SentinelOne

Real-time, Unified Endpoint Protection

Gary Mello, Sr. Director, Solutions Architects

January 19, 2017

Total Endpoint Protection

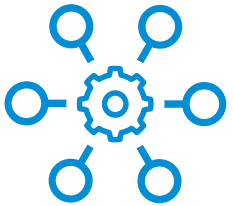
Defends against every type of attack, at every stage in the threat lifecycle.

Complete visibility

into all endpoint activity
without any performance drag

Dynamic behavior analysis

to detect threats across
all major vectors



Fully automated

threat mitigation
and remediation

Gartner

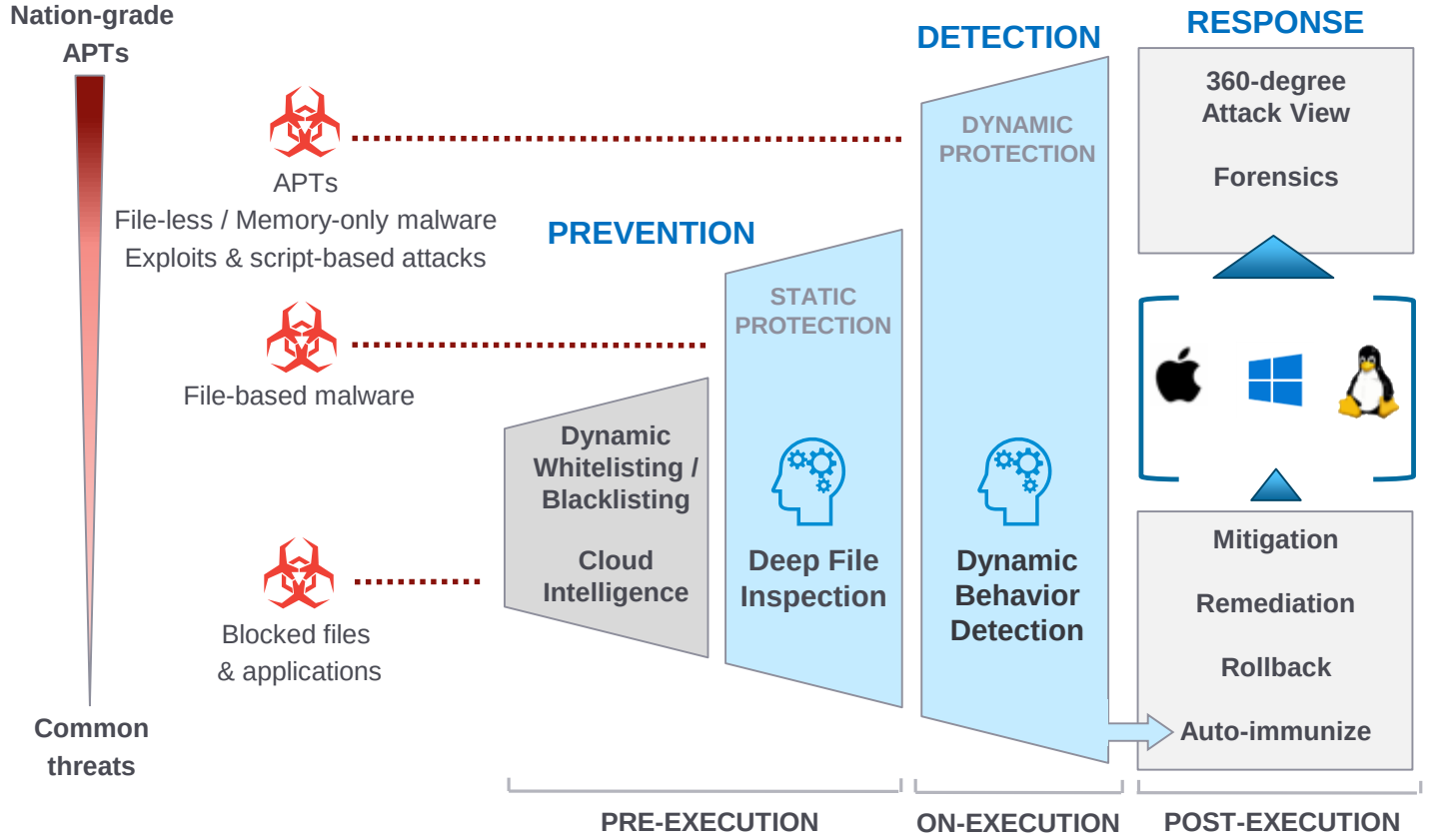
Visionary
2016 Magic Quadrant for Endpoint Protection Platforms

CYBER SentinelOne GUARANTEE

Certified Antivirus replacement

AV TEST APPROVED CORPORATE ENDPOINT PROTECTION

Endpoint Protection Platform (EPP)



Single Autonomous Agent

70MB

Memory Footprint

Single Management Console

Supports up to

25,000

Endpoints

Cloud or On-Premise Deployment

(Ransomware) File-less Attack

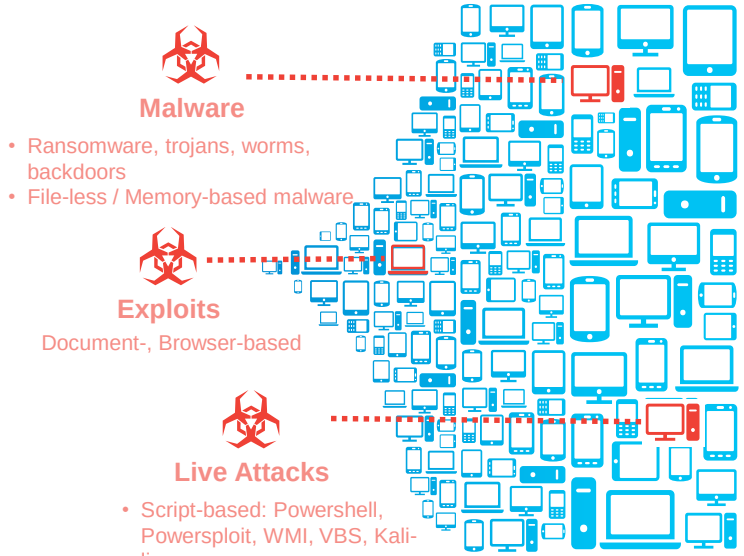
One of a “file-less” attack scenario

1. Browser-based drive-by infection, e.g. infected ad
2. Malicious software initiates its communication to its C2 →
3. ← C2 delivers *Ransomware* to the victim machine
4. Advanced (*Ransomware*) Malware executes on the victim’s machine memory, NOT on HD/Disk. This is a **file-less**, **memory-based** attack

SentinelOne

SentinelOne Dynamic Behavior Tracking Engine Detects and Protects endpoints from File-less, memory-based attacks.

Many Attack Vectors …



Malware

- Ransomware, trojans, worms, backdoors
- File-less / Memory-based malware

Exploits

Document-, Browser-based

Live Attacks

- Script-based: Powershell, Powersploit, WMI, VBS, Kali-linux
- Credentials: Mimikatz, tokens

Multi-Solution vs. Unified Approach

Unified Approach

- Single, lightweight agent
- Single management console
- Fewer FTEs
- Reduced TCO

SentinelOne
Endpoint Protection Platform

Pre-Execution

Advanced Static Prevention
+ Whitelisting / blacklisting

On Execution

Dynamic Malware Detection
Dynamic Exploit Detection

Post-Execution

Mitigation
Remediation
Forensics

Multi-Solution Approach

- Multiple agents
- Multiple management consoles
- More FTEs
- > 4x TCO of SentinelOne

Best-in-Class Endpoint Protection

Certified

SentinelOne is a certified replacement for Antivirus

Recognized

Gartner
Visionary - 2016 MQ
for Endpoint Protection Platforms

Guaranteed

- **Financial protection against ransomware**
- **Coverage up to $1000 per endpoint or $1M/company**

For more information
sentinelone.com/resources

Ready to evaluate?
sentinelone.com/contact

SentinelOne®