Symantec Endpoint Protection

Šta sve SEP može, a niste ni znali!

Siniša Stojanović
Solution consultant

Net++ technology

Date: 24.05.2018.

SEP Security Framework

SEP 12 Protection Technologies

Firewall & Intrusion Prevention

- Controls traffic and blocks malware before it spreads to your machine

Block Network Threats

Antivirus

- Scans and eradicates malware that arrives on a system

File

Reputation

- Determines safety of files and websites using the wisdom of the community

Reputation Analysis

Behaviour

- blocks files that exhibit suspicious behaviors

Behavioral Analysis

Power Eraser

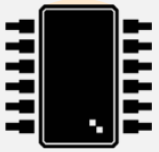
- Aggressive remediation of hard-to-remove infections

Repair

Application Control

- Monitor and control app behavior: automated system lockdown, whitelisting, & blacklisting

Granular Policy Controls



Device Control

- Blocks infections from USB devices, helps prevent data theft. Mac supported added.

USB Storage

Host Integrity

- Detect unauthorized change, conduct damage assessment and ensures compliance

Protection & Compliance

Essential protection technologies

Customized policies

SEP 14 Next Generation Protection Technologies and Enhancements

Machine Learning

- Pre-execution detection for new and evolving threats

Pre-Execution Detection

Application Protection

- Memory Exploit Mitigation

Secure Vulnerable Apps

Emulator

- Anti-evasion technique to detect hidden malware

Strong Anti-Evasion

Intelligent Threat Cloud

- Real-time cloud lookup , ~70% reduction in definition size

70% drop in daily updates

Performance Enhancements

- Faster real-time virus detection

Faster and Light Weight

Enabling Integrations

- REST APIs
- Enable Blue Coat integrations

Easy Integrations

Enhanced Automation

- Expanded LiveUpdate to deliver security updates for Windows clients

Automation

Superior Protection | **High Performance** | **Orchestrated Response**

Complex Environments + Smart Attackers = Advanced Threats

INCURSION

- Web
- Email
- Trusted Apps
- Devices

INFECTION

- File
- File-less (Macro's)
- Memory
- Network Recon
- Crypto-Malware
- Rootkits

INFESTATION

- Weaponization & Evasion
- C&C Communications
- Lateral Movement
- Unauthorized Execution

INOCULATION

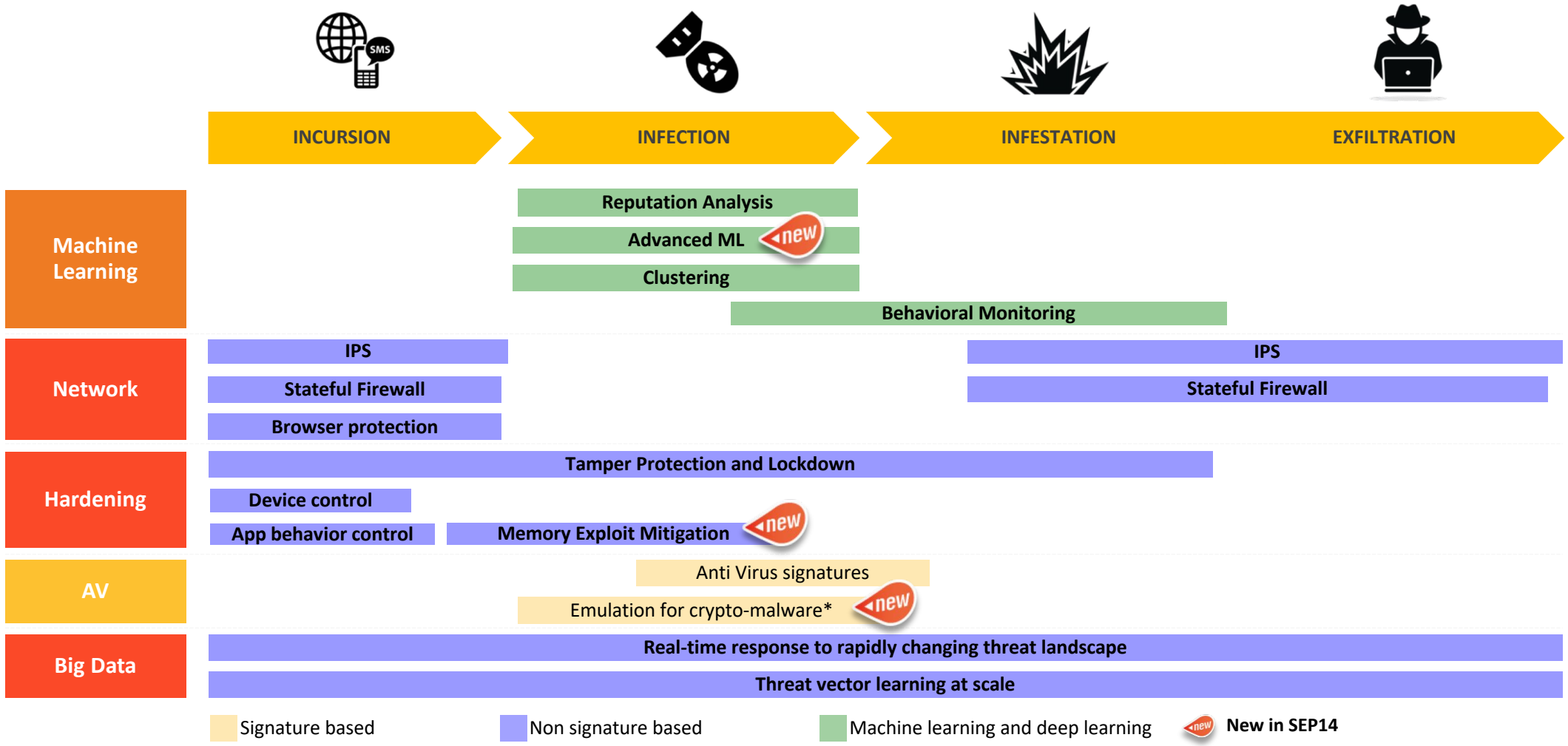
- Quarantine Files & Endpoints
- Removal and Remediation
- Harden System

MULTIPLE VECTORS DIVERSE PAYLOADS RAPID CONTAGION

Endpoint vendors lack effective technologies across the attack chain to block modern advanced threats

Protection Across the Attack Chain

Protection regardless of how your endpoints are attacked



SEP Security Framework

SEP 14 or SEP Cloud:

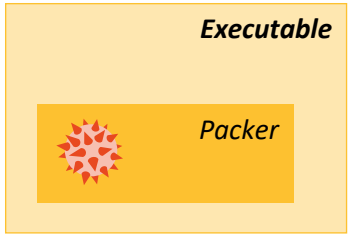
- DISCOVER
- BLOCK
- REMEDIATE
- REPORT

Emulation Capabilities

Fast and accurate detection of hidden malware

NO EMULATION

Malware hides behind custom polymorphic packers

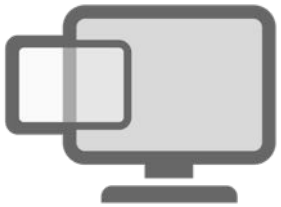


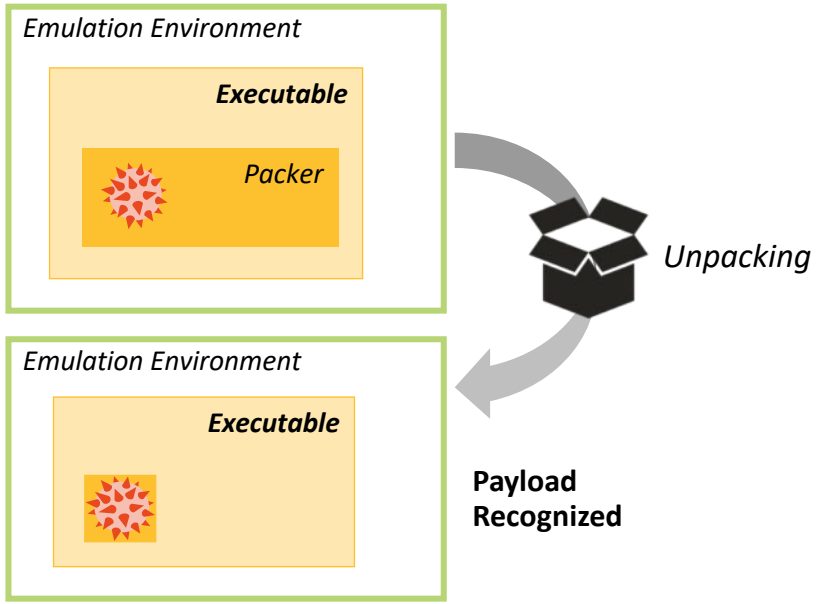
Packed, not recognized

Emulates file execution to cause threats to reveal themselves

EMULATION

Emulator 'unpacks' the malware in a virtual environment

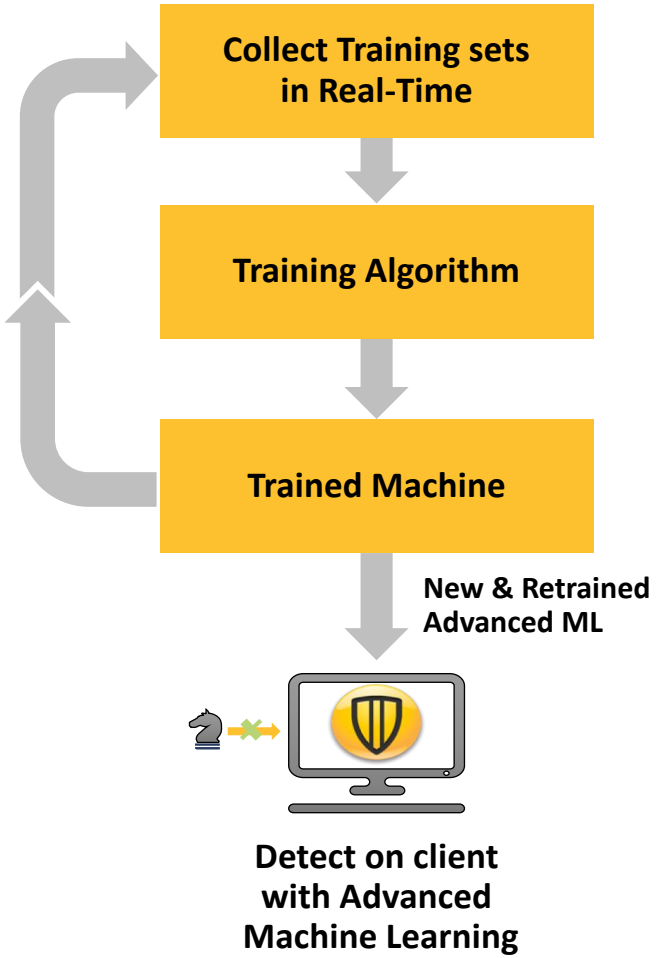




Lightweight solution runs in milliseconds with high efficacy

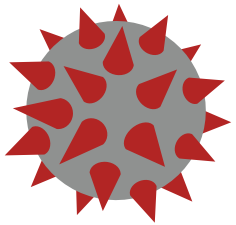
Advanced Machine Learning

Blocks unknown threats and mutating malware

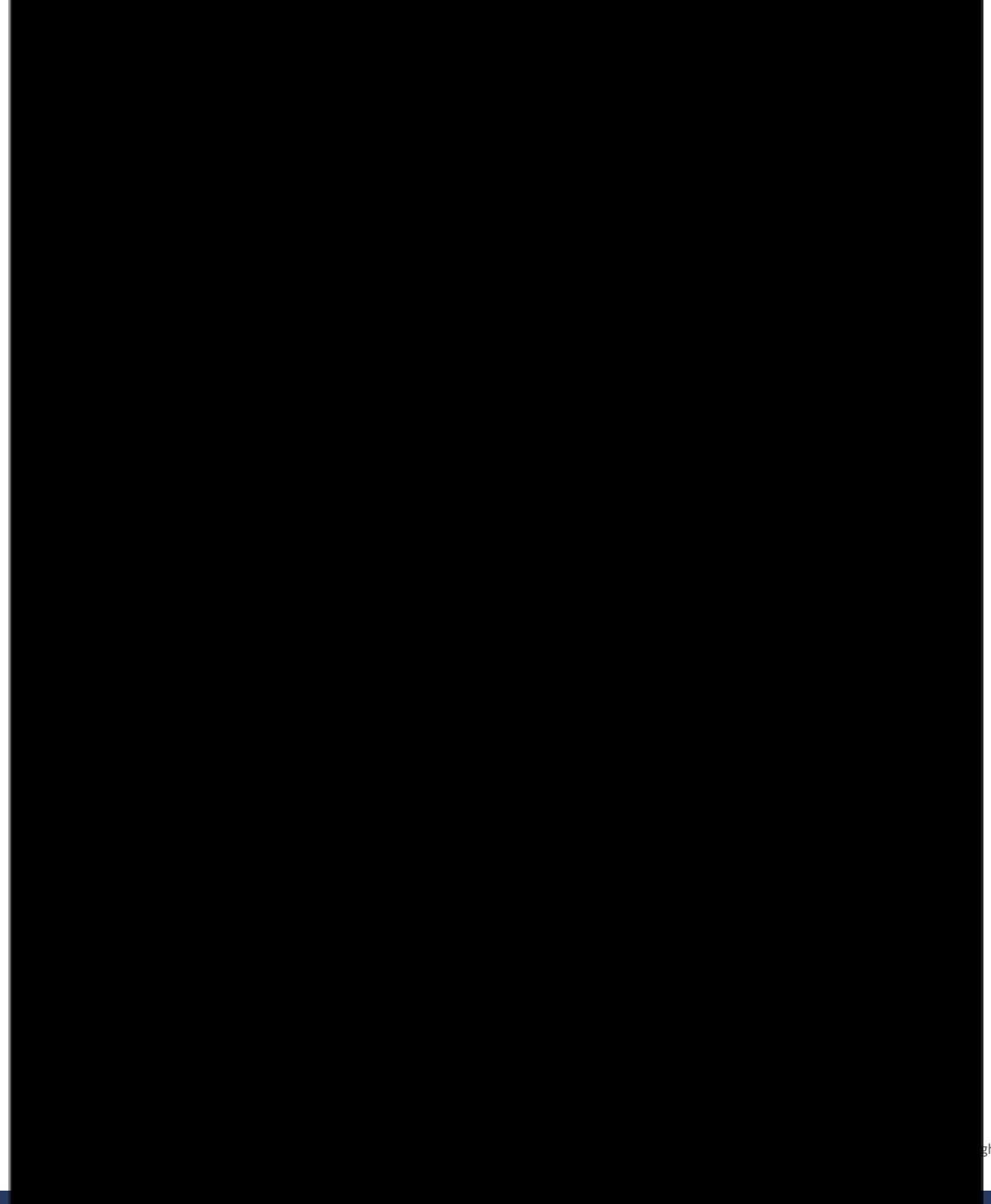


0-day protection against variants of the same malware family

Detects large classes of malware with a low false positive rate

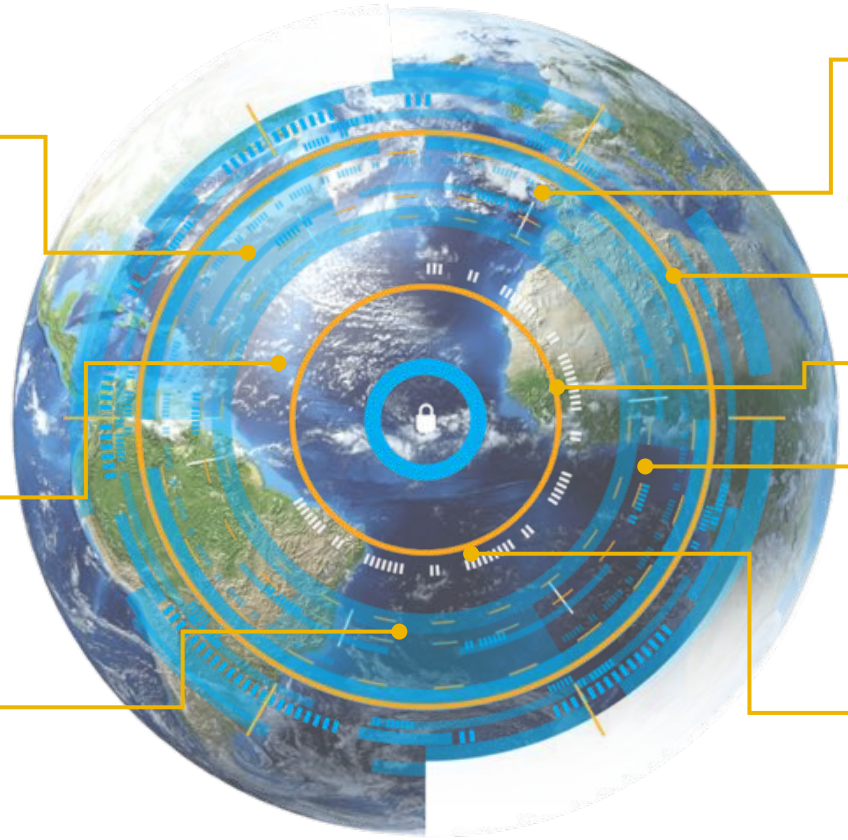


High efficacy with infrequent updates



The Largest Civilian Global Threat Intelligence Network in the World

Diverse data, advanced algorithms, highly-skilled threat experts



175M
Consumer and Enterprise endpoints protected

Discovered
430 million
new unique pieces of malware last year

Billions
of email traffic scanned/day

9 threat response centers

57M
attack sensor in **157** countries

12,000
Cloud applications protected

402M
web attacks blocked last year

1 Billion
web requests scanned daily

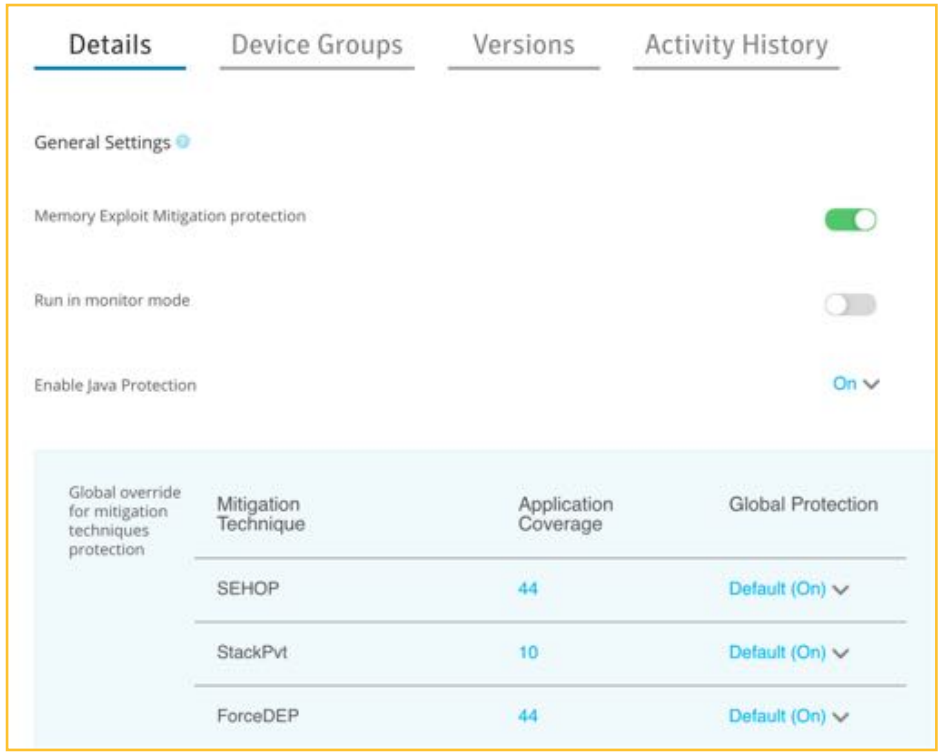
One of the largest civilian cyber intelligence networks
3.7 Trillion rows of security-relevant data

Memory Exploit Mitigation

Blocks zero day memory attacks in popular software

Vulnerability Discovered → Vulnerability Discovered → Patch Released → Patch Applied

- Preemptively blocks attacker exploit techniques
- Works without signatures or knowledge of the vulnerability
- Log-only mode supports testing individual techniques for individual applications



About Memory Exploit Mitigation

Exploit Mitigation

What does it do?

- Blocks all zero day attacks by hardening the operating system

Why is it helpful?

- Targeted attacks increasingly use zero-day exploits – taking advantage of a vulnerability before the software vendor knows it is there
- PEP foils attempts by an attacker to take over a machine by exploiting a vulnerability – thereby blocking every exploit

How does it work?

- When software (e.g., Acrobat, Office) has a bug, the bug can often be exploited by hackers to inject their attack onto a computer.
- There are roughly 10-20 different techniques a hacker can use to exploit such software bugs
- PEP effectively prevents all of these techniques, thereby preventing the attacker from injecting their attack, regardless of the flaw/bug/vulnerability

Results

- PEP blocks all exploits we have seen in the wild thus far (including zero-day exploits), proactively, without knowing anything about the exploit or the vulnerability

Example: Ransomware Attack Chain

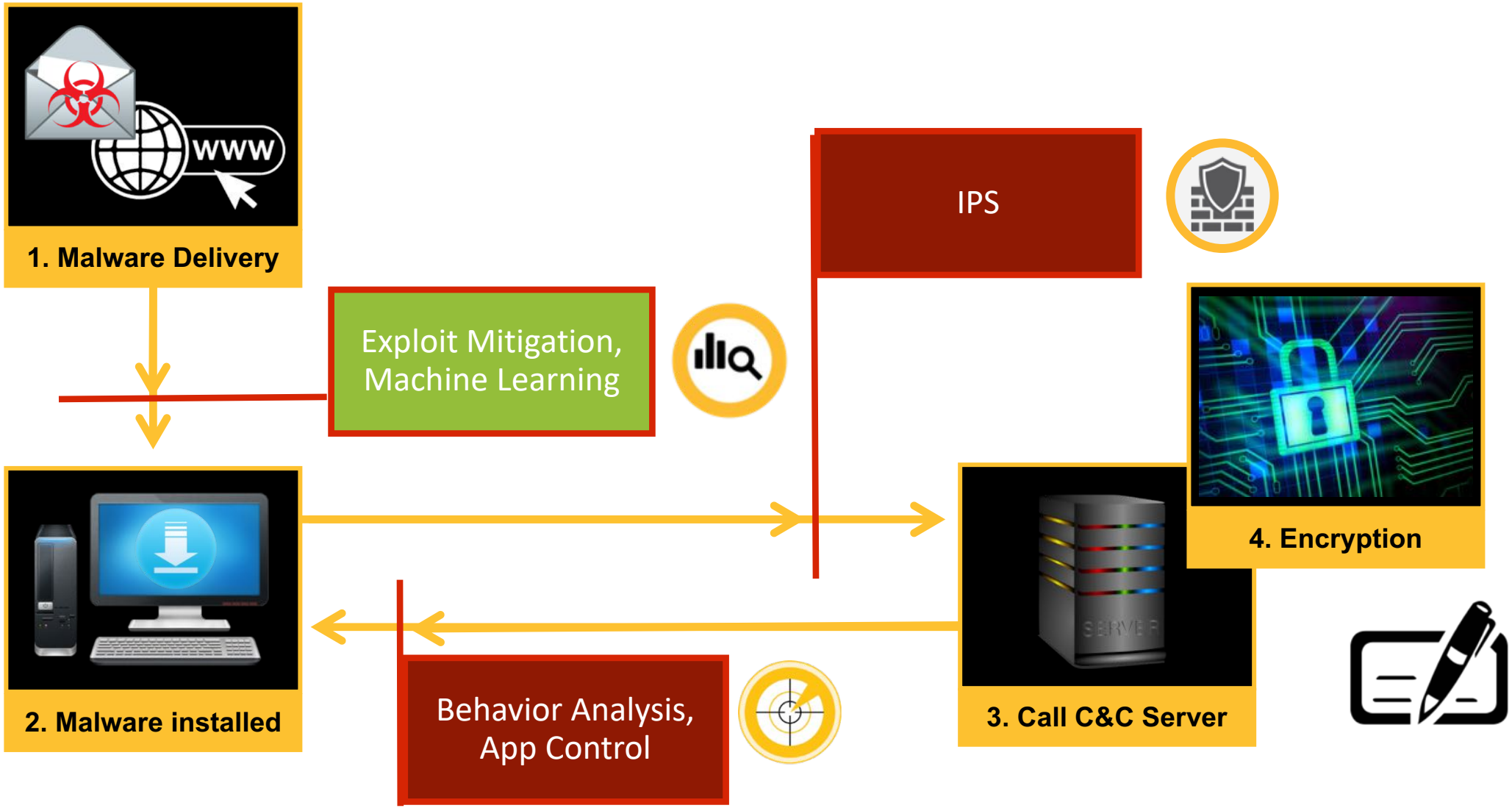
1. Malware Delivery

2. Malware installed

3. Call C&C Server

4. Encryption

SEP 14: Ransomware Attack Kill Chain



Effective Protection against Ransomware

#1 Reason why customers are adopting SEP14

WANNACRY:
1 billion+ infections blocked!

PETYA:
ZERO reported infections on SEP 14 endpoints

SEP Security Framework

EDR:

- EXPOSE
- PRIORITIZE
- INVESTIGATE
- HUNT
- CONTAIN
- RESOLVE

Symantec Endpoint Detection & Response Overview

Symantec EDR exposes, contains and resolves breaches resulting from advanced attacks

EDR with SEP (ATP: Endpoint)

Leverage SEP footprint
Full Endpoint Activity Recording
Correlation across Endpoint, Network and Email

EDR Cloud

Extend EDR to non-SEP endpoints
Point-in-time Scanning
Rule-based automation of best practices

Symantec Endpoint Detection and Response – ATP: Endpoint

Symantec

USE CASE #1

Endpoint Activity Recorder

"I need continuous visibility and real-time queries across endpoints to see what changes threats made to endpoints"

USE CASE #2

File-less Detections

"I need to detect and get alerted to threats that 'hide in plain sight' like PowerShell executions and memory exploits"

USE CASE #3

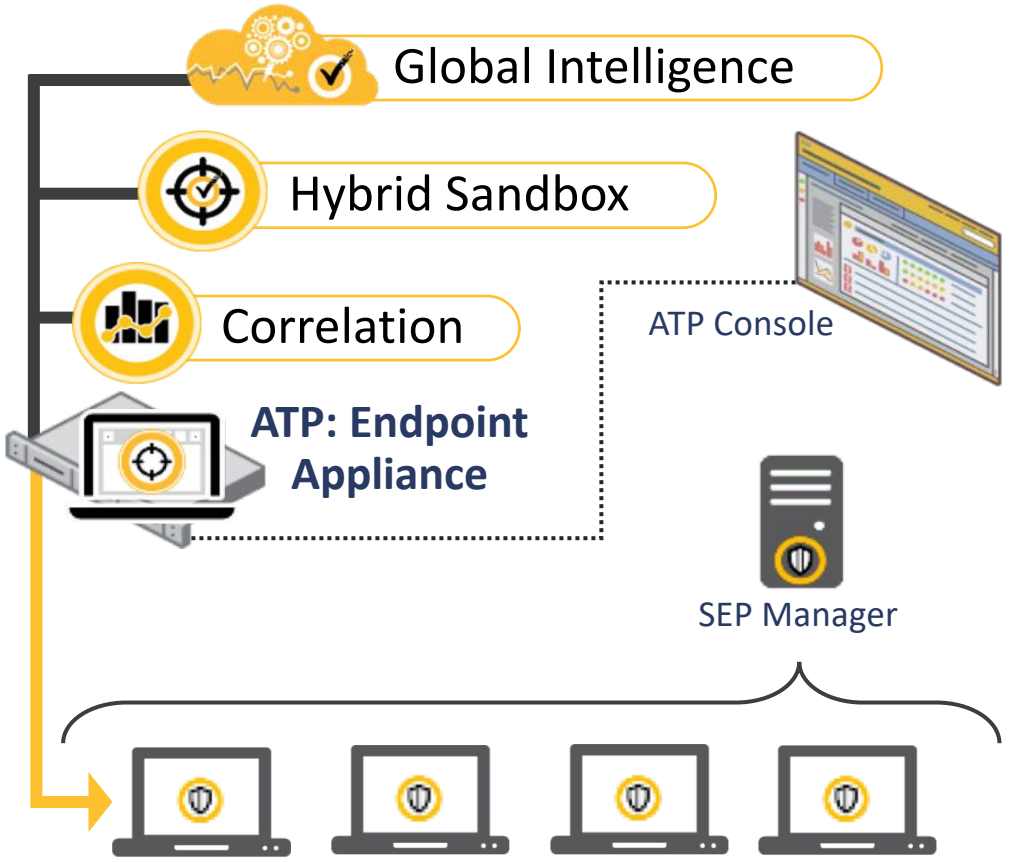
Hybrid Sandbox

"I want the flexibility to sandbox and detonate suspicious objects on-premises or in the cloud"

Integrated EDR with SEP for incident response and remediation.

Symantec Endpoint Detection & Response – ATP: Endpoint

Provide incident investigation and response, using SEP agent



Detect and **Investigate** suspicious events

Hunt for Indicators of Compromise

Record all events and get complete visibility with **incident playback**

Fix impacted endpoints, with one click

No new endpoint agent required

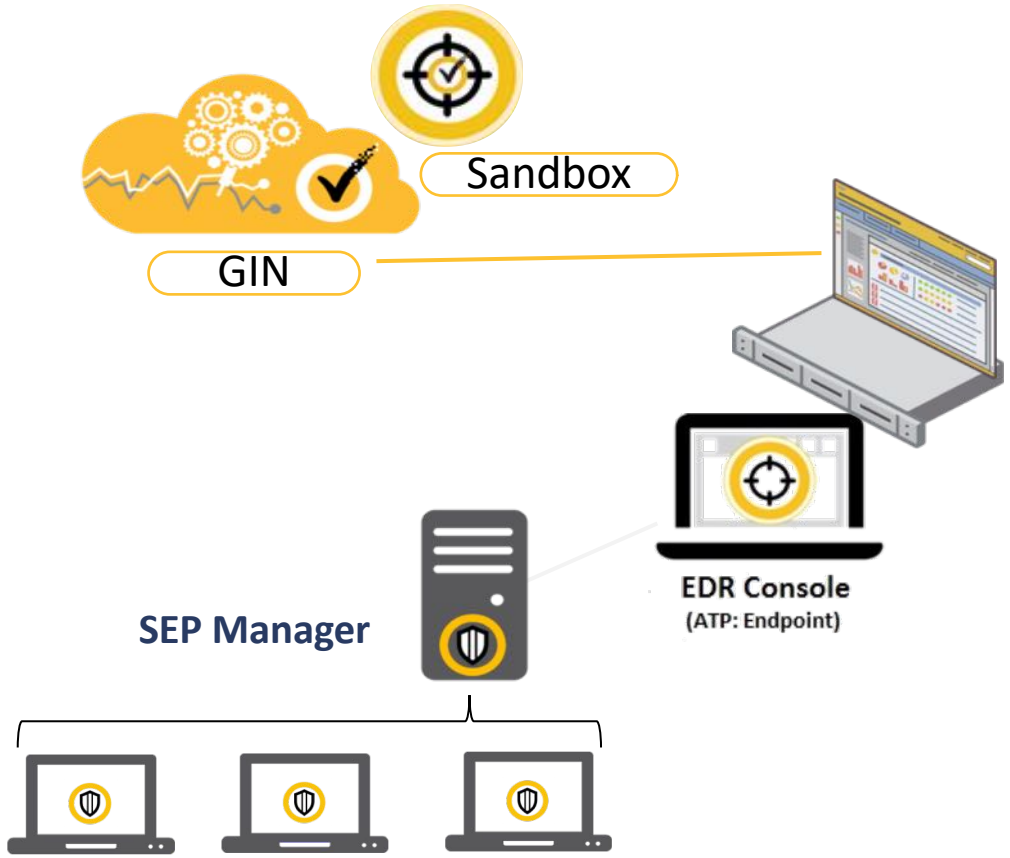
EDR with SEP: Identify Incidents from Real-Time Streaming Events

Provide me with smart incident alerts so I know where to spend my time

Event Type	Event Description
Session	User session logon and logoff
Process	Launch and terminate
Module	Loads and unloads
File	Create, Read, Delete, Rename
Folder	Folder operations
Registry Key	Operations on registry key
Registry Value	Operations on registry values
Network	Actor process network
Named object	Named object attributes

SEP 14: Endpoint Detection & Remediation on your Endpoint

Provide EDR capability without new endpoint agents



Investigate suspicious events and get full endpoint **visibility**

Instant search for any attack artifact and sweep endpoints for IoC

Remediate all instances of threats in minutes, with one click

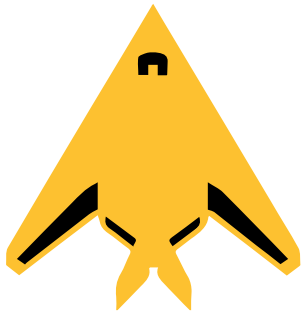
Leverage existing investment- both Symantec & non-Symantec products

SEP Security Framework

SEP Deception:

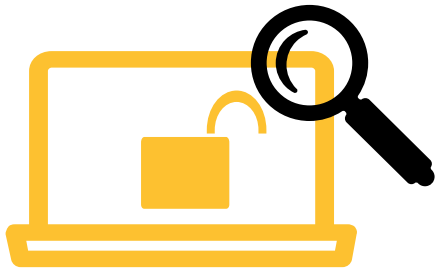
- DEPLOY DECEPTORS
- MONITOR
- ALERT
- ANALYZE

Current Challenges



Increasing usage of stealthy attacks

Lack visibility into attacker intent



Lack insight to improve security posture

Adversaries are using more stealthy attacks and “living off the land.”
IT security teams lack visibility into attackers’ intent and tactics.

SEP Deception

USE CASE #1

Expose Hidden Adversaries

"I want to uncover hidden attackers by creating a minefield against their tactics, techniques and procedures"

USE CASE #2

Generate High Fidelity Alerts

"I want to customize deceptors to my environment in order to generate high confidence alerts and reduce false positives"

USE CASE #3

Deploy At Scale

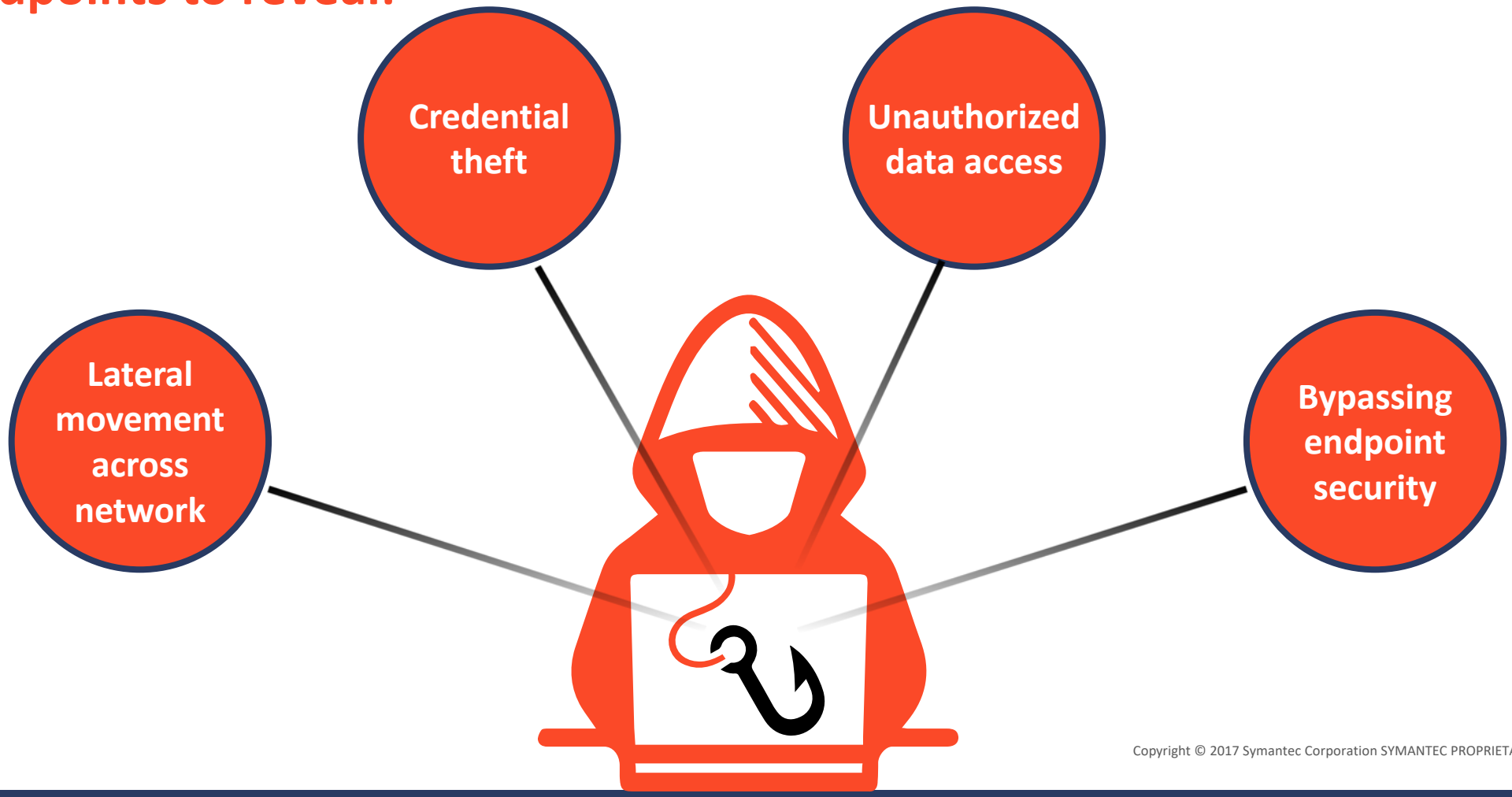
"I want to rapidly deploy deceptors across my enterprise by leveraging the SEP agents already running on my endpoints"

Deceive attackers. Reveal their intent. Improve security posture.

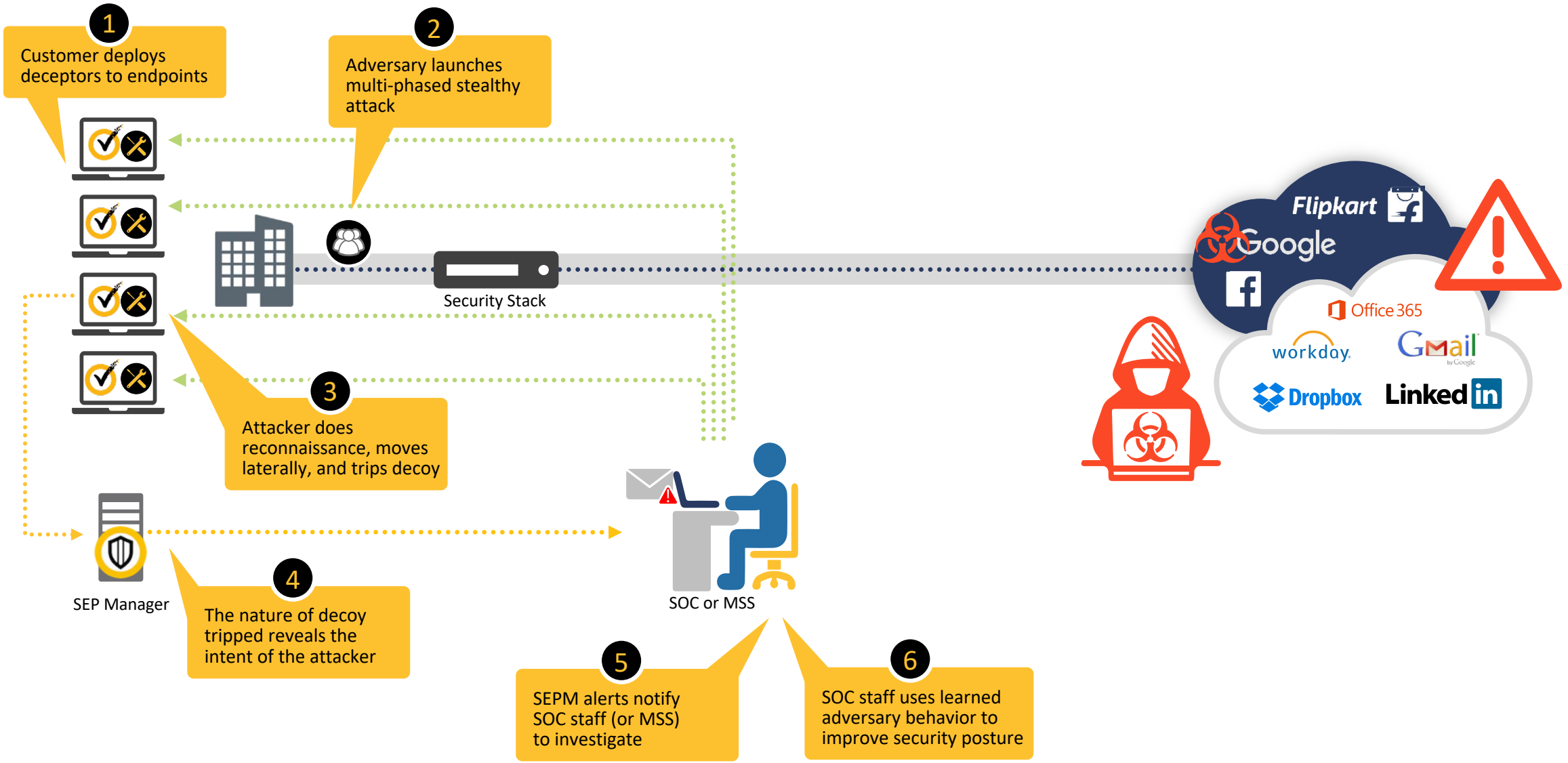
Deploying Granular Deceptors

Symantec

Bait is deployed onto endpoints to reveal:



SEP Deception In Action



The SEP Deception Difference

Fastest time to value

Most accurate and insightful detection

Only EPP vendor with Deception

SEP Security Framework

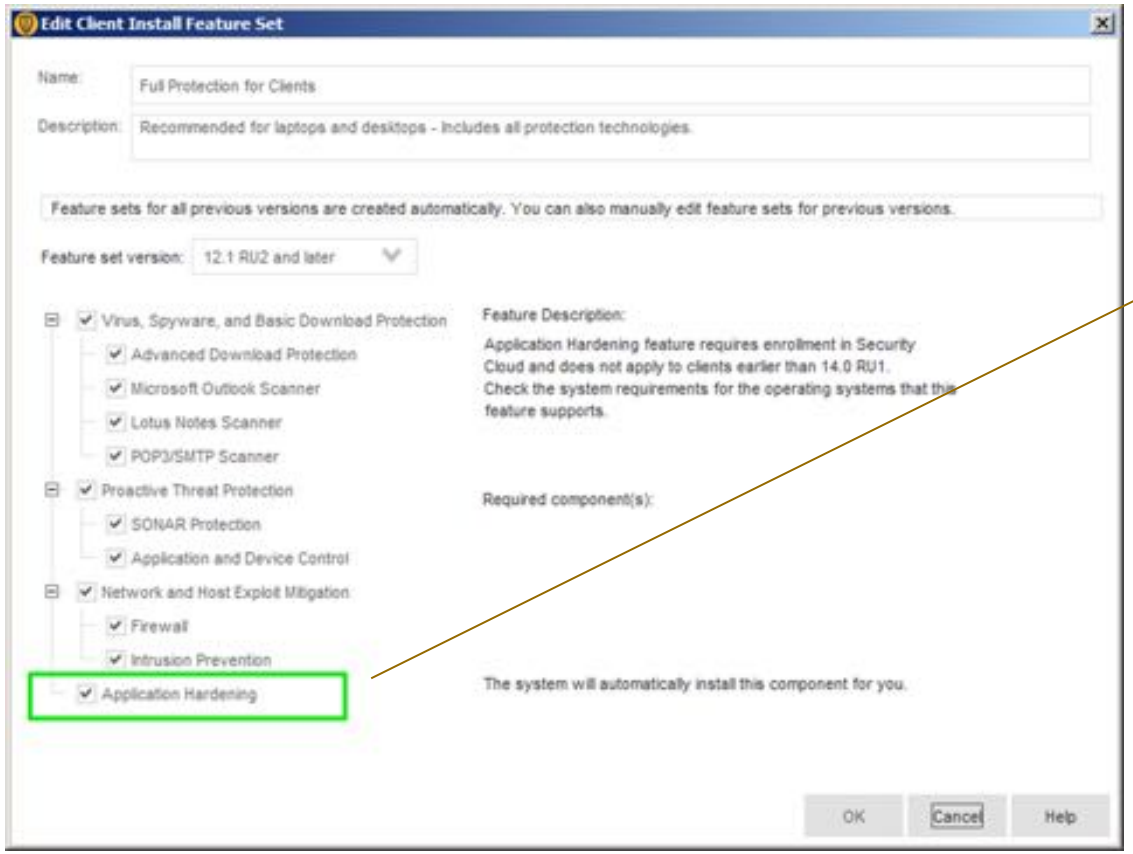
SEP Hardening:

- ANALYZE
- ISOLATE
- HARDEN

Risk Insight:

- VISUALIZE
- ANALYZE
- BENCHMARK

SEP Hardening included as SEP Install Feature



Visible as a new feature in the feature set.

Symantec customers have the option to activate and utilize Application Hardening in the SEP 14 RU1 environment after cloud enrollment and after they have purchased a license for Application Hardening.

Current Challenges

12+ weeks average time taken to patch an application vulnerability

Security training is ineffective; 10% median click rate for phishing attacks

Current hardening solutions negatively impact end user productivity

SEP Hardening Overview

Symantec

USE CASE #1

Assess & Auto-classify Every App

"I want to know what applications are running in my environment. I want to know how much risk I'm taking on due to app vulnerabilities"

USE CASE #2

Defend Known-good Apps

"I want to prevent zero day attacks from compromising trusted applications and gaining privileged system control"

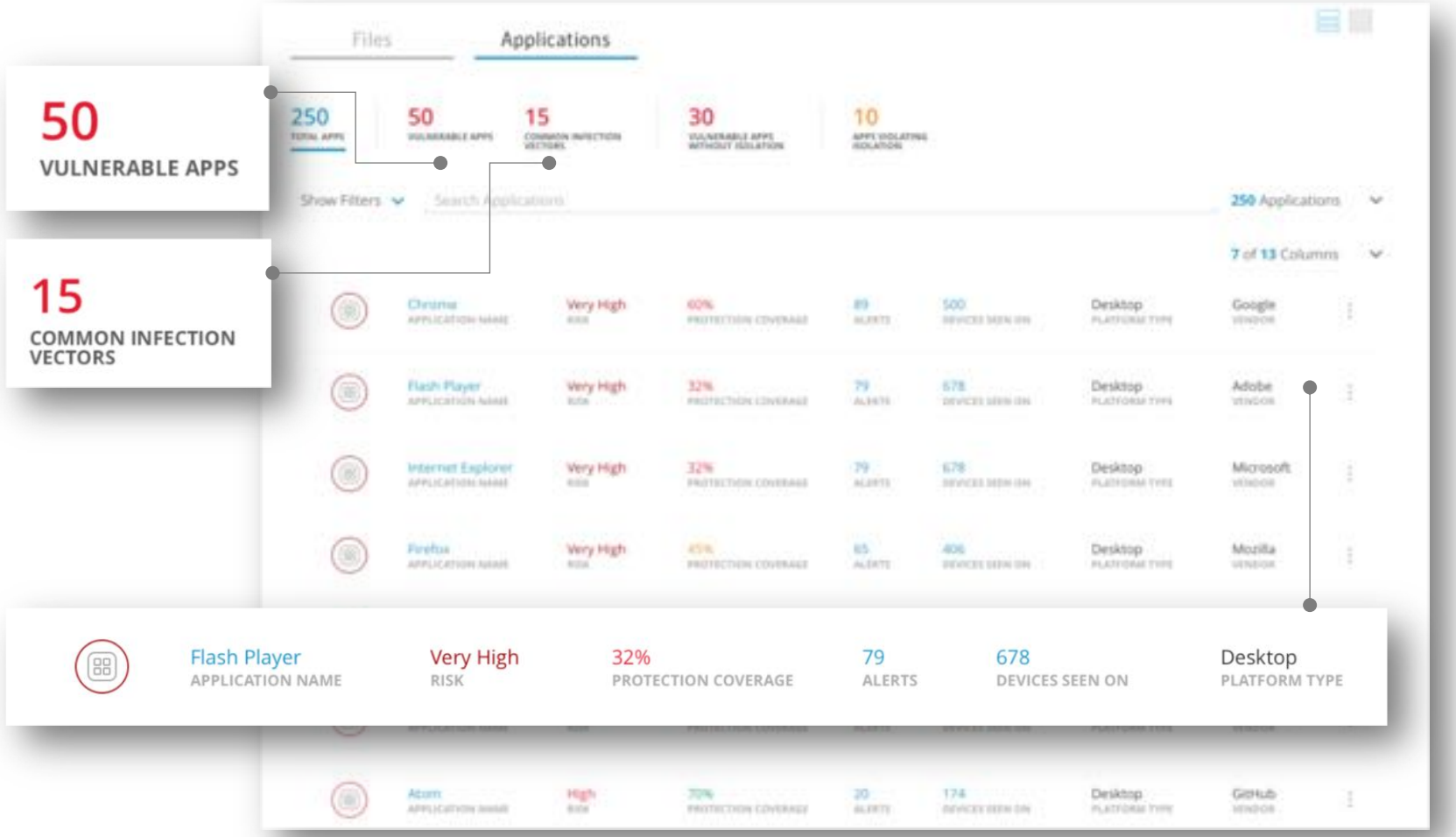
USE CASE #3

Isolate Suspicious Apps

"I want to allow end users to safely download and use applications without risk of infection"

1 Click Isolation: Browsers (IE, Edge, Chrome, Firefox); Office Apps (Word, Excel, PowerPoint); Adobe Apps (Acrobat)

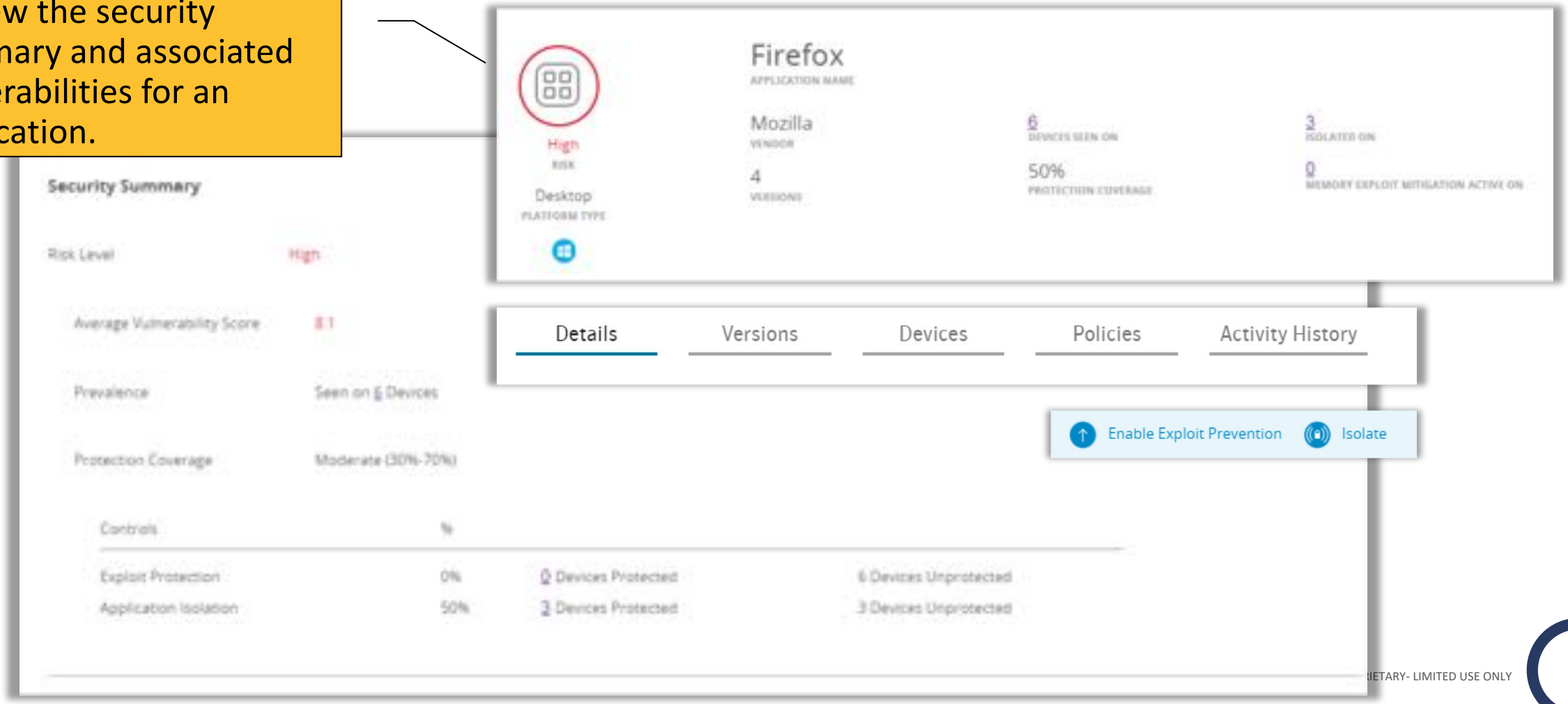
Assess & Classify Every Application



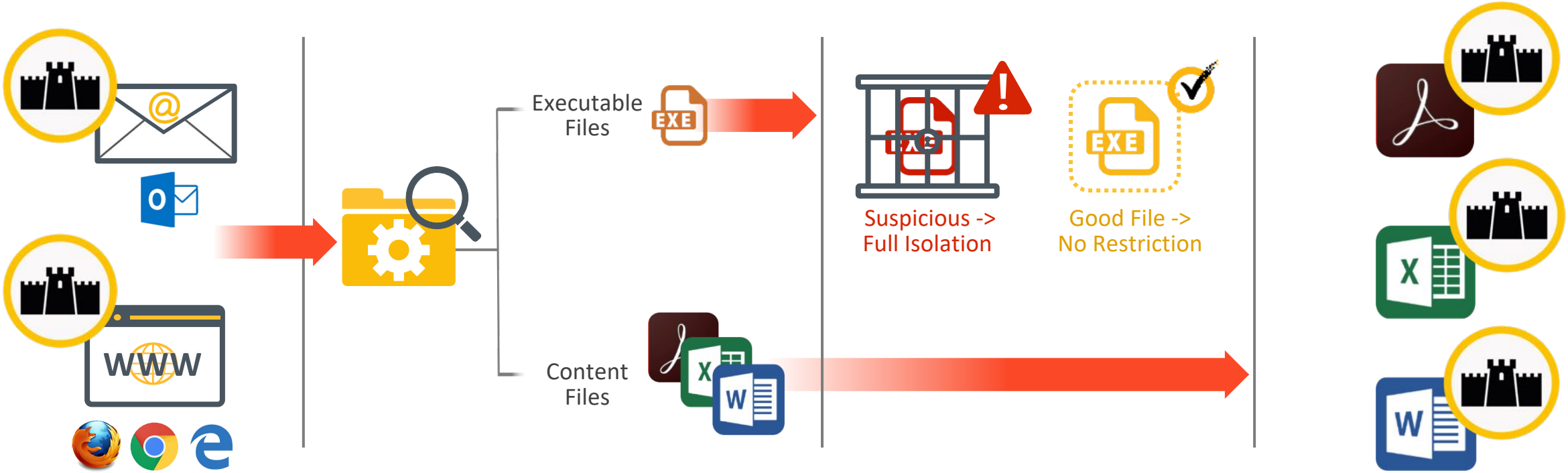
- Auto-classify all installed and running apps
- Identify Suspicious Apps
- Analyze attack surface for Known Good Apps

Application Details

Review the security summary and associated vulnerabilities for an application.



Isolate Suspicious Apps and Defend Known Good Apps



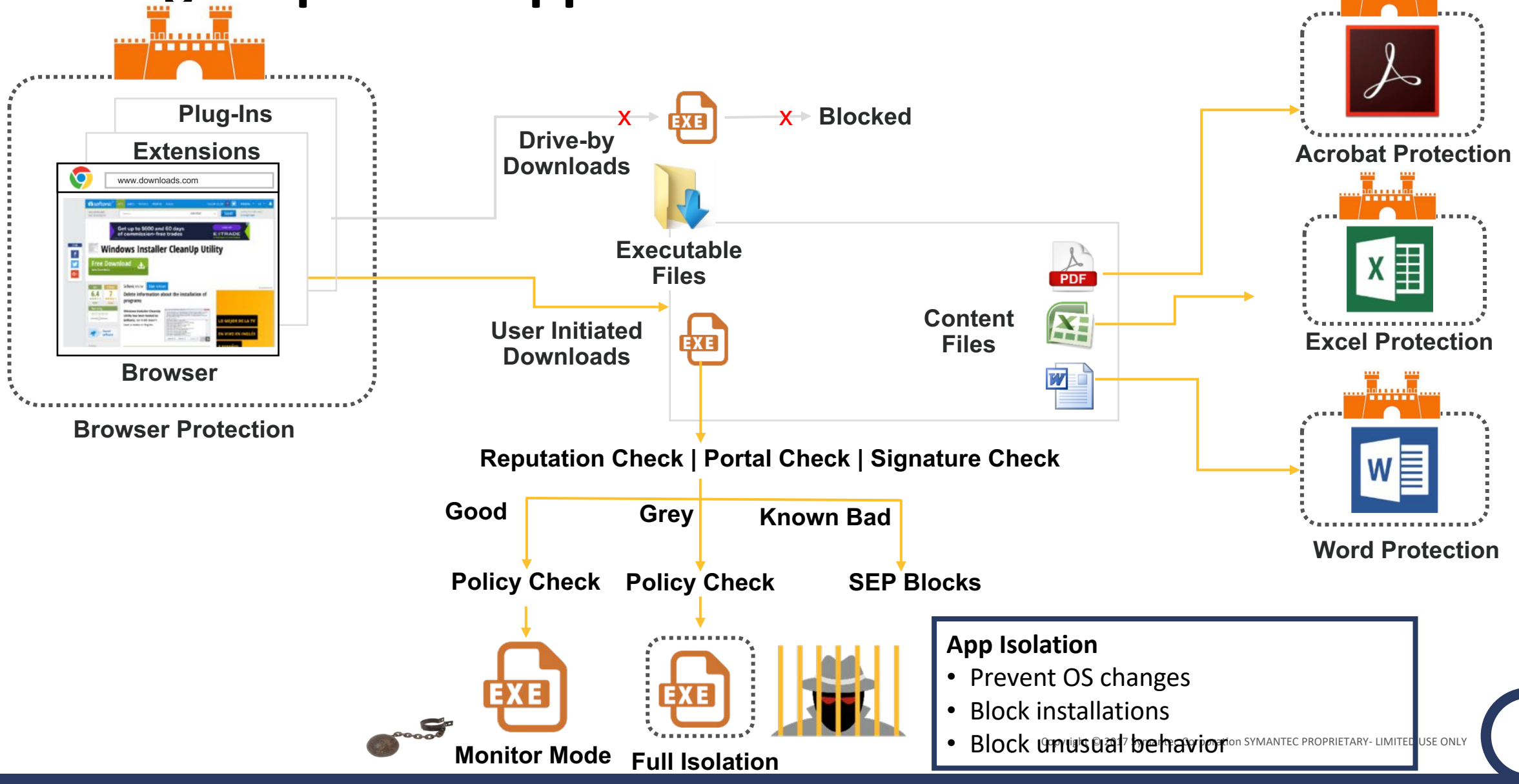
Shield browsers and email clients from attacks

Monitor download activity and auto classify downloaded files

Automatically isolate suspicious executable files

Shield applications from weaponized content

Isolating Suspicious Apps: Jail



App Isolation

- Prevent OS changes
- Block installations
- Block unusual behavior

The SEP Hardening Difference

Application discovery and attack surface assessment

Automatic detection and isolation of suspicious apps

Low impact to end user productivity

Integrated with SEP – No additional agents

Enabling Integrations with SEP Management APIs

Easily integrate with security infrastructure

Symantec Endpoint Protection Manager 

Client Management | Application & Device Control | Policy Control | Reports & Analytics

REST API's

SEP14 - API's
Login & Logout of SEPM
Obtain a list of groups
Retrieve the Symantec Endpoint Manager version information

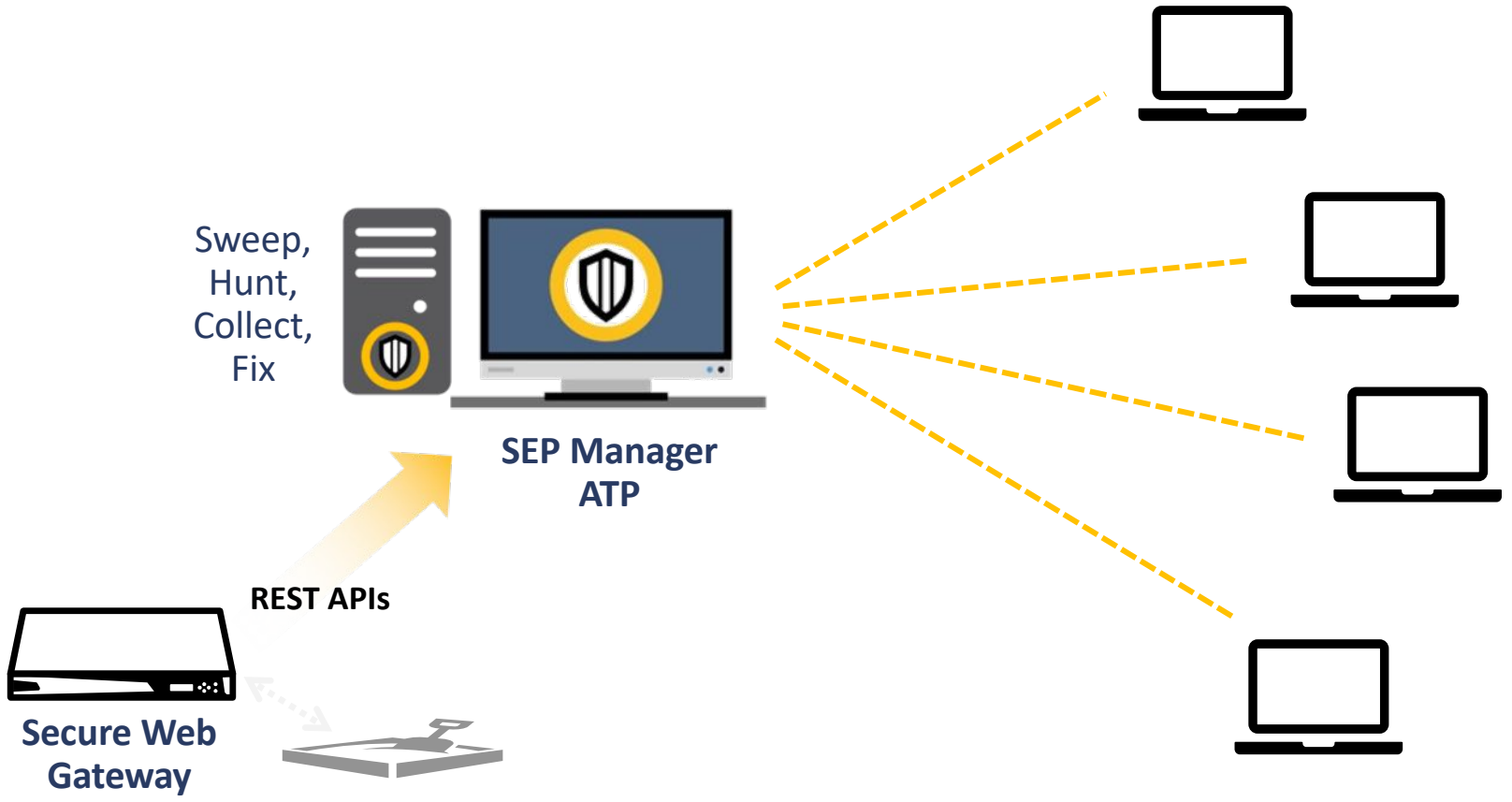
Orchestrate/Automate SEPM functionality from other applications and scripts

Connect to 3rd party platforms for control or network plane integration with the endpoint

Integration with Secure Web Gateway (Proxy SG)

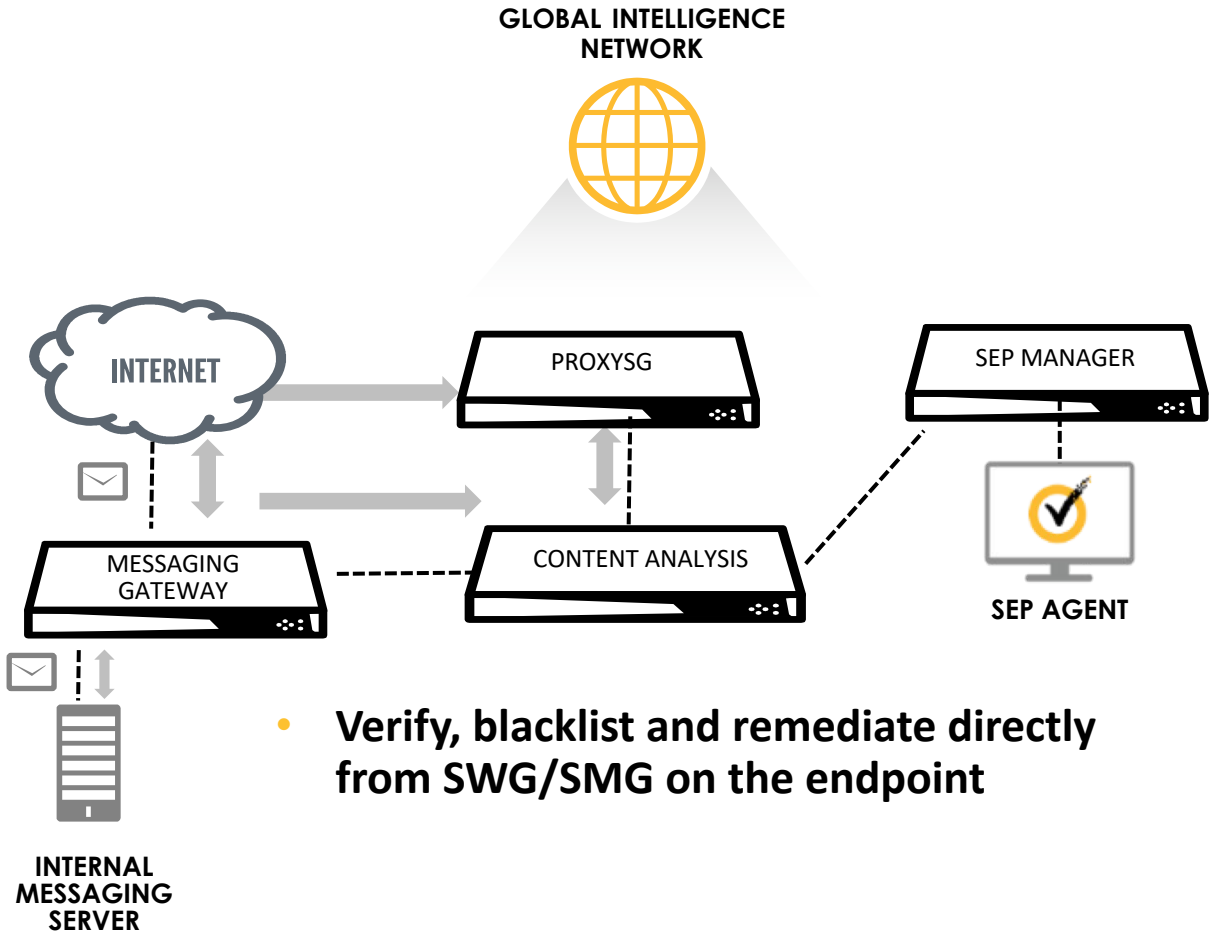
Protecting from the Network to the Endpoint

Orchestrate/Automate SEPM functionality from other applications and scripts



Orchestrated Response

SEP + Network Security Integrations



- **Verify, blacklist and remediate directly from SWG/SMG on the endpoint**

ROAMING USERS: ENDPOINT + WSS

- **Re-direct web traffic from roaming users to WSS to ensure same protection as on-premise**
- **Single agent on client**

SEP Mobile Overview

USE CASE #1

Malicious Apps

"I don't have protection against malware on my mobile devices"

USE CASE #2

Unpatched Vulnerabilities

"I don't have visibility into vulnerabilities affecting mobile OS/applications"

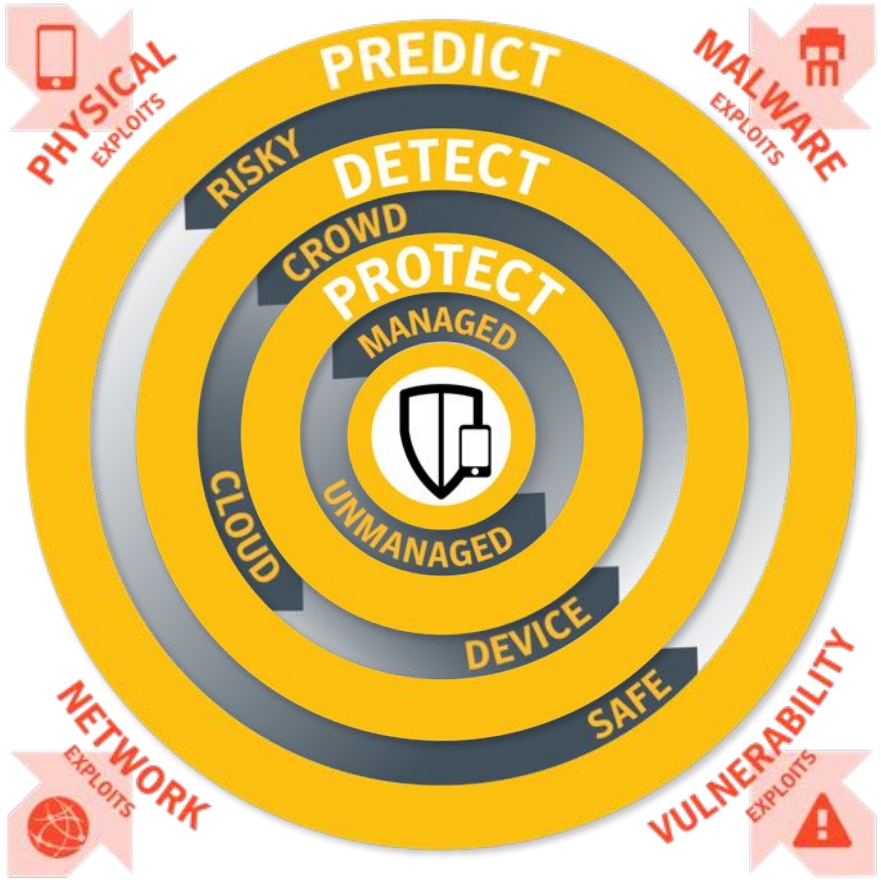
USE CASE #3

Risky Wi-Fi Networks

"I am worried about my users connecting to suspicious Wi-Fi networks"

Defend against malicious apps. Ensure devices are properly patched. Protect from network-based attacks.

SEP Mobile Security Framework



Symantec's Layered Mobile Security

Threat Intelligence

SEP Mobile crowd-wisdom
Integrated Global Intelligence Network

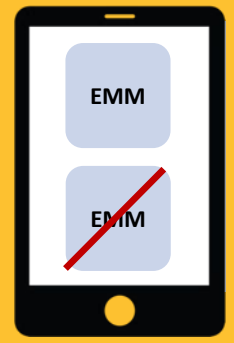
- 1000 Cyber Warriors. 175 M Endpoints. 8 B Daily Security Requests.

Cloud Server

Risk/compliance visibility
Advanced security
Automation & integration

Public App

Simple deployment & maintenance
Ensured privacy
Minimal footprint



Consistent across Managed & Unmanaged scenarios