
Nomios Security Cup
7-8 maja 2026
Hotel Mazurski Raj
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ectacom
EXCLUSIVE NETWORKS
CLICO

What’s Inside the File?

Jak zatrzymać zagrożenie zanim użytkownik kliknie

CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix

nomios | ARROW | ectacom | EXCLUSIVE NETWORKS | CLICO

Agenda

- **Background:** What is IVX
- **IVX** On-premises
- **IVX Cloud:** SaaS
- **Network & E-mail security**

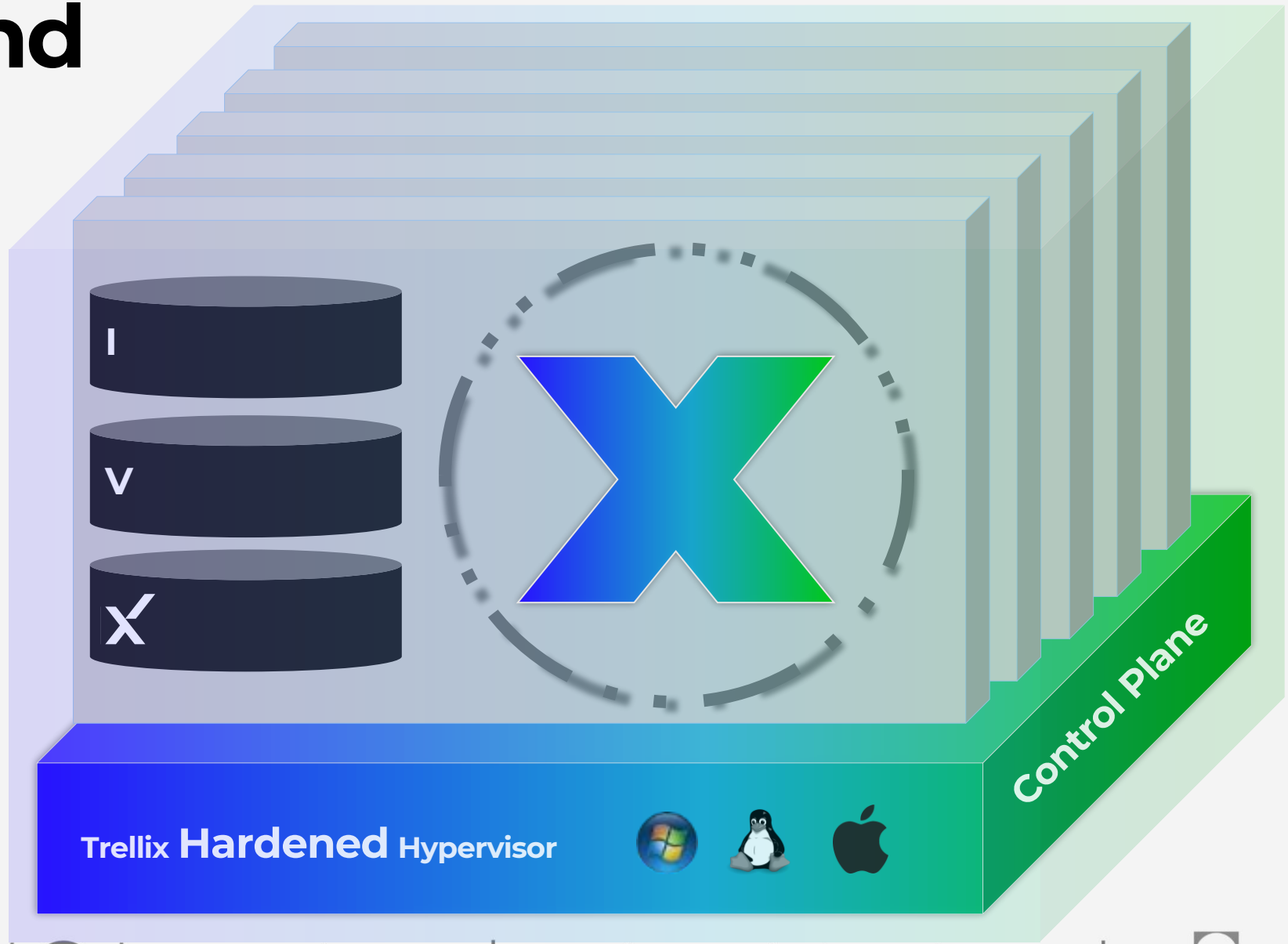
Background

- What is Trellix IVX

IVX Background

Best-of-Breed Dynamic Analysis based detection technology. Custom Hypervisor with built-in countermeasures, designed for Threat Analysis with different Operative Systems and more than 200 configurations. Over 200 simultaneous executions

- Reverse Engineering from the Threat
- Multi-Vector and Multi-Flow
- Hypervisor built for detection (not for data center virtualization)



nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

Static vs Dynamic

Static

Analyze malware without launching it

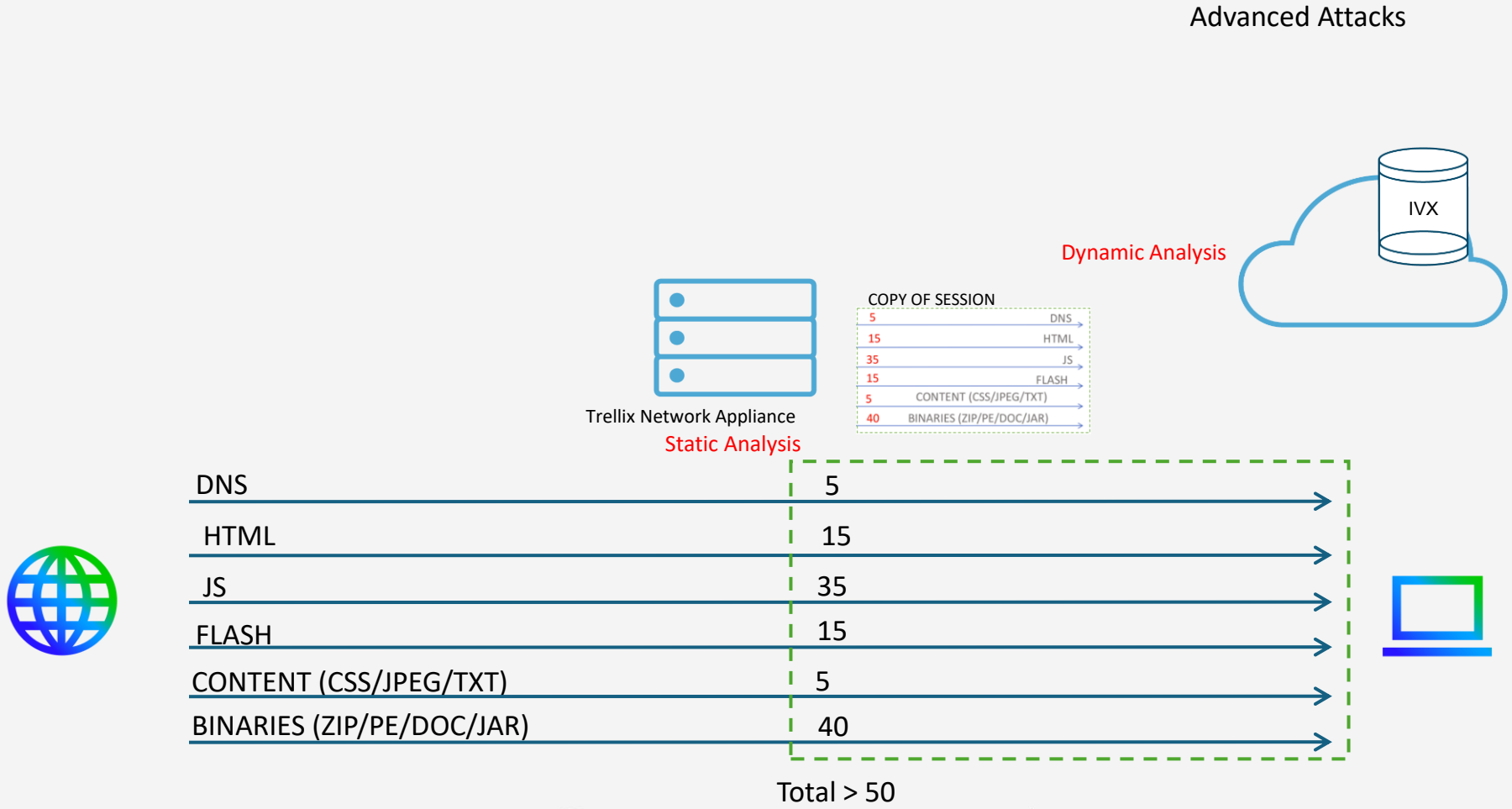
- Hashes
- Web analysis tools
- File identification
- PE files
- Strings
- Packers
- DLLs

Dynamic/Behavioral

Launch malware to monitor how it behaves

- Service and network emulation
- Process monitoring
- Registry modifications
- File modifications
- Network monitoring

Multi-Flow (Session-based) Analysis



IVX
On-Premises

- VX Appliances and VM

Trellix IVX

- Signature-less, dynamic analysis engine that captures and confirms zero-day, and targeted APT attacks
- 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
- Integrates with Trellix Network Security, Trellix Email Security, Trellix File Protect and Trellix Endpoint Security
- Analyzes threats across Windows, macOS and Linux operating system environments

Appliance

VX5600 — Up to 15,840 files per day
VX12600 — Up to 120,960 files per day

AX5600 — Up to 10,000 analyses per day
FX6600 — Up to 87,000 files per day

Cloud

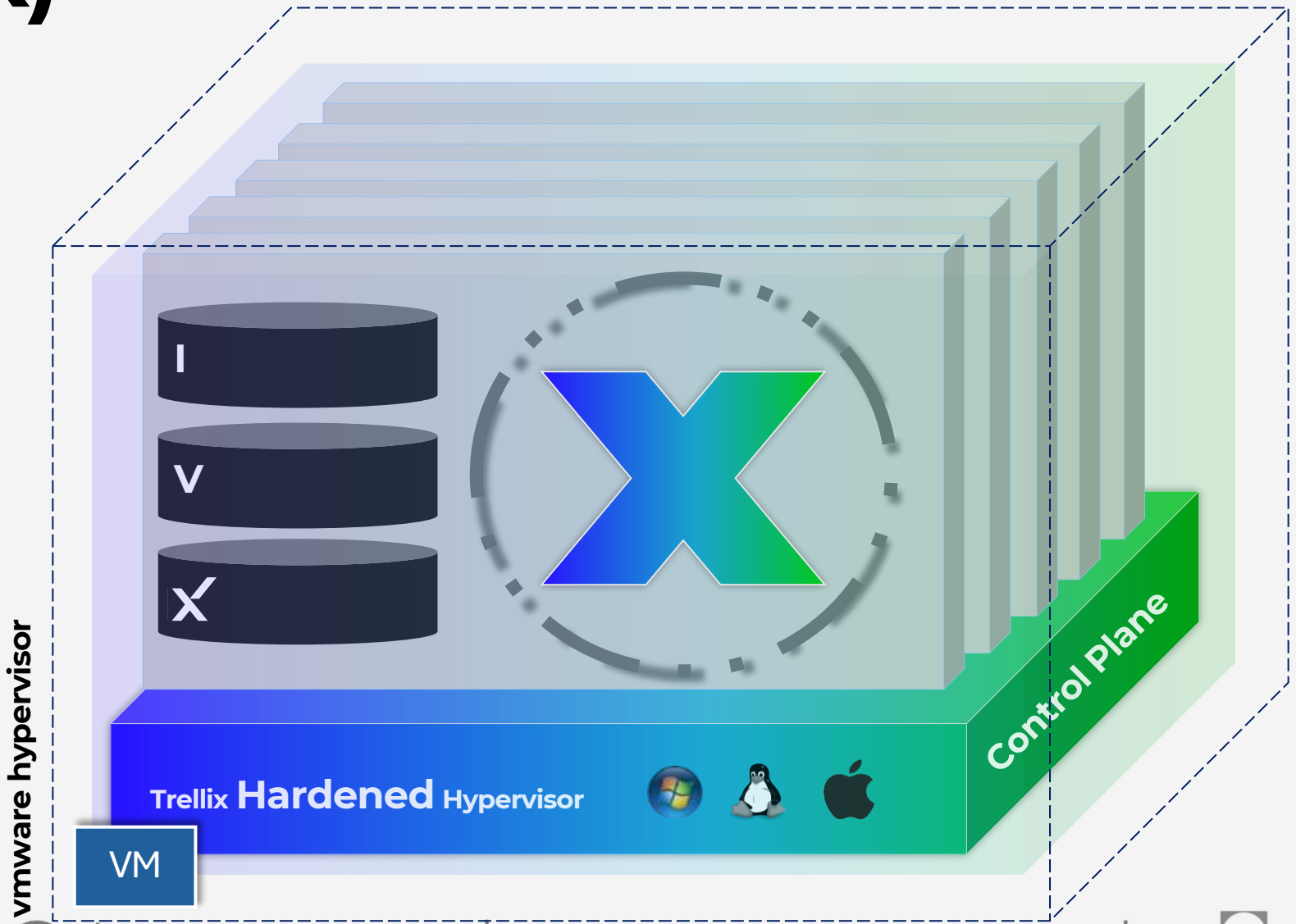
AWS Bare Metal c5.metal — Up to 150,000 files per day

Datasheet: https://www.trellix.com/en-us/assets/data-sheets/trellix-intelligent-virtual-execution-datasheet.pdf

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

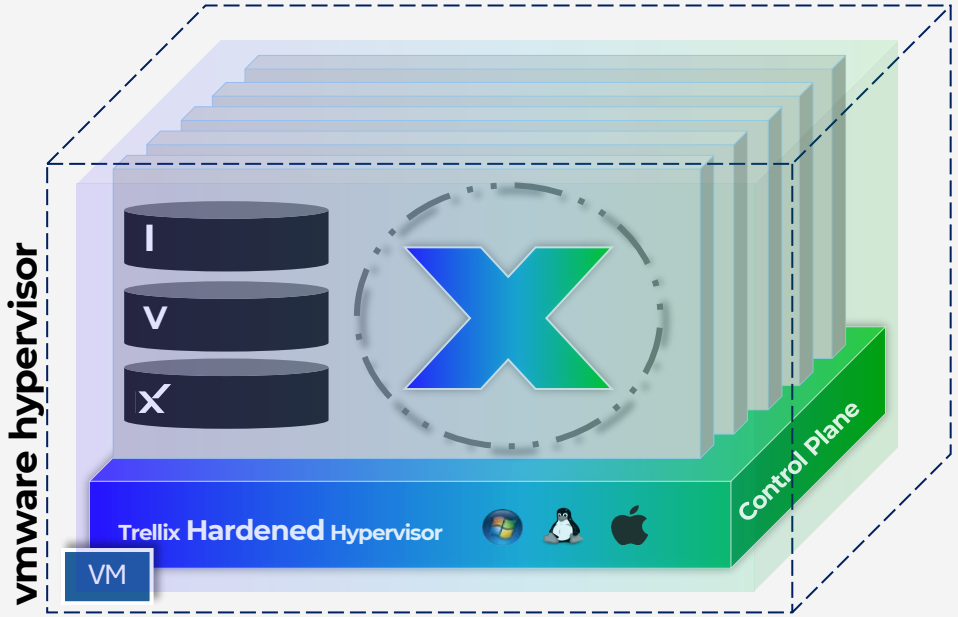
Virtual IVX (vVX)

- Current Support on ESXi
- Provides the same features of the hw
- Maintain Hypervisor Stealthiness
- Close the gap between virtual and physical offering



vmware detection testing

Brief Summary of Testing Areas



No traces of vmware found in any of these areas:

- Registry Checks
- Filesystem Checks
- Group policy Checks
- WMIC checks
- Services Checks
- Storage name Checks
- Mac Addresses checks
- Hypervisor Brand by CPUID

No traces of vmware registry keys in the guest OSs

No traces of vm* vmware* related files in guest OS local disk drive

No vmware related group policies were found

No wmi objects (DiskDrive, Process, Service) were found

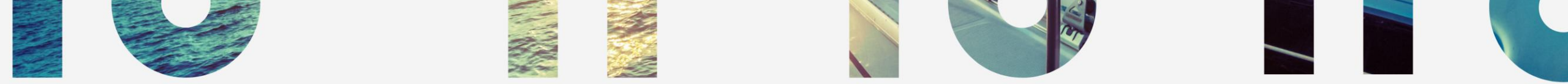
Checked for vmware related services. None were found.

Our mac addresses are hardcoded and start with 00:20

CPUID check Returned false for vmware (0)

nomios | CROWDSTRIKE | ExtraHop | FORTINET | HPE juniper networking | infoblox | Trellix | ARROW | EXCLUSIVE | ectacom | CLICO

Trellix Malware Analysis



AX – Use case

- Powerful workbench to get a quick verdict on samples or URL's
  - Obtain indicators to use in further investigation or to verify infection of the estate
  - Allows for automated analysis at scale and for manual submission with full control on the analysis environment
  - Option for Live Mode and interaction with the sample during analysis

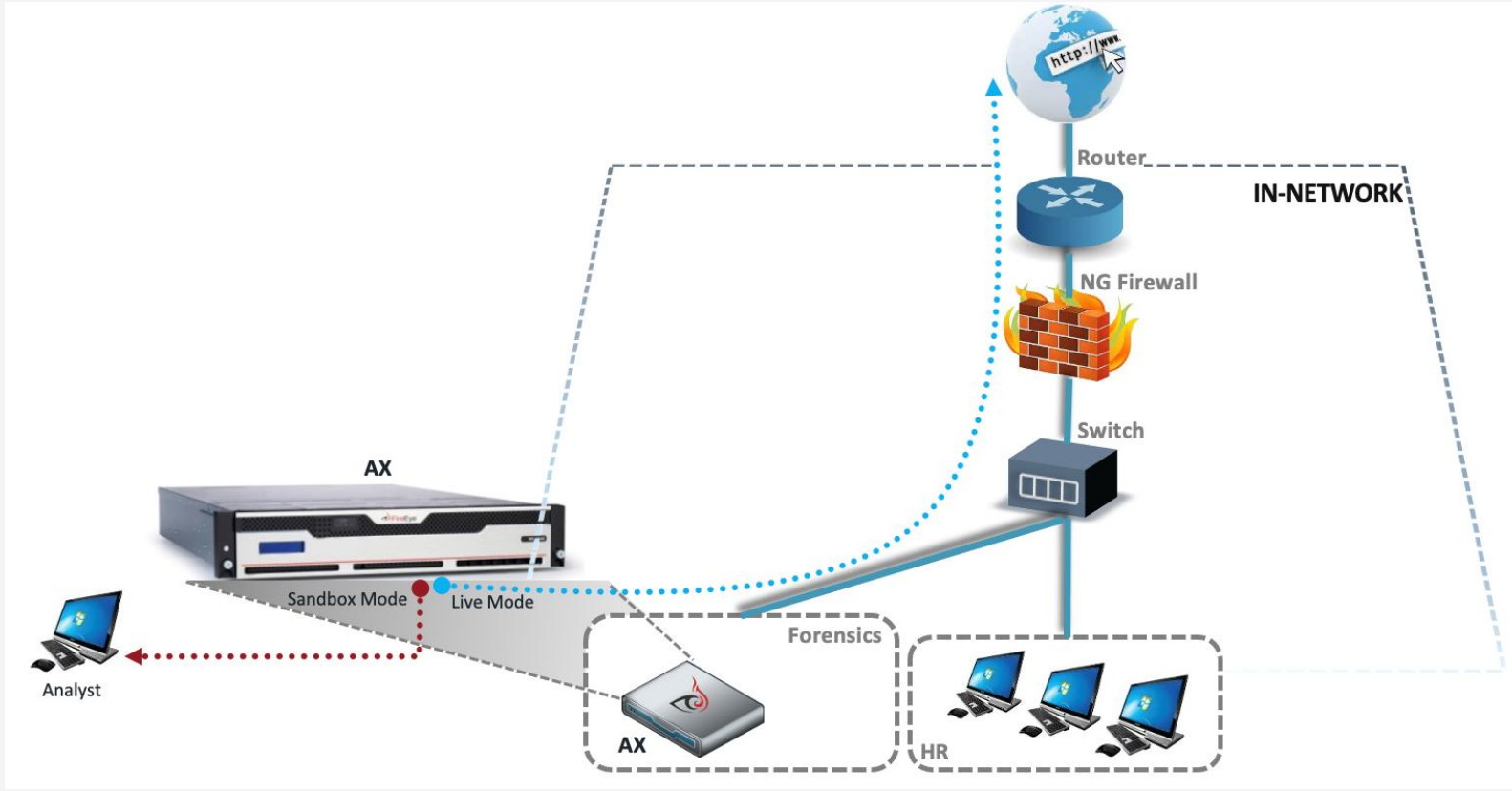
- Typical buyer is the SOC
  - *But we have use cases where we do a periodic scan of a hosted website, crawling all URL's in Live Mode (avoid serving malware to visitors)*

Malware Analysis Modes

URL

http://www....

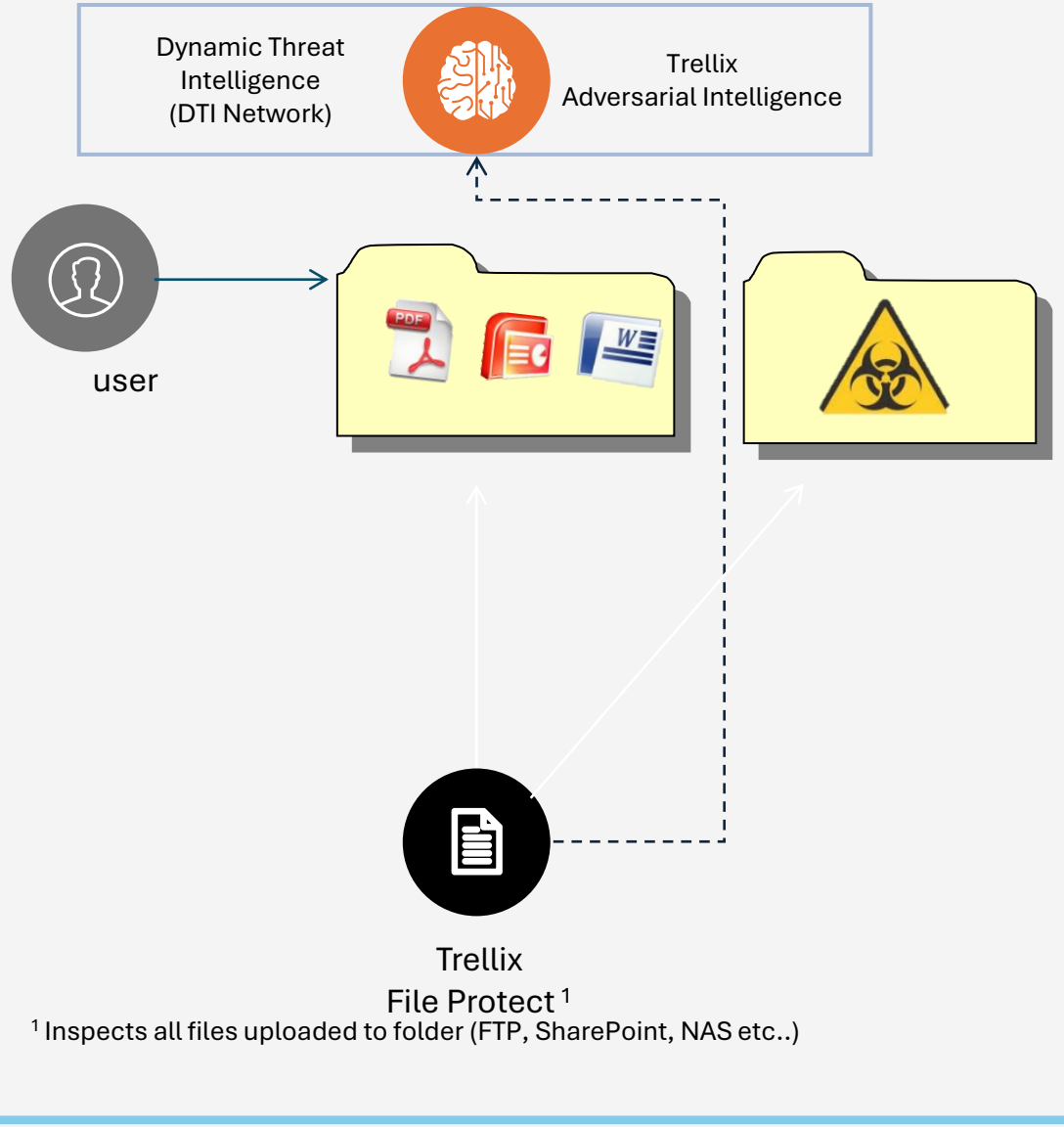
Object



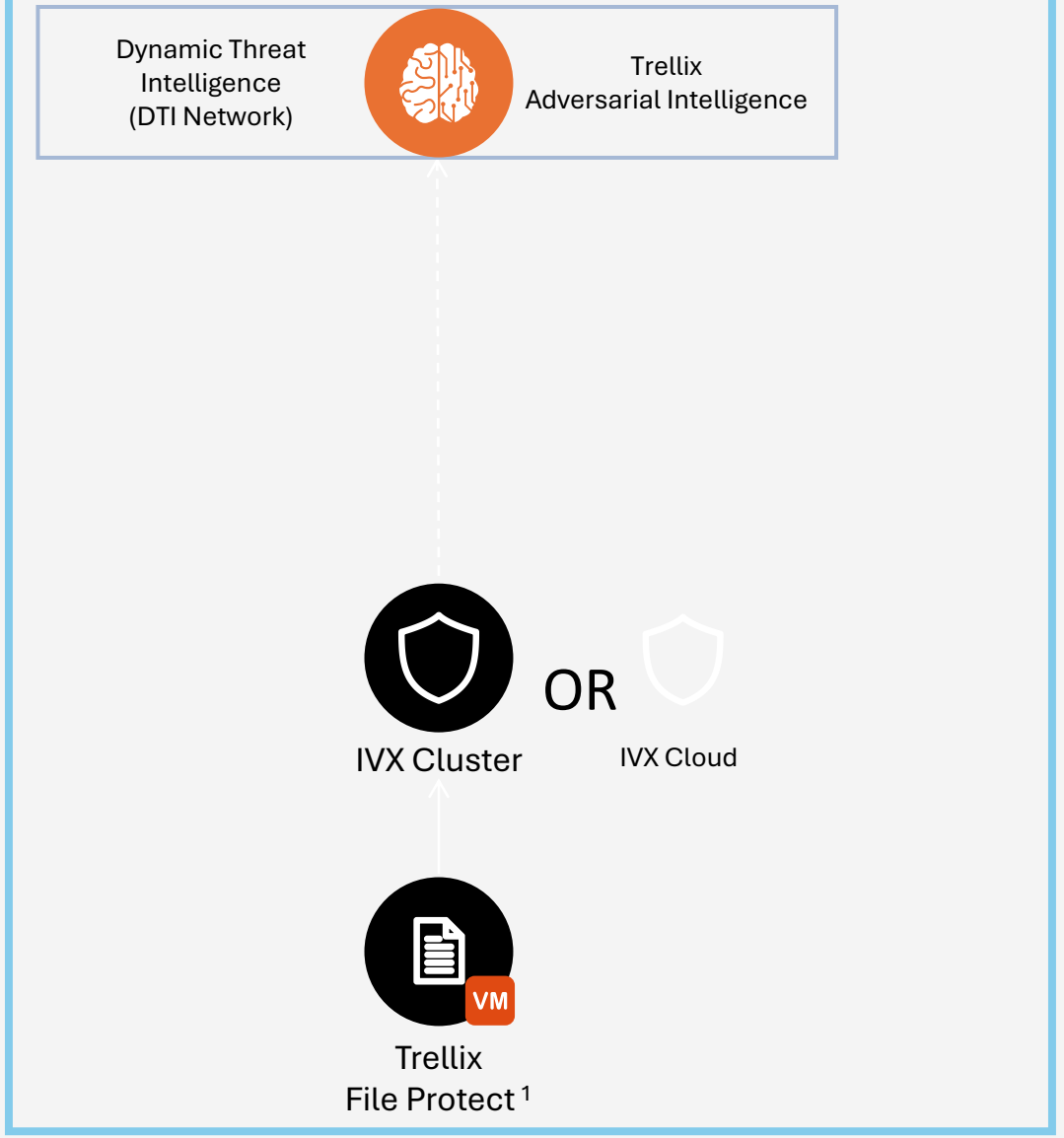
Live mode vs Sandbox

Trellix File Protect

FX – Hardware Appliance



FX – Virtual Appliance



VM Virtual Machine

Footnotes

Network Traffic Communications

DTI, software, signatures and licensing updates

FX – Use Cases

- Trusted vs Untrusted File Domains
- Protecting SharePoint Farms
- Scanning NetApp Filer
- Secure File Exchange
- Clean Backup

IVX Cloud SaaS

Malware Analysis at Scale

XDR Analyst SOAR

IVX Cloud

Enterprise Applications
Out-of-the-box support for dozens of apps

Manual or Automated File/UR/IP Submission
Supports 200+ file types

Comprehensive, multi-layered detection

Fast Match Against Trellix Global Threat Intelligence

Pre-Filter + Engine Selection

Signature-Based Detection

Signatureless Detection (Sandbox detonation)

Behavioral Analysis

Result Correlation Post Processing

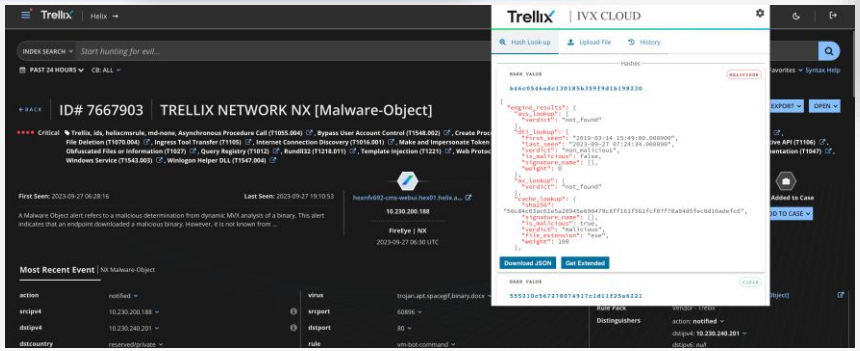
Analysis Verdict

CLEAN

MALICIOUS

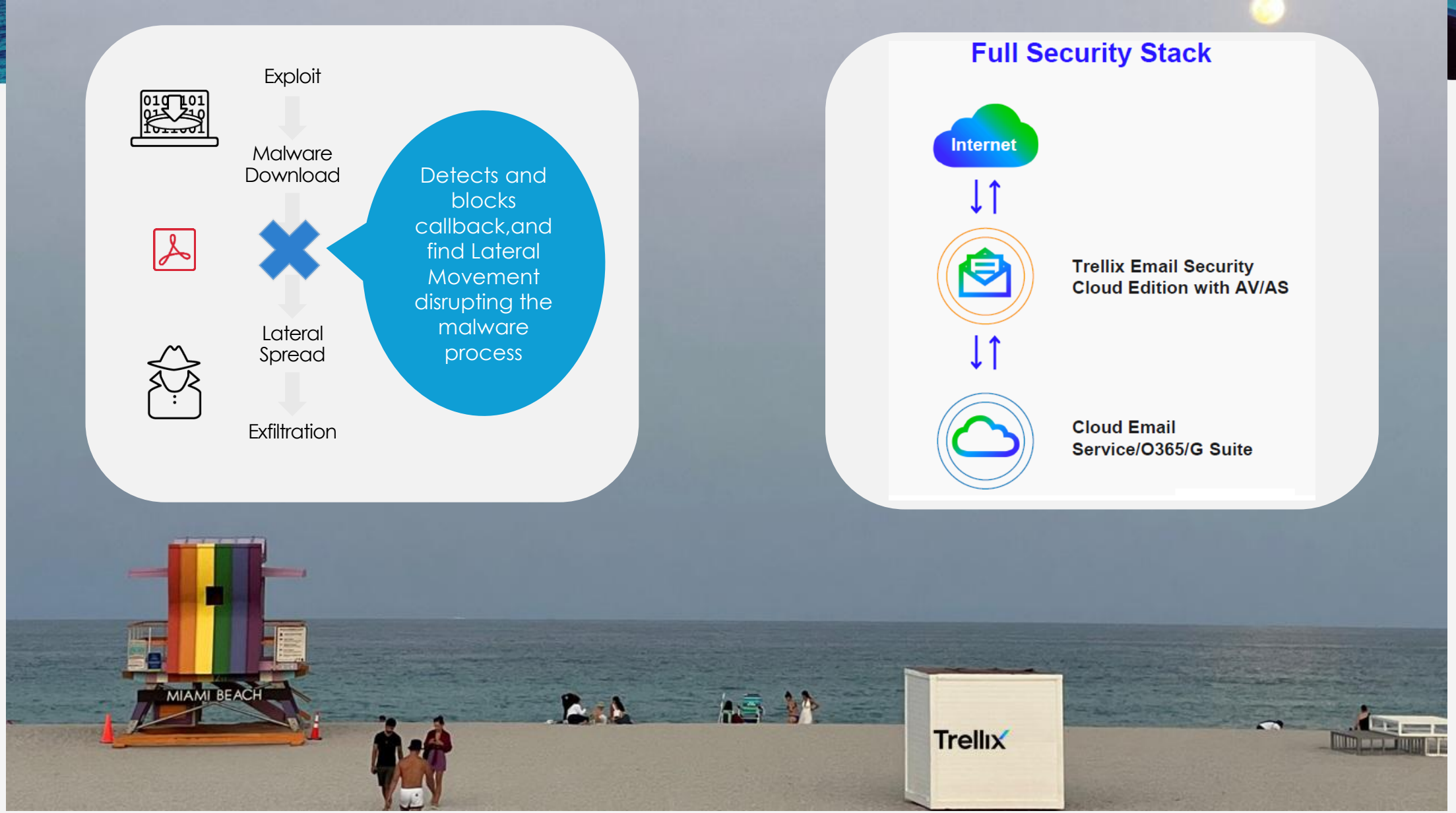
QUARANTINE*

Chrome plugin



nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

What else?



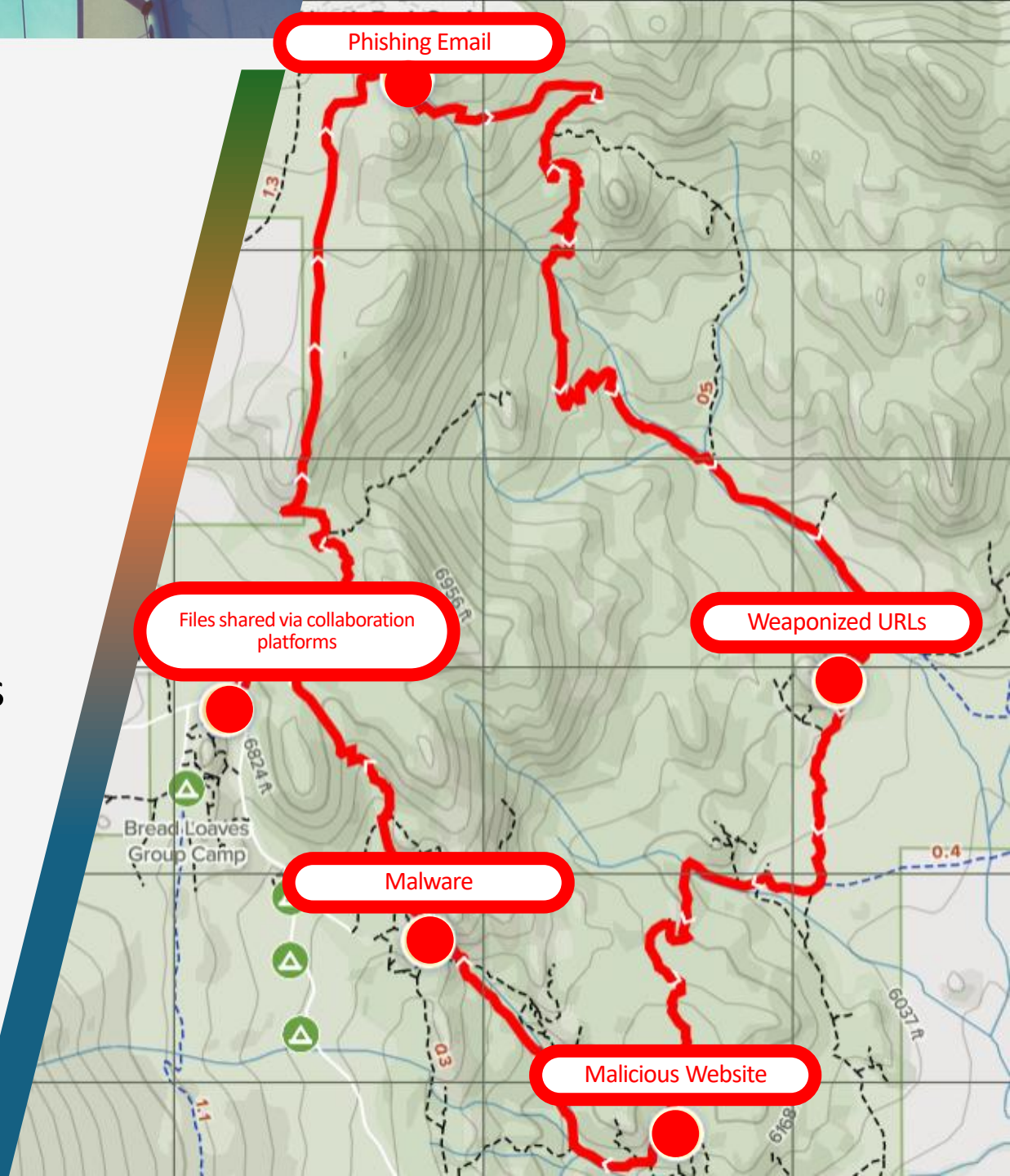
nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

Key Take Aways

Good enough security won't protect you from ransomware

'Detection-in-depth' is our heritage, we've invested 10+ years in AI/ML models

Add Trellix Email Security to detect what others miss



nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking


Dziękuję za uwagę!
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ectacom
EXCLUSIVE NETWORKS
CLICO