

**Fortimail: решения для защиты
электронной почты**

Мажидов С.

Представление FortiMail



**Шлюз безопасности
электронной почты**

**Швейцарский нож для защиты почты
Умеет почти все, и с ним легко работать**

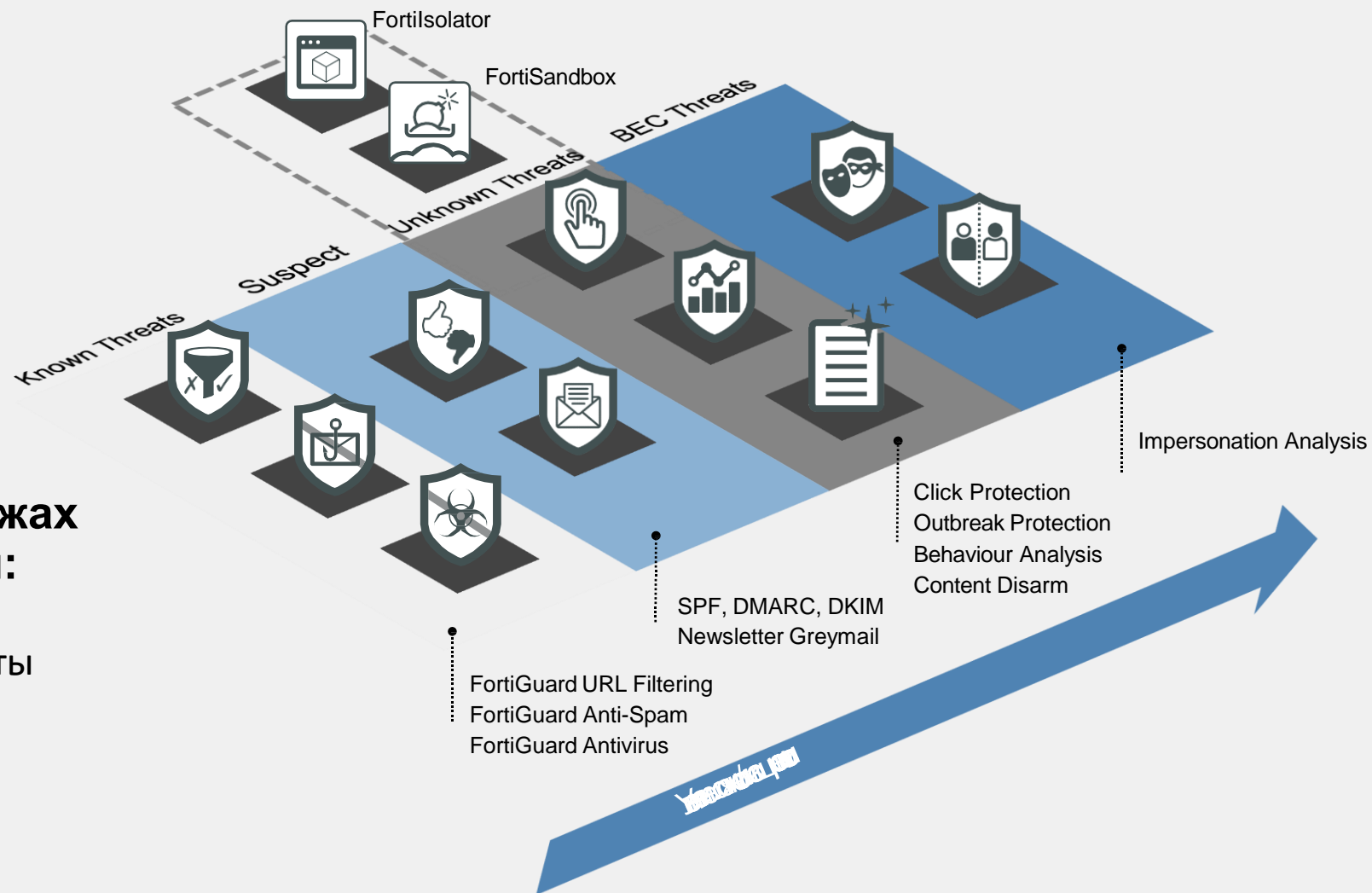
**Наивысшая эффективность
Лидер независимых тестов ICSA Labs, SE Labs,
Virus Bulletin по противодействию спаму,
фишингу, вредоносному ПО**

**Интегрирован в Fortinet Security Fabric
Все этапы жизненного цикла атаки в
разрезе инфраструктуры предприятия**

Снижает риск и ущерб от инцидентов безопасности, связанных с EMAIL, для инфраструктуры предприятия



FortiMail шлюз безопасности электронной почты



Противодействие на 4 рубежах защиты электронной почты:

1. Известные отправители/объекты
2. Подозрительные отправители
3. Угрозы нулевого дня
4. Попытки подмены личности, компрометация бизнес почты



FortiMail обзор функционала



Виды Угроз

Spoofing - называется практика злоумышленников маскироваться под конкретного пользователя или подключенного к сети устройства с целью похищения данных, распространения вредоносного ПО или обхода механизмов контроля доступа. Самой распространенной спуффинг атакой является Email спуффинг

Ransomware - Программа-вымогатель, программа-шантажист — тип зловредного программного обеспечения, предназначен для вымогательства, блокирует доступ к компьютерной системе или предотвращает считывание записанных в нём данных

Фишинг — рассылка массовых электронных писем от имени популярных брендов, а так же личных сообщений внутри различных сервисов. Например от имени банков или работников компании

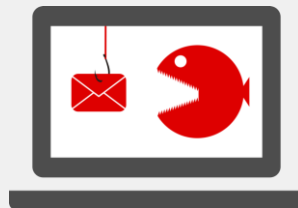
Спам — это **нежелательные сообщения в любой форме**, которые отправляются в большом количестве. Чаще всего спам отправляется в форме коммерческих электронных писем, присланных на большое количество адресов, а также через мгновенные и текстовые сообщения (SMS), социальные медиа или даже голосовую почту.

Проблемы безопасности электронной почты



Вредоносное ПО

1. 92,4% вредоносов доставляется через email
2. Расчет на кол-во или на вредоносы нулевого дня
3. Цель – неопытные пользователи – жертвы рассылок
4. Техники социальной инженерии



Фишинг

- 4% пользователей пройдут по любой ссылке
- Содержимое адаптировано и очень правдоподобно
 - Цель – конкретная организация и ключевые сотрудники
- Техники социальной инженерии



Утечка данных

1. Разглашение коммерческой тайны
2. Отправка конфиденциальной информации без шифрования
3. Корпоративный шпионаж
4. Ущерб репутации компании

Электронная почта основной вектор угрозы



Люди

82%

Процент нарушений, связанных с человеческим фактором, включая «использование украденных учетных данных, фишинг, неправомерное использование или просто ошибку».



Email

36% →

Процент нарушений, в которых электронная почта была «вектором действия» для социальных атак или вредоносных программ.



Ransomware

25% ↑

Процент взломов, связанных с программами-вымогателями, вырос примерно с 12 % в предыдущем году*.



BEC

58%

Процент атак с компрометацией деловой электронной почты (BEC), которые привели к потере денег, по данным Verizon DBIR за 2021 год.

All statistics are from Verizon Data Breach Investigations Report 2022, except for the BEC reference which is from the 2021 DBIR report.



Защита от спама

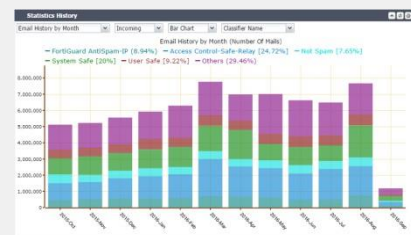
Антиспам/Антифишинг

• Сервис репутации FortiGuard

- Облачная база данных об отправителях и контенте спам писем
 - Репутационные сервисы: антивирус, антиспам, Категорирование URL
 - Репутация IP адресов отправителей
 - Фильтрация Основной доли спама с минимальными затратами

• Advanced Filtering Techniques

- Выявление новых кампаний по рассылке спама
- Анализ заголовков
- Эвристический анализ
- Репутация отправителя
- Определение маскировки под рассылки
- DKIM / SPF / DMARC
- Детектирование нежелательного ПО



Fortinet FortiMail contd.

Final score: 99.997

Project Honey Pot SC rate: 99.995%

Abusix SC rate: 99.999%

Newsletters FP rate: 0.0%



Противодействие таргетированным атакам

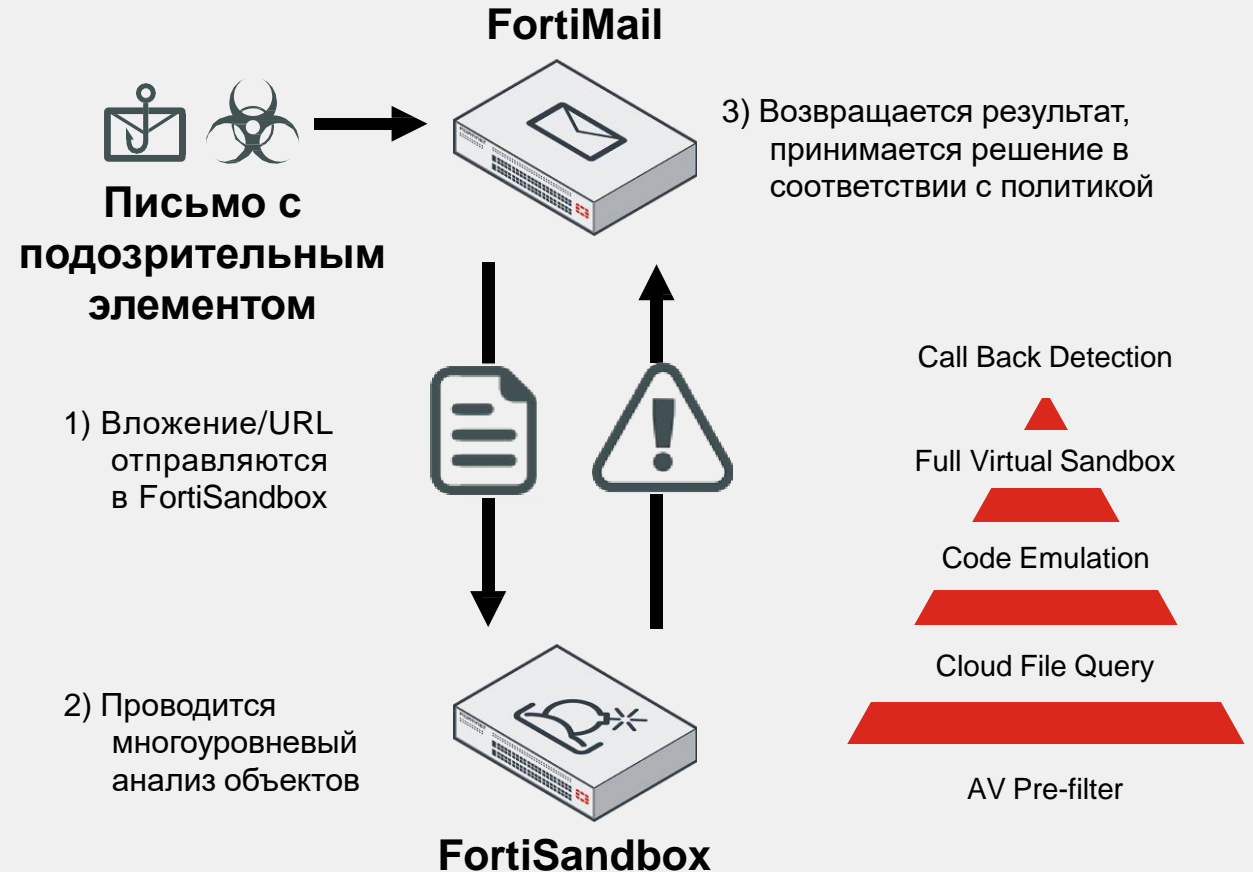
Анализ в песочнице FortiSandbox

Песочница локальная или в облаке

- FortiSandbox Cloud входит в Enterprise подписку

FortiMail помещает письмо в очередь и отправляет вложения и URL на анализ

- Статический сигнатурный и эвристический анализ
- Запрос репутации в облаке FortiSandbox Cloud
- Динамический анализ в виртуальной среде
- Выявление попыток связи с C&C
- Многоуровневое кэширование результатов



Нейтрализация контента и работа с архивами

Разоружение и Реконструкция

Нейтрализация активного контента во вложениях (PDF, Office)

- Удаление макросов, скриптов встроенных активных объектов из вложений (“Разоружение” и “Реконструкция”)
- Удаление\замещение вредоносных URL
- Исходное вложение может быть помещено в пользовательский карантин

Распаковка запароленных архивов, PDF и офисных документов

- Преднастроенный список паролей
- Поиск паролей в теле письма
- Можно загрузить свой список паролей

The screenshot shows a Microsoft Word document titled "example.docm - Microsoft Word". The document content includes a title "DOCX test file", a purpose statement, document type "DOCX", version "1.0", and a remark. An example content line contains a URL: <https://www.playboy.com>. Below this is a table with the following data:

| Test Data: | | | |
|------------|--|--|--|
| 1 | | | |
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |

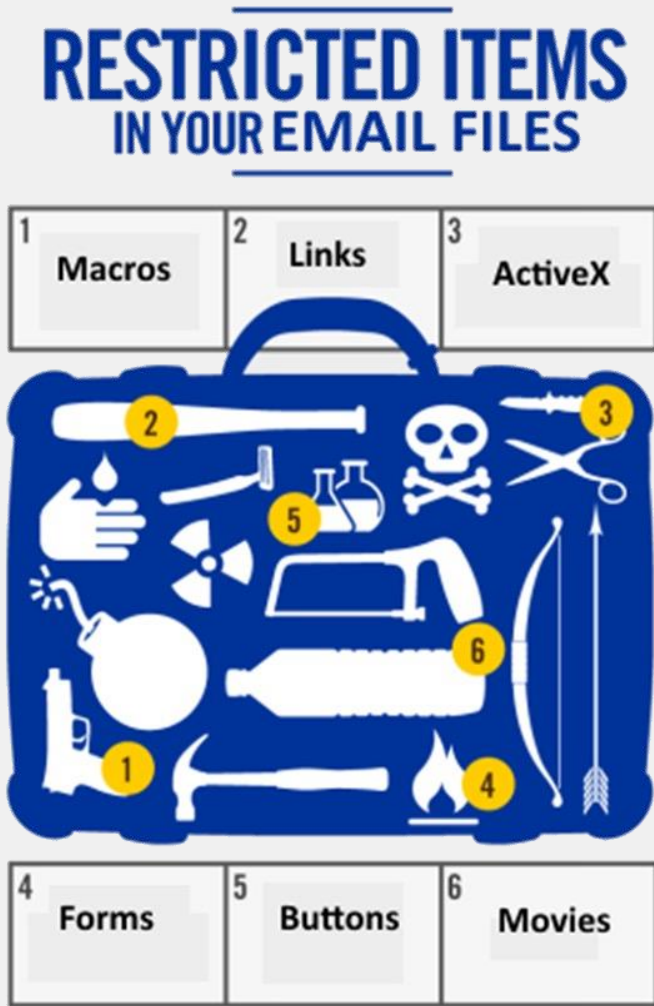
Below the table, there is a section titled "Content Disarm and Reconstruction" with a dropdown menu set to "--Default--". The menu is open, showing options: "Convert HTML to text", "Sanitize HTML content", "Remove URIs", and "Click Protection". The "Convert HTML to text" option is highlighted. Other options in the panel include "Scan Options", "HTML content", "Text content", "MS Office", "PDF", and "Archive Handling".

Red arrows point from the text labels on the right to the corresponding elements in the screenshot:

- Удаление макросов (points to the Developer tab in the ribbon)
- Нейтрализация гиперссылок (points to the URL in the example content)
- Удаление встроенного активного содержимого (points to the table)



Нейтрализация контента (Content Disarm and Reconstruction, CDR)



MS Office:

Word, Excel, PowerPoint

- office-macro
- office-hyperlink
- office-linked-object
- office-embedded-object
- office-dde

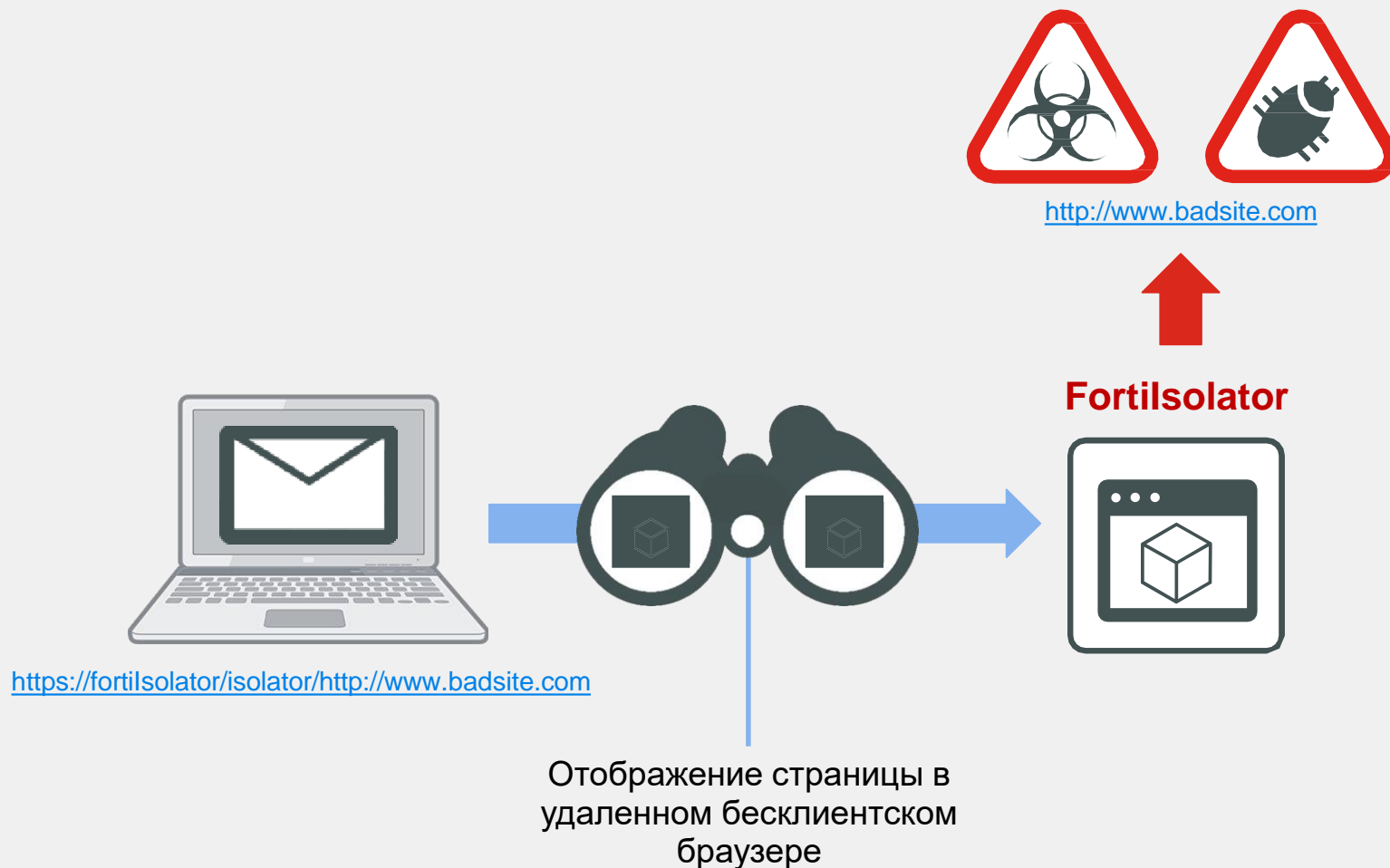
PDF

- office-macro
- office-hyperlink
- Javascript
- embedded-file
- action-gotor
- action-launch
- action-uri
- action-sound
- action-movie
- action-javascript
- action-form
- hyperlink

Защита при переходе по ссылкам в письмах

Интеграция с Fortisolator

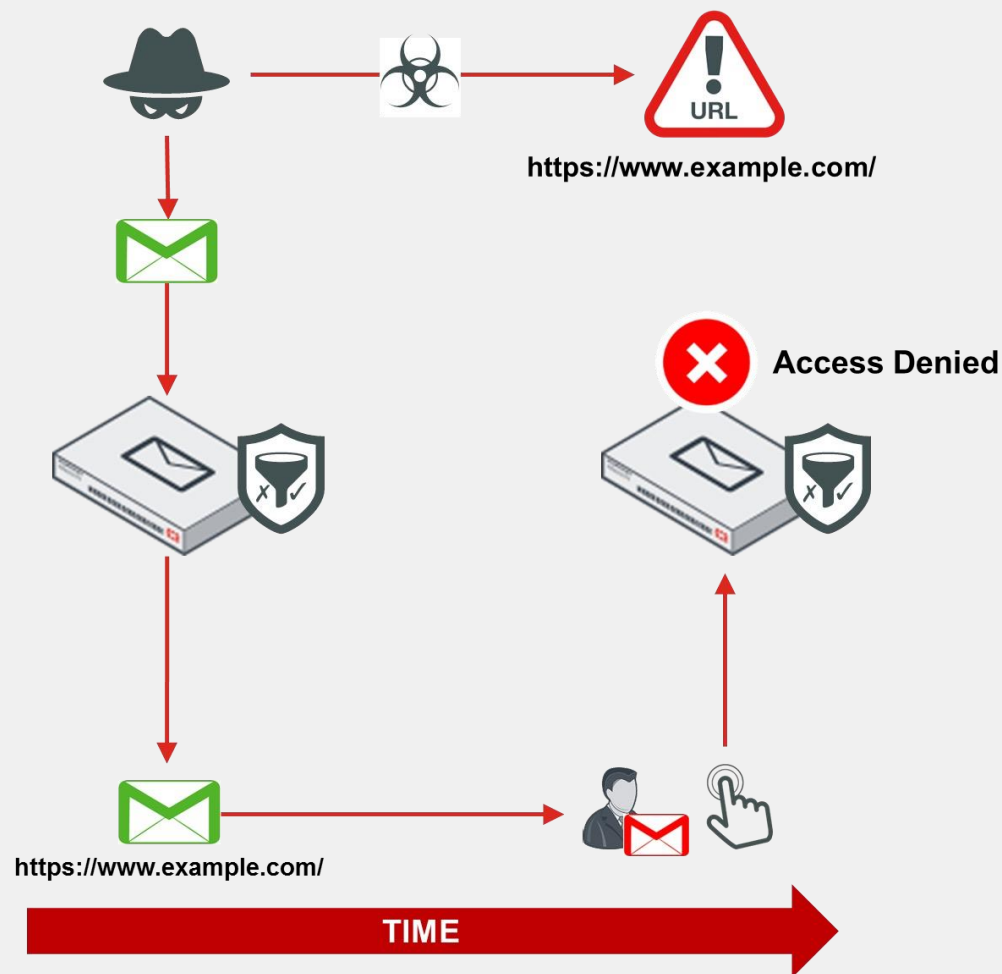
- Может применяться совместно с защитой в момент клика
- Переписывание ссылок в теле письма для перенаправления на сервис
- Fortisolator
 - Бесклиентский удаленный браузер
 - Соккрытие информации о пользователях от злоумышленников



Защита в момент клика по ссылке в письме

URL в теле писем проверяются дважды:

- В момент первого прохождения через FortiMail (при этом переписываются для перенаправления при последующих кликах)
- В момент непосредственного клика пользователя (чтобы убедиться, что переход по URL все еще безопасен)



Demo

☰ All Folders ▾

✕ Close ↩ Reply ↩ Reply All ↪ Forward 📁 Move More ▾

🗑 Delete 1 of 3 < >

Inbox

Drafts

Sent Items

Bulk

Trash

Encrypted Email

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

[Fortinet website here and visit us on FaceBook!!!!](#) and [Don't miss any news on CNN](#)

Original Email

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



Попытки подмены личности

- Выявление маскировки отправителя под топ-менеджмент
 - » Задаем корректное Отображаемое имя/Email
 - » Выявляем спуффинг во входящей почте
 - » Предупреждаем получателя



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

Warning: Suspected Impersonation



Impersonation

Profile name: ImpersonationProfile

Domain: system

Impersonation Entry

+ New... Edit... Delete

Records per page: 50

Selected: 1 / 1

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

AntiSpam Profile

Domain: --System--

Profile name: AS_Inbound

Default action: UserQuarantine

Scan Configurations

- FortiGuard Action: --Default--
- Greylist
- SPF check Action: --Default--
- DMARC check Action: --Default--
- Behavior analysis Action: --Default--
- Header analysis Action: --Default--
- Impersonation analysis Action: --Default--
Impersonation profile: ImpersonationProfile
- Heuristic
- SURBL [Configuration...]
- DNSBL [Configuration...]
- Banned word [Configuration...]



Варианты исполнения

Режим работы и кластеризация



Варианты исполнения



Программно-аппаратные комплексы

- Линейка устройств
- Фильтрация от 30 тыс. до 2 млн сообщений в час
- Поддержка 10GE интерфейсов
- **Количество пользователей не ограничивается**

vmware® Hyper-V KVM

CITRIX® XenServer NUTANIX™

amazon web services™



Microsoft Azure

Виртуальные устройства

- Линейка устройств
- Лицензирование по числу ядер и доменов
- **Количество пользователей не ограничивается**



Облачный сервис

- Режим Gateway или Server
- Хостится Fortinet, управляется совместно
- Подписка по числу пользователей в год



FortiMail

| Feature | We want full control | | |
|--|----------------------|--|---|
| | Base Bundle | Enterprise Advanced Threat Protection Bundle | Ent. ATP with Microsoft O365 API Support Bundle |
| 99.7% Spam detection rate | • | • | • |
| Advanced multi-layer malware detection | • | • | • |
| Inbound and outbound filtering | • | • | • |
| Integration with customer LDAP | • | • | • |
| Secure message delivery (TLS and DANE) | • | • | • |
| Message tracking | • | • | • |
| Virus Outbreak Service | • | • | • |
| Identity-Based Encryption (IBE) | • | • | • |
| Reporting | • | • | • |
| Email Data Loss Prevention | • | • | • |
| Content Disarm and Reconstruction | | • | • |
| URL Click Protection | | • | • |
| Impersonation Analysis | | • | • |
| Cloud Sandboxing | | • | • |
| Real-time scanning of Microsoft 365 mailboxes | | | • |
| Scheduled scanning of Microsoft 365 mailboxes | | | • |
| Post-delivery clawback of newly discovered email threats | | | • |



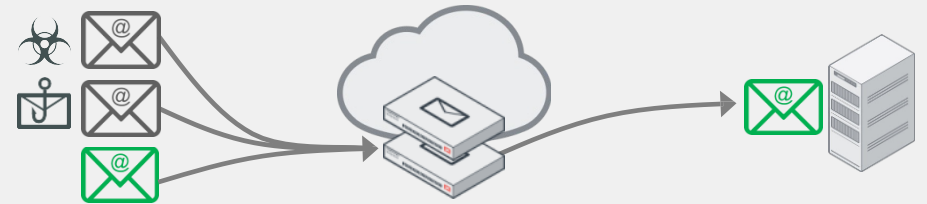
Режимы работы

Отказоустойчивость и горизонтальное масштабирование

Active-Passive кластер

2 полностью синхронизированных устройства

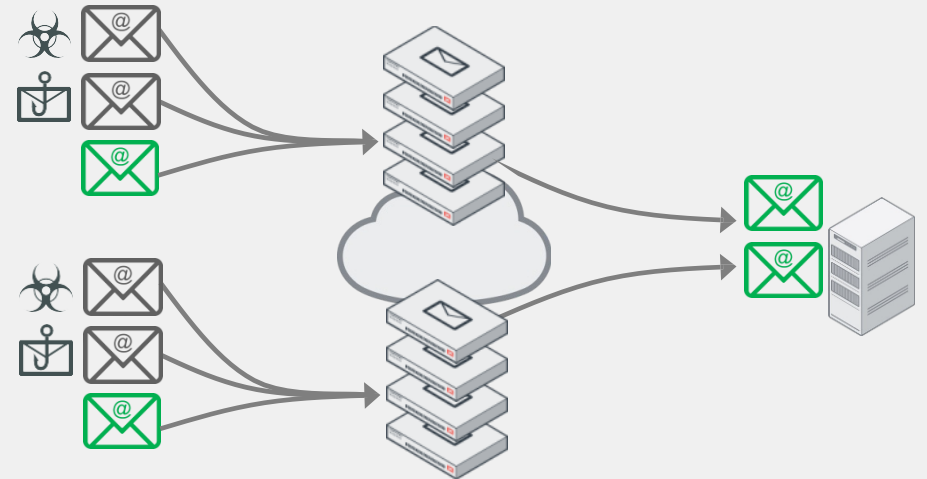
- Heartbeat и мониторинг состояния
- Полная синхронизация почтовых ящиков, архива, карантина, логов и очередей



Синхронизация конфигурации

Горизонтальное масштабирование (ISP/MSSP)

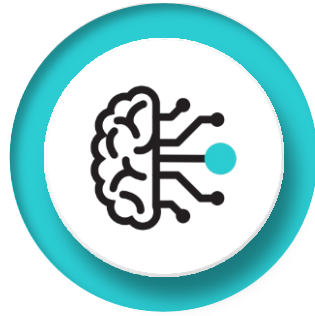
- Централизованный карантин, управление, шифрование
- Отказоустойчивость, географическая распределенность
- Балансировка нагрузки с использованием FortiiADC или сторонних производителей



Дополнительные функции



FortiNDR



FortiNDR

Работает на основе глубоких нейронных сетей, которые идентифицируют и классифицируют, исследует, и блокирует изощренные угрозы.

- Дополнительная защита оборудования
- Несколько узлов
- Высокая производительность

The screenshot displays the FortiMail VM04 FortiMail configuration interface. The main window shows the FortiNDR configuration page with the following fields:

- Status:
- Base URL: fortindr.fortidemo.com
- API key: *****
- Test Connection: [button]
- Upload timeout: 10 (seconds)
- Rating time: [field] (seconds)

An 'AntiVirus Profile' dialog box is open, showing the following settings:

- Domain: --System--
- Profile name: FortiNDR Check
- Comment: [empty field]
- Default action: Reject
- AntiVirus:
- Malware/virus outbreak: Action: --Default--
- Heuristic: Action: --Default--
- File signature check: Action: --Default--
- Grayware:
- FortiNDR:
- Malicious/Virus: Action: --Default--
- High risk: Action: --Default--
- Medium risk: Action: --Default--
- Low risk: Action: --Default--
- FortiSandbox:
- Scan mode: Submit and wait for result | Submit only
- Attachment analysis:

The FortiNDR section has a dropdown menu open showing the following options: --None--, --Default-- (selected), Discard, Reject, and SystemQuarantine. The dialog box has 'Create' and 'Cancel' buttons at the bottom right.



Fortisolator

- Позволяет пользователям просматривать веб-страницы в изолированной среде, которая отображает контент в удаленном контейнере

Прямой доступ через Хром

MarketWatch Latest Coronavirus Watchlist Markets Investing Barron's Personal Finance Economy More 50% OFF 1 YEAR

US Europe Asia FX Rates Futures Crypto RANGE 1D S&P 500 Movers Latest News ALL TIMES EASTERN

Dow 32,727.19 99.22 0.30% ▲
S&P 500 3,948.16 35.06 0.90% ▲
Nasdaq 13,441.73 226.49 1.71% ▲
GlobalDow 3,819.58 -4.27 -0.11% ▼
Gold 1,738.80 -2.90 -0.17% ▼
Oil 61.20 -0.22 -0.36% ▼

10am 12pm 2pm

THE FUTURE OF CYBERSECURITY. COMING THIS MAY. JOIN US! RSAConference2021 May 17 - 20 | Virtual Experience

LATEST NEWS Market Snapshot Vaccine stocks EV stocks Heavily shorted stocks U.S. economic calendar Biden's first 100 days Daily Coronavirus Update Pandemic: Year 2 New ideas in retirement The Moneyist

A bitcoin winter ahead? Crypto expert predicts just that, but after digital asset hits \$300,000 at end of 2021

IRS: More \$1,400 stimulus payments are coming — so check your mail

- 7 things you should not buy with your \$1,400 stimulus check.
- Opinion: How COVID assistance for a family of 4 can balloon to \$69,440 over 17 months

Nasdaq soars 1.6% to kick off last full week of March as Treasury yields retreat, Dow sees slight gain

The MarketWatch Need to Know Newsletter

Guiding investors to the most important news ahead of each trading day

SIGN-UP FREE

Trending Tickers Higher volume than normal. HOFV \$5.22 -30.50% 1.22 JFIN \$11.76 -43.05% 3.54 MRKR \$2.96 -22.11% 0.54 SNCA \$2.01 -22.56% 0.37 WKEY \$12.80 -18.41% 1.99

Доступ через Fortisolator к Хром

MarketWatch Latest Coronavirus Watchlist Markets Investing Barron's Personal Finance Economy More 50% OFF 1 YEAR

US Europe Asia FX Rates Futures Crypto RANGE 1D S&P 500 Movers Latest News ALL TIMES EASTERN

Dow 32,727.19 99.22 0.30% ▲
S&P 500 3,948.16 35.06 0.90% ▲
Nasdaq 13,441.73 226.49 1.71% ▲
GlobalDow 3,819.58 -4.27 -0.11% ▼
Gold 1,738.80 -2.90 -0.17% ▼
Oil 61.20 -0.22 -0.36% ▼

10am 12pm 2pm

THE FUTURE OF CYBERSECURITY. COMING THIS MAY. JOIN US! RSAConference2021 May 17 - 20 | Virtual Experience

LATEST NEWS Market Snapshot Vaccine stocks EV stocks Heavily shorted stocks U.S. economic calendar Biden's first 100 days Daily Coronavirus Update Pandemic: Year 2 New ideas in retirement The Moneyist

A bitcoin winter ahead? Crypto expert predicts just that, but after digital asset hits \$300,000 at end of 2021

IRS: More \$1,400 stimulus payments are coming — so check your mail

- 7 things you should not buy with your \$1,400 stimulus check.
- Opinion: How COVID assistance for a family of 4 can balloon to \$69,440 over 17 months

Nasdaq soars 1.6% to kick off last full week of March as Treasury yields retreat, Dow sees slight gain

The MarketWatch Need to Know Newsletter

Guiding investors to the most important news ahead of each trading day

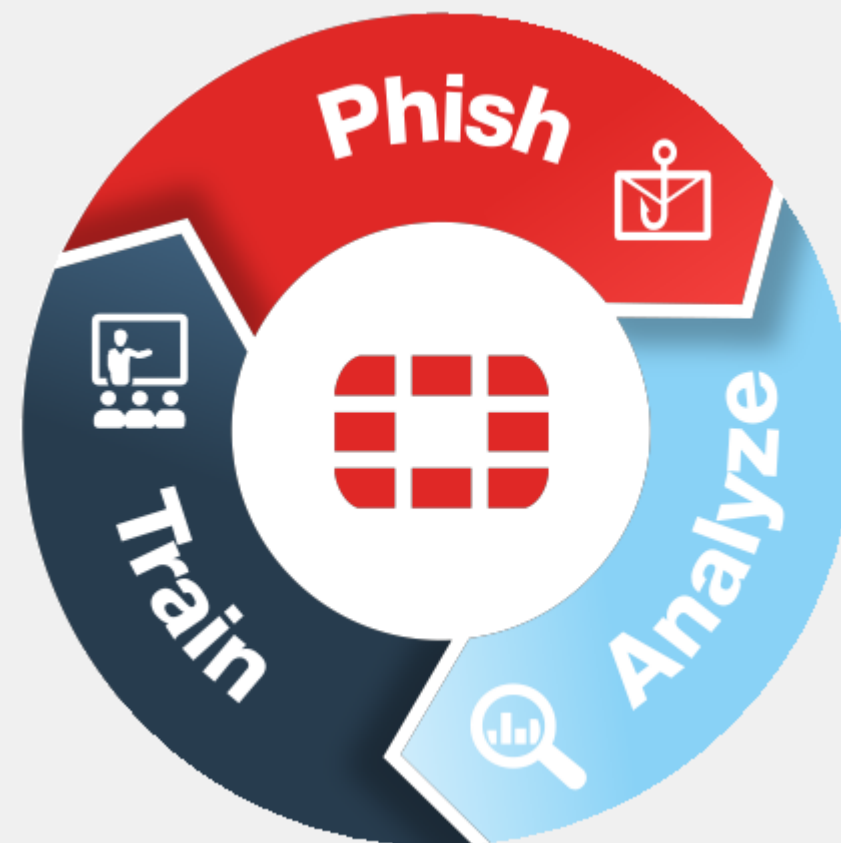
SIGN-UP FREE

Trending Tickers Higher volume than normal. HOFV \$5.22 -30.50% 1.22 JFIN \$11.76 -43.05% 3.54 MRKR \$2.96 -22.11% 0.54 SNCA \$2.01 -22.56% 0.37 WKEY \$12.80 -18.41% 1.99



FortiPhish

- Облачный сервис имитации фишинга
- Области внимания:
 - Phish: Проверка осведомленности о фишинге в режиме реального времени
 - Analyze: Использование аналитику для выявления пользователей, подверженных риску и областей требующих улучшения
 - Train: Использование результатов что бы быть информированным о попытках фишинга и защитится от этих атак



Карантин

Пользовательский дайджест, Junkmail/Newsletter папки

- **Централизованный карантин**

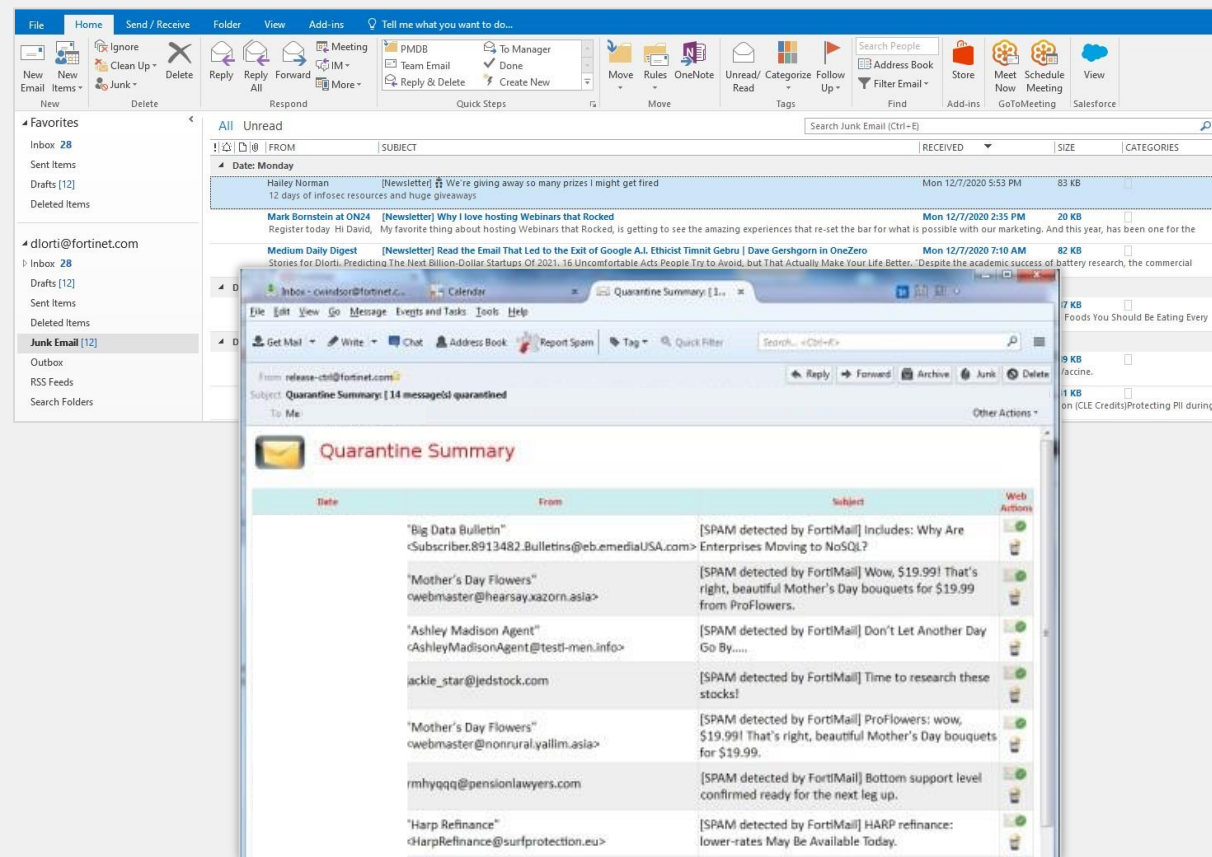
- Удобный в администрировании
- Можно консолидировать для всех шлюзов в кластере

- **Дайджест с возможностью самообслуживания**

- Отправитель и тема
- Ссылки на выпуск и удаление
- Извлечение по web и электронной почте

- **Автоматическая маркировка**

- **Выявление новостных рассылок**



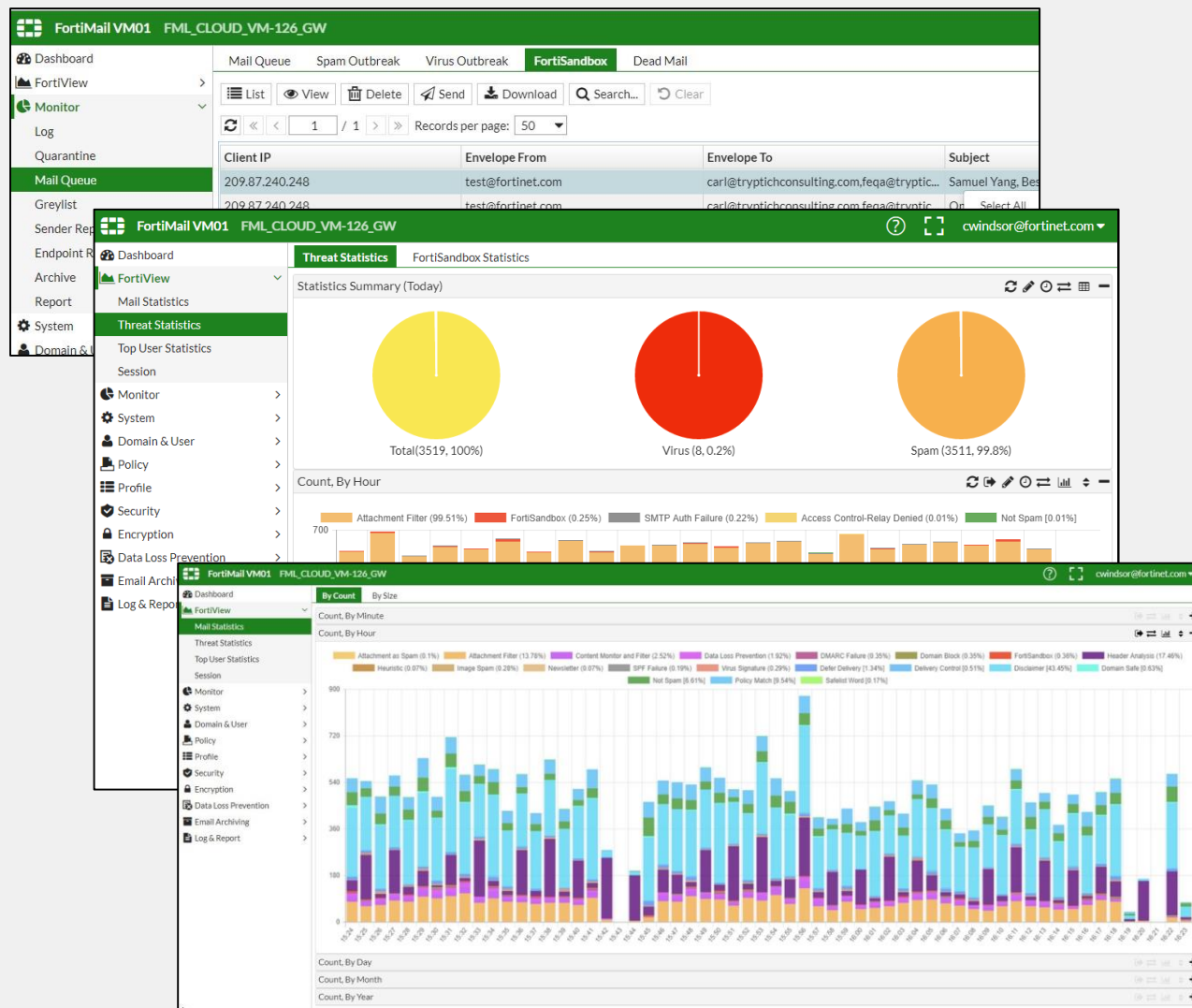
Возможности мониторинга

FortiView

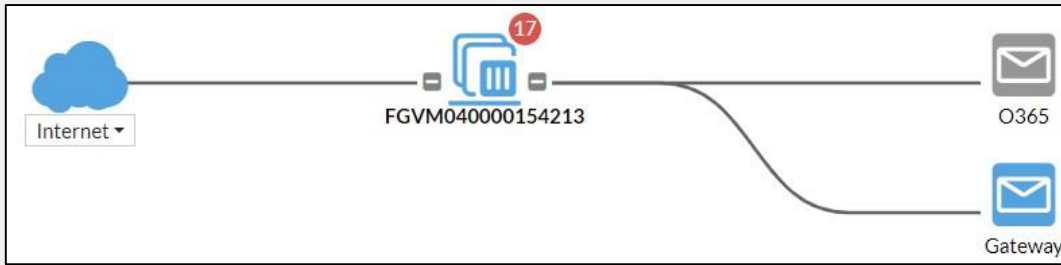
- Статистика по пользователям и угрозам

Мониторинг

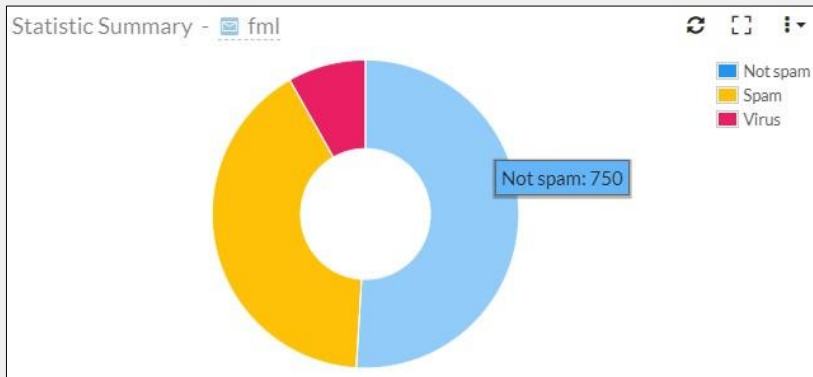
- Настраиваемые дашборды
- Широкий набор фильтров
- Сквозной поиск по типам логов
- Интеграция с FortiSIEM, FortiAnalyzer
- Поле “Session ID” в Очередях и Карантине для удобного перекрестного поиска



Фабрика безопасности: FortiMail в консоли FortiGate

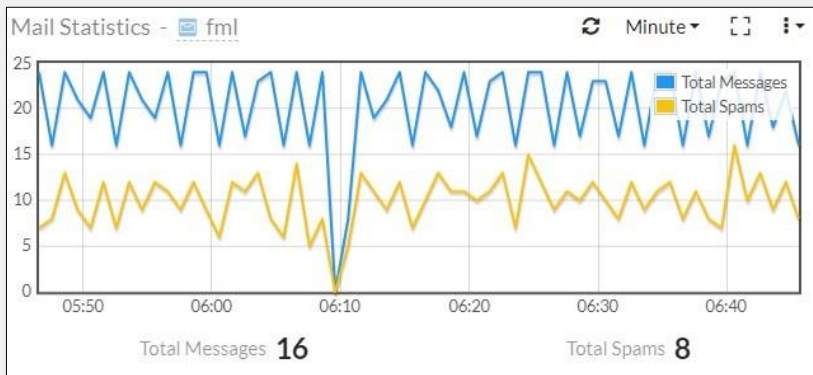


Security Fabric



System Information - fml

| | |
|----------------------|--|
| Serial number | FEVM040000185357 |
| Up time | 0 day(s) 0 hour(s) 35 minute(s) 54 second(s) |
| System time | Wed Aug 21 06:45:51 PDT 2019 |
| Reboot time | Wed Aug 21 06:09:57 PDT 2019 |
| Firmware version | v6.2,build249,190808 (6.2.0 GA) |
| Operation mode | Gateway |
| HA mode | Configured: Off, Effective: Off |
| Log disk information | Capacity 48 GB, Used 34 MB (0.08%), Free 48 GB |



System Usage - fml

| | |
|-----------------|-----|
| CPU usage | 1% |
| Memory usage | 63% |
| Log disk usage | 0% |
| Mail disk usage | 0% |
| System load | 15% |
| Active sessions | 1 |



Защита конфиденциальности

DLP, соответствие требованиям, архив

- **Защита конфиденциальности**

- Словари для обеспечения соответствия HIPAA, GLBA, SOX, PCI DSS
- Scanning Построение отпечатков файлов с помощью загрузки вручную или сканирования общих папок Windows

- **TLS & S/MIME шифрование**

- **Технология шифрования почты Identity Based Encryption**

- Не требуется дополнительной лицензии
- Нет обмена ключами шифрования, минимальное управление ключами

- **Архивация на основе политик**

- По отправителям/получателям, ключевым словам в теме/письме/вложении
- Поддерживается архивация в сетевую папку
- Архивация Microsoft Exchange Journal



Policies

- Политика определяет способ фильтрации трафика на основе двух разных методов:
 - Политика на основе получателей: фильтрация электронных писем по отправителю и/или получателю
 - Политика на основе IP: фильтрация на основе исходного или целевого IP-адреса сеанса SMTP
- Использование политик для применения профилей проверки и проверки подлинности
- Политики на основе получателей и политики на основе IP можно использовать вместе

The screenshot shows the configuration for an Inbound Recipient Policy. The 'Enable' toggle is turned on. The 'Domain' is set to 'acmecorp.net'. The 'Sender Pattern' is configured with 'User (wildcard)' type and a pattern of '* @ *'. The 'Recipient Pattern' is also configured with 'User (wildcard)' type and a pattern of '* @ acmecorp.net'. Under the 'Profiles' section, 'AntiSpam', 'AntiVirus', and 'Content' are all set to '--None--'.

| Profile | Value | Action |
|-----------|----------|----------|
| AntiSpam | --None-- | + [icon] |
| AntiVirus | --None-- | + [icon] |
| Content | --None-- | + [icon] |

Профили Антивируса

- FortiMail сканирует заголовки и текст на наличие вирусов
- Профили Антивируса определяют, FortiMail предпринимает действия при обнаружении вируса:
 - Заменяет подозрительные письма
 - Отклоняет
 - Карантин

AntiVirus Profile

Domain: --System--

Profile name: AV_Discard

Default action: Discard [+] [✎]

AntiVirus

| | | |
|--|---------------------|-------------|
| <input checked="" type="checkbox"/> Malware/virus outbreak | Action: --Default-- | [+] [✎] |
| <input checked="" type="checkbox"/> Heuristic | Action: --Default-- | [+] [✎] |
| <input type="checkbox"/> File signature check | Action: --Default-- | [+] [✎] |
| <input checked="" type="checkbox"/> Grayware | | |

Разоружение и реконструкция содержимого(CDR)

- FortiMail удаляет или нейтрализует потенциально опасное содержимое и реконструирует сообщение электронной почты и вложенные файлы.
- Нейтрализует HTML и активный контент различными способами:
 - Преобразует контент в текст
 - Удаление любых URL-адресов или активного контента
 - Перенаправление на FortiSolator или Click Protection
- Обезвреживает потенциально опасное содержимое во вложениях почты, в Microsoft Office и PDF

The screenshot shows the 'Content Disarm and Reconstruction' configuration page. At the top, there is a title bar with a minus icon and the text 'Content Disarm and Reconstruction'. Below this, there is a dropdown menu for 'Action' set to '--None--', with '+' and 'x' icons to its right. The main configuration area consists of several sections, each with a toggle switch and a dropdown menu for 'URL'. The first section is for 'HTML content', with the toggle turned on and the URL set to 'Modify content'. Below it, there is a 'Active content' section with the toggle on and the URL set to 'Remove'. The 'URL' dropdown for this section is set to 'Redirect to Click Protection', with a 'View settings...' link to its right. Below the 'Active content' section, there are two toggle switches: 'Tag attribute' (turned on) and 'Tag text content' (turned off). The second section is for 'Text content', with the toggle on and the URL set to 'Remove', also with a 'View settings...' link. The third section is for 'MS Office', with the toggle on. The fourth section is for 'PDF', with the toggle on.

URL Click Protection

- Удалить или оставить URL-адреса, содержащиеся в сообщениях почты
- Сканировать URL-адреса с помощью FortiGuard и FortiSanbox
- Изолирует угрозы с помощью Fortisolator

URL Click Protection Option

URL Rewrite

Category

Base URL

URL Click Handling

Category

Action

FortiSanbox Scan

Enable

Action

Timeout action

Timeout (seconds)

Fortisolator Integration

Category

Base URL



Спасибо за внимание

