Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Trellix IVX
Sandboxing

Speaker Intro

Tanja Hofmann

Solutions Consultant

Rahul Iyer

Senior Product Manager

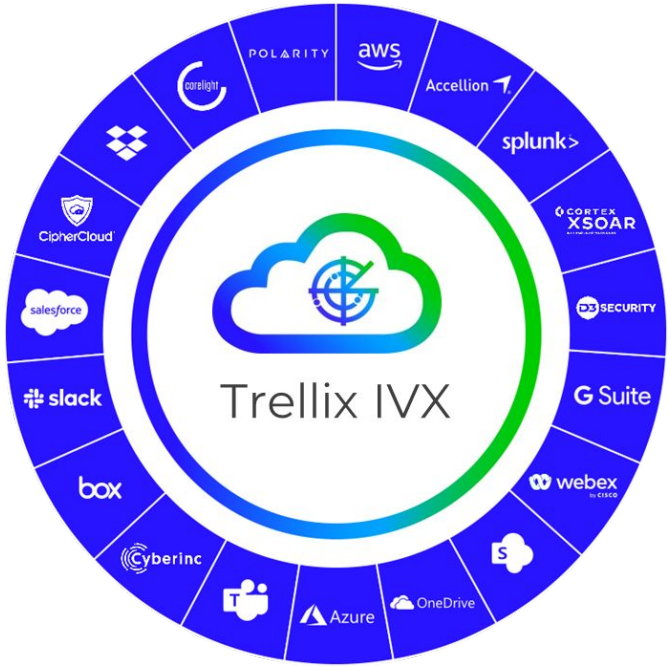
Trellix

Trellix

IVX Cloud

Trellix IVX Cloud

- Cloud-native service that delivers flexible file and content analysis capabilities to identify zero-day, and targeted APT attacks
- Integrate with security operations center workflow, SIEM analytics, data repositories, customer web applications
- Integrates with cloud services like AWS, Azure, Google, and cloud tools like Dropbox, Box, OneDrive and enterprise applications like Salesforce.com, Webex, Slack, Microsoft Teams
- Compiles in-depth analysis details, including MITRE ATT&CK mapping, extracted objects, IOCs, memory dumps, pcap, screenshots
- Available through Trellix channels or directly through the AWS Marketplace



aws

File submissions rate at 100 per minute

Hash submission rate at 200 per minute

Trellix

Trellix

ATD to IVX Migration

Some best practices and need to know

Why should customers migrate to IVX and why not

Benefits of IVX (as of October 24)

Why migrate?

Better overall detection

- Support for over 200 file types
- Advanced URL analysis capabilities

Operational efficiencies

- Support for MacOS and Linux, preinstalled Images - no license costs for Images
- Guest images are hardened, tuned and OS/application updates provided by Trellix. No need for customers to maintain Guest images. (yes, customization is possible)

Why migrate?

Operational efficiencies

- Patented technology to run multiple versions of an application within the same Guest OS
- Multiple versions of Office, Java, PDF reader etc on the same guest image for higher chance of exploit execution

Strategic detection engine for future development and integrations

- Native ICAP support
- Native File scanning through FX integration
- Less False Positives

Trellix

Why should customers migrate to IVX and why not

Benefits of IVX (as of October 24)

Why migrate?

Current integrations

- Trellix TIE with 4.5 and higher
- Skyhigh Webgateway 12.2 and higher
- IVX comes with a free Trellix File Protect VM for scanning of CIFS, Webdav, SharePoint etc
- Manual submission via GUI

And why not?

Features not yet available in IVX

- Reports - when a file is submitted through any API integration
- No DXL Client on OS
- No ePO integration

Trellix

Trellix NFR licenses

Not for Resale licenses

Available in the NFR Pricebook

IVX Enterprise - Virtual Appliances					
IVX-VM300	**Trellix Intelligent Virtual Execution VM 300**				
IVX Sandbox VM300 Inc 2 W DTI 1:1 TE	1 +	IVX3002WECE-AB-AA	43,975.27	0.00	100%
IVX Sandbox VM300 Inc 1W DTI 1:1 TE	1 +	IVX3001WECE-AB-AA	46,081.46	0.00	100%
IVX Sandbox VM300 Inc OF DTI 1:1 TE	1 +	IVX300OFECE-AB-AA	46,781.59	0.00	100%

In addition to IVX, partners “should” get the following products as well

Central Management Virtual Appliance Deployment Options - IVX/ATD					
CM-VA-IVX	**Central Management - Virtual Appliance - IVX**				
CM Virt Appl IVX SW PERP LIC	1 +	VCMIVX-AT-AA	0.00	0.00	100%
CM-VA-DTI-IVX	**CM Virtual Appliance - Dynamic Threat Intelligence - IVX**				
CM Virt Appl DTI IVX 2W 1:1TE	1 +	VCM2WECE-AT-AA	0.00	0.00	100%

Standard Offering					
Perpetual Software License					
1-+	File Share Connector SW PERP LIC(T)	VNWFXCXE-AT		0.00	VNWFXCXE-AT-AA

Trellix

Virtual IVX

Trellix

ATD/TIS to IVX - HARDWARE migration

Some Best Practices and Lessons learned

Applies to all supported Hardware Appliances

- 3100 and 6100 - Hardware and TIS Software EOL 12/25
- 3200 and 6200 - Hardware EOL 12/2028, TIS Software EOL 12/25

Customers can “just” migrate by downloading the MSU file and applying the image - this will IMAGE the appliance.

Licenses will be automatically downloaded from the Backend Server - this is a 2WAY License. Customers can also request the license from Support with the serial number of the box.

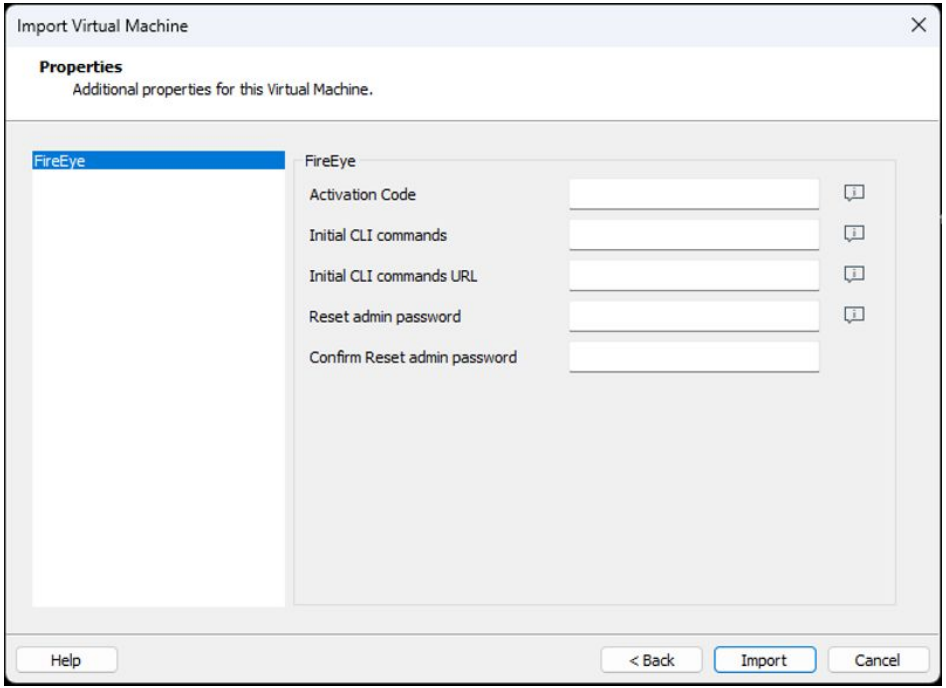
ATD/TIS to IVX - Virtual Deployment

Some Best Practices and Lessons learned

- Migration requires Sales interaction and a 0$ Quote.
- Default License is 2-Way
- Licensing is 1:1 - so if customer has 4 vATD1008 he also gets 4 IVX300
- It is “OK” to run them in parallel until the vATD licenses expire.
- EOL will be moved to December 2025

ATD/TIS to IVX - Virtual Deployment

Some Best Practices and Lessons learned



Trellix

ATD/TIS to IVX - Virtual Deployment

Some Best Practices and Lessons learned - Nothing was added on previous screen

```
fireeye-5f0928 > enable
fireeye-5f0928 # configure terminal
fireeye-5f0928 (config) # configura
% Unrecognized command "configura".
Type "?" for help.
fireeye-5f0928 (config) # configuration jump-start
% Unrecognized command "configuration".
Type "?" for help.
fireeye-5f0928 (config) #
```

```
    You can enter it using the 'license activation code <code>' command
    in the CLI.

    Until you enter an activation code, the HTTPS service will not
    be available.


************************
*** Admin User notice ***
************************

    Network access for the 'admin' user will remain disabled until the
    password is set.


*****************************
*** Password change notice ***
*****************************

    Your password has either expired or has been flagged for a
    forced change. You will be required to set a new password
    before you can take any action on this system.
    Please use username <name> password <enter> command to change password.
```

Password change via

enable
configure terminal
Username admin password *******
Logout - Login

Trellix

What about email

Customers get EX

- ATD/TIS has a very basic email functionality
- IVX has no email functionality at all
    - IF a customer is asking for email functionality, he will get Trellix EX for Servers for free for the remaining runtime of the ATD support contract
    - Requires a 0$ Quote for EX for Server
    - Requires vEX appliances (which integrate with the existing IVX / viVX)
    - Talk about Sizing and Upsell at that customer

Some commands from “Lessons learned”

CLI commands

- Change Appliance ID - *license activation code*
- URL Defense in 1 way
  - analysis **one-way**-override enable
  - analysis url policy adv-url-defense enable
  - https://thrive.trellix.com/s/article/000002741
- URL Analysis - when an URL is submitted
  - static-analysis embedded-urls limit 20
- Global Cache enablement
  - analysis **one-way**-override enable
  - show static-analysis config
- Does it work?
  - show mvx submission

Trellix


Trellix