Trellix

Intelligent Virtual Execution (IVX) goes beyond a Sandbox

Learn how IVX protects collaboration platforms and enterprise applications

Vinoo Thomas
Carlo Bolzonello

Speaker Intro

Vinoo Thomas

Principal Product Manager,
Trellix

Carlo Bolzonello

Country Leader South Africa,
Trellix

Trellix

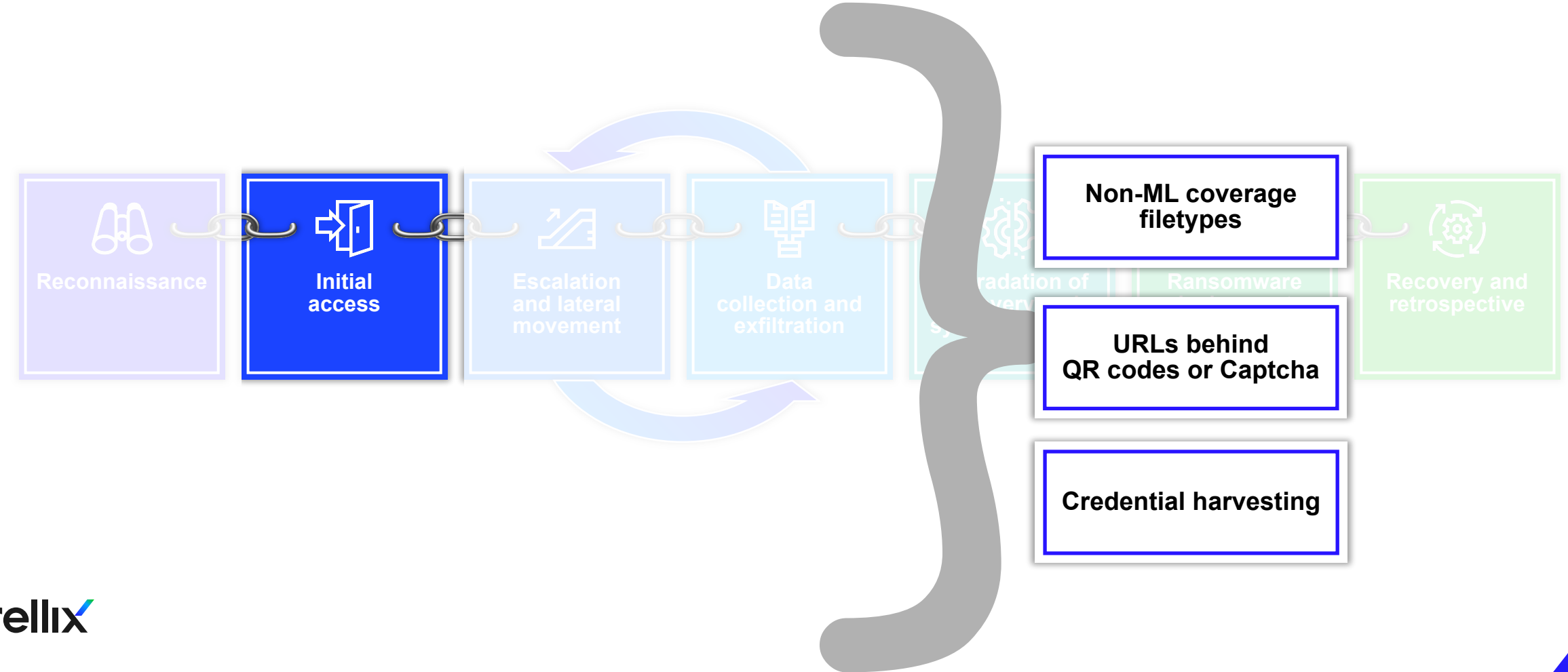
Agenda

1. Why invest in a Sandbox?
2. The Trellix Sandbox differentiator
3. Some Cool Demos
4. ATD-IVX migration path

Trellix

Is there still a role for Network Security?

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

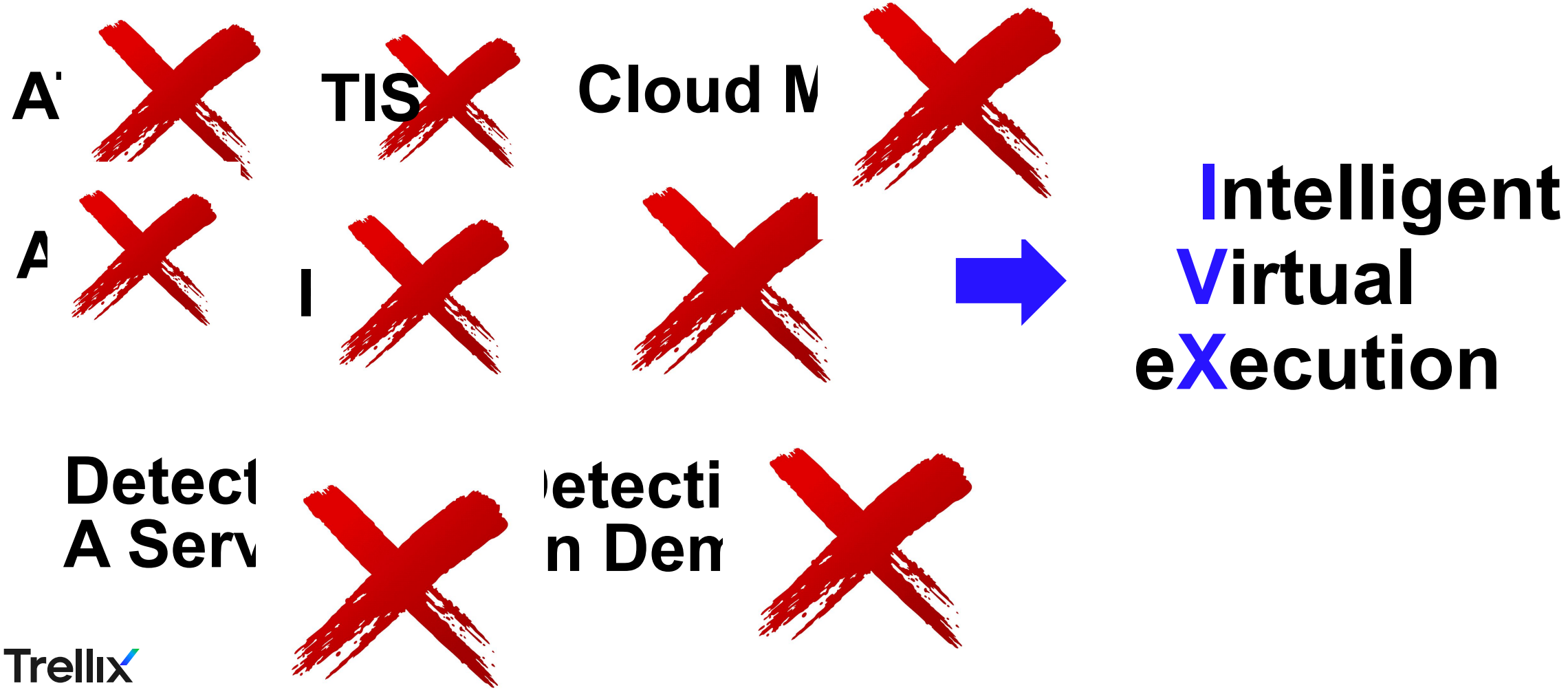
Mitigate the risk of working with external organizations and vendors

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



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

Appliances

VX5600 — Upto 15,840 files per day

VX12600 — Upto 120,960 files per day

NUTANIX

vmware

Upto 4,320 files per day

Cloud

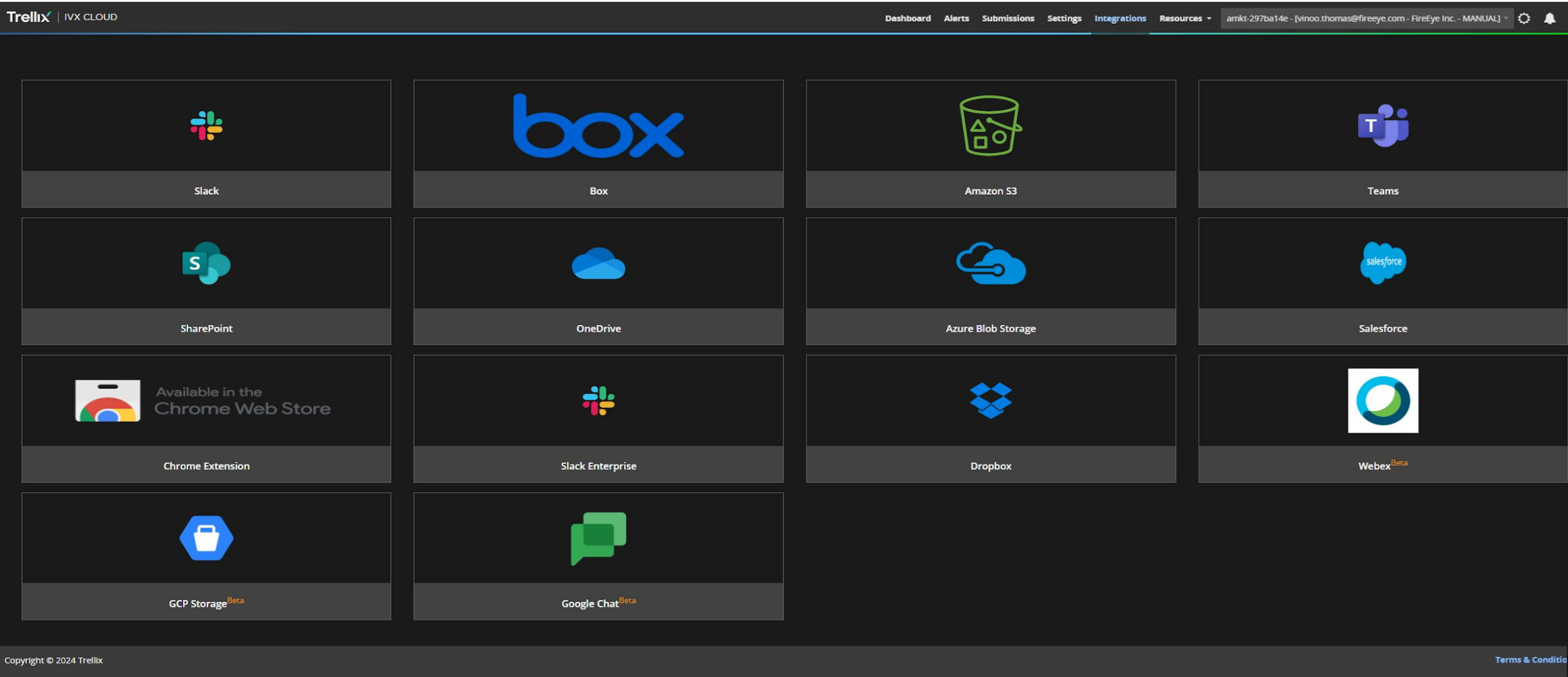
aws

AWS Bare Metal c5.metal — Upto 150,000 files per day

[Trellix IVX Datasheet]

Trellix

IVX Cloud: Integrations available

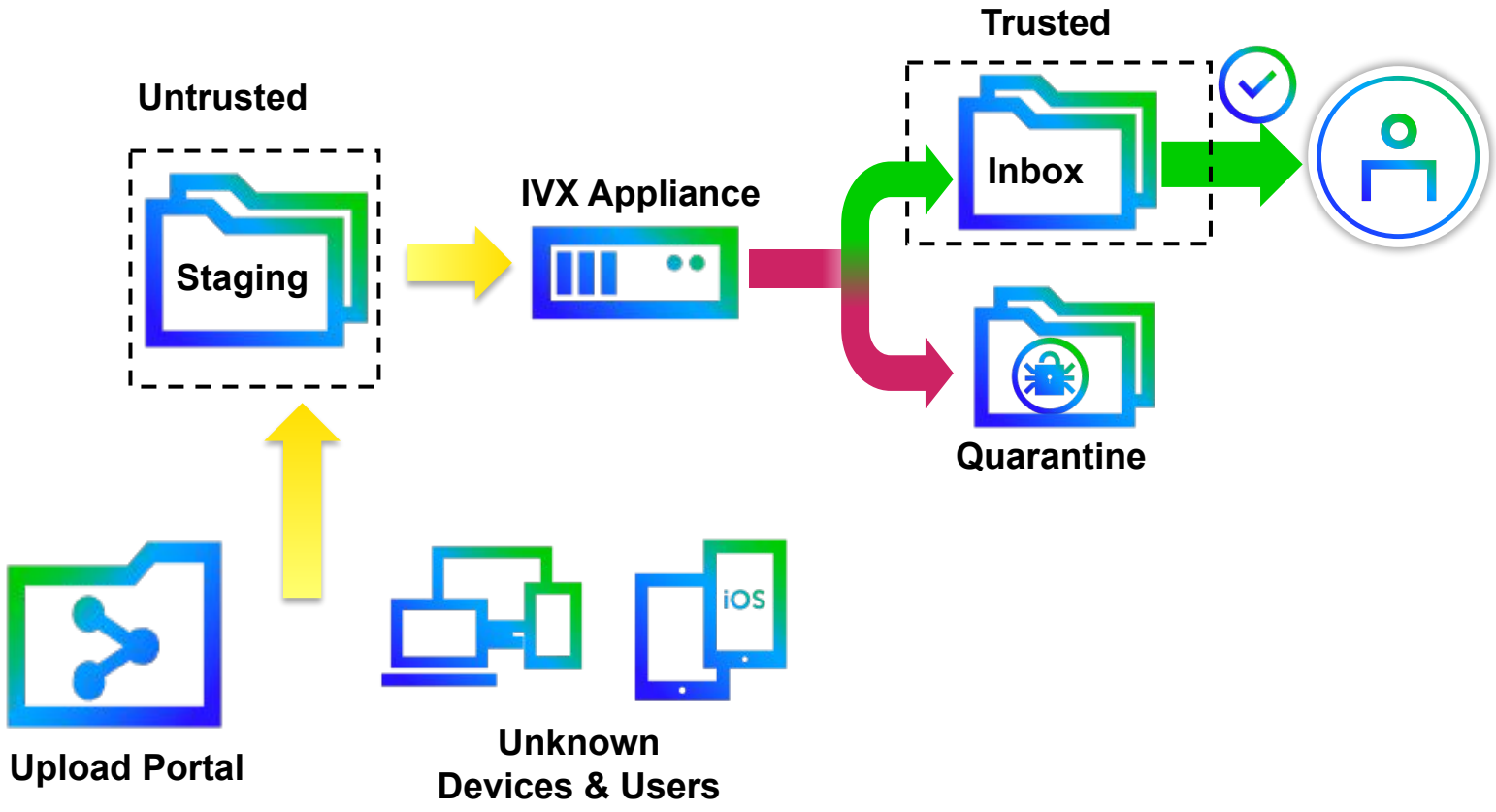


Demo
IVX Cloud integration

- Chrome Extension
- S3 bucket scanning
- Custom Workflow using APIs

Trellix

Trusted & Untrusted File Domains



Benefits

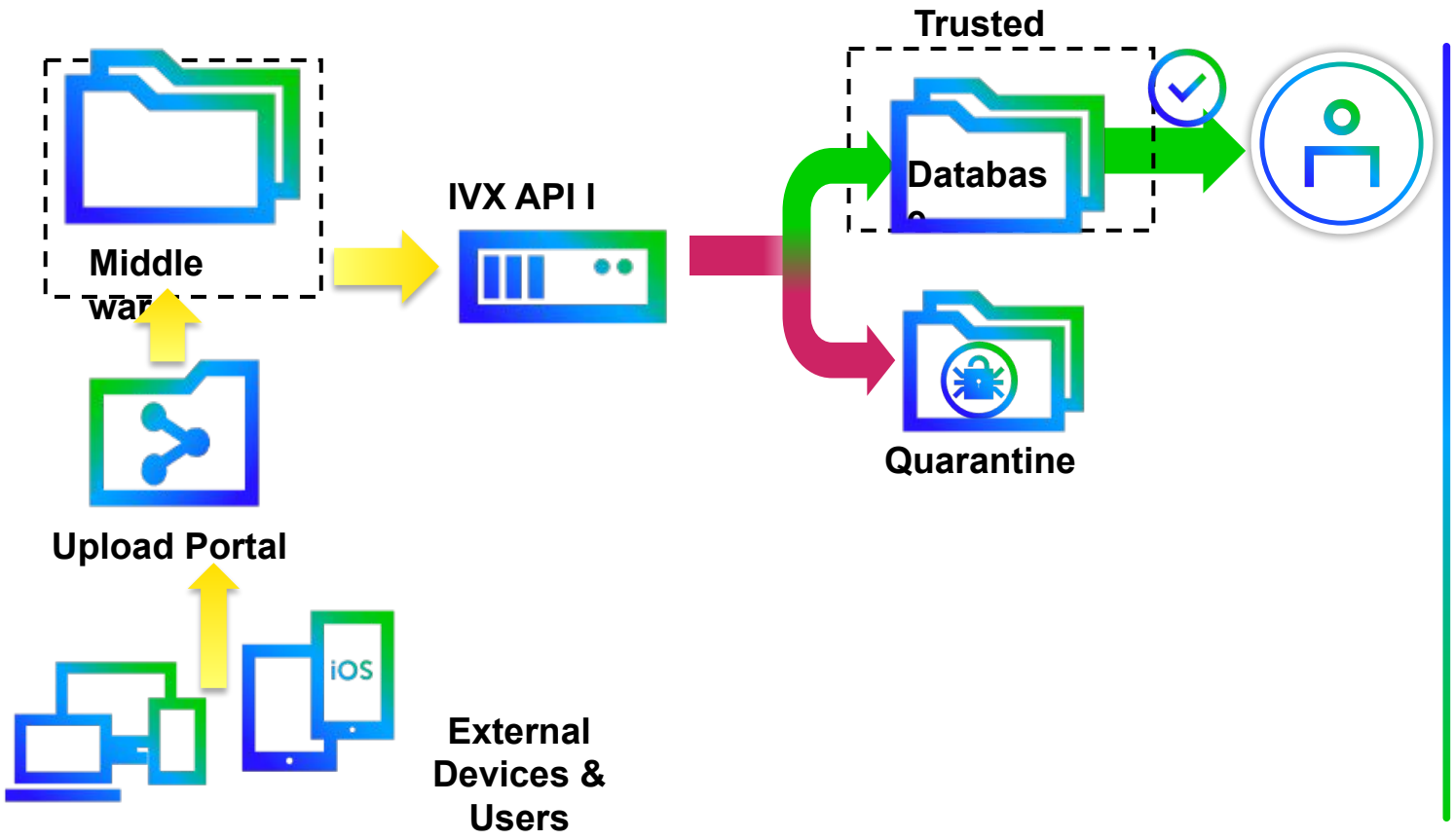
- Stop malware entering enterprise storage from untrusted area
- Ensure files are clean before end users access them

Scenarios

- Insurance Claims
- Bank Account Registration
- Visa Processing

Trellix

External User Files



Benefits

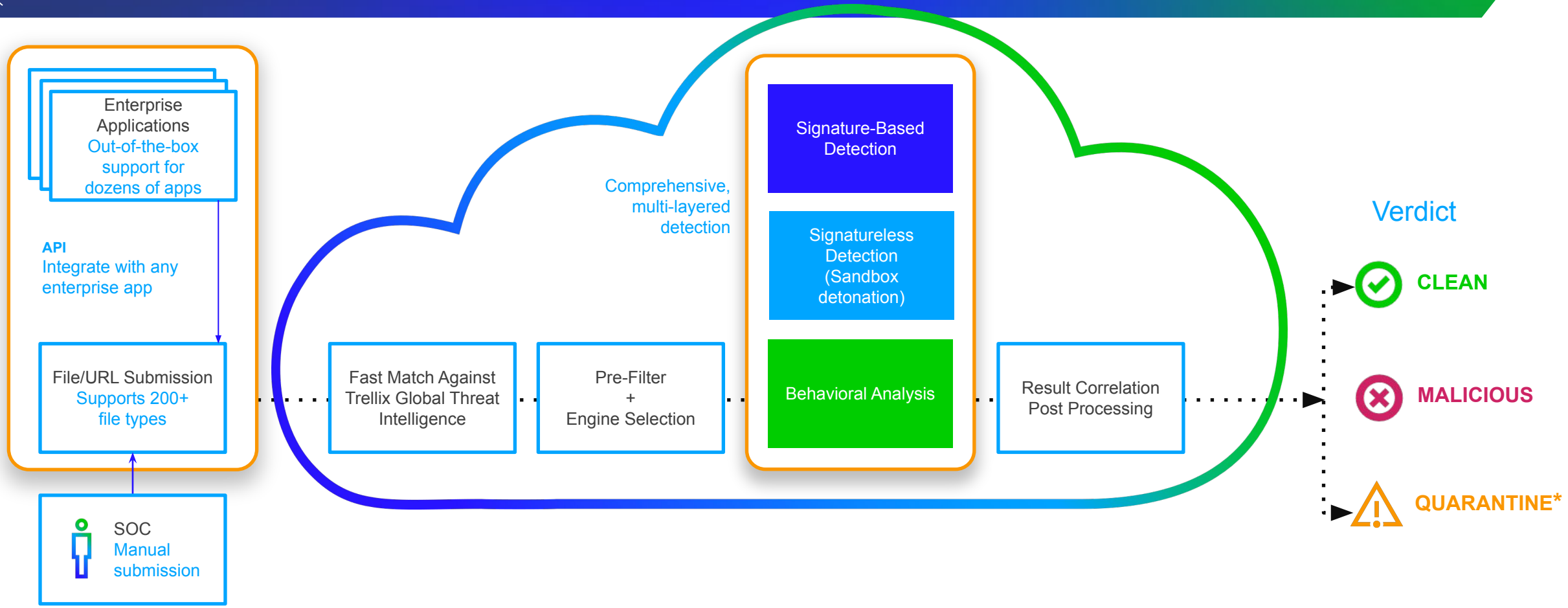
- Stop malware entering enterprise storage from untrusted users
- Ensure files are clean before end users access them

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

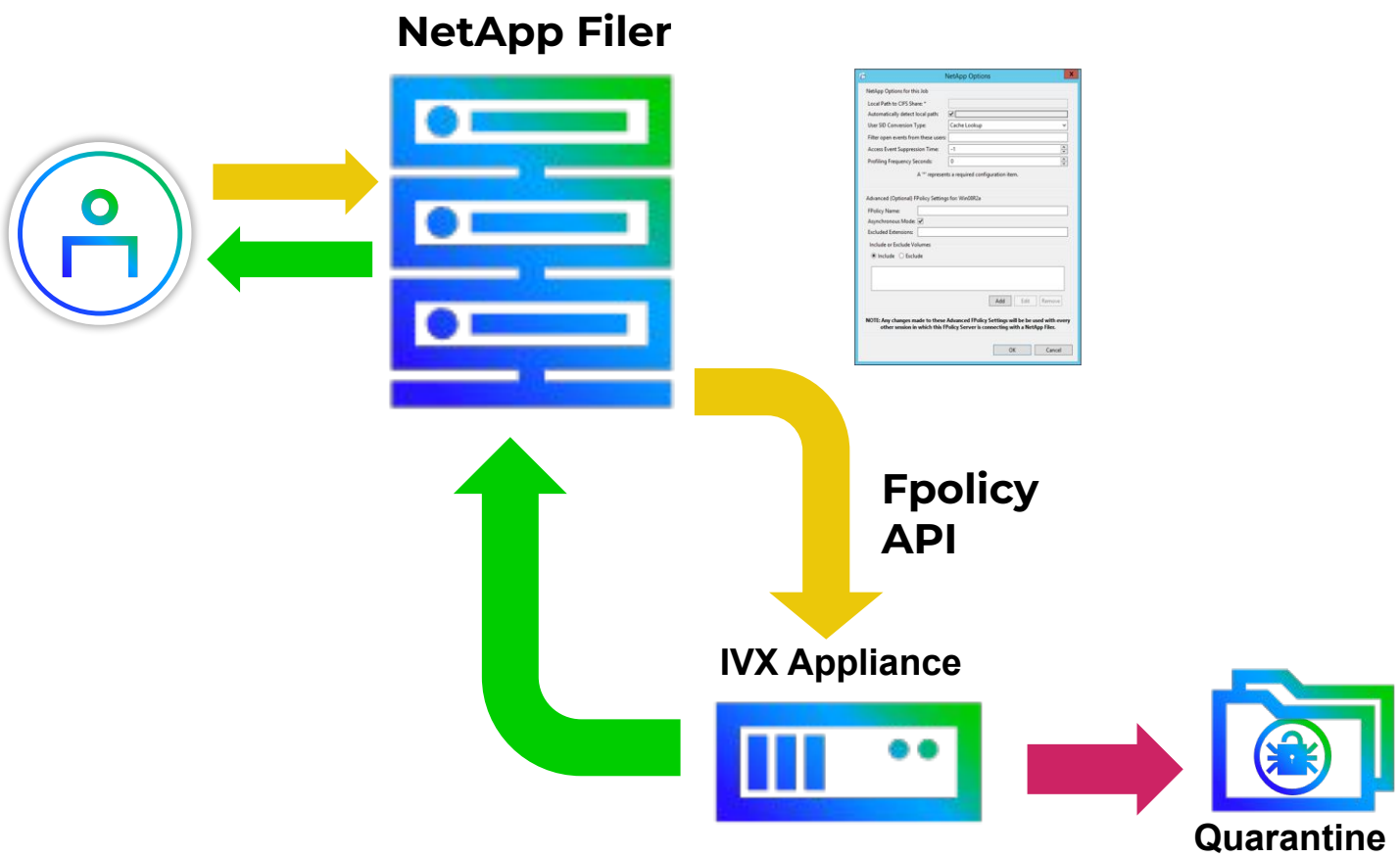
Demo
Trellix File Protect (FX)

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

Trellix

Trellix

Scanning NetApp Filer (Event Driven)



Benefits

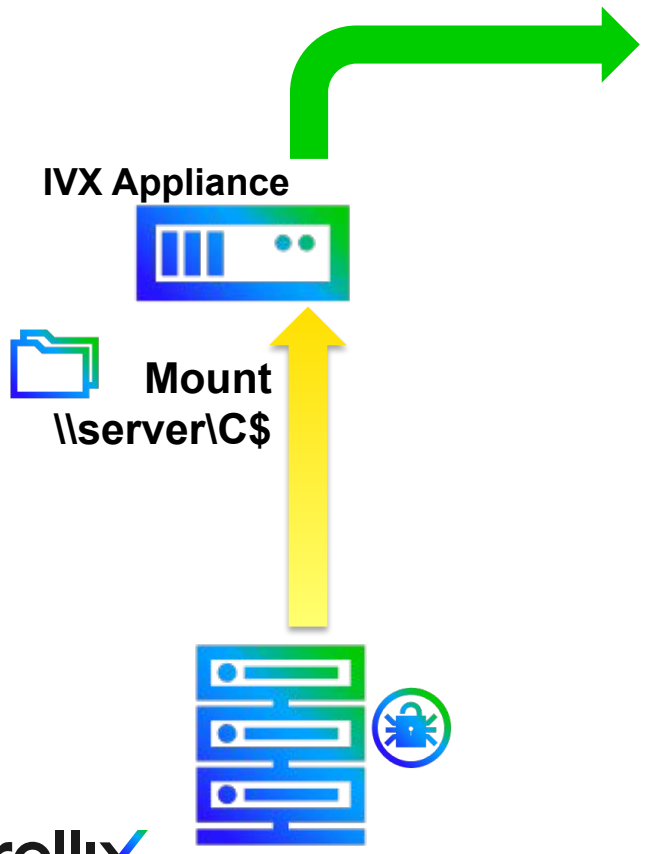
- Monitor and Scan the changes of NetApp Filer in real time through integration with Fpolicy API

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