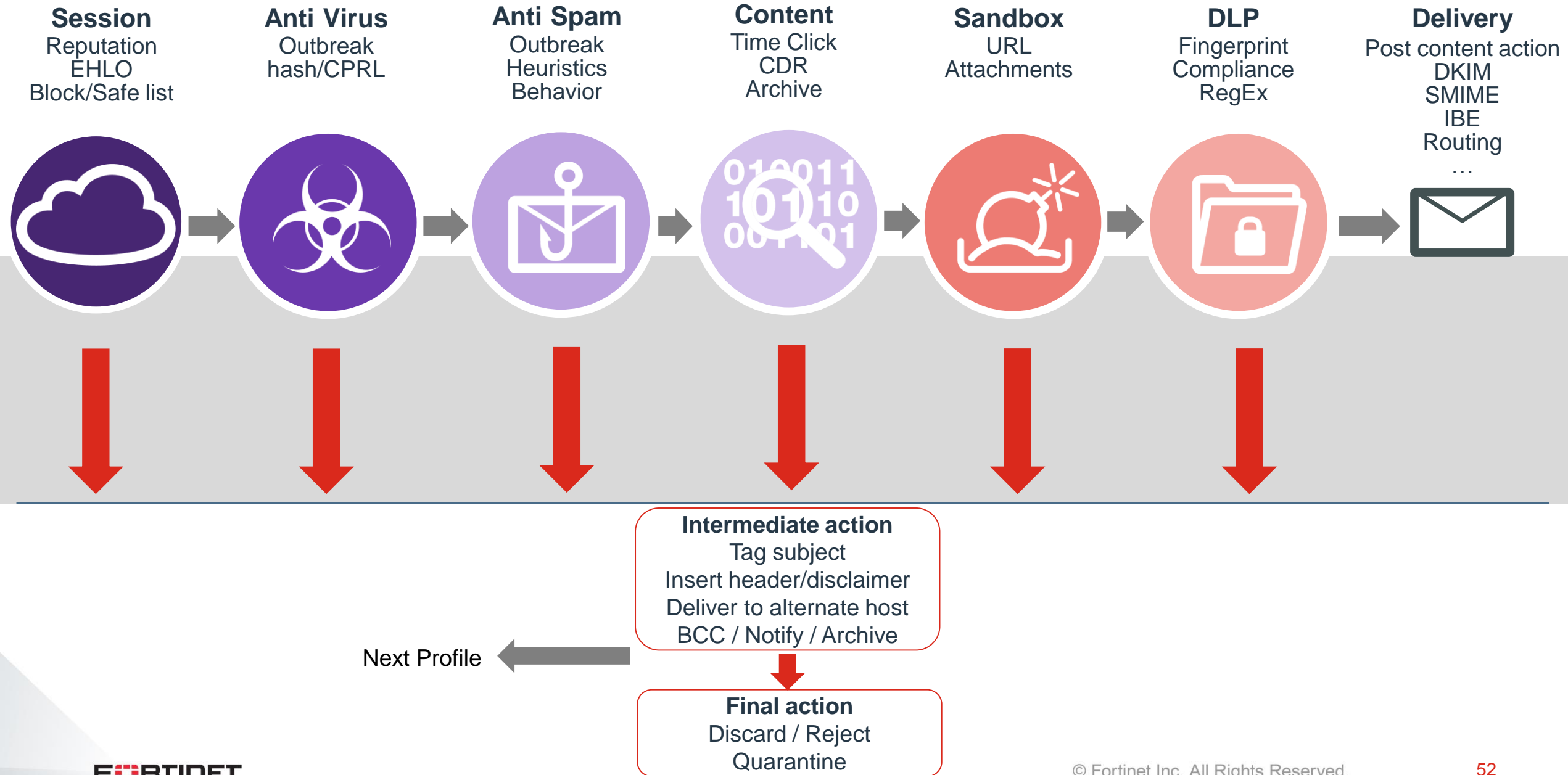
Plus many more features ... (please see docs.fortinet.com)

- Aliases / address mapping
- LDAP support
- Recipient/Sender verification
- Syslog / SNMP
- Email alerts
- High availability / Scalability cluster
- IBE / S-MIME Encryption & Signing
- Archiving
- DLP – Data Loss Prevention
- Backscatter prevention
- Disclaimer insertion
- UI Customization/internationalization
- DSN – Delivery Status Notification
- Deferred delivery (inbound/outbound)
- Network Access Control
- Rate Limiting in/out
- Sub-domain support
- DKIM/SPF/DMARC
- Brute force document decrypt
- SSO – Single Sign On
- ...

FortiMail

Typical Mail Flow

Typical e-mail flow FortiMail – Going through the profiles...



Resources

- Online documentation
 - <https://docs.fortinet.com>
- API documentation
 - <https://fndn.fortinet.net>
- NSE Training / NSE 6 Fortimail
 - <https://training.fortinet.com>



FORTINET. | **NSE** Institute

FORTINET®