Trellix

Catch what other solutions miss

EMAIL and IVX collaboration security update

Vinoo Thomas
Gustavo Arias

July 9, 2024

Speaker Intro

Vinoo Thomas

Principal Product Manager,
Trellix

Gustavo Arias

Principal Solutions Engineer,
Trellix

Trellix

Agenda

1. Why invest in Trellix Email and Collaboration Security?
2. The Trellix differentiator
3. Some Cool Demos
4. ATD-IVX migration path

Trellix

Takes only one email to get through defenses

KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Phish Leads to Breach at Calif. State Controller

March 23, 2021 35 Comments

A phishing attack last week gave attackers access to email and files at the California State Controller's Office (SCO), an agency responsible for handling more than $100 billion in public funds each year. The phishers had access for more than 24 hours, and sources tell KrebsOnSecurity the intruders used that time to steal Social Security numbers and sensitive files on thousands of state workers, and to send targeted phishing messages to at least 9,000 other workers and their contacts.

Fake DHL emails allow hackers to breach Microsoft 365 accounts

HARMONY EMAIL APRIL 15, 2024

Microsoft and Google Top the List in Q1 2024 Phishing Attacks

Cyber Attack | Cyber Security | Cyber Security News

Hackers Launch Business Email Compromise attacks on The Automotive Industry

Articles / News

QR code and image-based email attacks rising, AI isn't helping

Email-based phishing attacks has surged 464% in 2023: Report

A new report by Acronis unveils troubling trends - cybercriminals exploit AI, persistence in ransomware attacks, and significant surge of data stealers.

CYBERSECURITY

Black Friday phishing attacks

42,000 Records Breached in Cancer Treatment Center Phishing Hack

A Cancer Treatment Centers of America employee fell victim to a targeted phishing email in May, providing the hacker with their network credentials.

Home > News > Computing

Nearly all Microsoft 365 customers have suffered email data breaches

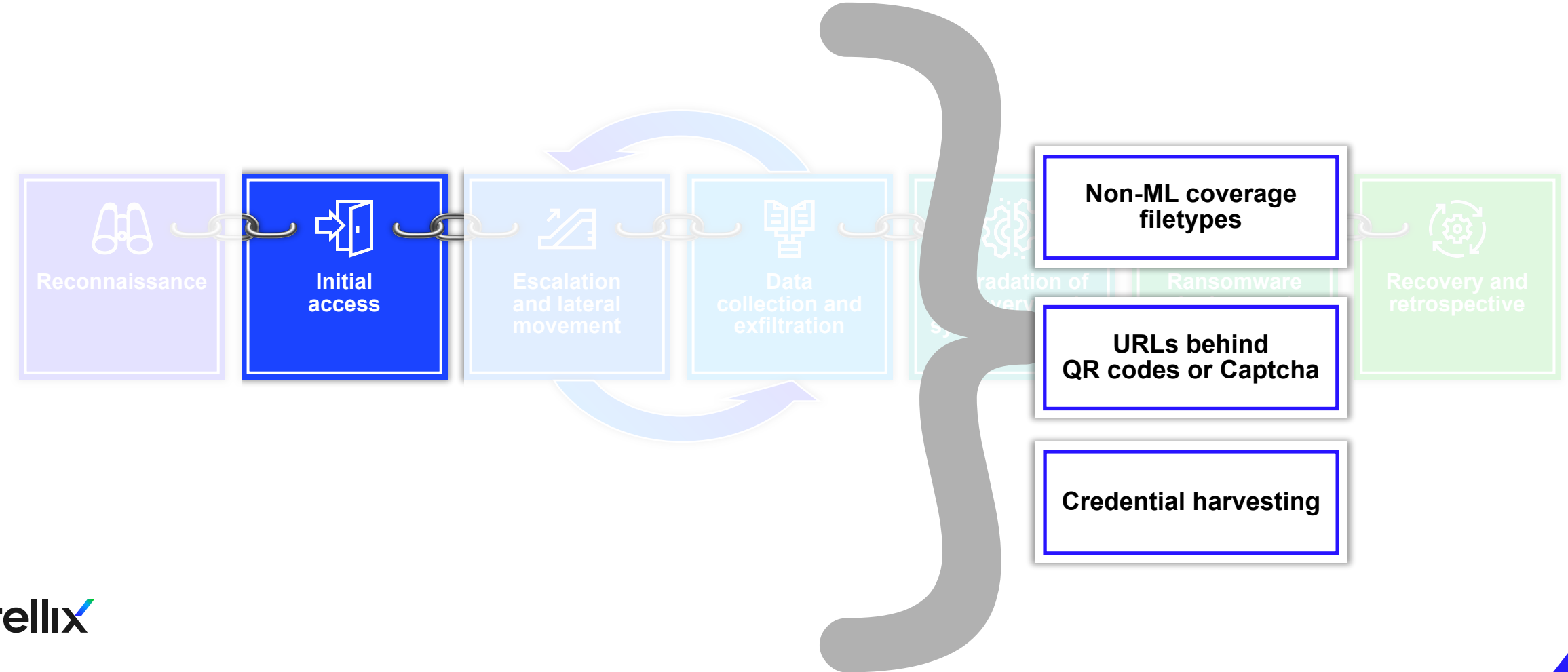
By Sead Fadilpašić published May 11, 2021

85% of Microsoft 365 business customers affected

(Image credit: Pixabay)

Trellix

Where we see the biggest gaps



Trellix

Nature of collaboration has changed

Trellix Collaboration Security

Email

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

Collaboration Platforms (Box, Teams, Slack etc.)

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

Enterprise Applications (Workday, Salesforce etc.)

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

Trellix

Proven technology to address distinct use cases

IVX for Products

Targeted for Trellix Appliances

MVX 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

Product: Trellix IVX

IVX for Investigators

Targeted for the SOC

Used during investigative workflows

Detonate suspicious content

Reverse engineer malware

Product:
Trellix Malware Analysis

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

Products: Trellix IVX Cloud
Trellix File Protect

Trellix

IVX Brand Name for all Sandbox Product Lines

We have an array of sandbox products available to customers today

Intelligent Virtual eXecution

Trellix

Key Features

Signature-less, dynamic analysis engine — Captures and confirms zero-day, and targeted APT attacks

Proprietary hypervisor — Detonates files, URLs, web objects, and email attachments within proprietary hypervisor instrumented for over 200 potential simultaneous executions

Static scanning — Includes object decomposition & emulation, machine learning and statistical analysis to conduct one-to-many analysis

Cross portfolio integration — Integrates with Trellix Network Security, Trellix Email Security, Trellix File Protect and Trellix Endpoint Security

Broad OS support — Analyzes threats across Windows, macOS and Linux operating systems

VX5600
VX12600

Hardware Appliance

Upto 15,840 files per day
Upto 120,960 files per day

NUTANIX

vmware

Virtual Appliance

Upto 4,320 files per day

aws

AWS Bare Metal
c5.metal

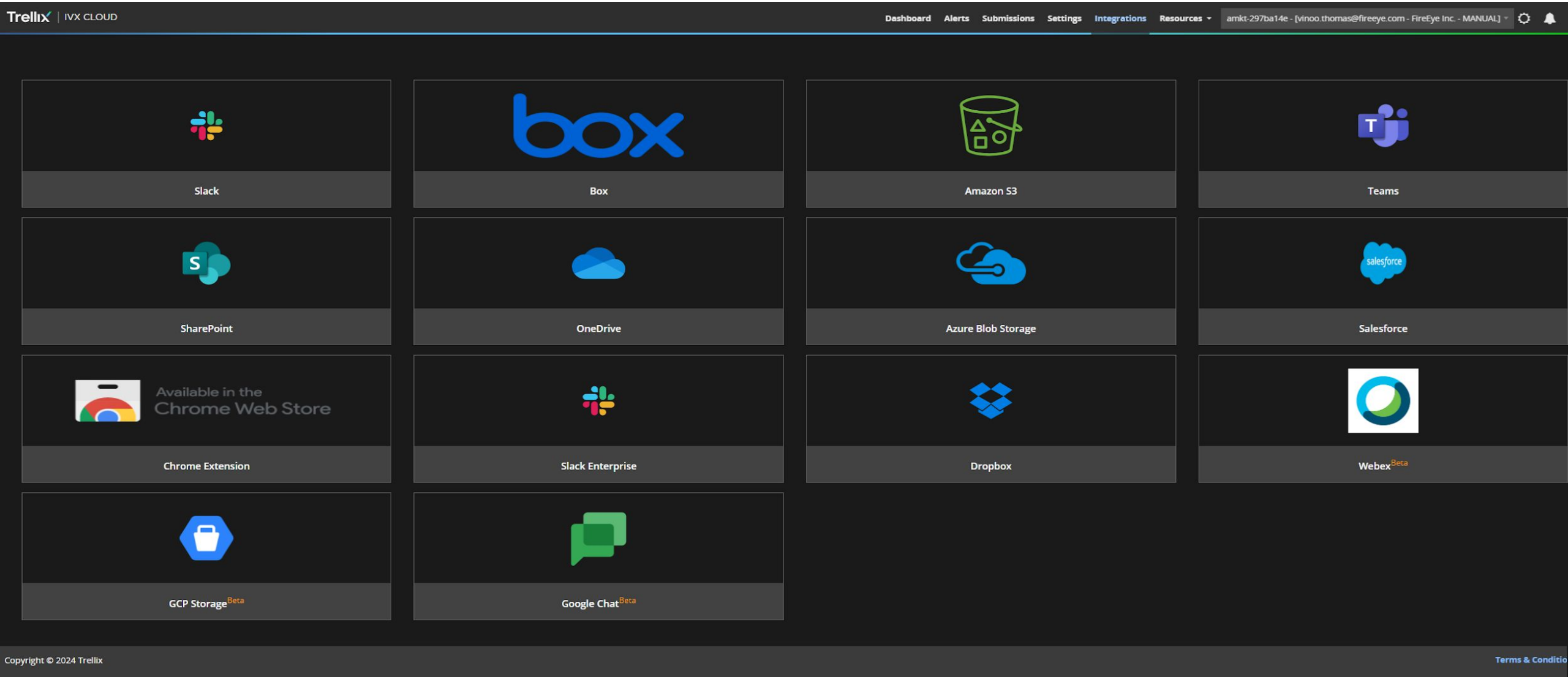
Cloud Appliance

Upto 150,000 files per day

[Trellix IVX Datasheet]

Trellix

IVX Cloud: Integrations available



Trellix Email Security for MS O365

- Detection of malicious content across O365 - Email, SharePoint, One Drive, Teams
- Bundled Offering available from April Pricebook
- Email Security Cloud and IVX Cloud Integrations

Defender for Office Plan 2 Step-up
+$51 user/year*
*with commitment

Trellix Email Security for Office 365

- ETP + IVX bundle - single SKU in April
- Security for O365 including Teams, SharePoint
- Includes 30 days storage, unlike Sentinel
- Open to any collaboration platform
- Superior Email Protection compared to MS
- Deep analysis in IVX - better detection & investigation

ASP $36 user / year –
30% less, technically superior!


Trellix

DATA SHEET

Trellix Email Security for Microsoft Office 365

Step up your email defense while decreasing your spend.

Benefits

- Reduce the risk of email-borne threats
- Superior protection without the premium license cost
- Seamlessly protect Microsoft Office 365 with cloud-native API-enabled integration
- Automatically extract emails weaponized post-delivery
- Inspect and block malicious objects shared via Sharepoint, Teams, and Slack

It only takes one email to breach an organization.

Email continues to be the most successful attack vector. Over 90% of cyberattacks begin with email-borne techniques such as phishing, business email compromise, and executive and vendor impersonation. Cybercriminals use targeted social engineering to trick users into opening compromised attachments or clicking on malicious URLs that steal credentials. It only takes one malicious email to breach your organization, putting corporate and customer assets at risk.

And as companies use Sharepoint, Teams and Slack to transform employee and partner collaboration, threat actors are already exploiting this largely unprotected attack vector.

Microsoft users are not stepping up

In an effort to simplify operations, many organizations have moved to Microsoft 365 Enterprise, with the vast majority opting for the Microsoft 365 E3 license.

Tre

We detect what other vendors miss

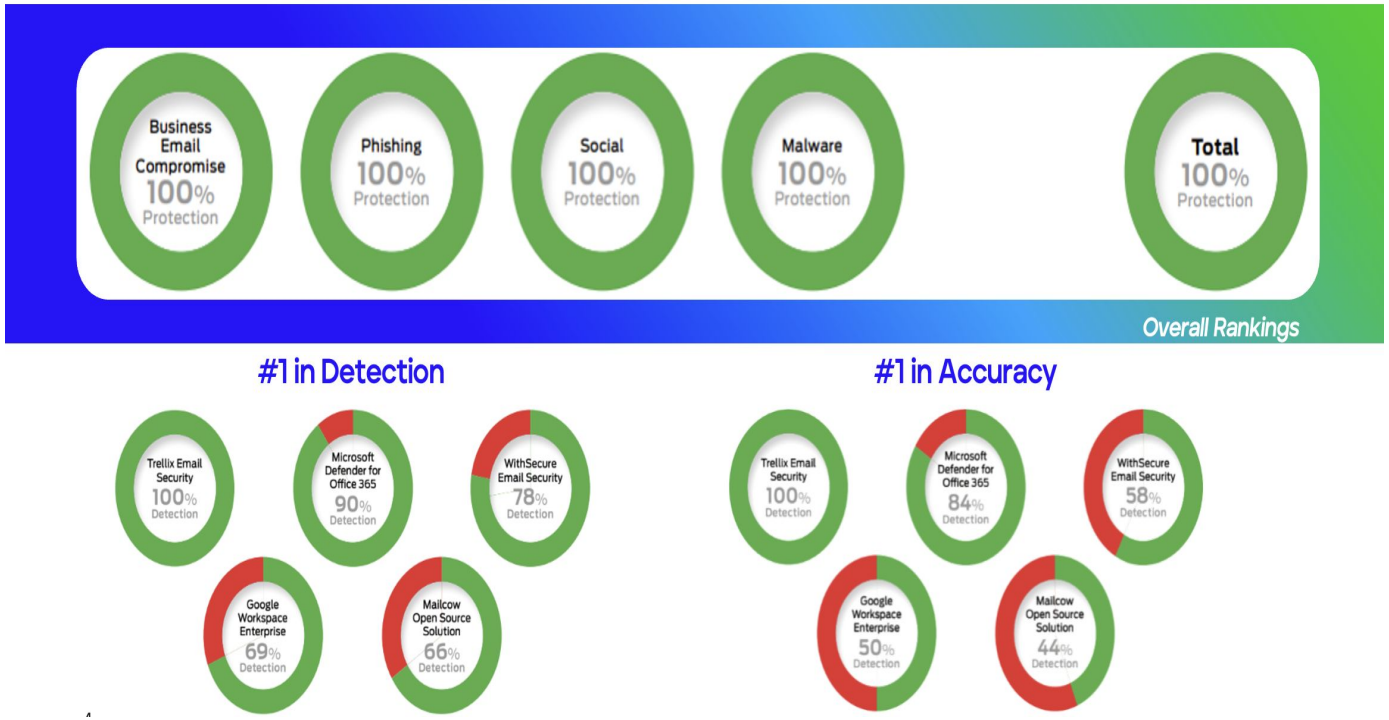
Trellix

Industry Awards & Recognition

Best Email Security Service Award

Email is the primary vector for cyber threats. As such, there is much opportunity for email security services to stop cyber attacks at their earliest stages. With the rising menace of targeted assaults, often leveraging sophisticated social engineering tactics, the imperative for email security services to evolve and counter such threats becomes ever more pressing. This year's champion has consistently showcased its prowess in discerning malicious intent from legitimate communication, reaffirming its role as a stalwart defender against digital adversaries.

The winner of this year's Best Email Security Service Award is Trellix.

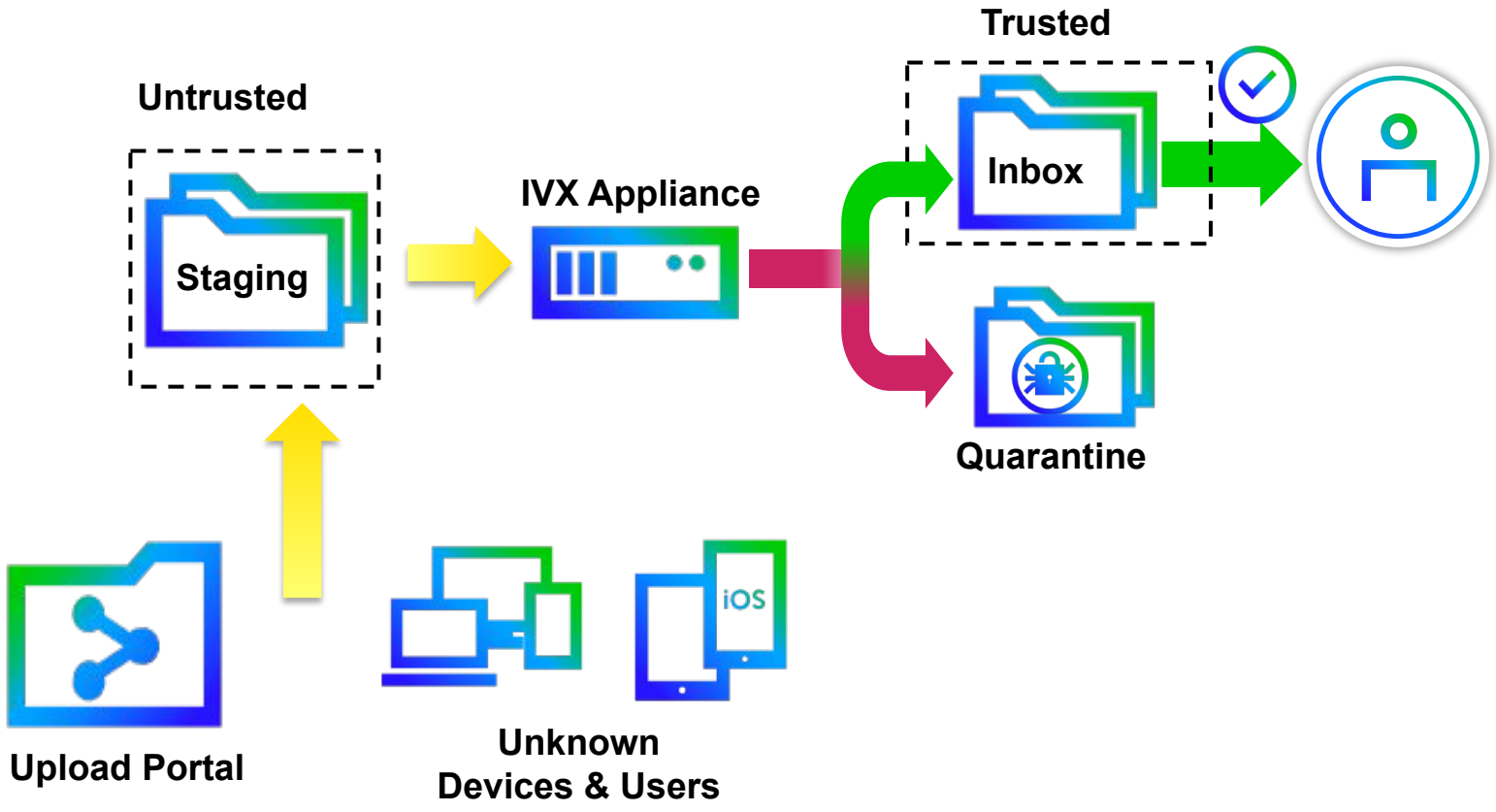


Demo
IVX Cloud integration

- Chrome Extension
- S3 bucket scanning

Trellix

Trusted & Untrusted File Domains



Benefits

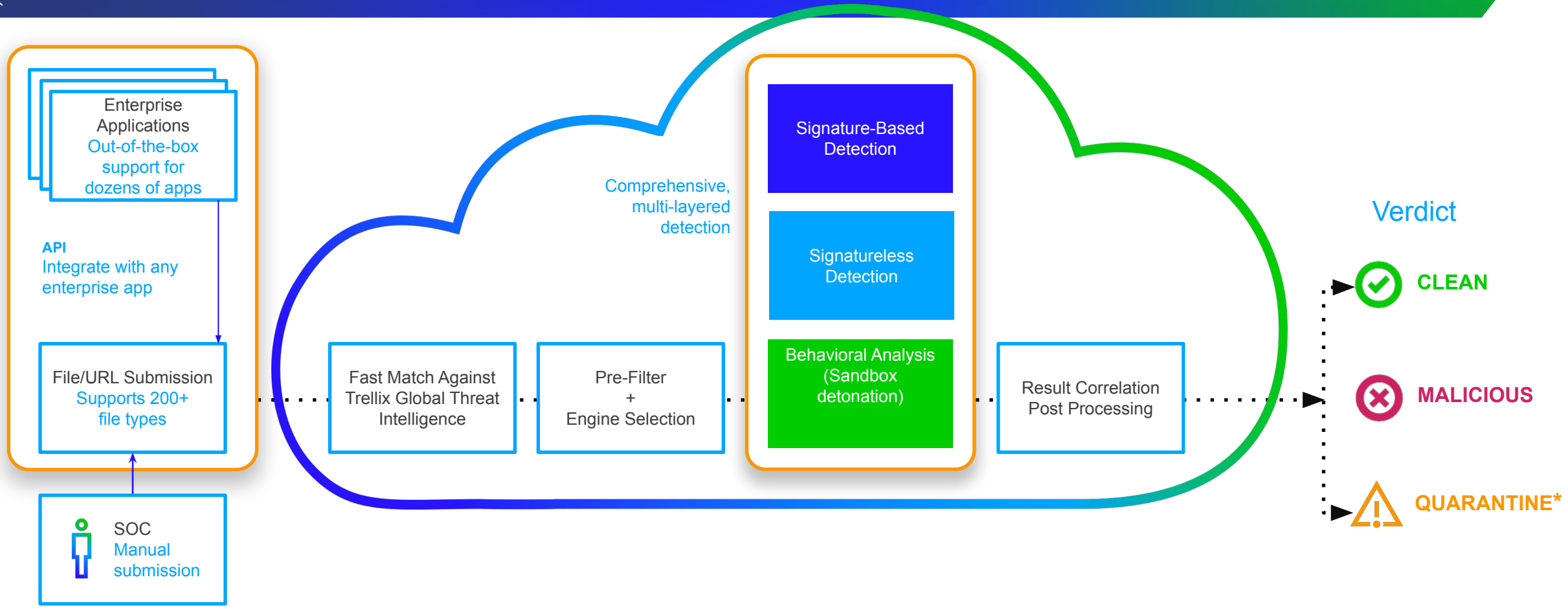
- Stop malware entering enterprise storage from untrusted area
- Ensure files are clean before end users access them

Scenarios

- Insurance Claims
- Bank Account Registration
- Visa Processing

Trellix

Trellix IVX - How it works



Trellix

Sandbox Evasion Techniques

Malware can easily detect a public sandbox **before executing** its payload:

Disk Drive
Disk volume serial number
Display Adapter
Domain
Host Name
MAC address
Environment variable name
Debugger present?

Trellix

Sandbox Evasion Techniques

Malware can check running environment **before executing** its payload:

Mouse activity
No recent files presence
Processors Count
Performance counter frequency
Screen resolution
Sleep evasion
Time zone
Locale

Trellix

Trellix IVX - Sandbox Customizations

User Name
Domain Name
Host Name
Home Directory
Windows Recent Files
Office Recent Files
Browser History URL
Honey Credentials
Honey Files & Directories
DNS Cache Entries
Host File Entries
Outlook Account
FTP Account
Skype Account
Locale & Time zone

Trellix

Trellix IVX – Custom Detections

Link within Email Body
Scripts Delivered via Email
Executable Delivered via Email Attachment
Encrypted PDF Document
Encrypted Office Document
Office Document With Embedded Object
Office Document with Embedded SWF
Office Document With Macro Activity
Excel Formula Python Script
Email with MS Access DB Attached
Password Protected Archives
Attacker Abused Legit Tool
Corrupt Windows PE File
Potential Zip Bomb

+ YARA

Trellix

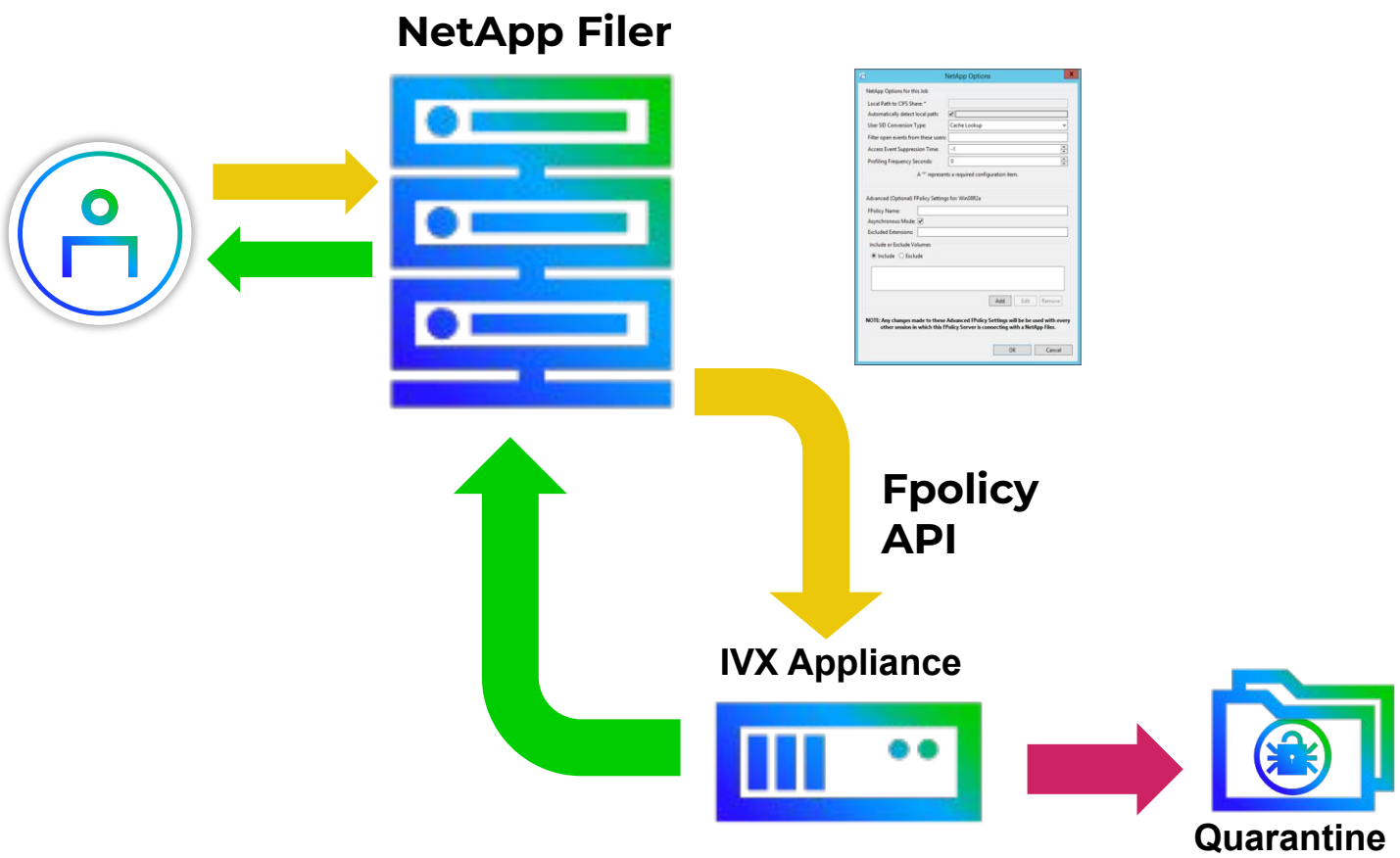
Demo
Trellix File Protect (FX)

- NetApp scanning
- Mount NFS/CIFS/SMB share for scan

Trellix

Trellix

Scanning NetApp Filer (Event Driven)



Benefits

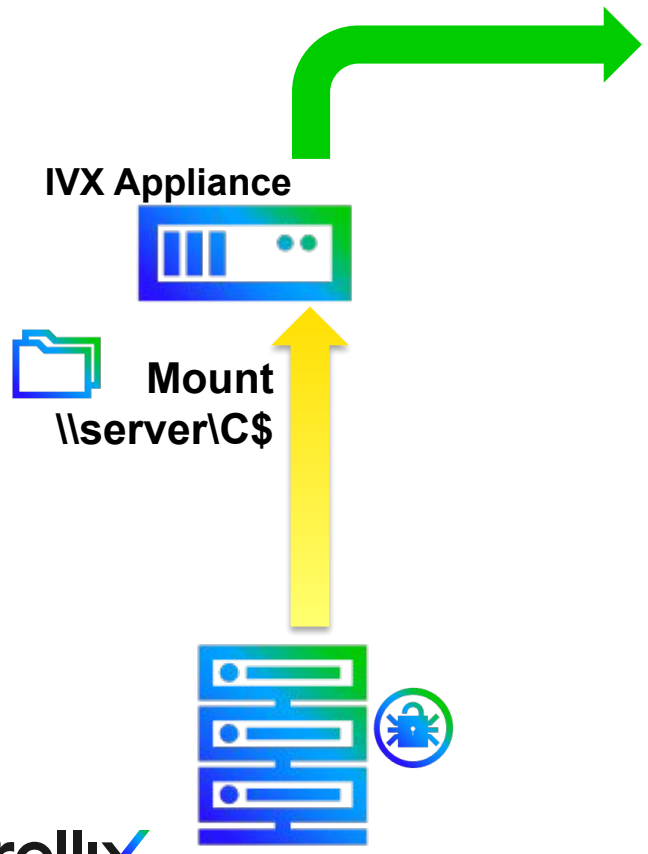
- Monitor and Scan the changes of NetApp Filer in real time through integration with Fpolicy API

Scenarios

- File storage and sharing in NetApp Filers

Trellix

Server Hard Drive Scanning



Detailed Logs

25178 files processed
125 files malicious

Filename	Malware
budget2012.xls	Malware.binary
default.jpg.exe	Malware.binary
imgis.swf	Trojan.banco
directory.pdf	Worm.mydoom
Invitation.doc	Trojan.hiloti
SalesBrochure.pdf	Malware.binary
a.exe	Trojan.agent

Benefits

- Proactive scanning of server hard drive for advanced malware
- Off-box scanning of infected or legacy servers
- Identify malware not found by end-point AV

Scenarios

- Server admin team to proactively protect critical infrastructure
- CSIRT or Forensics team investigating infected servers

Trellix

ATD-IVX

Upgrade Path

1) **Update Package**
   Trellix Product download site

2) **Physical & Virtual ATD upgrade**
   License auto populated in the backend

3) **Virtual CMS and Virtual EX**
   $0 offering to assist with ATD migration

4) **No additional OS guest image license**
   Microsoft Windows, macOS and Linux covered

5) **1-Way and Offline License available**
   At additional cost – talk to your account team

Trellix

Benefits of IVX over TIS (ATD)

Targeted for Trellix Appliances

- **Better overall detection** efficacy through proven VX multi-session execution engine technology:
  - Support for over 200 files types
  - Advanced URL analysis capabilities

- **Operational Efficiencies:**
  - Support for static and **dynamic analysis of macOS and Linux** malware.
  - **No additional license fees** for Windows, MacOS guest images.
  - The Guest **images are hardened, tuned and OS/application updates provided by Trellix**. No need for customers to maintain Guest images. (yes, customization is possible)
  - Patented technology to **run multiple versions of an application within the same Guest OS**. Ex: Multiple versions of Office, java, PDF reader, Flash etc. on the same guest image

- **Strategic** detection engine for **future development** and **integrations:**
  - Critically, future R&D investment and new features will be focused on IVX going forward.
    Ex: Adding native ICAP interface and other integrations.
  - Collaboration Platforms and Enterprise Applications

Q&A

Trellix


Trellix