Trellix

APJ Partner Summit'24

Partnering for a Secure Future

Join us at the APJ Partner Summit

Phuket, Thailand

10-12 JULY 2024

Trellix Email Security Solutions

APJ Partner Summit 2024

July 8, 2024

Speakers for Today

Ron Wang
Sr Director, APJ SE

Hidemitsu Sakurai
Sr Director, Japan SE

Manish Sinha
Director, India SE

Carl Thaw
Global Enablement

Trellix

“In your experience, what are the most common misconceptions about email security?”

Trellix

Agenda

1) **Why the need for Trellix Email solution?**
   Challenges it solves

2) **How does Trellix solve the problem?**
   How we are different

3) **About the Trellix solution**
   Overview & Demo

4) **Personas**
   Who to target

5) **Proof Points**
   Customer Case Study

6) **Product Packaging**
   Product SKUs

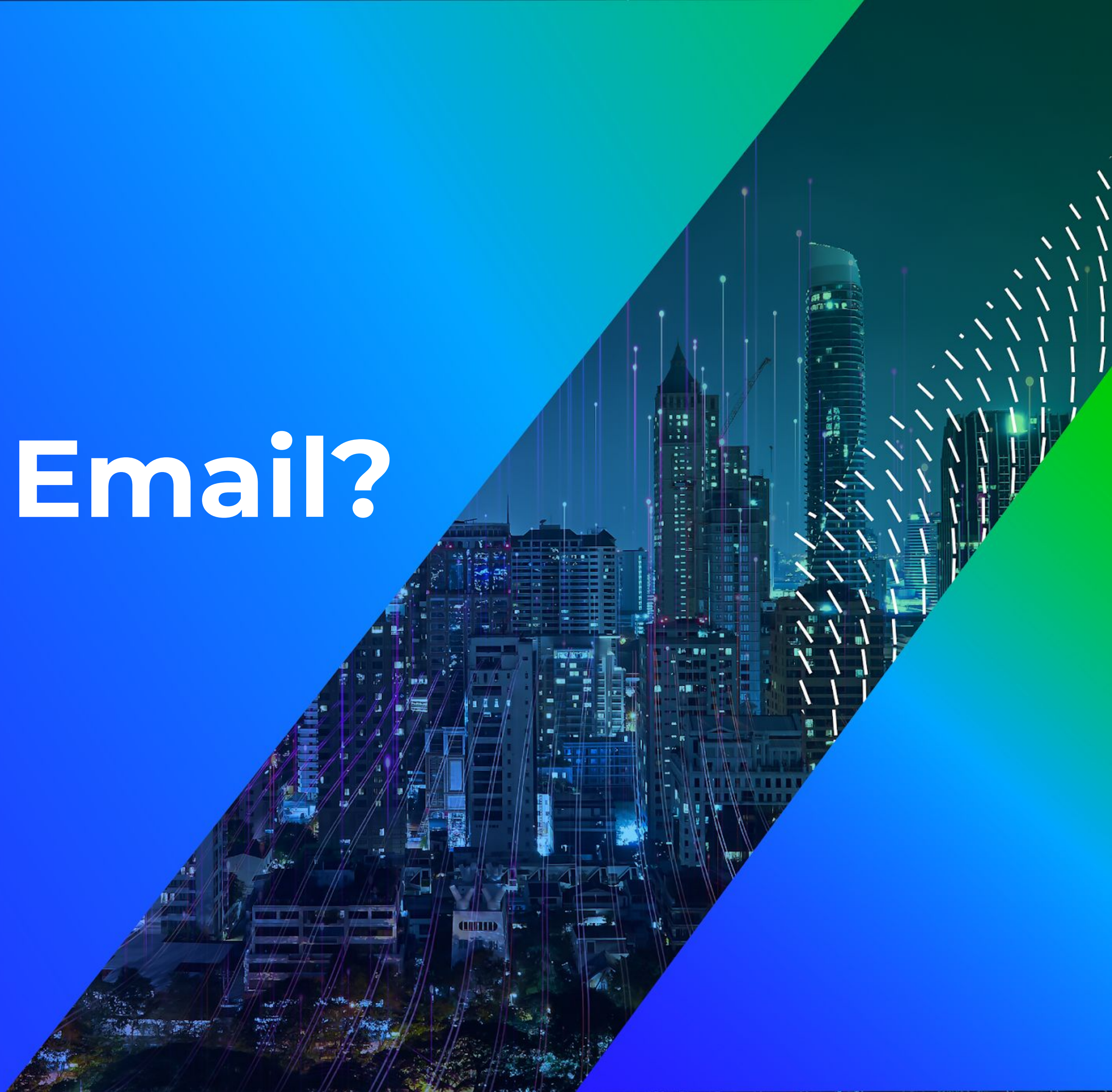
7) **Upsell and Cross-Sell**
   Positioning the solution to customers

Trellix

Trellix

Why Trellix Email?

Challenges, Status Quo



Current Situation: Why the need?

There is no such thing as a safe email!

Primary Attack Vector

91% of cyberattacks begin with spear phishing***

Cloud Email Adoption

70% of organizations use cloud email solutions and growing**

Microsoft isn’t good enough

3M attacks missed by Microsoft in a year across 1058 customers*

Average breach lifecycle

277 days 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

Required Capabilities to solve it?

Advanced Analysis

Detect threats in email, pre- and post-delivery

Share threat intelligence

Extract threat intelligence from email attack and share with SOC team

Catch the unknown

Defend from new attacks including ransomware, URLs, credential theft, and QR phishing

No slowdown

Decrease impact on user without impeding productivity

Status Quo? - What if we don't do anything?

More Victims

- More breaches
- More data will be stolen or held hostage
- More losses

Decrease in Collaboration

- Lower productivity due to emails not being actioned on
- More time spent on validating emails
- Revert to physical paper

Need for More End-User Training

- More trainings and consistent reinforcement are needed to ensure employees are trained to spot email attack

Analysts Overwhelmed with Alerts

- Security Operation Center (SOC) Teams are overwhelmed with security alerts, unable to prioritize

Trellix

How Trellix Solves it

How we are different

Trellix Email Security

How we do it…Better

Full Threat Detection Efficacy

Unmatched threat detection: cloud-based, multi-tenant, advance URL defense and attachment detonation

Comprehensive protection against numerous attack vectors

Block threats and provide contextual insights to prioritize and accelerate response

Integrated Investigation and Response

Detect and prioritize threats to help quick remediation of advanced threats

Remediation capabilities to automatically or manually pull email out in inboxes post delivery

Prioritize, correlate, and remediate emails from Sec Ops platform

Comprehensive and Resilient

Secure Email Gateway or behind existing solution

Native integration into MS365 and Google Workspace

Telco grade resiliency

Trellix

About Trellix Email

Trellix Email Security

How we do it…Better

Full Threat Detection Efficacy

Unmatched threat detection: cloud-based, multi-tenant, advance URL defense and attachment detonation

Comprehensive protection against numerous attack vectors

Block threats and provide contextual insights to prioritize and accelerate response

Integrated Investigation and Response

Detect and prioritize threats to help quick remediation of advanced threats

Remediation capabilities to automatically or manually pull email out in inboxes post delivery

Prioritize, correlate, and remediate emails from Sec Ops platform

Comprehensive and Resilient

Secure Email Gateway or behind existing solution

Native integration into MS365 and Google Workspace

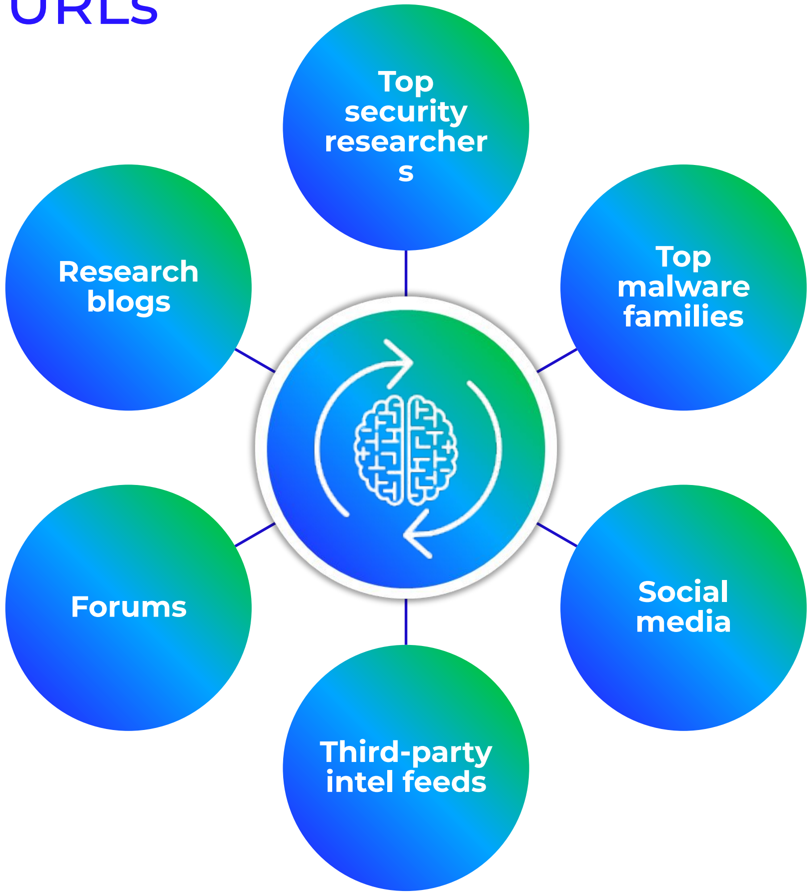
Telco grade resiliency

Trellix

1. Full Threat Detection Efficacy: How We Achieve It

Key Ingredient - Real-time Visibility into Malicious URLs

- Gathers intel on malicious URLs pointing to malware payloads, Command and Control domains, and other URL-blocked lists
- Crawls more than 60 sources, ensuring real-time collection
- Fully automated, processing +10M URLs per day
- Maintains blocked list of malicious URLs
- Updates Trellix Email Security hourly



Trellix

1. Full Threat Detection Efficacy: How We Achieve It

Key Ingredient - Deep Content Inspection

Text Classification

Identifies commonly used patterns

Natural Language Processing (NLP) model analyzes large volumes of unstructured text data

Trained on the latest phishing trends

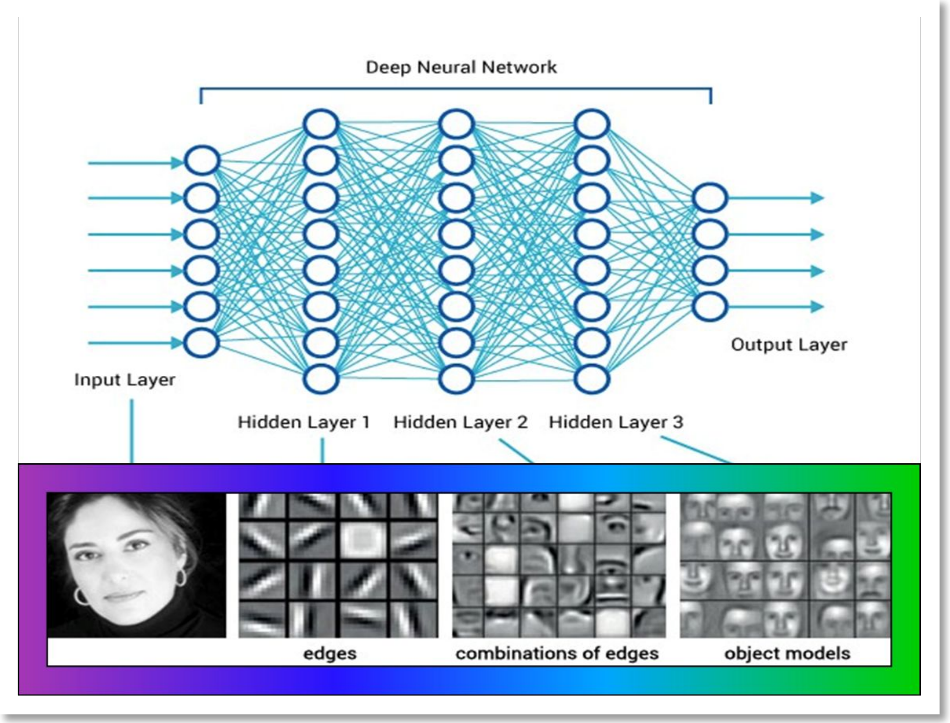
Content Interaction

Crawlers interact with URLs, and content and extract embedded URLs providing multi-layer inspection

1. Full Threat Detection Efficacy: How We Achieve It

Key Ingredients - Image Inspection and Classification

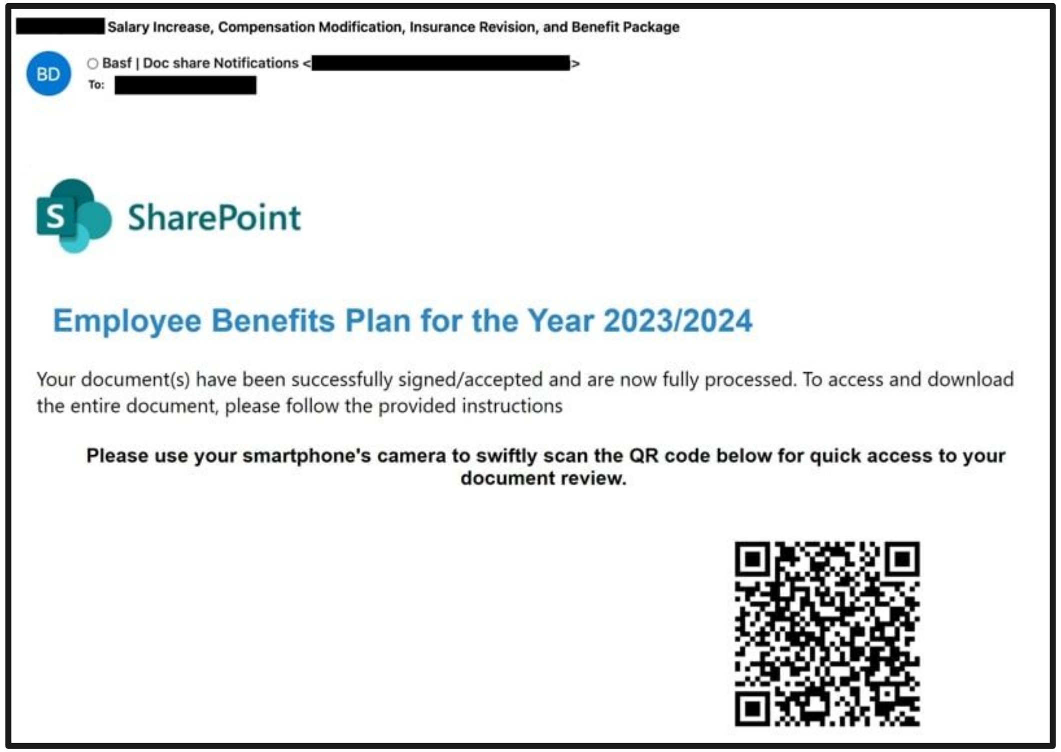
- Inspired by facial recognition systems
- Collects webpage screenshots of trusted and commonly targeted brands
- Follows suspicious URLs to collect screenshots from malicious, credential-phishing sites
- Uses Convolutional Neural Networks (CNN), a deep learning architecture, to detect altered images
- Newly identified webpages are manually verified and labeled accordingly to ensure detection efficacy



Trellix

1. Full Threat Detection Efficacy: How We Achieve It

NEW - QR-Code Phishing (Quishing) Detection



[redacted] Salary Increase, Compensation Modification, Insurance Revision, and Benefit Package

BD ○ Basf | Doc share Notifications <[redacted]>

To: [redacted]

SharePoint

Employee Benefits Plan for the Year 2023/2024

Your document(s) have been successfully signed/accepted and are now fully processed. To access and download the entire document, please follow the provided instructions

Please use your smartphone's camera to swiftly scan the QR code below for quick access to your document review.

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 within email body, images within email body (jpeg, png, etc.), and pdf files

Detected over 150K QR code attacks in 2H '23

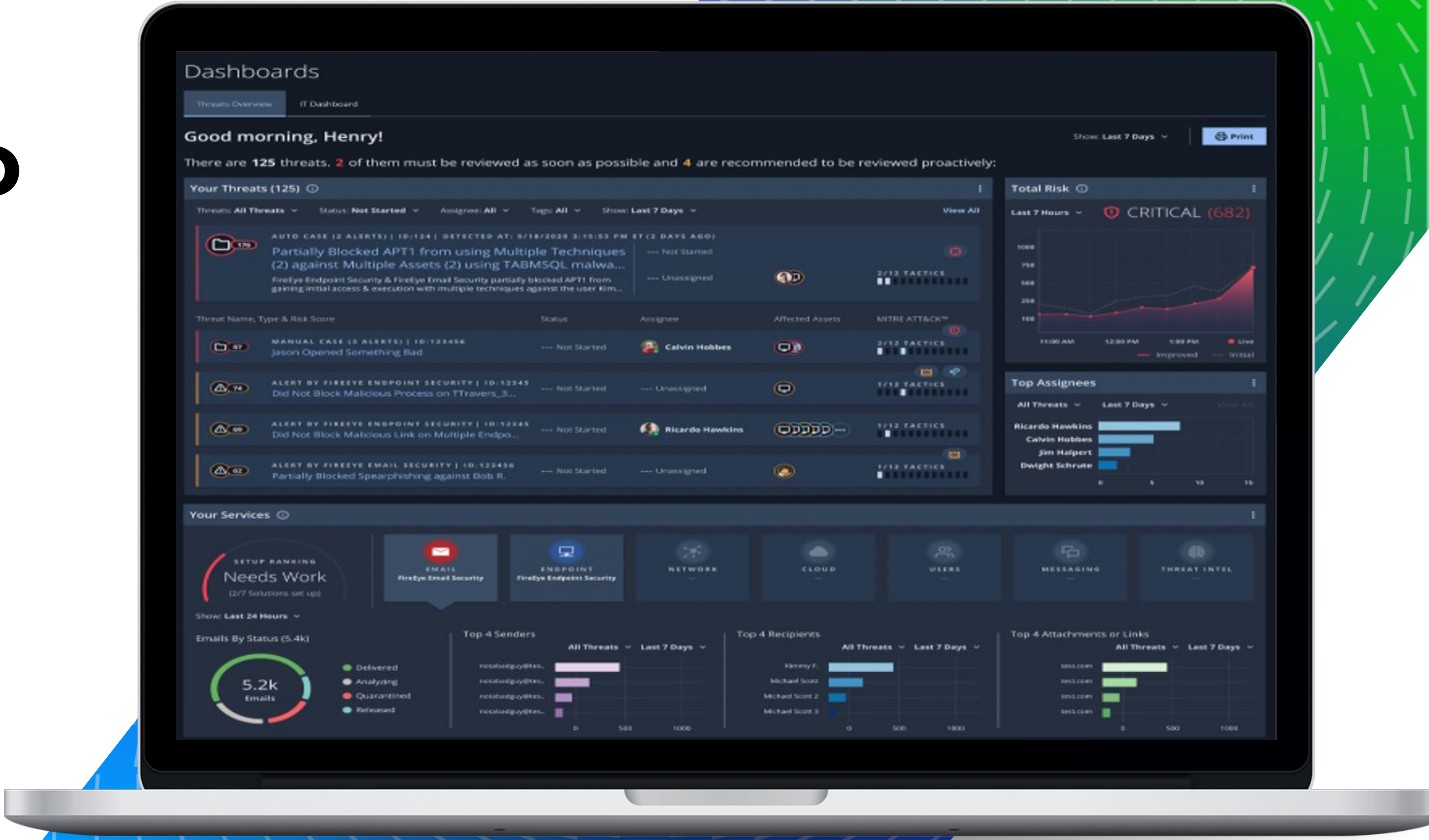
2. Integrated Investigation and Response

Enables integrated investigation and response as part of security operations

- Email alerts with rich metadata are available to Trellix Helix Connect (and third-party SIEM / XDR) to enable analysts to quickly identify source of compromise
- Trellix Helix Connect empowers SOC analysts to clawback emails weaponized post-delivery; other XDR vendors don’t offer a clawback functionality
- Uses newly identified IOCs to search previously received emails and perform retrospective analysis

Stream Email Metadata to Trellix Helix Connect

Accelerating analyst investigation and response workflows



Dashboards

Good morning, Henry!

There are 125 threats. 2 of them must be reviewed as soon as possible and 4 are recommended to be reviewed proactively:

Your Threats (125)

Threats: All Threats · Status: Not Started · Assignee: All · Tags: All · Show: Last 7 Days · View All

AUTO CASE (2 ALERTS) | ID:124 | DETECTED AT: 5/18/2020 3:15:53 PM ET (2 DAYS AGO)

Partially Blocked APT1 from using Multiple Techniques (2) against Multiple Assets (2) using TABMSQL malwa...

FireEye Endpoint Security & FireEye Email Security partially blocked APT1 from gaining initial access & execution with multiple techniques against the user Kim...

--- Not Started · --- Unassigned · 2/12 TACTICS

Threat Name, Type & Risk Score	Status	Assignee	Affected Assets	MITRE ATT&CK™
87 MANUAL CASE (3 ALERTS) | ID:123456 Jason Opened Something Bad	--- Not Started	Calvin Hobbes		2/12 TACTICS
74 ALERT BY FIREEYE ENDPOINT SECURITY | ID:12345 Did Not Block Malicious Process on TTravers_3...	--- Not Started	--- Unassigned		1/12 TACTICS
69 ALERT BY FIREEYE ENDPOINT SECURITY | ID:12345 Did Not Block Malicious Link on Multiple Endpo...	--- Not Started	Ricardo Hawkins		1/12 TACTICS
62 ALERT BY FIREEYE EMAIL SECURITY | ID:123456 Partially Blocked Spearphishing against Bob R.	--- Not Started	--- Unassigned		1/12 TACTICS

Total Risk

Last 7 Hours · CRITICAL (682)

Top Assignees

All Threats · Last 7 Days

Your Services

SETUP RANKING Needs Work (2/7 Solutions set up)

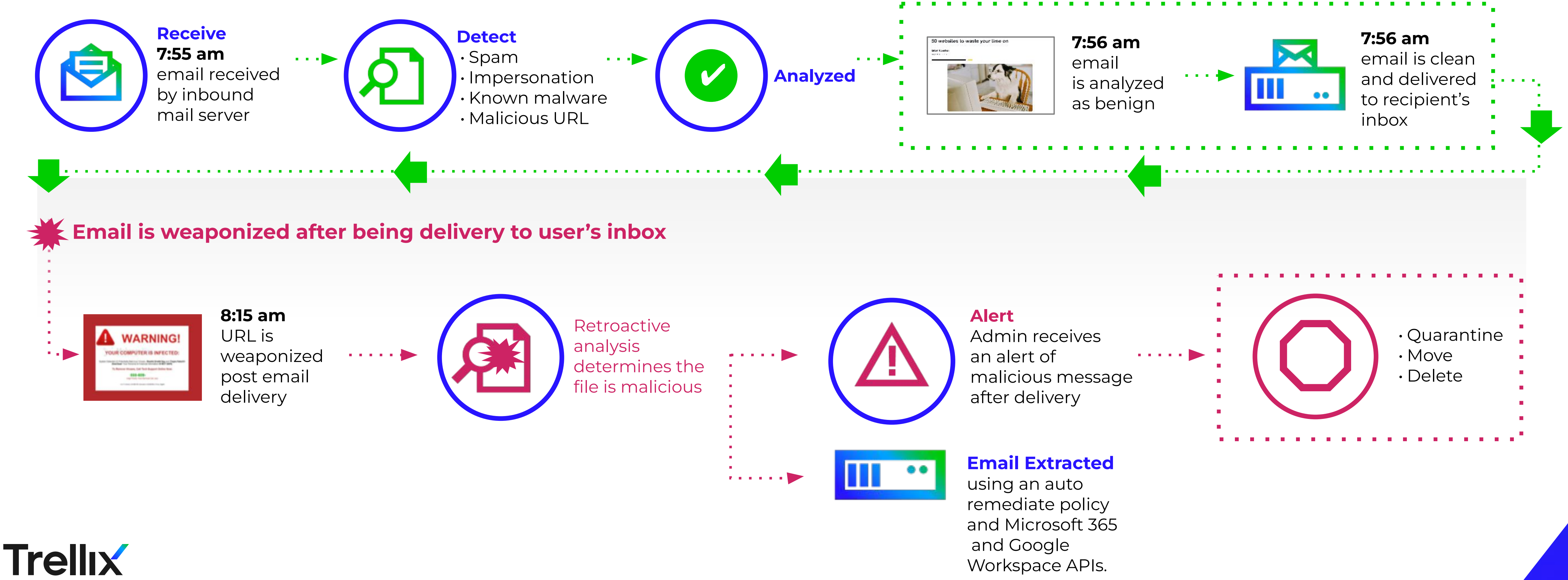
Show: Last 24 Hours

Emails By Status (5.4k)

Trellix

2. Integrated Investigation and Response: How We Achieve It

Clawback emails after delivery



Receive
7:55 am
email received by inbound mail server

Detect
- Spam
- Impersonation
- Known malware
- Malicious URL

Analyzed

7:56 am
email is analyzed as benign

7:56 am
email is clean and delivered to recipient's inbox

Email is weaponized after being delivery to user's inbox

8:15 am
URL is weaponized post email delivery

Retroactive analysis determines the file is malicious

Alert
Admin receives an alert of malicious message after delivery

- Quarantine
- Move
- Delete

Email Extracted
using an auto remediate policy and Microsoft 365 and Google Workspace APIs.

Trellix

3. Comprehensive and Resilient

Trellix Email Security Offerings

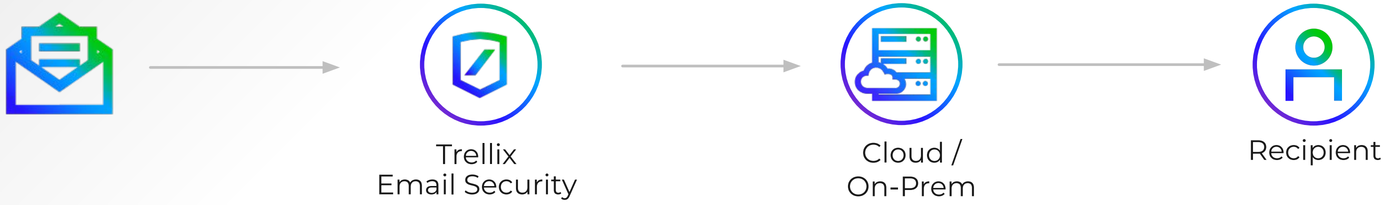
Email Security
Cloud

Email Security
Server

3. Comprehensive and Resilient: Flexible Deployment Cloud Email

Scan/Block

1. **Primary SEG with Full Hygiene**



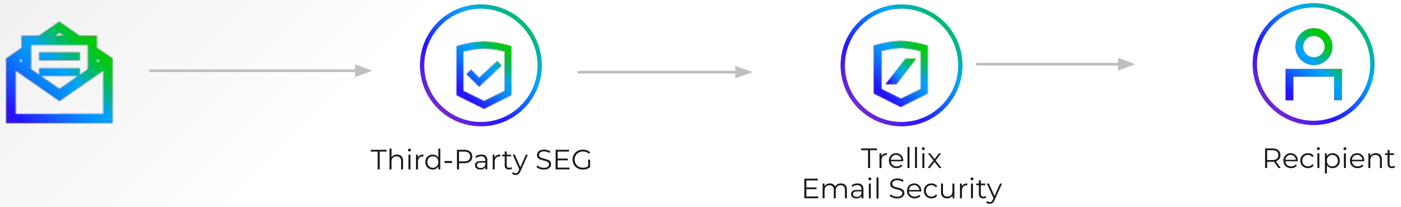
Trellix Email Security

Cloud / On-Prem

Recipient

Scan/Block

2. **Full Hygiene inline, second hop, behind a third-party SEG**



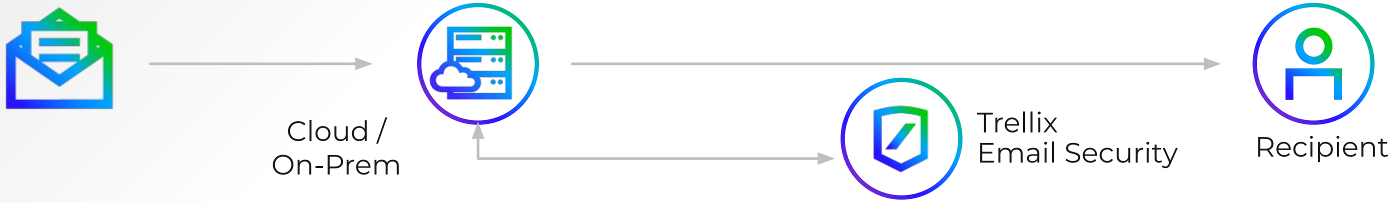
Third-Party SEG

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

3. Comprehensive and Resilient

Telco-Grade Resiliency

Highly Resilient

- 99.995% uptime in last 12 months
- 100% uptime for over 300 days

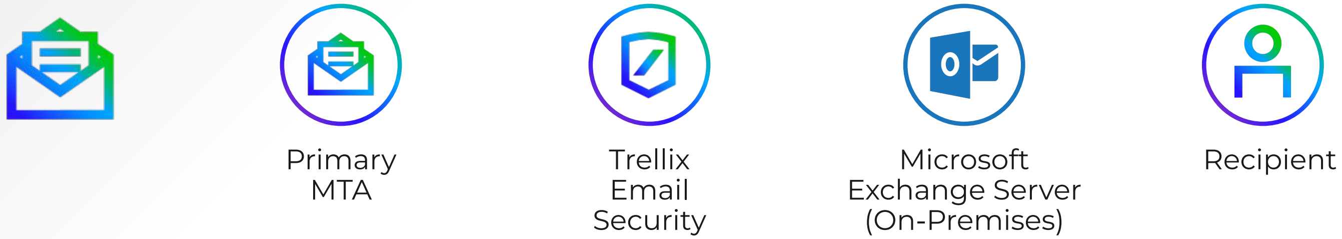
Rapid Processing of Emails

- Average email processing time is less than 10 seconds across all inbound email

FedRAMP

3. Comprehensive and Resilient: Flexible Deployment Server Email

1. **On-prem inline mode**



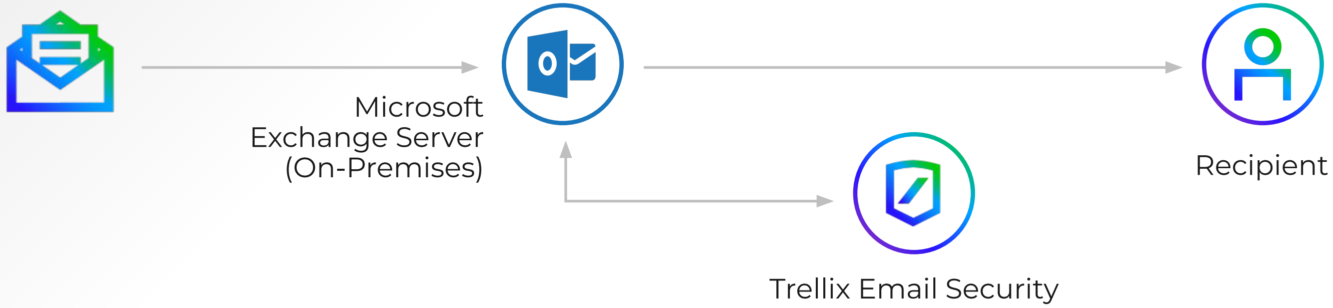
Primary MTA

Trellix Email Security

Microsoft Exchange Server (On-Premises)

Recipient

2. **On-prem in BCC / monitor modes**

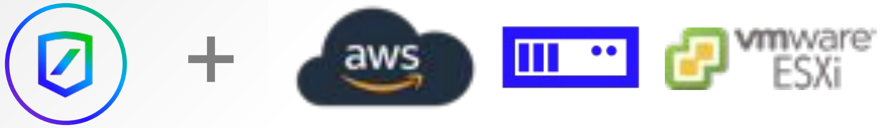


Microsoft Exchange Server (On-Premises)

Recipient

Trellix Email Security

3. **Appliance deployments (Form factors)**



DEMO

DEMO

Trellix Email Security

Trellix

Personas

Who should you engage

Personas

CIO

Economic Buyer

CISO

Technical Buyer

Head of Messaging

Technical Buyer / Influencer

Head of SOC

Influencer

Trellix

CIO

Economic Buyer

Key Responsibilities

Driving digital transformation and enterprise agility while usually having to reduce costs. Security is important, but that is why I hired a CISO.

Before Scenario

- Concern Microsoft is not sufficiently protecting the organization’s email
- Existing email security solution is sufficient, or have another two years before a renewal

Needs

- Value for money
- Uninterrupted employee experience - no noise about False Positive (FP) blocked emails
- Minimal operational effort
- Lower security risk would be nice

Positive Outcomes

- Reduced spend with Microsoft, reduced risk of compromise Able to pursue digital transformation / SaaS while keeping consistent security

Success Measures

- Reduce total cost of ownership
- Simplicity of purchase
- Mail availability
- Reduced infrastructure complexity

Trellix

CISO

Technical Buyer

Key Responsibilities

Focused on minimizing risk, cost, and complexity associated with protecting the organization.

Before Scenario

- Concern over executive impersonation leading to mistaken transactions & data leakage
- Credential phishing opening up organization to ransomware

Needs

- Reduced reported phishing / endpoint incidents from email
- Consistent protection on all collaboration / SaaS connections
- Avoid being a vector for infection of partners and customers

Positive Outcomes

- Improved Security Operation Center (SOC) metrics - lower missed threats
- Ease of scoping potential compromised endpoints from similar emails
- Rapid Indicator of Compromise (IoC) dissemination to other control points

Success Measures

- Reduced FNs reported by users
- Reduction in laptop remediations
- Visibility into identified and blocked campaigns with context
- Executive protection from impersonation and phishing

Trellix

Head of Messaging

Technical Buyer / Influencer

Key Responsibilities

Focused on improving collaboration, ease of use and service availability. Doesn't really care about security.

Before Scenario

- Concern that change will be an effort on their team

Needs

- Clear visibility into message volumes, delivery success, rate limiting
- Simple policy management and reporting

Positive Outcomes

- Simple deployment
- Confidence in 5 9's availability and low latency
- Reduction in operational costs if moving from on-prem to cloud

Success Measures

- Maintain high availability
- Performance - reduce delivery latency

Trellix

Head of SOC

Influencer

Key Responsibilities

Focused on reducing ops effort on user reported spam. Every missed email threat is another hit to investigate.

Before Scenario

- Concern about Mean Time to Detect (MTTD) and Meant Time to Response (MTTR) metrics

Positive Outcomes

- Reduced FNs and user-reported phishing
- Faster investigation pivots
- Ability to report FNs directly to Trellix

Needs

- Availability of email data to support investigations
- Low effort for policy configuration and tuning
- Adopt third-party intel

Success Measures

- Reduced number of employee reported phishing emails
- Improved MTTD and MTTR metrics

Trellix

Pain Point & Discovery Questions

Pain Points	Discovery Questions
Inadequate protection against phishing, ransomware, and BEC attacks	● How often do you validate that your current solution can protect against latest ransomware attacks? ● How does your solution help prevent your executives from becoming victims to impersonation attacks? ● If a partner inadvertently shared a malicious link or file with you via a collaboration platform, do you have a security solution in place to block it? ● How many missed email threats do you see through user reporting and hunting? ● Does your current provider only have email as a source of intelligence?

Pain Point & Discovery Questions

Pain Points	Discovery Questions
Mean time to investigate and remediate still takes too long	● Will you walk me through how your existing solution detects and analyzes threats to help your analysts respond quickly to advanced attacks? ● How quickly can you identify new campaigns, affected users and remove all malicious emails? ● How does your current solution disseminate indicators of compromise found in an email to your endpoint and network solutions? ● What context is provided to help you determine whether a delivered email is benign or malicious?

Pain Point & Discovery Questions

Pain Points	Discovery Questions
Microsoft O365 security is insufficient	● How satisfied are you with the efficacy of your current security solution for Office 365? ● In addition to Defender for Office 365, what other email and collaboration security solutions are you running? ● What Microsoft license package do you have deployed for all of your users; when does it renew? ● Are you interested in learning how you could improve your Office 365 security at a lower price?

Trellix

Proof Points

Customer Case Studies

Case Study #1

Large Government Agency

Saves 15 hours per day with automated remediation

The Challenges

- A prime target for hackers, the agency needed to employ full-time security analysts to address emails, which included malicious attachments and URLs causing them to divert resources from other high-priority projects

The Solution

- Customer using Trellix Email Security – Cloud and MS 365
- Integrated Trellix Email Cloud into MS 365 tenant natively
- Used automated threat remediation feature to manage alerts efficiently

The Results

- Customer's ability to transition the bulk of manual remediation efforts to an automated function has resulted in the ability to recover 15 hours per day!
- With an ever-expanding array of cyber threats, customer was able to redirect those resources towards monitoring other threats, reducing our overall response times.
- Migrating from a fully manual to a primarily automated email threat response has reduced customer's response time for a majority of threats to within minutes.

Trellix Email Security - Catching what others missed

We catch what competitors missed

Our customers are protected from:

- An average of **3.1 Million** targeted attacks per year ***missed by Microsoft*** across **1,560 customers**
- An average of **1.7 Million** targeted attacks per year ***missed by Proofpoint*** across **1107 customers**
- An average of **9.8 Million** targeted attacks per year ***missed by Ironport*** across **1059 customers**

3rd Party Validation

Trellix was awarded SE Lab's 2024 Annual Security Awards for winning the Best Email Security Service Award. This award win confirms Trellix Email Security delivers industry-leading email protection to stop advanced threats through a unique combination of detection, threat intelligence, and security expertise.

SE Labs also awarded Trellix Email Security AAA and 100% Total Accuracy Ratings in its 2023 Email Security Services (ESS) Test, outperforming Microsoft Defender and Google Workplace Enterprise. Trellix also achieved 100% protection against business email compromise, phishing, malware, and social engineering attacks.

Trellix

Product Packaging

What SKUs

Trellix Email Security Offerings

Trellix Email Security Offerings

Email Security
Cloud

Email Security
Server

Trellix Email Security Offerings - Cloud

Protecting customers against the #1 attack vector

Trellix Email Security Cloud deployment types:

- Email Security Cloud with AntiVirus / AntiSpam Edition (deployed as a secure email gateway)
- Email Security Cloud without AntiVirus / AntiSpam Edition (deployed behind secure email gateway)

Trellix Email Security for Office 365: Email Security Cloud without AntiVirus / AntiSpam Edition + IVX Enterprise Cloud

SKU	Capabilities
	Per user based subscription pricing
EMCL	● Email Cloud without AntiVirus / Anti Spam functionality
EMCA	● Email Cloud with AntiVirus / Anti Spam functionality
EMCLVX	● Trellix Email Security for Office 365 (Protects Office 365 including Email + SharePoint + Teams + OneDrive) ● Email Cloud without AntiVirus / Anti Spam + IVX Enterprise Cloud

Trellix Email Security Offerings - Server

Protecting customers against the #1 attack vector

Trellix Email Security Server

- Email Security Server Edition

Requires either deployment of physical or virtual appliance

SKU	Capabilities
	Per user based subscription pricing
EMUSE	• Email Security Server Edition
EM7700-BM -VA	• VM deployment option
EM3600 / 5600 / 8600	• Appliance HW unit

Trellix

UpSell and Cross Sell

How to position to customer

Upsell Motion

Trellix Email Security for Microsoft Office 365

Competitive Replacement of Declining Security Vendors

On-premises Email Security to Cloud Migration

Trellix

Trellix Email Security for Microsoft Office 365

Description:

Organizations running Exchange Online and additional productivity apps in the Office 365 Suite such as Teams, OneDrive, SharePoint ***AND only using*** Microsoft Office 365 Security.

Target Customers:

- Existing Trellix customers not running Trellix Email Security Cloud and IVX for Collaboration with more than 1,000 users
- Territory target prospects with more than 1,000 users

Trellix Email Security for Microsoft Office 365

Solution	Value Add	Value Messaging	Customer Positive Outcomes
Trellix Email Security Cloud + IVX for Collaboration Platforms	**Advanced threat defense for Office 365**	● Seamlessly protect Microsoft Office 365 with cloud-native API integration for superior protection without the premium license cost ● Trellix Advanced Research caught over 3M malicious emails missed by Microsoft from 1,560 joint customers in 2023 ● On average, every customer with Microsoft E5 security still sees 60-70 email-based campaigns get through every week - and an attacker only needs ONE!	● Reduce risk of compromise through your collaboration platforms ● Save your Security Operation Center (SOC) team's time investigating phishing reports ● Prevent executive impersonation to reduce financial loss or compromise ● Reduce risk of ransomware through improved email protection ● Reduce risk of credential theft and subsequent intrusion

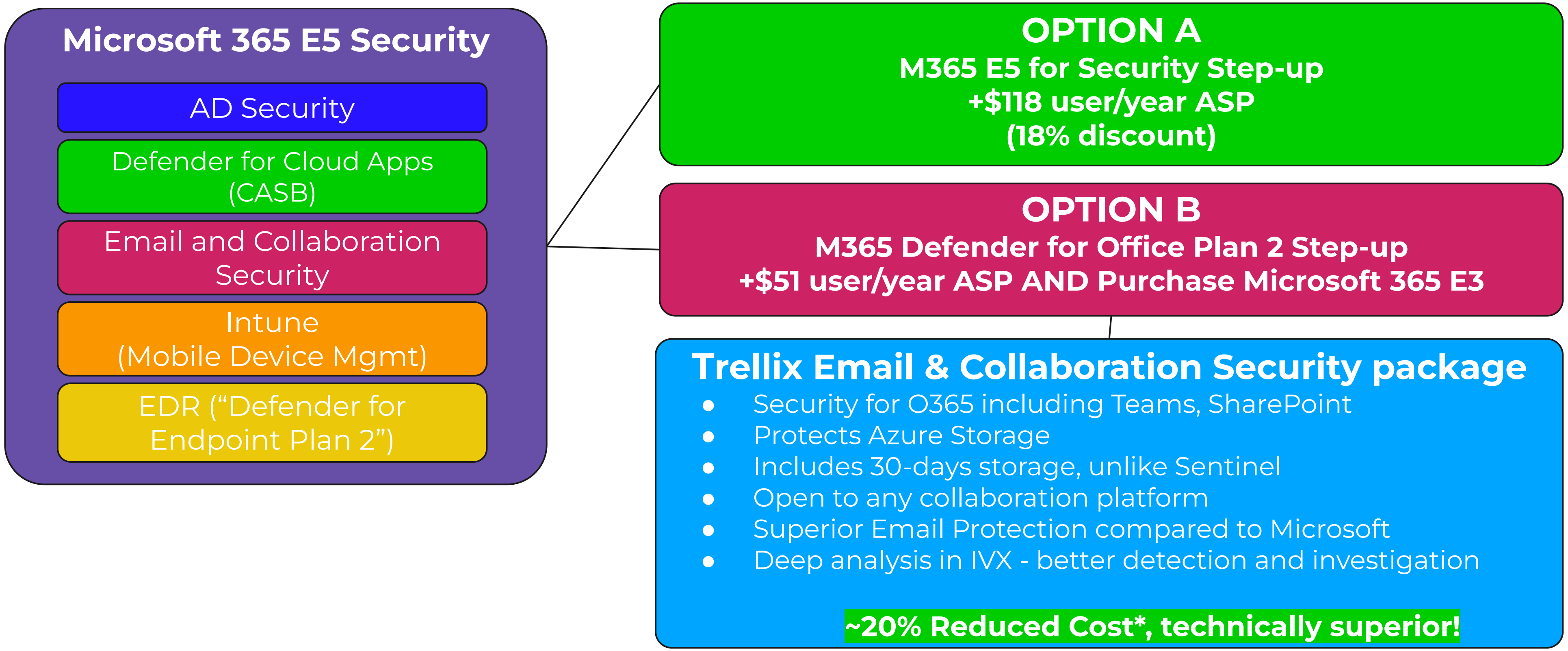
Discovery Questions

- How satisfied are you with the efficacy of your current security solution for Office 365?
- In addition to Defender for Office 365, what other email and collaboration security solutions are you running?
- What Microsoft licensing package do you have deployed for all of your users?
- When does your Microsoft Enterprise Agreement renew?
- Are you interested in learning how you could improve your Office 365 security at a lower price?

Cautions:
Customer may state that Microsoft Office 365 security is free with the E5 license.
Respond with: Opting for Microsoft E3 and supplementing it with Trellix Email Security for Office 365 could lead to savings of up to $180 per employee annually, on average.

Microsoft 365 Security Options

Probe on what packages are currently purchased for ALL employees



Microsoft 365 E5 Security

- AD Security
- Defender for Cloud Apps (CASB)
- Email and Collaboration Security
- Intune (Mobile Device Mgmt)
- EDR ("Defender for Endpoint Plan 2")

OPTION A
M365 E5 for Security Step-up
+$118 user/year ASP
(18% discount)

OPTION B
M365 Defender for Office Plan 2 Step-up
+$51 user/year ASP AND Purchase Microsoft 365 E3

Trellix Email & Collaboration Security package

- Security for O365 including Teams, SharePoint
- Protects Azure Storage
- Includes 30-days storage, unlike Sentinel
- Open to any collaboration platform
- Superior Email Protection compared to Microsoft
- Deep analysis in IVX - better detection and investigation

~20% Reduced Cost*, technically superior!

*Based on analysis with cost comparisons of comparable organizational sizing, packaging and typical customer cost

If E3 Customer, Say This:

"Trellix Security for Office 365 provides the best level of protection at a significantly lower price than Microsoft Plan 2 for Office 365."

If E5 Customer, Say This:

"You could save up to $200 per user per year if you downgraded to E3 and adopted Trellix Security for Office 365."

Trellix

Competitive Replacement: Declining Security Vendors

Description:

Organizations running Microsoft Exchange Online **OR** Google Gmail **AND** using additional email security vendor protection such as Cisco IronPort or Broadcom (Symantec) with large install bases, but declining.

Target Customers

- Existing Trellix customers not running Email Security Cloud or On-Prem with more than 1,000 users.
- Territory target prospects with more than 1,000 users

Competitive Replacement: Declining Security Vendors

Solution	Value Add	Value Messaging	Customer Positive Outcomes
Email Security Cloud	**Advanced threat defense for Microsoft Exchange Online OR Google GMAIL**	● Trellix Email Security provides higher threat efficacy than our other security vendors according to internal Trellix testing, as well as 3rd-party testing ● Trellix observed Cisco Ironport missed on average 1,980 malicious emails weekly, per customer in 2023 ● Trellix observed Broadcom missed on average 460 malicious emails weekly, per customer in 2023	● Reduced reliance on employees to spot phishing emails ● Protection of your executives from impersonation ● Prevention of employee credentials being stolen through fake application log on pages ● Prevention of supply chain partner impersonation

Discovery Questions

- How many phishing emails have to be investigated by your SOC team every week?

- How many endpoint malware alerts do you see per week, and how many of these came in through email?

- What is the cost for your SOC and IT teams of every malicious email that gets through and is actioned by a user?

Cautions:

Customers may question what we miss and others see.

Response: "That's why we submit our solution to SE LABS for an objective external audit at least once per year. Most of our competitors do not."

On-Prem Email Security to Cloud Migration

Description:

On-prem email organizations migrating to Exchange Online (Office 365) OR Gmail (Workspace) and running email security appliances from vendors such as Trellix, Cisco, Broadcom (Symantec), Barracuda, Sophos, or Fortinet.

Target Customers

- Territory target prospects with more than 1,000 users
- Trellix on-prem Email Security customers with more than 1,000 users

On-Prem Email Security to Cloud Migration

Solution	Value Add	Value Messaging	Customer Positive Outcomes
Trellix Email Security Cloud	**Advanced threat protection of Microsoft Exchange Online and Google Gmail**	• Flexibility in deployment: Customers on-prem can move to our SaaS offering, or deploy in their own cloud tenant • No duplicate costs: Customers migrating to the cloud benefit from our email per user model, and permit 12 months to migrate users from on-prem to cloud without incremental cost	• Reduced reliance on employees to spot phishing emails • Protection of your executives from impersonation • Prevention of employee credentials being stolen through fake application log on pages • Prevention of supply chain partner impersonation • Automatic sharing of IoC's through to Trellix endpoint and network products

Trellix

Discovery Questions

- Are you planning to keep your email platform on-premises or move to the cloud? Over what timeframe?
- What are the reasons for remaining on-prem? / When is your current solution up for renewal?
- Most on-prem solutions are for hygiene protection, how are you protecting against advanced threats? / Have you recently tested your email protection via a red-team exercise?
- What's the impact for your team of the reported vulnerabilities in Barracuda and Fortinet mail gateways?

Cautions:
Customer may have regulatory / security reasons for remaining on-premises. ***Emphasize our strategy for hybrid protection, options for offline / one-way in highly regulated and secure environment.***

Trellix

What new information that you have learned today?

Trellix