COMGUARD
communication security

Trellix – Network Security and Forensics

Martin Votava | Sales Director
Michal Mezera | Technical Director

Agenda

1. Trellix o společnosti
2. Trellix Network Security and Forensics
3. Klíčové vlastnosti
4. Architektura

Trellix

2022
Founded

5K
Employees

40K
Customers

78%
Fortune Global 500

90+
Countries

$1.7B
Revenue

2.3T
Annual intel queries

1B+
Threat sensors

100M
ML model inputs

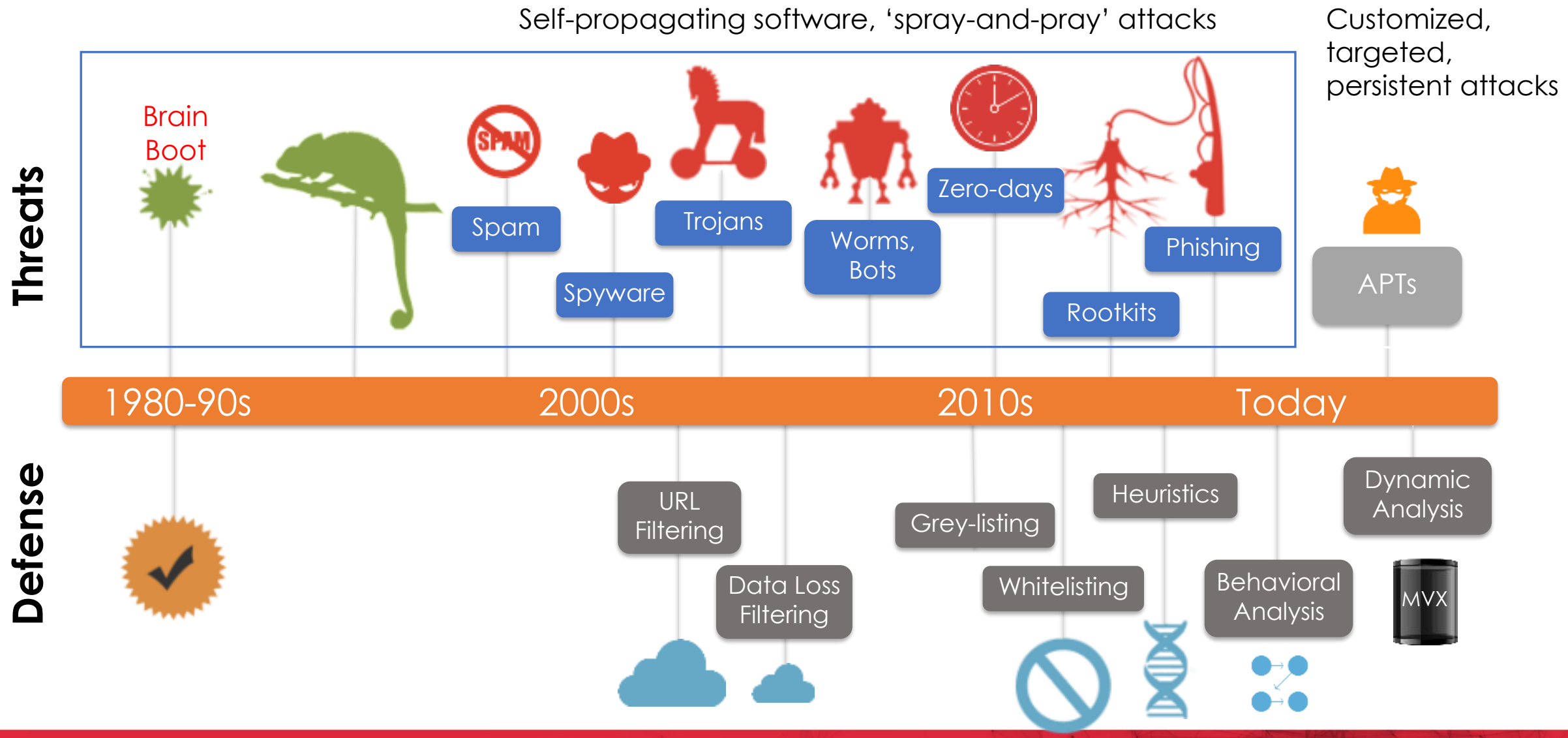
~700
Campaigns tracked

418
New malware / minute

Learn more at
Trellix.com

Trellix

Evolution of Threats Drives Development of New Security Tools



Network Security Capabilities Must Evolve with the Threats

Ransomware

- Ransomware infections continuing to grow month over month
- Enhanced distribution frameworks and Ransomware-as-a-Service have lowered the barrier to entry
- iSIGHT has observed over 60 new ransomware families introduced in each quarter of 2017
- Attack distributed broadly across sectors

State Sponsored

- Nation-state actors are still setting a high-bar for sophistication; however some financially focused actors have improved their tactics, techniques and procedures
- No longer "Smash and Grab". Now, showing a sophistication for maintaining persistence and removing forensic artifacts

Network Blind Spots

- Increasing need for greater traffic visibility
- Use of SSL has increased distribution of encrypted malware
- Insider threats on the rise
- Stolen / harvested credentials increases the difficulty of detection

Financial

- Increasing trend of targeted attacks used to disrupt M&A and influence stock price
- Attackers are becoming adept at Privilege Escalation, allowing undetected movement across environments

Key Benefits of FireEye Network Security

Detecting the Undetectable for Unequaled Protection

INTELLIGENCE DRIVEN
Infused intelligence with advanced technologies

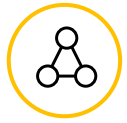
SMARTVISION
Detect suspicious lateral network traffic

MULTI-OS SUPPORT
Stopping threats that target Macs and PCs

Making Security Investments and Teams More Efficient

HIGH FIDELITY ALERTS
Low false positives to target alerts that matter

FLEXIBILITY
Multiple deployment options (inline, out of band) and form factors



ORCHESTRATION
Pivot to Helix Platform to automate tasks

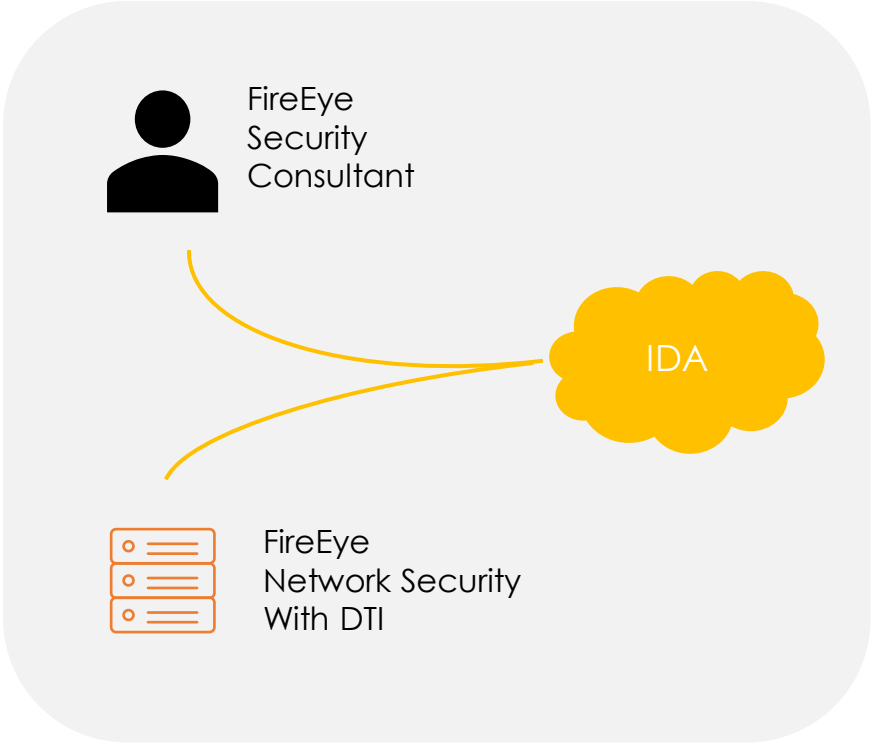
Additive Protection via FireEye's Global Footprint

DYNAMIC THREAT INTELL
Automated protection gained from threats detected worldwide

BREACH EXPERTISE
Applied intelligence gained from the frontline

ATTACKER INSIGHT
Deep insight of attacker tactics, techniques and procedures

Intelligence Driven Analysis (IDA)



Overview

- Combination of Human Intelligence and Machine Learning
- Uses FireEye Frontline Expertise and Intelligence and End-to-End Security Platform Information
- Can see Trends Across Industries and respond accordingly

Benefits

- Faster detection and resolution of new threats
- Awareness of threats to specific customer industries

Integrated IPS

Source: Gartner (January 2018)

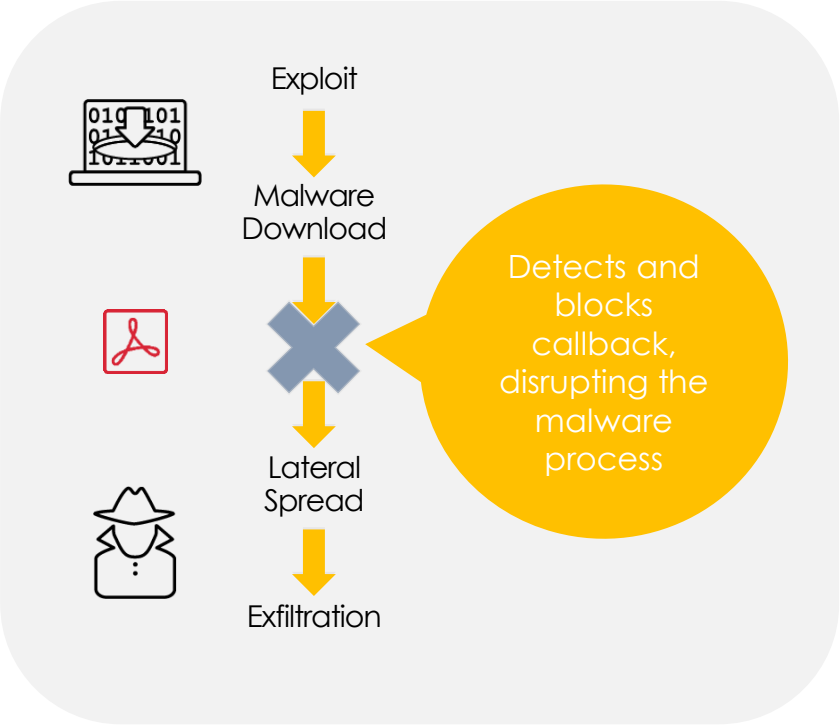
Overview

- Provides real-time threat protection against known threats
- Reduces workload for the MVX engine, which improves efficiencies and reduces false positives

Benefits

- Integrated IPS reduces costs, simplifies management and improves security posture

Malware Callback Detection



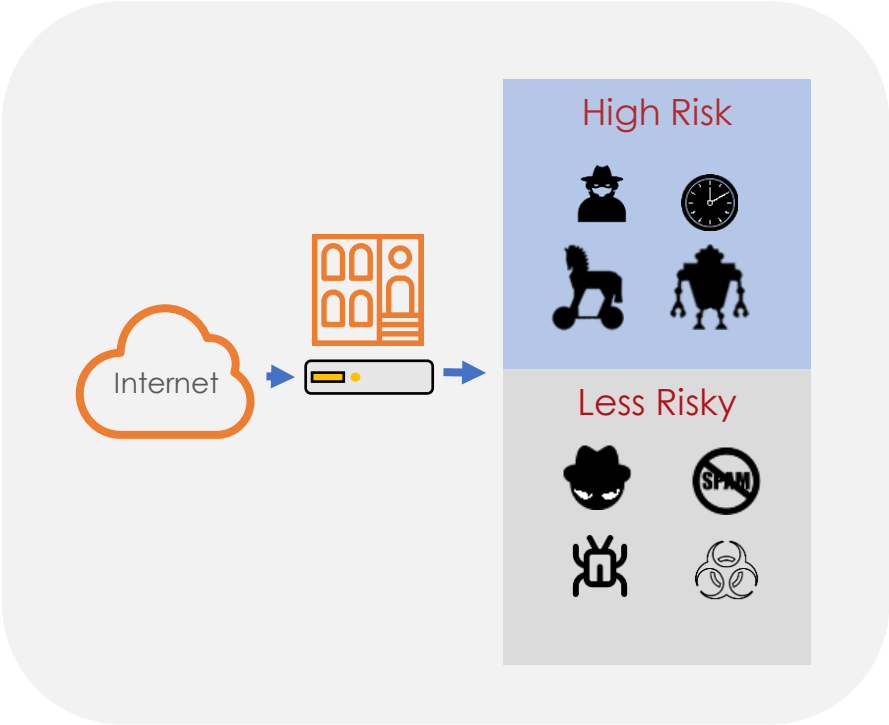
Overview

- Callback is a type of network behavior generated by malware for collecting data or for remotely controlling threats

Benefits

- Superior time-to-detection of botnets, backdoors and other forms of malware that utilize callbacks

Riskware Detection



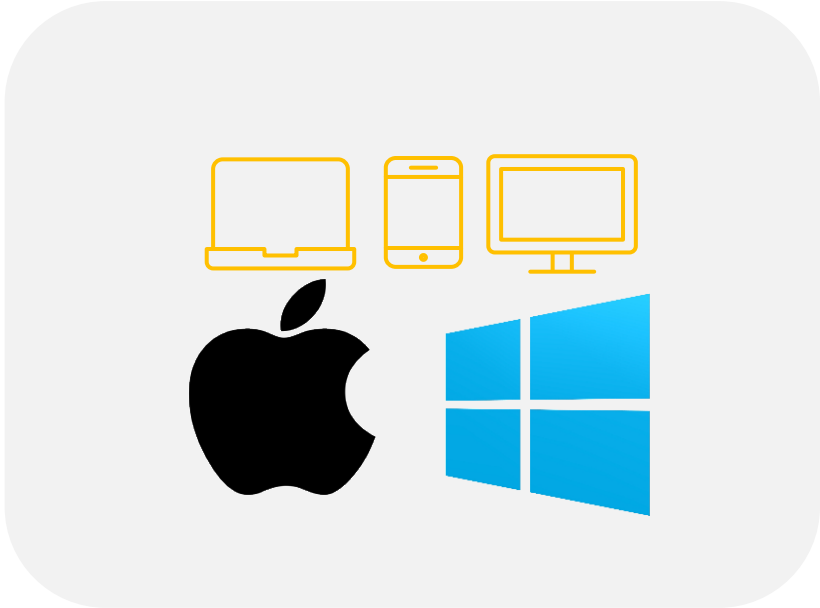
Overview

- Separates genuine breach attempts from undesirable, but less malicious activity

Benefits

- Focuses security response team on real threats

Multi-OS Support



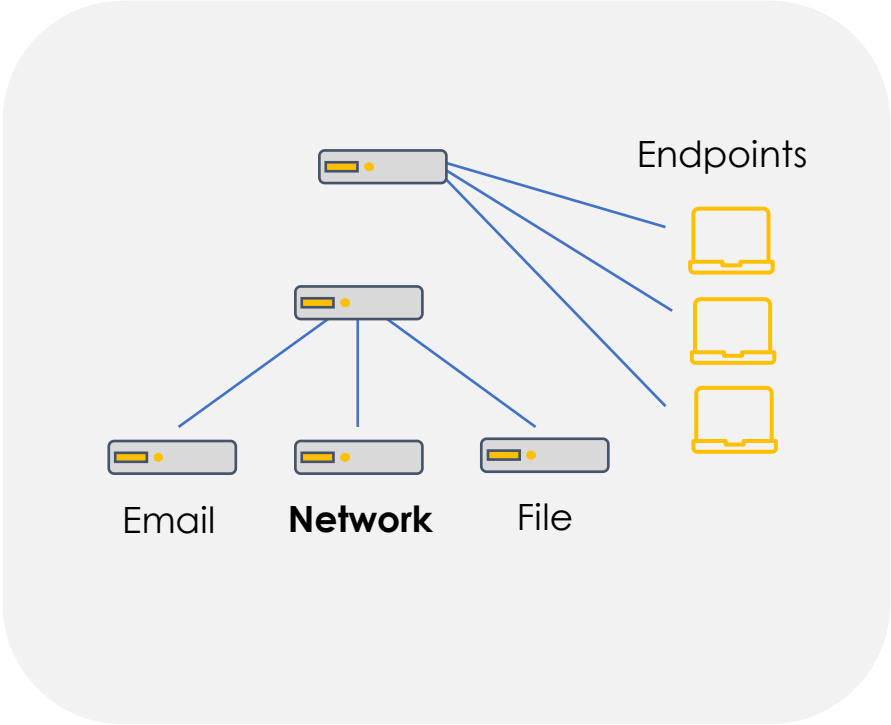
Overview

- Detection for Microsoft Windows and Apple OSX as well others threats, leveraging combination of FireEye detection and threat intelligence

Benefits

- No worrying about unprotected devices in the company network

Integration with Endpoint Security



Overview

- Extend network detection to endpoints
- Confirm alerts from network
- Create IOCs automatically
- Validate and analyze network traffic alerts
- Rapid interrogation of all endpoints

Benefits

- Quicker detection and remediation of threats
- Better use of personnel, solve problems not hunt down threats

Detection and Protection: How Network Security Does It Better

Content Updates – Signatures / Threat Feeds
Cloud Assist – Cache for File & URL Analysis
Cloud Assist – File Sandboxing & Analysis

STATIC ANALYSIS

IPS
Proprietary/Custom Signatures (Snort, YARA)
Static Network Rules/Blacklists
Antivirus

DYNAMIC ANALYSIS

Web Shell Detections
Server-Based Vulnerabilities
URL-based Phishing Attacks (Cloud-Assisted)
Malware Binaries Check (Cloud-Assisted)

FILE

Multi-Vector Execution
Web Infection
Riskware
Callback Detection

ANALYTICS & MACHINE LEARNING

Analytics Rules
Lateral Movement
Data Exfiltration
Malicious C2 Communications

VISIBILITY

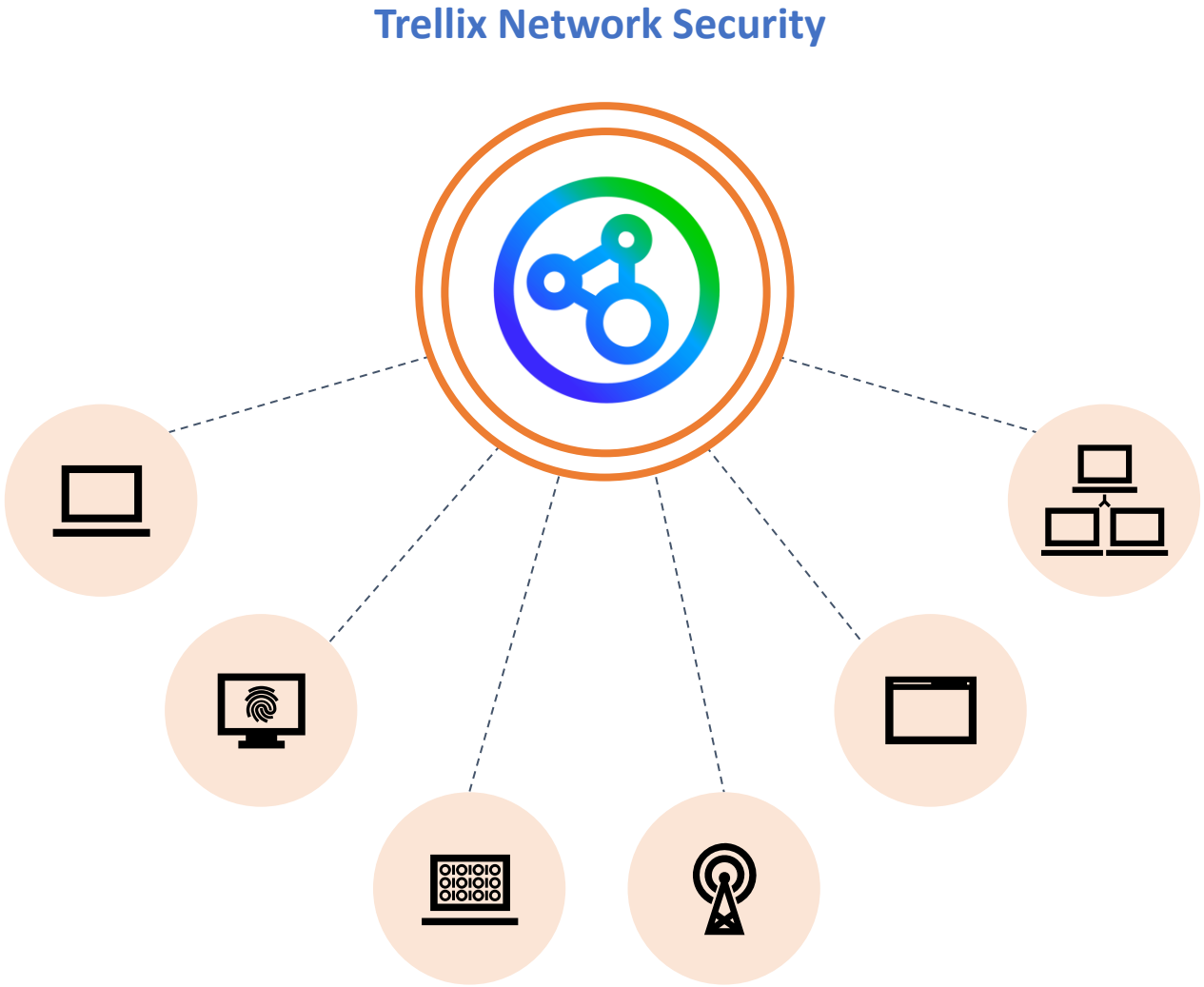
Protocol Application and Visibility
Metadata Generation
IoT Visibility
TLS/JA3 Fingerprinting
Endpoint Correlation

Trellix

Greater Functionality

More than just a **sandbox:**

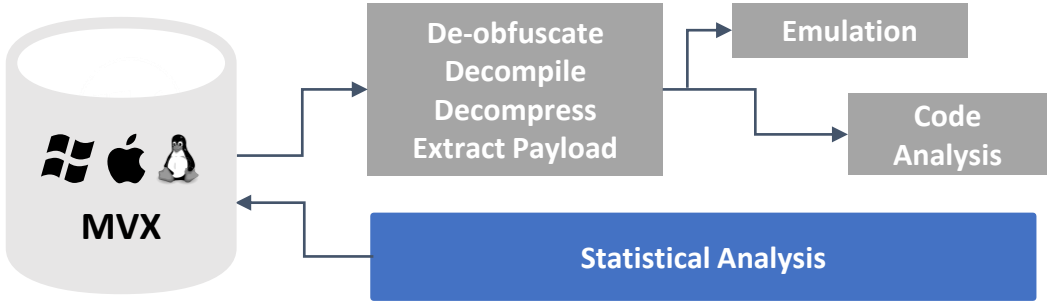
- Riskware
- TLS Intercept
- TLS JA3 Session Fingerprinting
- Call back detection
- Web shell detection
- IoT detection
- Metadata generation
- East/West lateral detection
- IPS



Industry-Leading Malware Analysis

Adds a multitude of heuristics, deep code and content analysis, including:

- **Code Analysis:** includes Function and Similarity
- **Statistical Analysis:** includes N-gram and Entropy
- **Embedded URL Analysis** capability
- **Emulation Analysis:** includes object emulation
- **Global cloud-based Analysis** of known and unknown objects

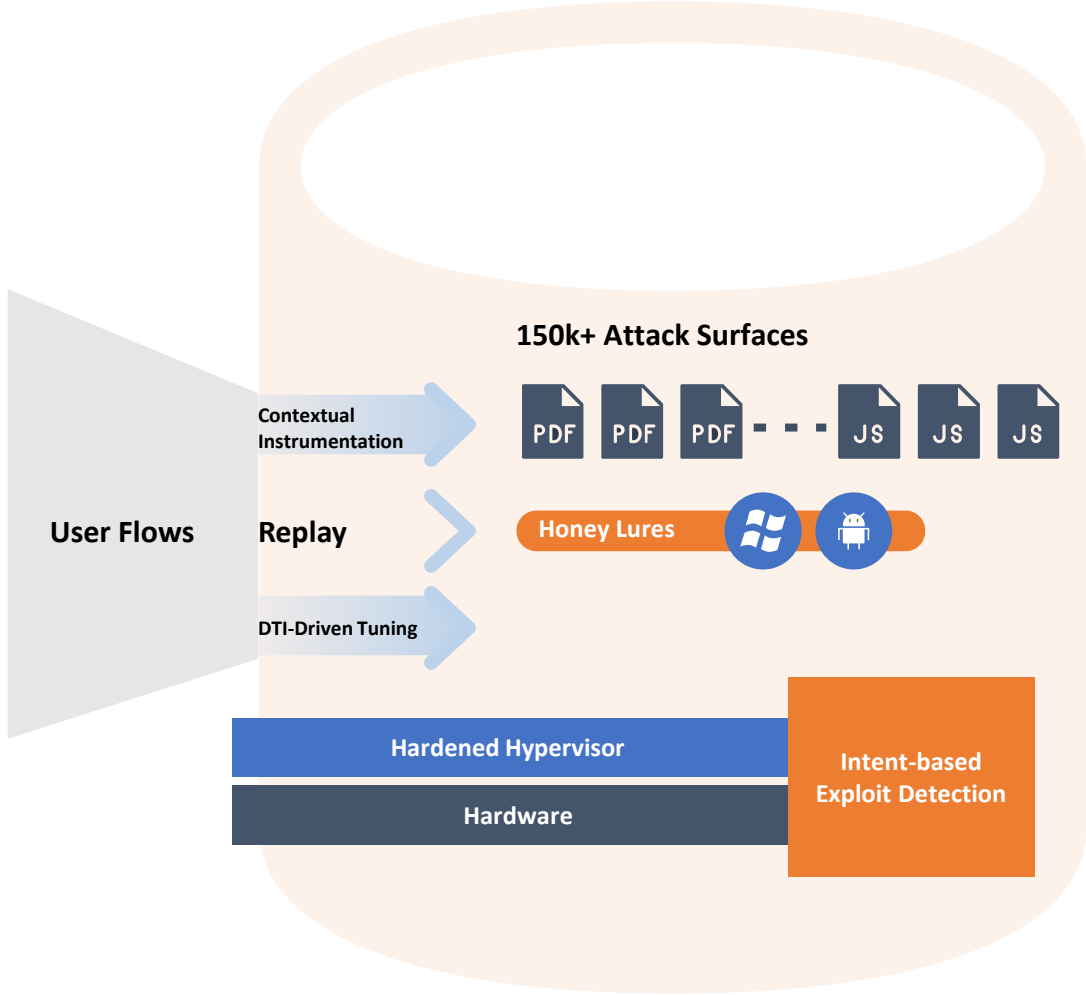


Behind the Scenes

Machine-Learning Capabilities with MalwareGuard

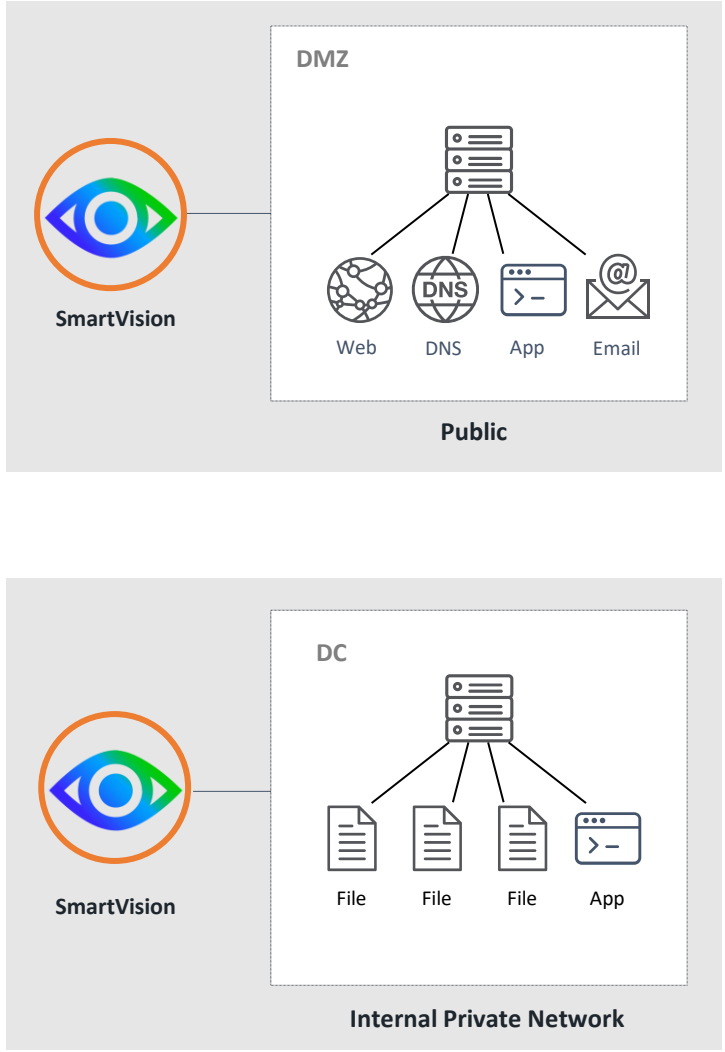
Correlate Flows / Events Across Multiple Vectors (Email, Endpoint, and Network)

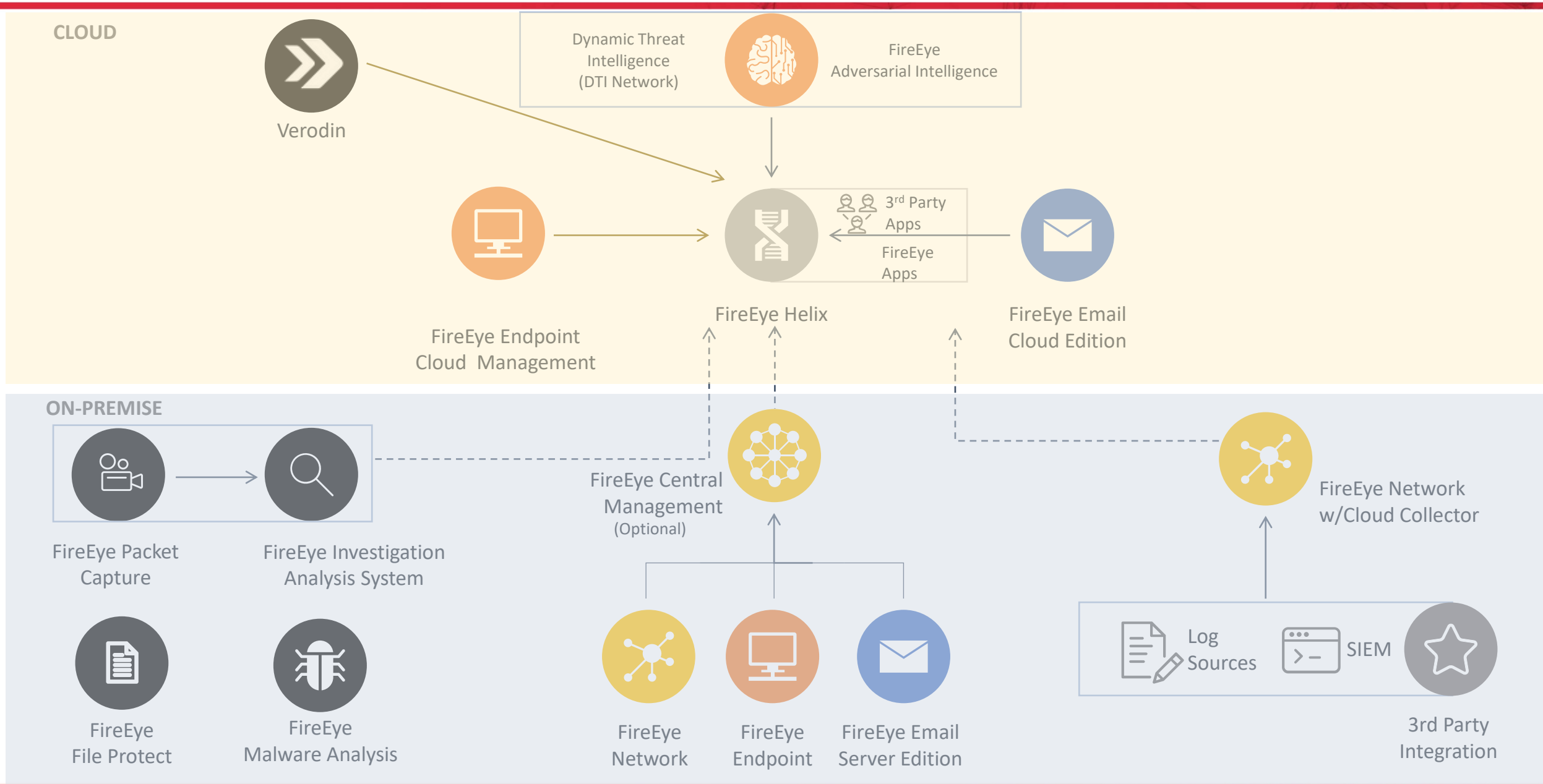
Lateral Threat Detection with SmartVision with event details mapping to MITRE ATT&CK framework



SmartVision Lateral Threat Detection

- 180+ rules for lateral movement detection
- Provides full kill chain detection that targets east-west, server-facing deployments
- Machine learning framework with data-exfiltration detection
- JA3 detection for identifying encrypted communication
- Web-Shell Detection (visibility into attacks on Webservers)
- Lateral movement of malware (MVX detonation)
- Provides L7 context around every real-time alert
- Map adversarial techniques with the MITRE ATT&CK Framework
- Ability to record and capture packets for SmartVision alerts




CLOUD
Verodin
Dynamic Threat Intelligence (DTI Network)
FireEye Adversarial Intelligence
3rd Party Apps
FireEye Apps
FireEye Endpoint Cloud Management
FireEye Helix
FireEye Email Cloud Edition
ON-PREMISE
FireEye Packet Capture
FireEye Investigation Analysis System
FireEye Central Management (Optional)
FireEye Network w/Cloud Collector
FireEye File Protect
FireEye Malware Analysis
FireEye Network
FireEye Endpoint
FireEye Email Server Edition
Log Sources
SIEM
3rd Party Integration

TOP advantages

1. MVX - Multi-Vector Virtual Execution
2. Multiple deployment options
3. Multi-OS support
4. Extensibility to XDR
5. Multiple attack vectors protection
6. No gold images
7. Integration with 3th parties
8. Endpoint Secuirty Integration
9. SSL/TLS inspection
10. Integrated IPS

COMGUARD
communication security

Děkujeme za pozornost

martin.votava@comguard.cz
+420 734 442 468
michal.mezera@comguard.cz
+420 604 223 589