Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Speakers

Rahul Iyer

Senior Product Manager

TG Singham

Solutions Engineer

Trellix

Trellix

Features & Innovation

Digital transformation has introduced a new threat vector

Extended Enterprise

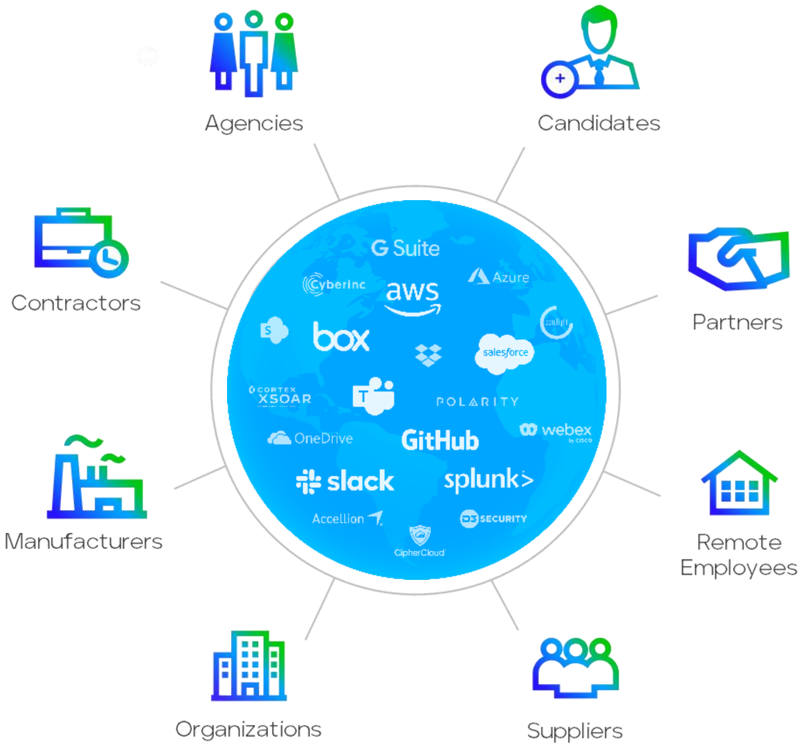
Business agility and innovation require third-party relationships to extend enterprise capabilities

Digital Transformation

Digitally-enabled partner ecosystem creates significant risk exposure

SaaS Insecurity

Vendors secure their platform but don't worry that they provide an open door to your environment



Trellix

To protect against threats introduced by digitally-enabled partner ecosystems

What if you could have a security solution that is…

…**comprehensive** across all enterprise applications & collaboration tools

…**unobtrusive**, with no impact on end users or application infrastructure

…**easy** on the SOC and Enterprise Applications teams

Trellix

Trellix Collaboration Security

Ensures teams can work confidently and securely across the extended enterprise

Email

Still the primary attack vector. Over 90 % of cyber attacks begin with phishing.

Collaboration Platforms

Allow us to freely share information, but do not ensure the integrity of what is being shared

Enterprise Applications

Digital transformation initiatives grant access to suppliers, vendors, customers – and threat actors

Proven technology to address three distinct use cases

IVX for Products

Targeted for Trellix Appliances

- IVX detection created the sandbox market. Detection is our founding competency
- Flexible deployment options that scale for scanning throughput with Network Security, Email Security, Endpoint, etc.
- Clustered architecture instrumented for 200 potential simultaneous executions

IVX for Investigators

Targeted for the SOC

- Used during investigative workflows
- Detonate suspicious content
- Reverse engineer malware

IVX for Collaboration Security

Targeted for Enterprise Applications

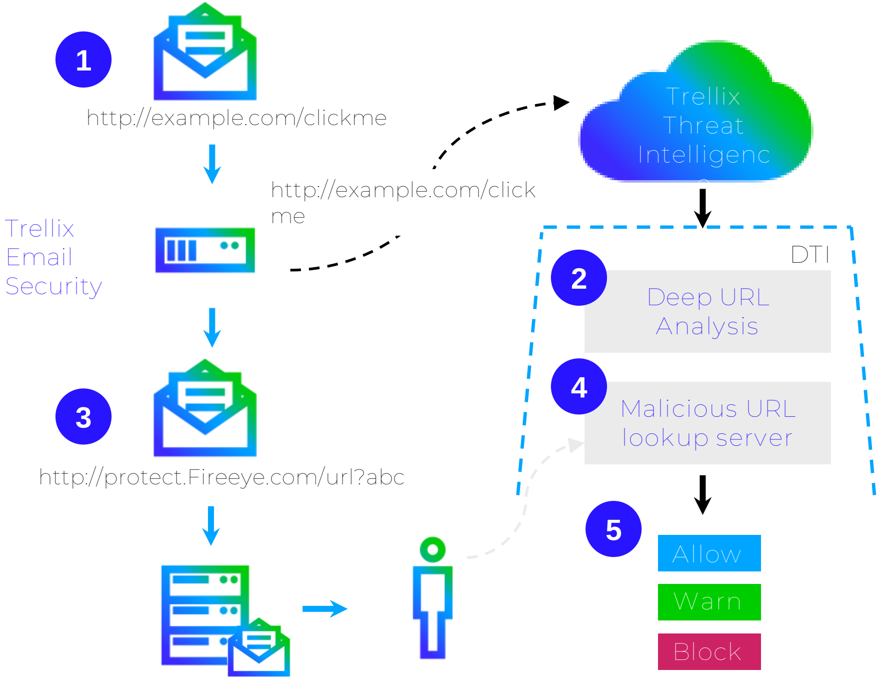
- Organizations focused on digitizing their extended enterprise value chain
- Integrates with enterprise applications
- Mitigate the risk of working with external organizations and vendors

Trellix

Trellix identifies and blocks all threat categories

- QUISHING
- ATTACHMENTS
- URLs
- DEFERRED PHISHING
- SOCIAL MEDIA MALWARE
- IMPERSONATION
- MULTI-STAGE
- OUTBOUND MALWARE

Detection of Spear Phishing Websites (URLs & Content)


1
http://example.com/clickme
Trellix Email Security
http://example.com/click me
Trellix Threat Intelligenc
DTI
2
Deep URL Analysis
4
Malicious URL lookup server
3
http://protect.Fireeye.com/url?abc
5
Allow
Warn
Block

1 Checks AUD fast path if suspicious URL is known to be malicious

2 Unknown suspicious URLs submitted to AUD Slow Path for real time analysis

3 URL is rewritten and email delivered to prevent delays (inline deployments only)

4 End user redirected to warning page upon clicking suspicious link

5 Based on results of lookup, URL access either allowed, warned or blocked

Overview

- Detects zero-day, low-volume, highly-targeted phishing attacks
- Analyzes website content for malicious behavior by scanning the whole phishing site (links, content, etc.)

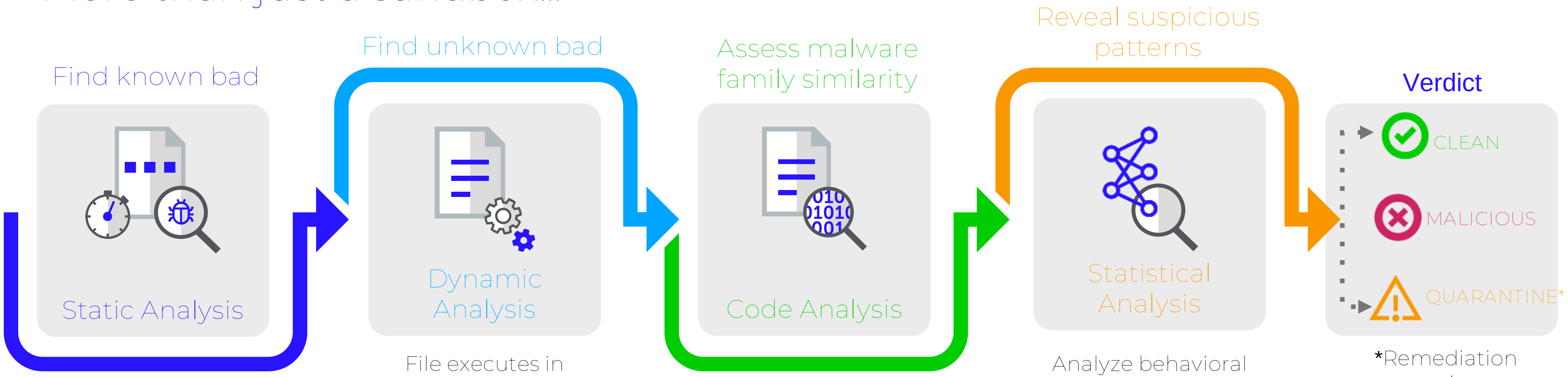
Benefits

- High-fidelity detection
- Blocking of multi-stage malware and evolving URL based threats
- Low false positive rate
- Simplified alert prioritization and faster attack prevention

Trellix

Multi-stage Inspection Process

More than just a sandbox…



Find known bad

Static Analysis

Lower intensity analytical methods: signatures, reputation, and emulations

Perform high speed analysis at scale

Find unknown bad

Dynamic Analysis

File executes in a safe and instrumented environment.

Observe file execution and look for malicious behavior

Assess malware family similarity

Code Analysis

Remove obfuscation to expose original executable code

Analyze attributes and instruction sets to identify characteristics similar to known bad behaviors

Reveal suspicious patterns

Statistical Analysis

Analyze behavioral patterns to identify maliciousness

Uncover patterns in code to identify emerging threats

Verdict

- CLEAN
- MALICIOUS
- QUARANTINE*

*Remediation actions configurable by integration

Trellix

QR Code and HTML Attachments

QR Code

- Email Cloud (ETP) supports QR code detection within *email body, images* within email body (*jpeg, png,* etc.), *pdf, and doc* files
- Email Server (EX) supports QR code detection (Release 10.0.1)
- Detected over **133K QR code attacks during Q4’23 – Q1’24**

HTML Attachments

- Email Cloud (ETP) supports HTML-Attachments based detection
- Email Server (EX) supports HTML-Attachments based detection (Release 10.0)
- Detected over **1.9M HTML-based attacks during Q4’23 – Q1’24**

Trellix blog on QR code detection: https://www.trellix.com/about/newsroom/stories/research/scanning-danger-unmasking-the-threats-of-quishing/

The New York Time article with Trellix reference: https://www.nytimes.com/2023/12/10/business/qr-code-scam-ftc.html

Catching What Other Vendors Miss

2.37m

Targeted attacks missed per year by Microsoft across 1572 customers

1.05m

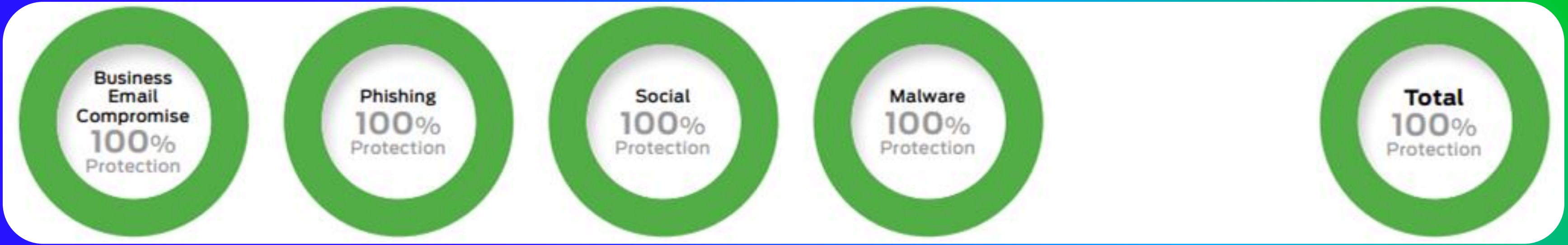
Targeted attacks missed per year by Proofpoint across 1018 customers

10.2m

Targeted attacks missed per year by IronPort across 967 customers

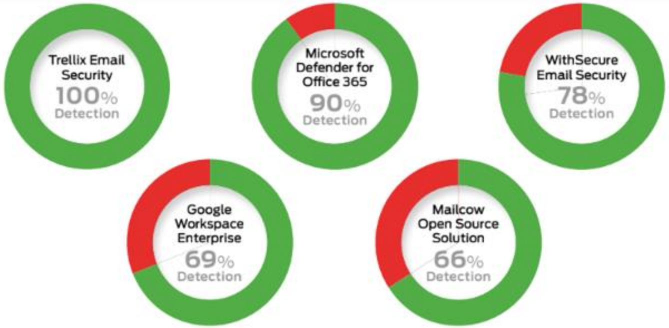
From Q2 2023 – Q1 2024

Trellix ranks #1 in SE Labs Report beating Microsoft and Google

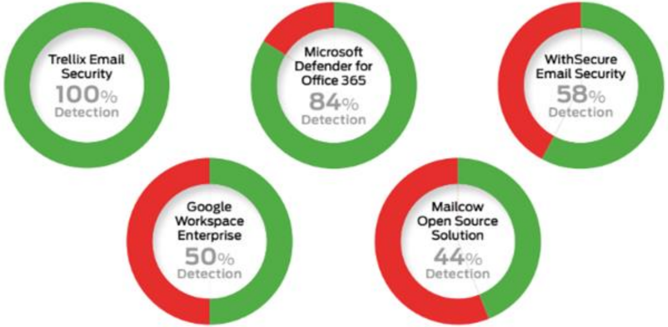


Overall Rankings

Threat Detection Results



Total Accuracy Ratings



Source: SE Labs: Email Security Services (ESS): Enterprise 2023 Q1

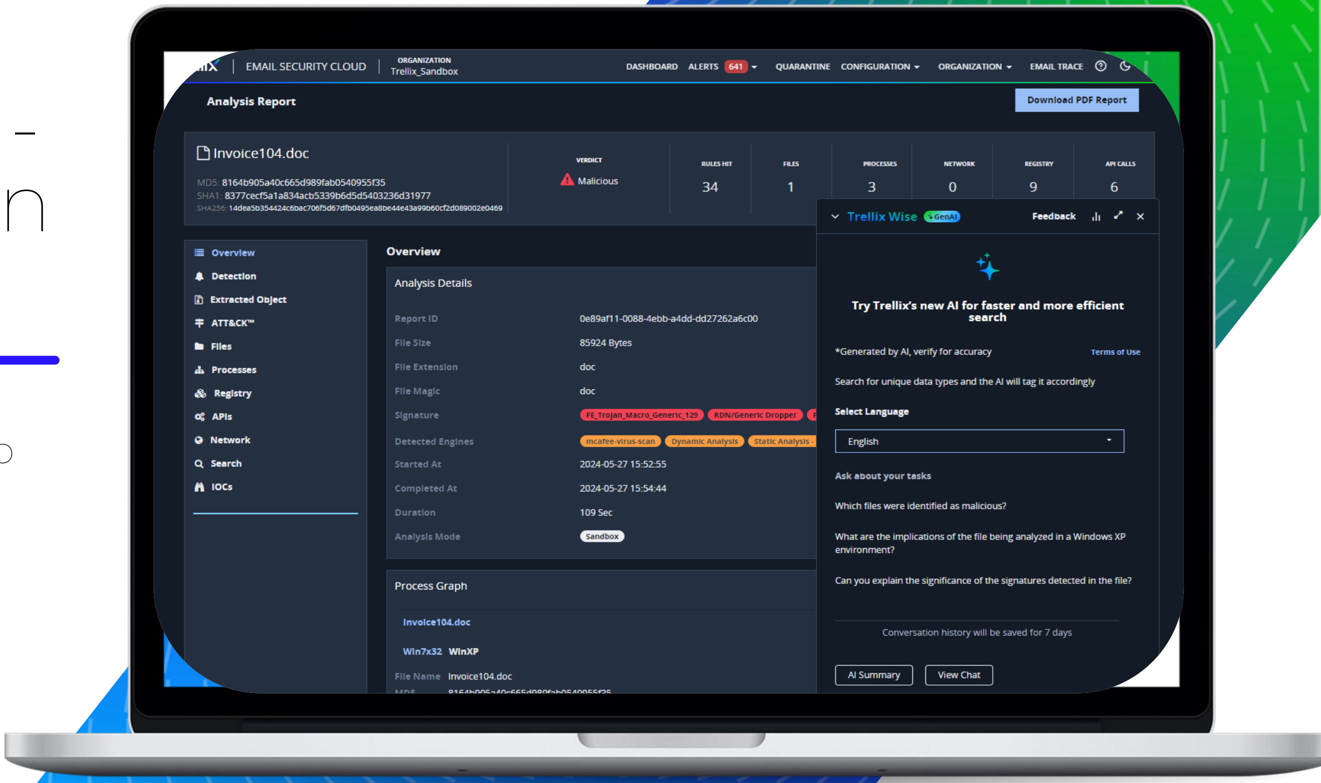
SE Labs Annual Security Awards 2024

SE Labs
INTELLIGENCE-LED TESTING
BEST
Email Security Service
WINNER 2024
Trellix
Trellix

Source: SE Labs: Annual Security Awards 2024

Trellix WISE - Collaboration Security

- Reduce time to respond to incidents
- Get deeper insights using natural query language
- Reduce analyst effort with Wise generated alert summary



ORGANIZATION
Trellix_Sandbox

Analysis Report

Invoice104.doc

MD5: 8164b905a40c665d989fab0540955f35
SHA1: 8377cecf5a1a834acb5339b6d5d5403236d31977
SHA256: 14dea5b354424c6bac706f5d67dfb0495ea8be44e43a99b60cf2d089002e0469

VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
Malicious	34	1	3	0	9	6

Overview

Analysis Details

Report ID	0e89af11-0088-4ebb-a4dd-dd27262a6c00
File Size	85924 Bytes
File Extension	doc
File Magic	doc
Signature	FE_Trojan_Macro_Generic_129 RDN/Generic Dropper F
Detected Engines	mcafee-virus-scan Dynamic Analysis Static Analysis -
Started At	2024-05-27 15:52:55
Completed At	2024-05-27 15:54:44
Duration	109 Sec
Analysis Mode	Sandbox

Process Graph

Invoice104.doc

Win7x32 WinXP

File Name Invoice104.doc

MD5 8164b905a40c665d989fab0540955f35

Try Trellix's new AI for faster and more efficient search

*Generated by AI, verify for accuracy

Search for unique data types and the AI will tag it accordingly

Select Language

English

Ask about your tasks

Which files were identified as malicious?

What are the implications of the file being analyzed in a Windows XP environment?

Can you explain the significance of the signatures detected in the file?

Conversation history will be saved for 7 days

Email is still the most successful attack vector

Primary attack vector

91%

Of cyberattacks begin with spear phishing***

Microsoft isn't good enough

3M

Attacks missed by Microsoft in a year across 1058 customers*

Cloud email adoption

70%

Of organizations use cloud email solutions and growing**

Average breach lifecycle

277Days

Resulting from business email compromise ****

*Trellix Advance Research Center
**Gartner Market Guide for email security
***Knowbe4.com Nov 29, 2022
****IBM Cost of a Data Breach Report 2022

Trellix

Product Deployment

Trellix Email Security

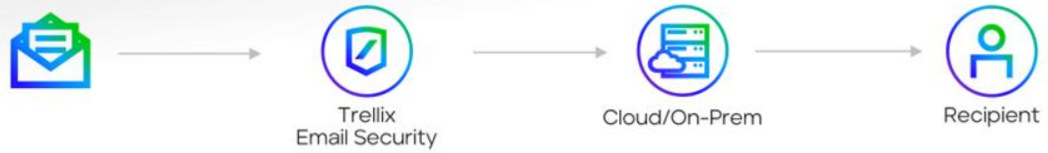
Email Security -
Cloud

Email Security -
Server

Flexible Deployment Options
Cloud Email

Scan/Block

1. **Primary SEG with Full Hygiene.**



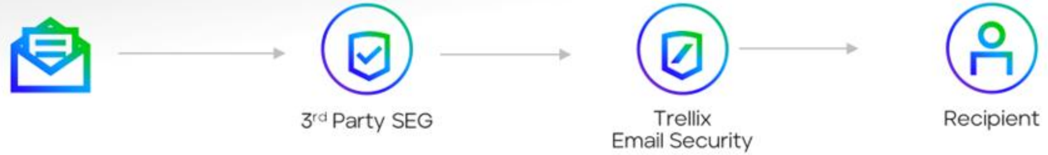
Trellix Email Security

Cloud/On-Prem

Recipient

Scan/Block

2. **Full Hygiene inline, second hop, behind a 3rd party SEG.**



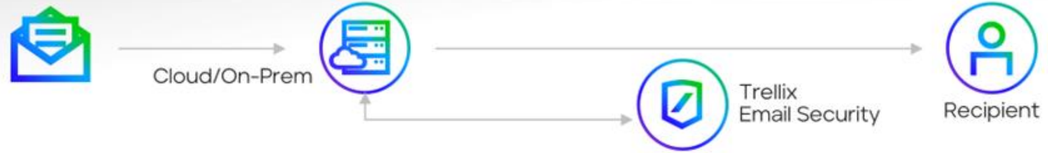
3rd Party SEG

Trellix Email Security

Recipient

Scan/Drop

3. **Full Hygiene in BCC mode and sends alerts.**



Cloud/On-Prem

Trellix Email Security

Recipient

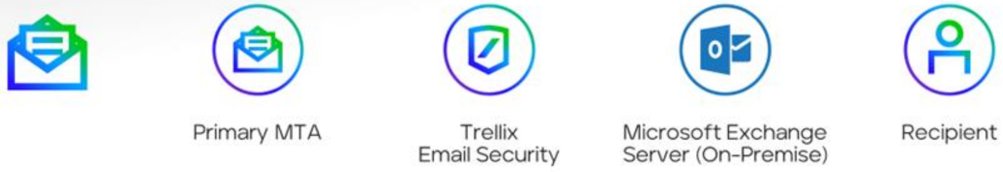
4. **MS365/Google Workspace Native API Integration**

Google Workspace

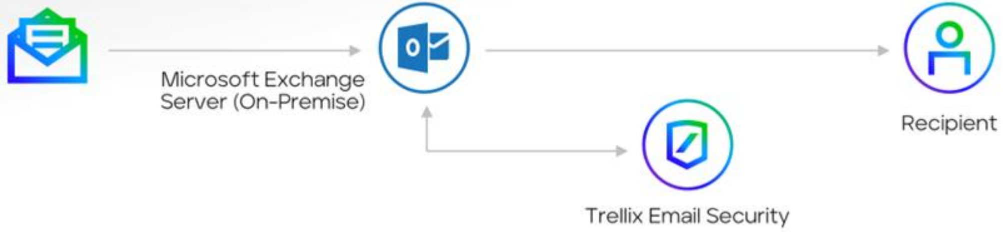
Microsoft 365

Flexible Deployment Options
Server Email

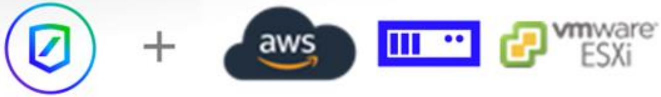
1. On prem Inline mode



2. On prem in BCC/Monitor modes



3. Appliance deployments (Form factors)



Trellix Email Security

Example – On-prem MS Exchange

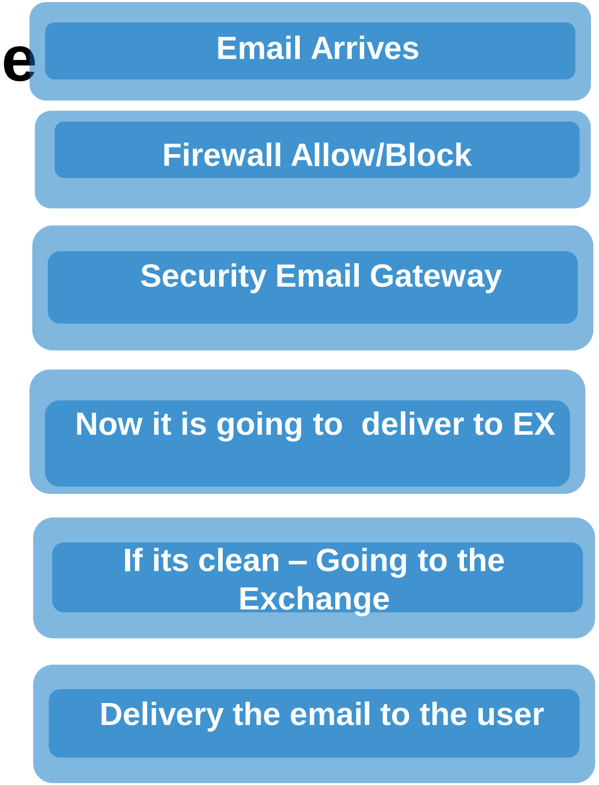
- Arrives on port 25 over Secure SMTP

- Which is going to do the filtering, AS hygiene, MX record checks, Authentication and Authorisation (SPF, DKIM,DMARK)

- EX is going to do the advance phishing analysis
- Advance malware analysis, and open the attachments (Virtualise needed)

- Exchange will do its own security checks

- Email deliver to the user's inbox



Email Arrives

Firewall Allow/Block

Security Email Gateway

Now it is going to deliver to EX

If its clean – Going to the Exchange

Delivery the email to the user

Demo

Optional subtitle

Trellix