

COMGUARD
communication security



Trellix – Sandbox již není jen o analýze souborů

Martin Votava | Sales Director

Agenda

1. Trellix o společnosti
2. XDR technologie Trellix
3. Trellix Network Security and Forensics

Trellix

2022

Founded

5k

Employees

2.3T
Annual intel queries

1B+
Threat sensors

100M
ML model inputs

~700
Campaigns tracked

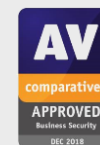
418
New malware / minute

40k

Customers

78%

Fortune
Global 500



90+

Countries

\$1.7B

Revenue

Learn more at
Trellix.com

What is XDR?

[XDR] is a platform that integrates, correlates and contextualizes data and alerts from multiple security prevention, detection and response components. XDR is a cloud-delivered technology comprising multiple point solutions and advanced analytics to correlate alerts from multiple sources into incidents from weaker individual signals to create more accurate detections.

- [Gartner, 2021 XDR Market Guide](#)



Extended goes across several security vectors including endpoints, network, cloud, email and other third-party products.

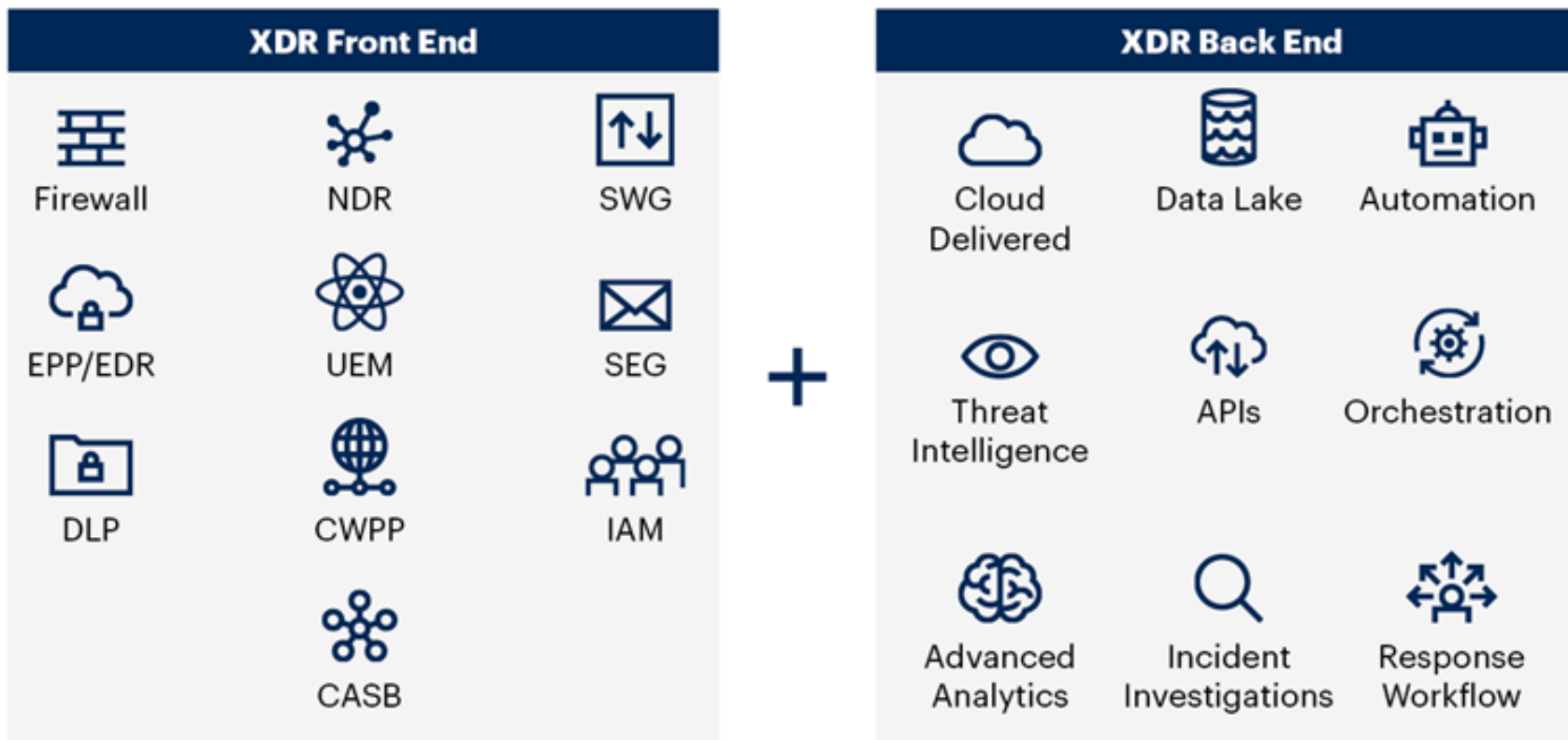


Detection comes from the ability to detect and correlate threats across multiple vectors the moment they arise.






Response enables your organization to be better prepared to respond effectively to attacks in real time.



XDR Overview



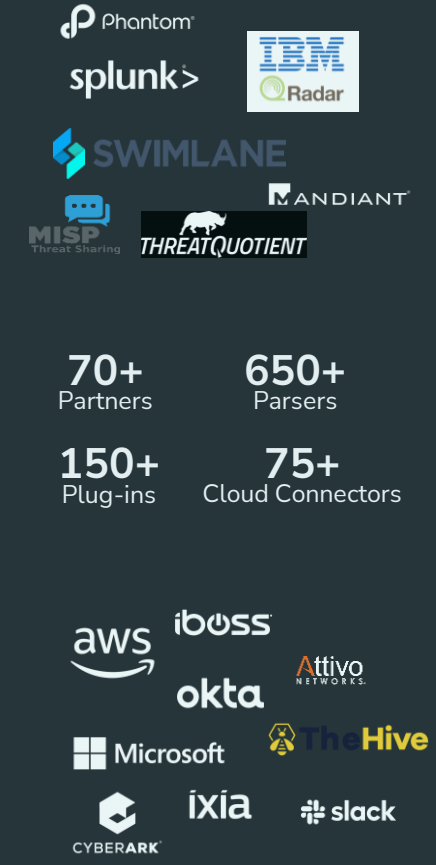
Source: Gartner
747261_C

Gartner.

 Helix Platform	 Detect on Demand	 Threat Labs
Investigative Workflows	Dynamic IOCs	Contextual Threat Intelligence
SOAR and Threat Hunting Capability	Analytics & ML	Automatic Enrichment and Correlation
Event Streaming / Analytics	File & URL Analysis	Mandiant + McAfee + NewCo
	Delivery & Payload	
	Signatures	

 Workplace	 Multi-Cloud
EPP/EDR/Forensics	Cloud Infrastructure Intrusion Prevention
Data Protection	Data Center Intrusion Protection
Mobile Security	Server Protection
Email Gateway	Cloud Visibility
Phishing Protection	Cloud Compliance
Business Email Compromise	Cloud Posture Assessment

Partners
(Not Exhaustive)



70+ Partners 650+ Parsers

150+ Plug-ins 75+ Cloud Connectors

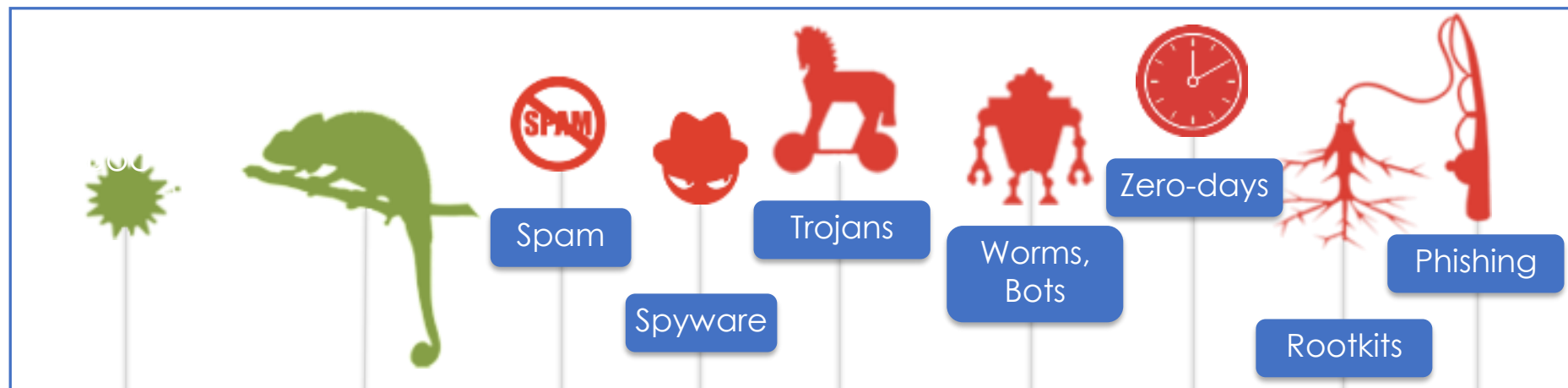
Proč řešit minimálně NDR?

Evolution of Threats Drives Development of New Security Tools

Self-propagating software, 'spray-and-pray' attacks

Customized, targeted, persistent attacks

Threats



Spam

Spyware

Trojans

Worms, Bots

Zero-days

Rootkits

Phishing

APT's

1980-90s 2000s 2010s Today

Defense



URL Filtering

Data Loss Filtering

Grey-listing

Whitelisting

Heuristics

Behavioral Analysis

Dynamic Analysis



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

FireEye Technology: Magic of MVX

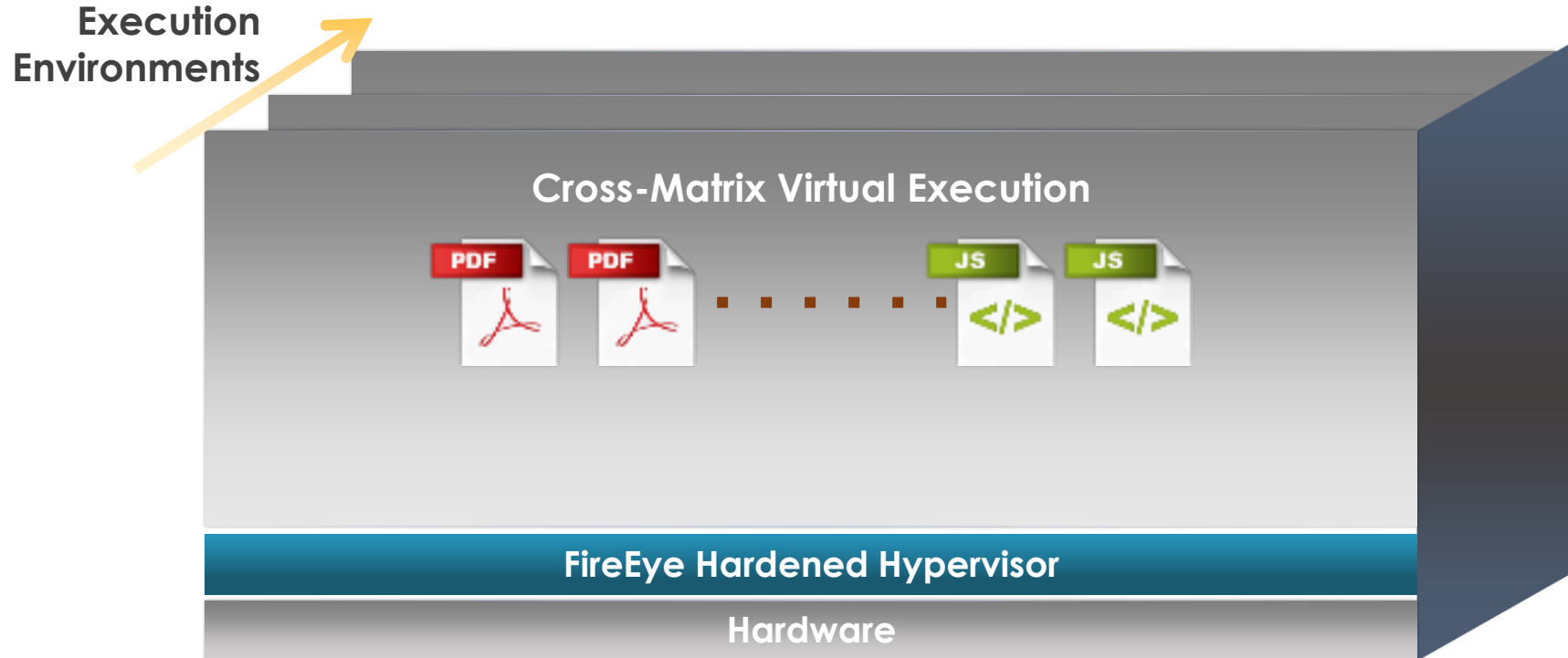
1 FireEye Hardened Hypervisor

2 Massive cross matrix of virtual execution

3 Threat Protection at Scale

Simultaneous executions

Multi-flow analysis



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

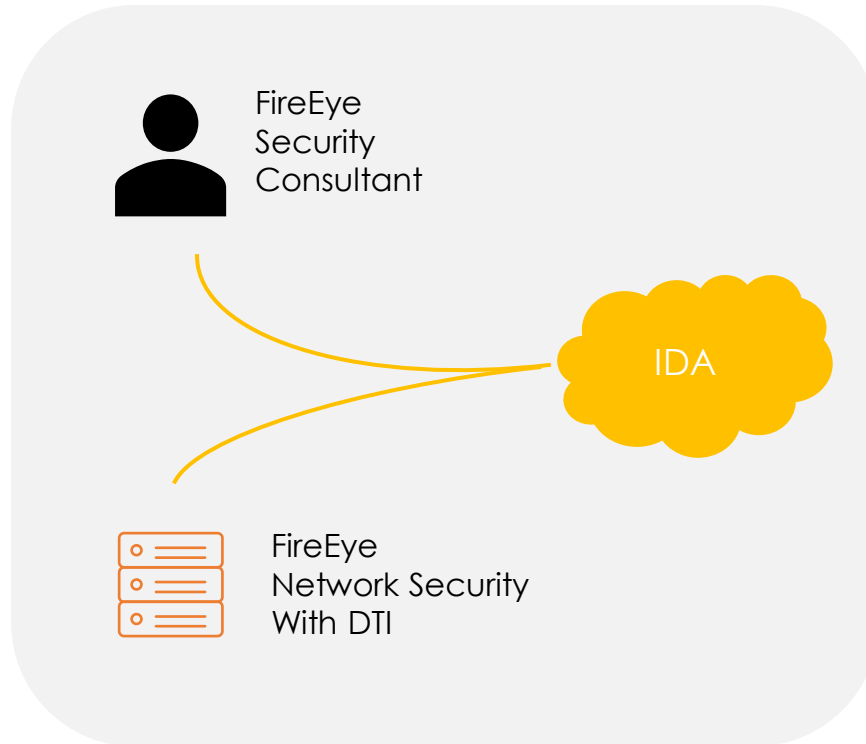
Applied intelligence gained from the frontline



ATTACKER INSIGHT

Deep insight of attacker tactics, techniques and procedures

Intelligence Driven Analysis (IDA)



Overview

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

Benefits

1. Faster detection and resolution of new threats
2. Awareness of threats to specific customer industries

Integrated IPS



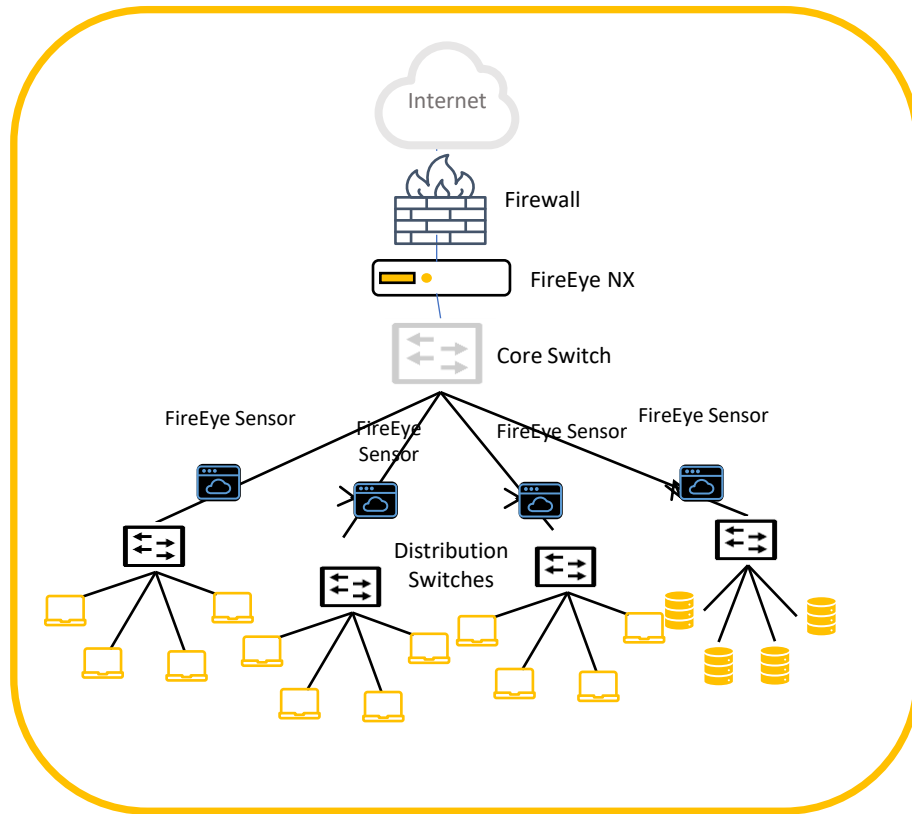
Overview

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

Benefits

1. Integrated IPS reduces costs, simplifies management and improves security posture

SmartVision



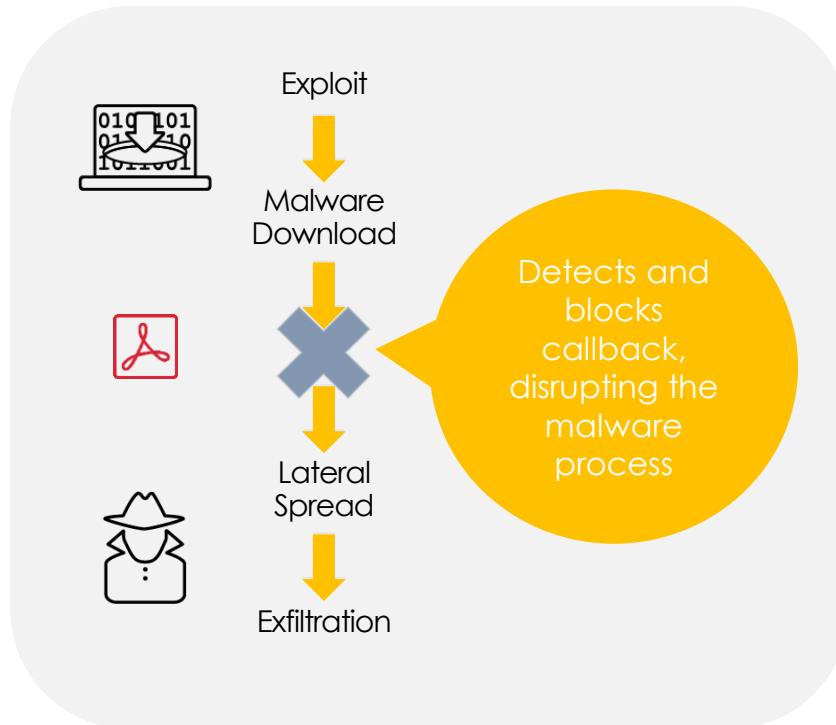
Overview

1. SmartVision is an advanced correlation and analytics engine that detects stealthy, lateral (east/west) attacks within the network

Benefits

1. Protects from threats moving laterally within the network
2. Reduces the time to detection
3. Helps minimize risk of data theft
4. Helps reduce the spread of malware throughout the network

Malware Callback Detection



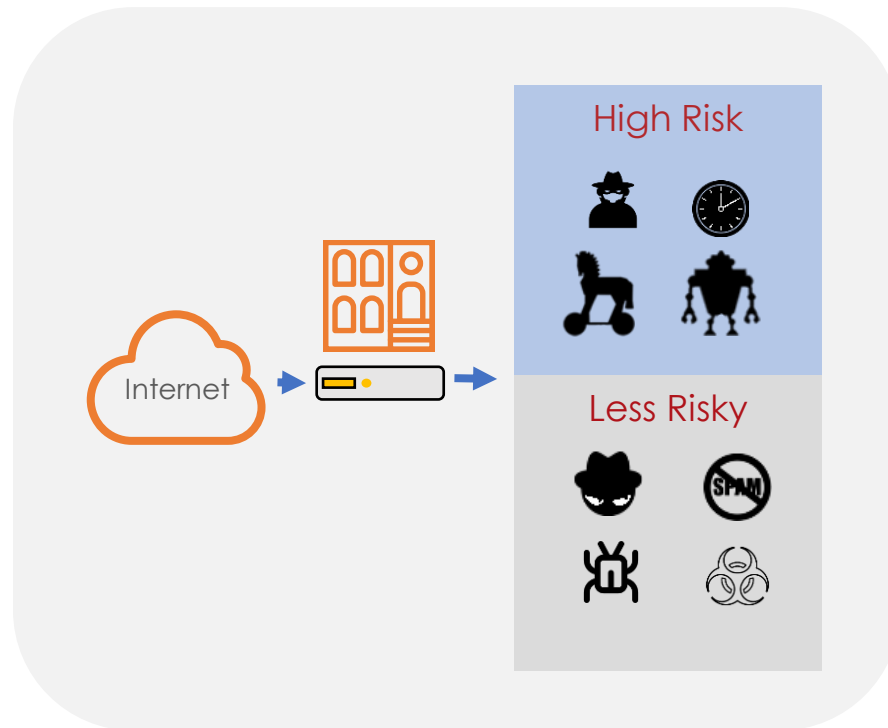
Overview

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

Benefits

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

Riskware Detection



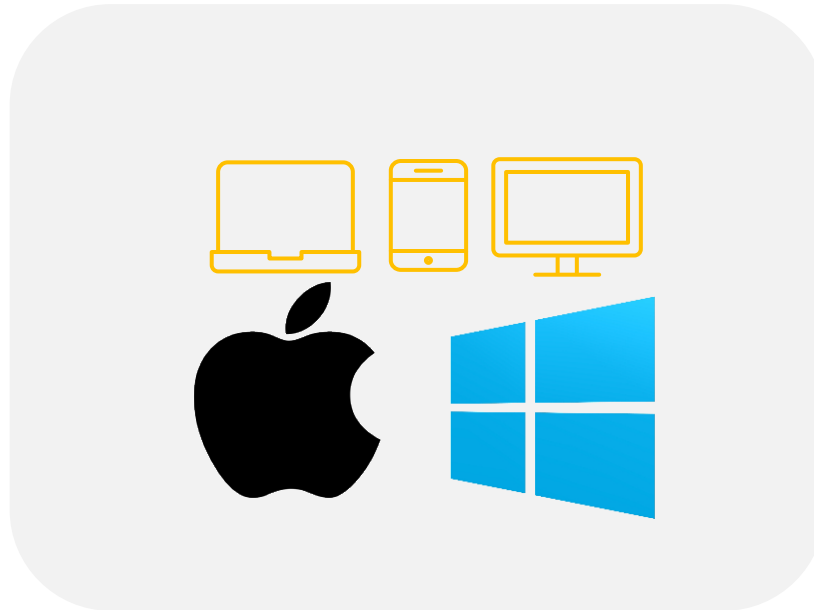
Overview

1. Separates genuine breach attempts from undesirable, but less malicious activity

Benefits

1. Focuses security response team on real threats

Multi-OS Support



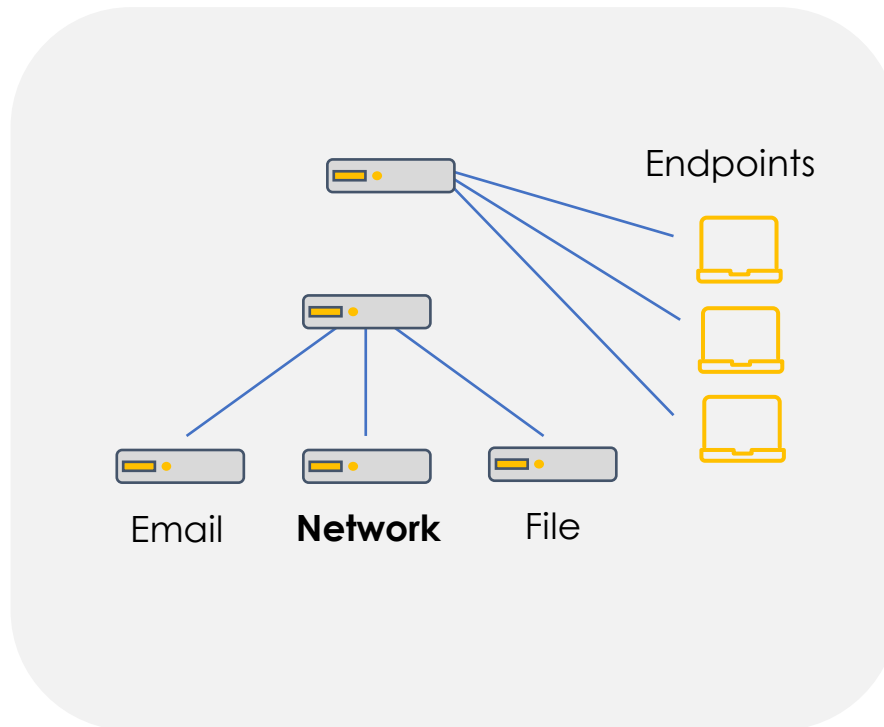
Overview

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

Benefits

1. No worrying about unprotected devices in the company network

Integration with Endpoint Security



Overview

1. Extend network detection to endpoints
2. Confirm alerts from network
3. Create IOCs automatically
4. Validate and analyze network traffic alerts
5. Rapid interrogation of all endpoints

Benefits

1. Quicker detection and remediation of threats
2. Better use of personnel, solve problems not hunt down threats

Visibility into Encrypted Traffic



Overview

1. FireEye are providing integrated man in the middle SSL/TLS inspection to detect threats hidden in encrypted traffic

Benefits

1. Visibility into encrypted traffic
2. Greater detection of malware

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 Security Integration

9

SSL/TLS inspection

10

Integrated IPS

COMGUARD
communication security

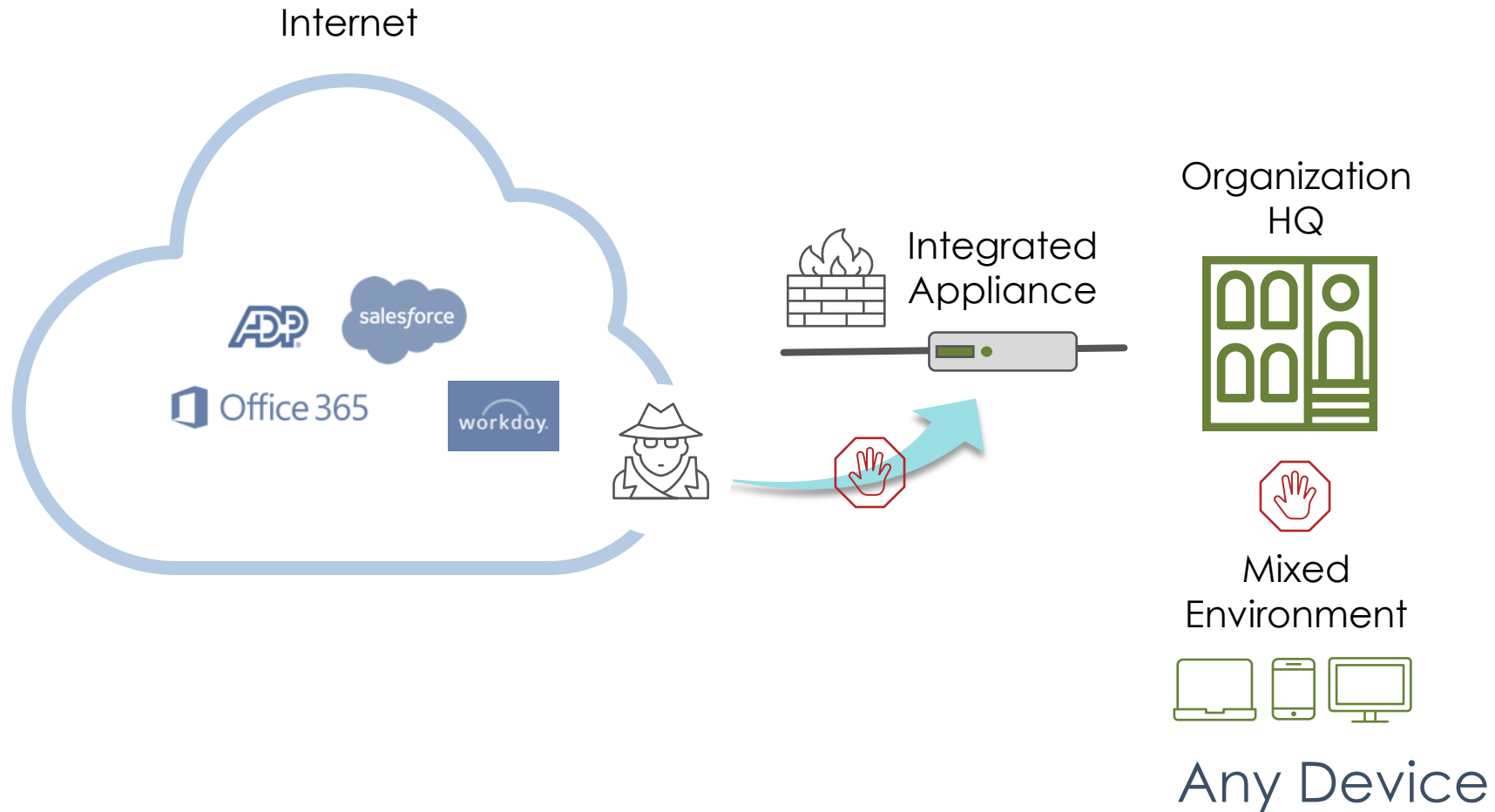


Děkuji za pozornost

martin.votava@comguard.cz
+420 734 442 468

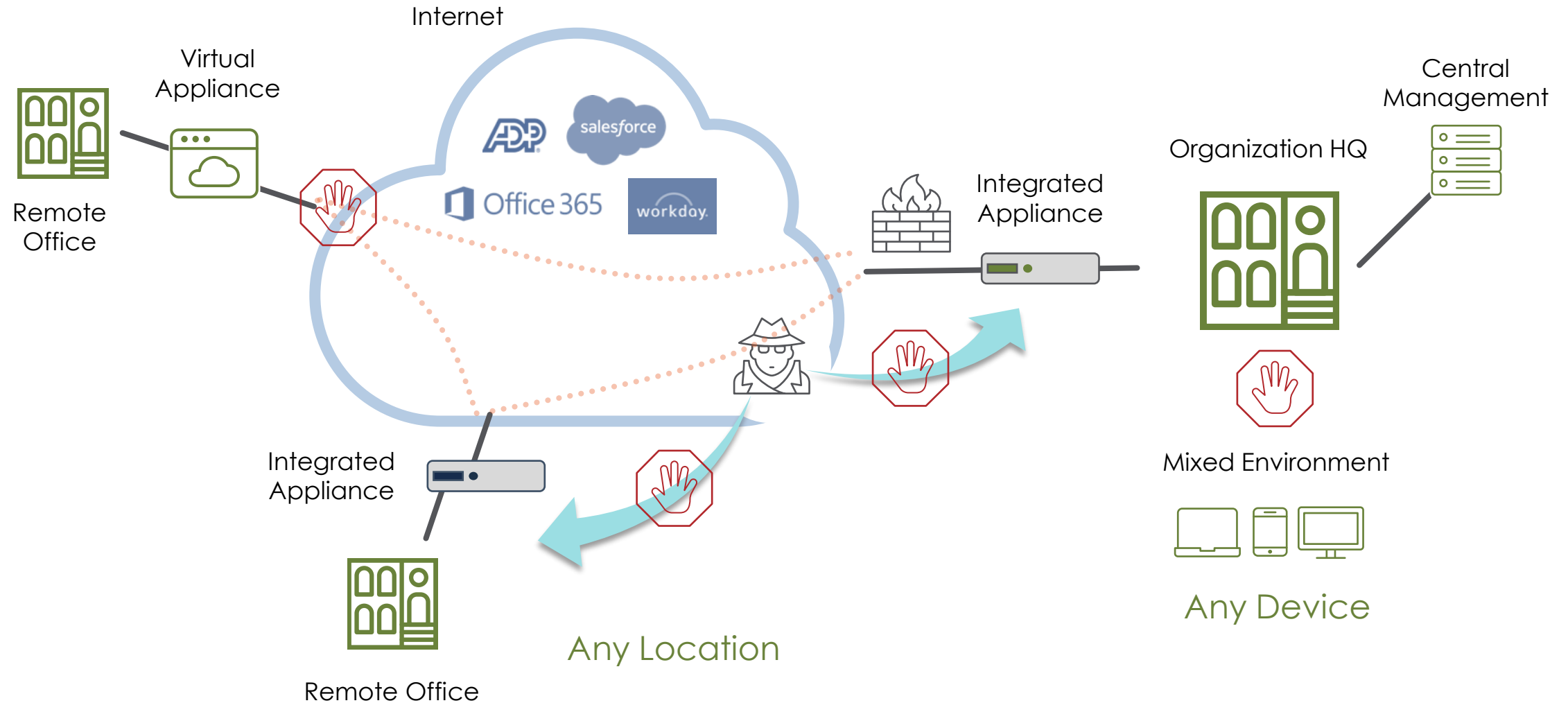
Network Security – Flexible Architecture

Simple Deployment, single appliance



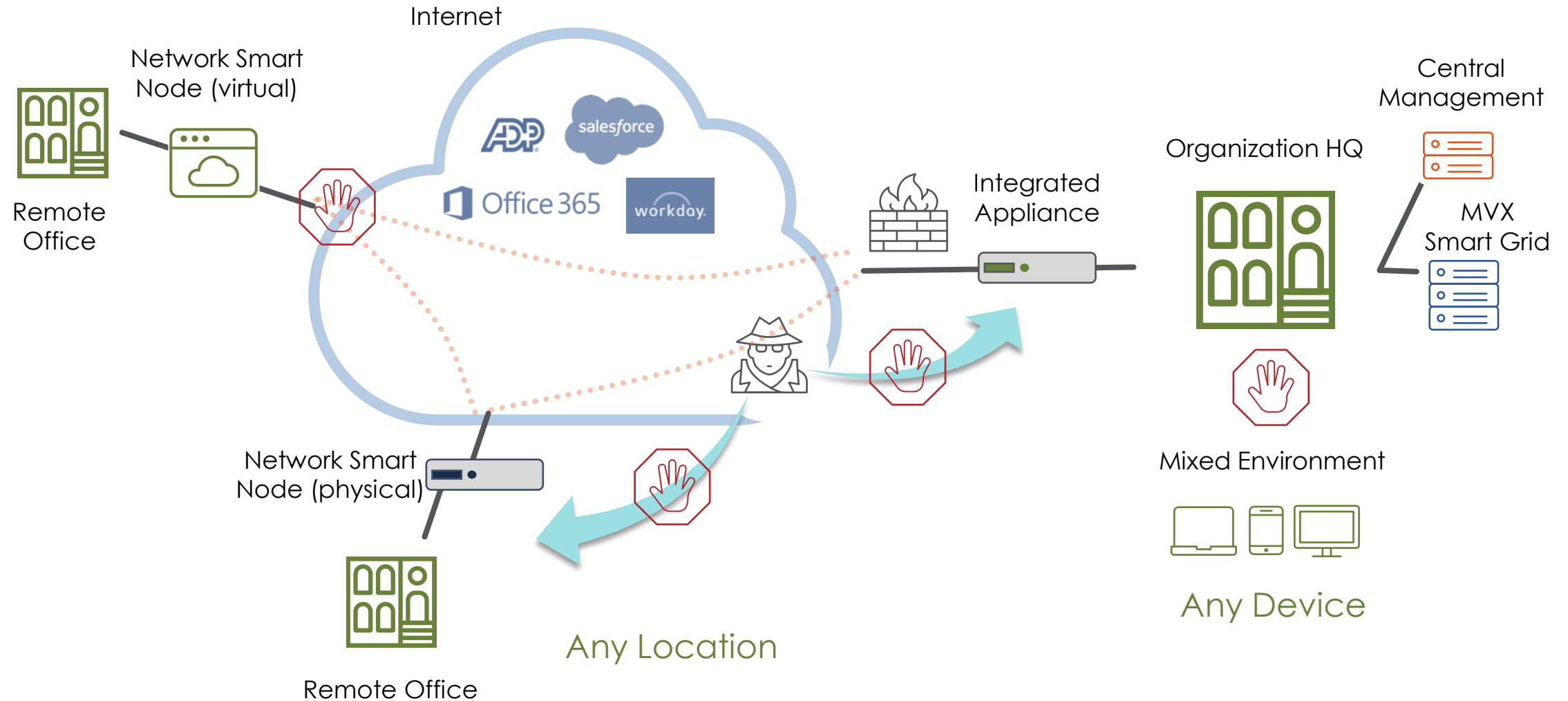
Network Security – Flexible Architecture

Distributed Enterprise, Integrated Appliances



Network Security – Flexible Architecture

Distributed Enterprise with MVX Smart Grid



Network Security – Flexible Architecture

Distributed Enterprise with Cloud MVX

