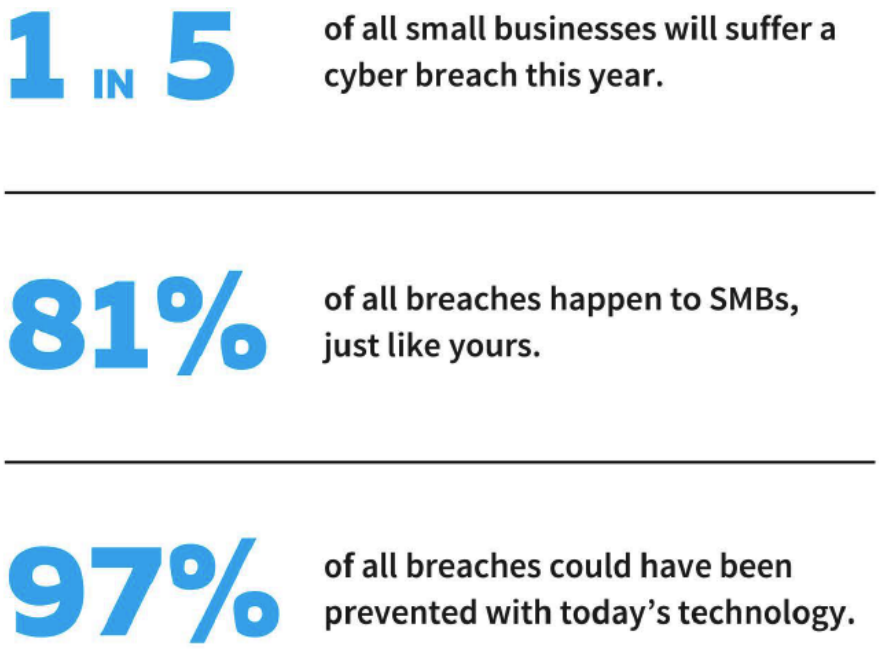
Hi-Link Technology Group

Managed Cyber Security Services

Vasim Limbadiya

04/05/2018

Why Managed Security ?



1 IN 5 of all small businesses will suffer a cyber breach this year.

81% of all breaches happen to SMBs, just like yours.

97% of all breaches could have been prevented with today’s technology.

24 x 7 SOC Threat Response Team

- Hi-Link partnered with CARVIR Cyber Security
- SOC located in metro Atlanta, GA
- All CARVIR Employees
- Complete Background Checks
- Several Analysts are FBI, NSA or DoD trained

CARVIR
CYBER SECURITY

Hi-Link Managed Cyber Security Services

SentinelOne : Managed Next Generation End Point Protection

EventTracker : Managed SIEM, Threat Intelligence & Log Management

SentinelOne

Real-time, Unified Endpoint Protection

[Vasim Limbadiya]

[04/05/2018]

Real-Time, Unified Endpoint Protection

SentinelOne

Go beyond prevention with a total protection platform. SentinelOne is the only platform that defends every endpoint against every type of attack, at every stage in the threat lifecycle.

Complete visibility

into all endpoint activity
without any performance drag

Advanced static prevention + Dynamic behavior detection

to protect against threats across
all major vectors

Fully automated

threat mitigation
and remediation

Gartner

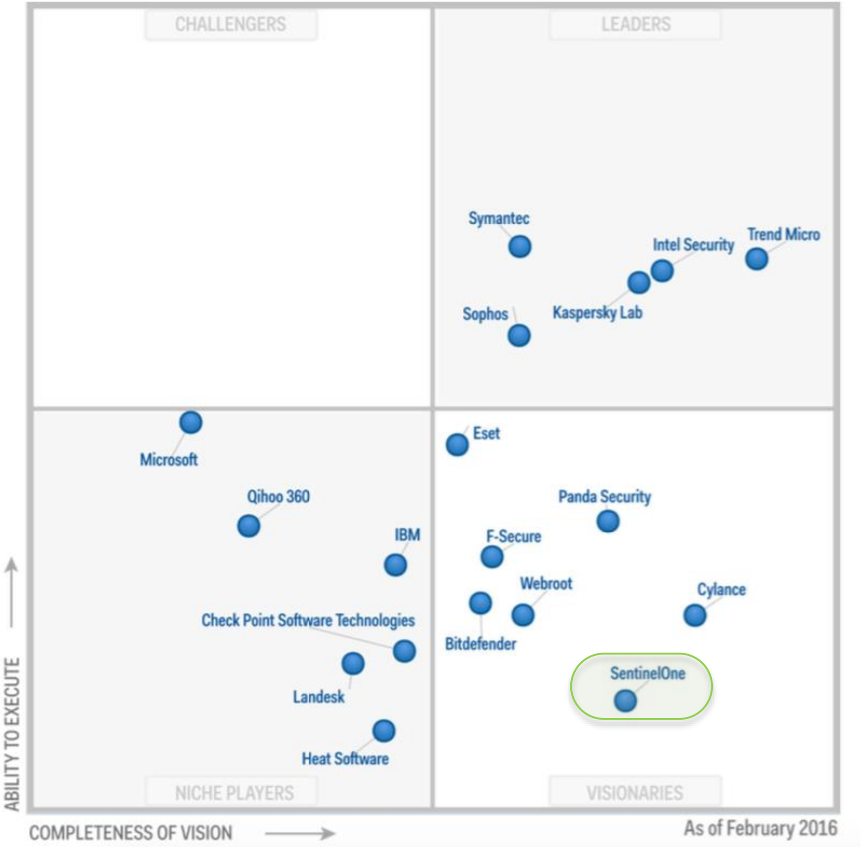
Visionary
2017 Magic Quadrant for Endpoint Protection Platforms

CYBER
SentinelOne
GUARANTEE

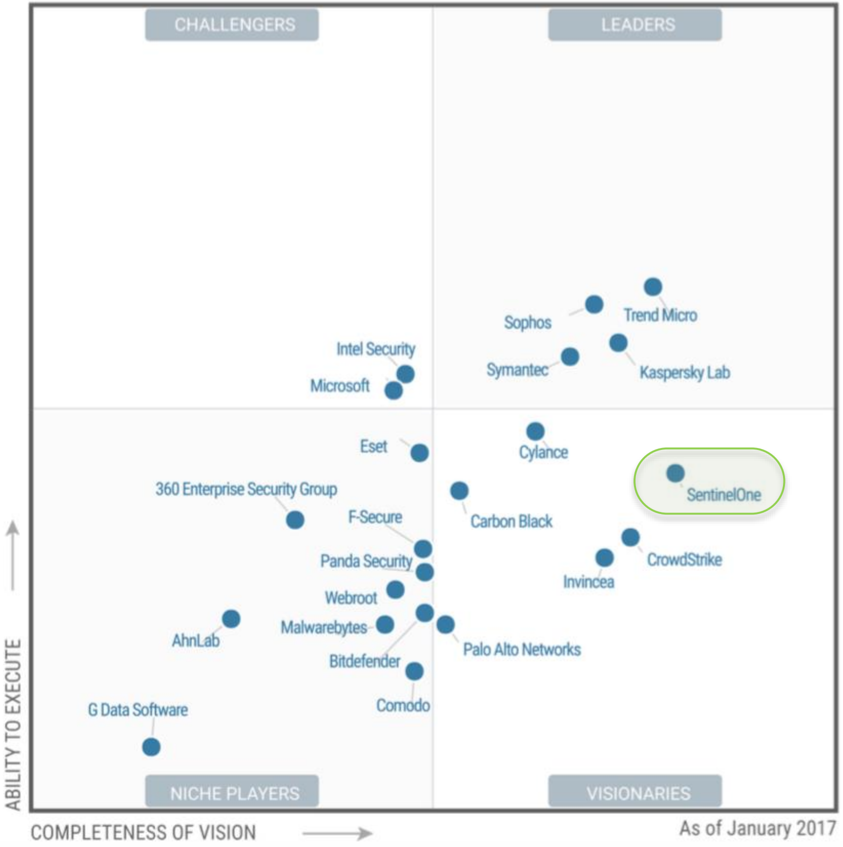
Certified Antivirus replacement

AV TEST
av-test.org
APPROVED
CORPORATE
ENDPOINT
PROTECTION

2016 to 2017: a dramatic leap forward

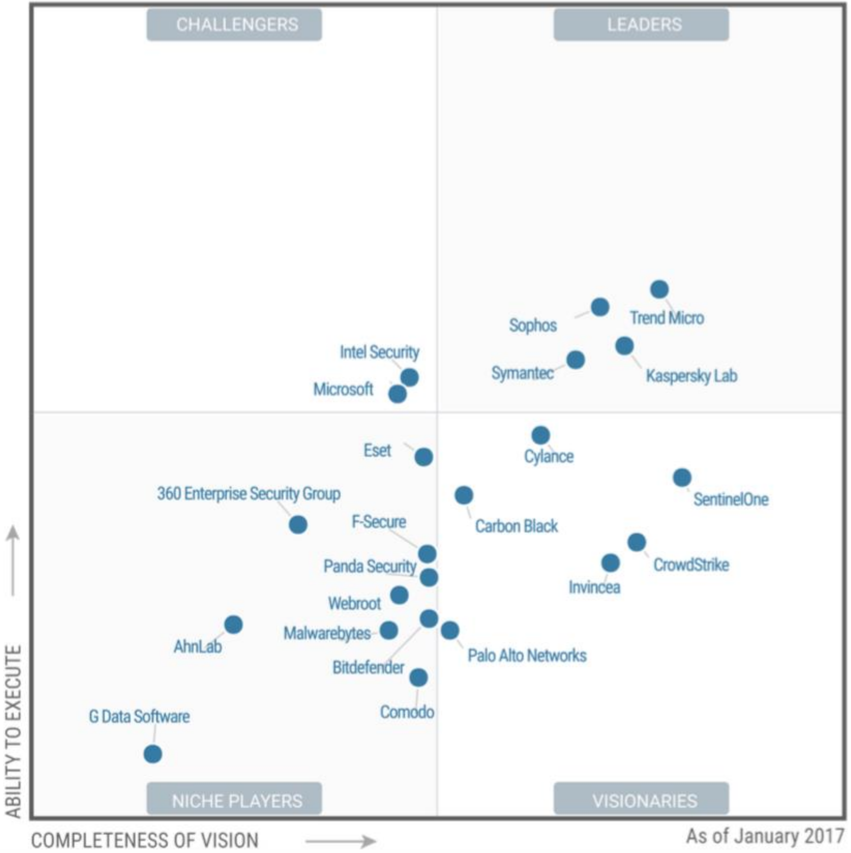


As of February 2016



As of January 2017

A Visionary on the 2017 Gartner MQ



"…SentinelOne has had stellar growth in the enterprise EPP market, and expects it to continue for the next couple of years as it maintains a reputation as a leading NGAV vendor."

A Visionary

Gartner 2017 Magic Quadrant
Endpoint Protection Platforms

Gartner, Magic Quadrant for Endpoint Protection Platforms, 30 January 2017

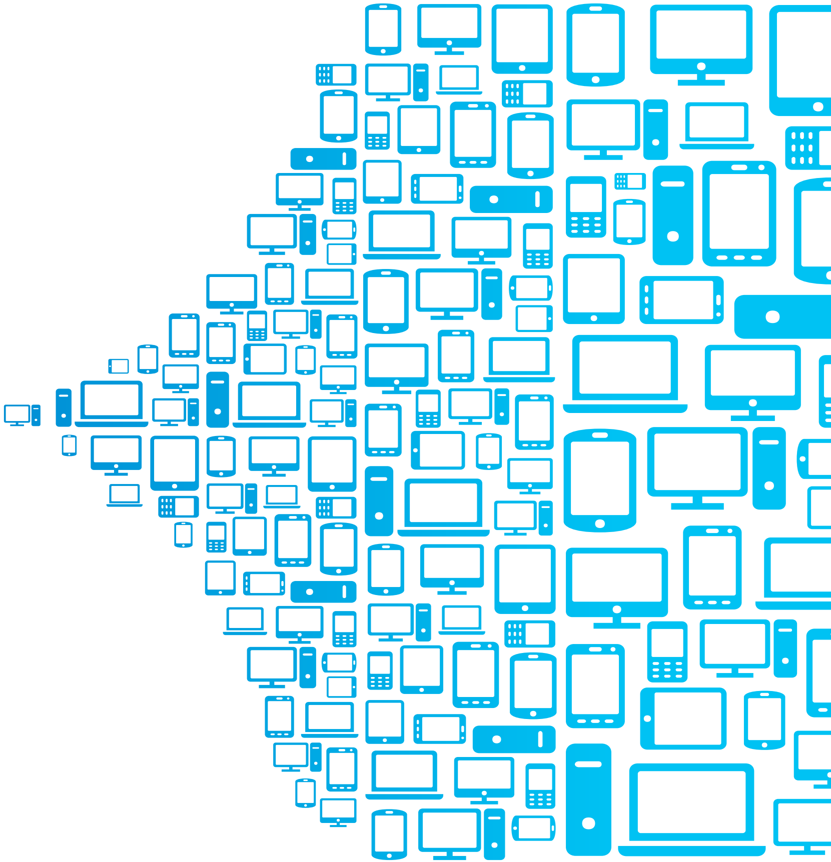
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

95% of Breaches Originate at the Endpoint

Endpoints are primary targets.
This is where sensitive data lives.

Endpoints are your organization’s weakest link.

Endpoint platforms are diverse, and often drift from standard configuration with frequent exposure to unsecured networks



AV is no Match for the New Threat Landscape

Malware

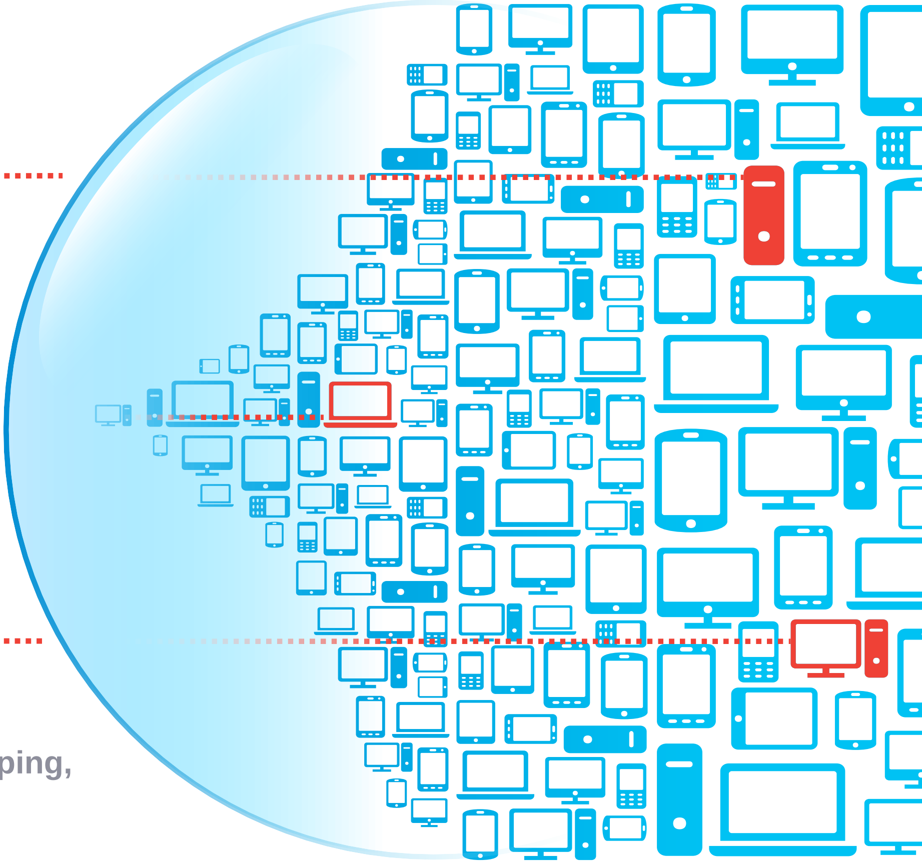
- Ransomware, trojans, worms, backdoors
- File-less / Memory-based malware

Exploits

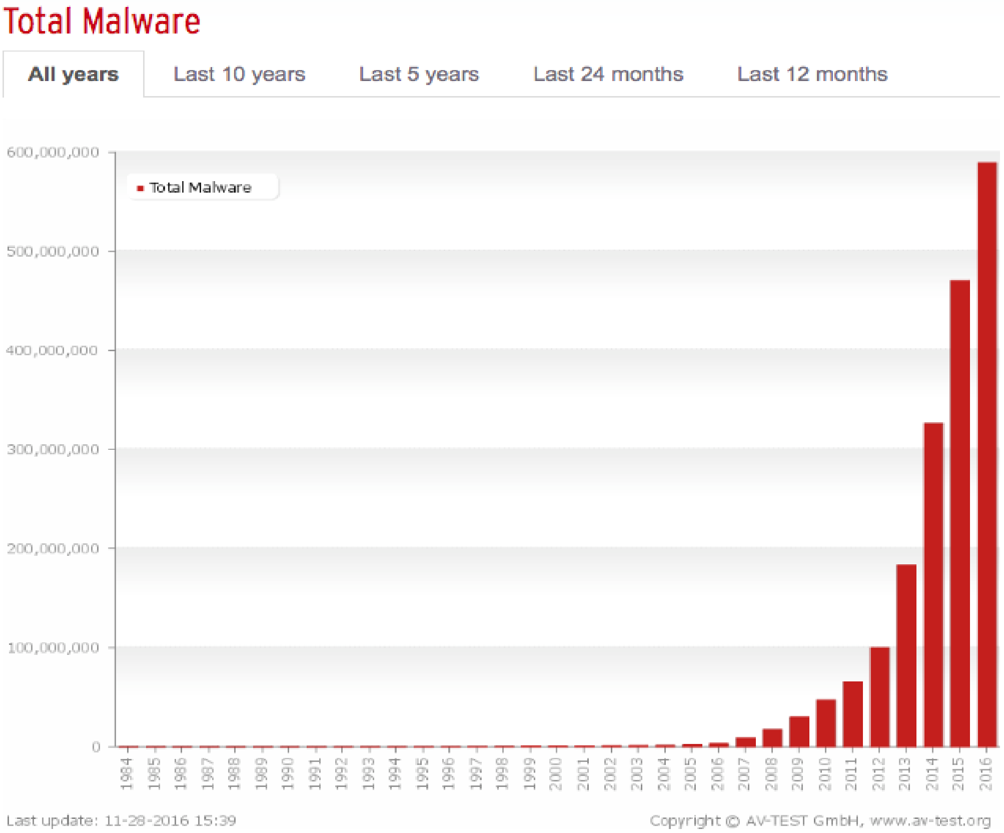
- Document-based exploits
- Browser-based exploits

Live Attacks

- Script-based: Powershell, Powersploit, WMI, VBS
- Credentials: credential-scraping, Mimikatz, tokens



Traditional AV Solutions Cannot Keep Pace



Total Malware

Last update: 11-28-2016 15:39

Copyright © AV-TEST GmbH, www.av-test.org

390K

new malicious code samples per day (according to AV-Test.org)

NGEP Offerings are Based on Different Philosophies, Technologies

Legacy AV + Add-ons

- Prevention focused
- Includes HIPS, Anti-Exploit, Application control

CAUTIONS:

- Multiple agents, multiple tools
- Same AV-related deficiencies

Scan-based Predictive Analysis

- Scan file system and crunch metadata to predict the existence of threats

CAUTIONS:

- Still limited to file-based malware
- Algorithm requires constant tuning by experts

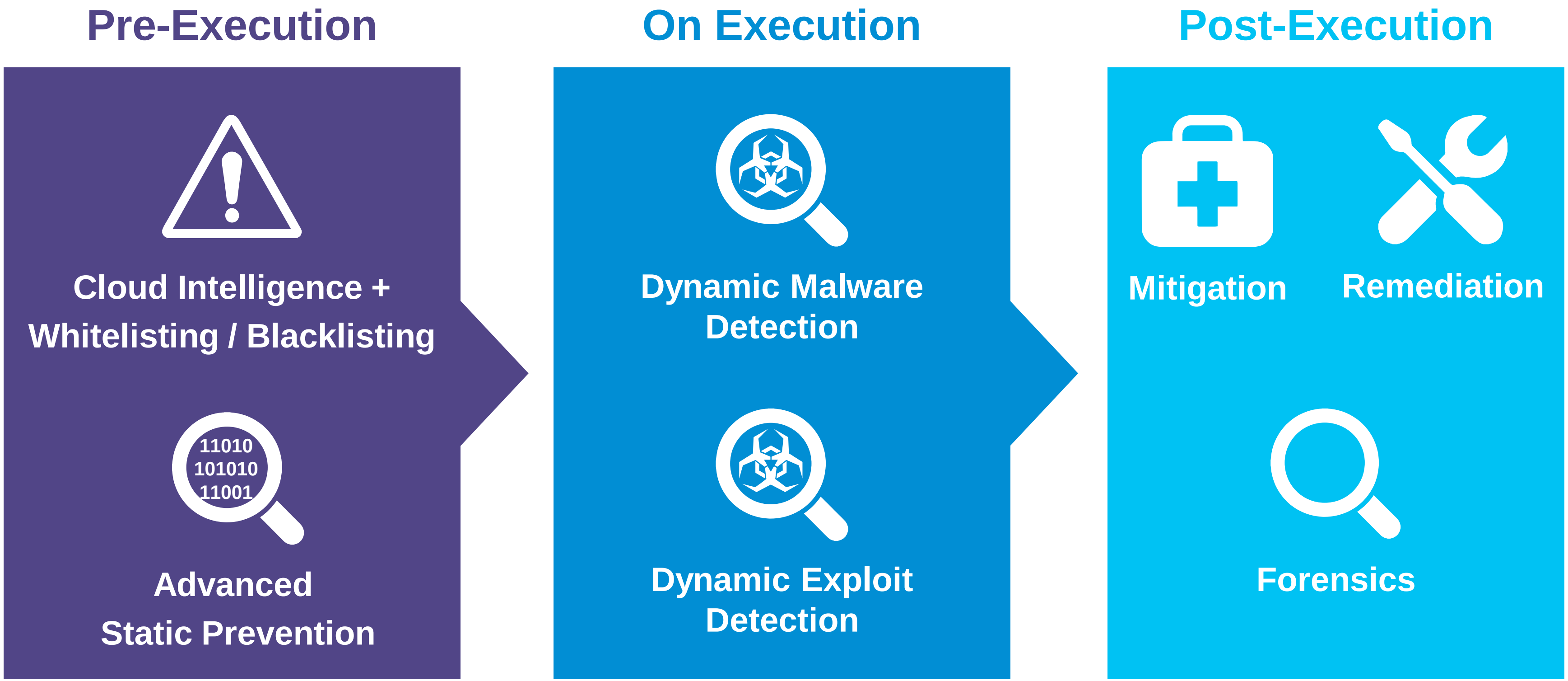
EDR

- Threat detection based on behavior and/or IOCs, coupled with mitigation and forensics

CAUTIONS:

- No prevention
- Requires specialized personnel operating in SOC capacity

Multi-layered Approach Addresses the Entire Threat Lifecycle



Pre-Execution

Cloud Intelligence + Whitelisting / Blacklisting

Advanced Static Prevention

On Execution

Dynamic Malware Detection

Dynamic Exploit Detection

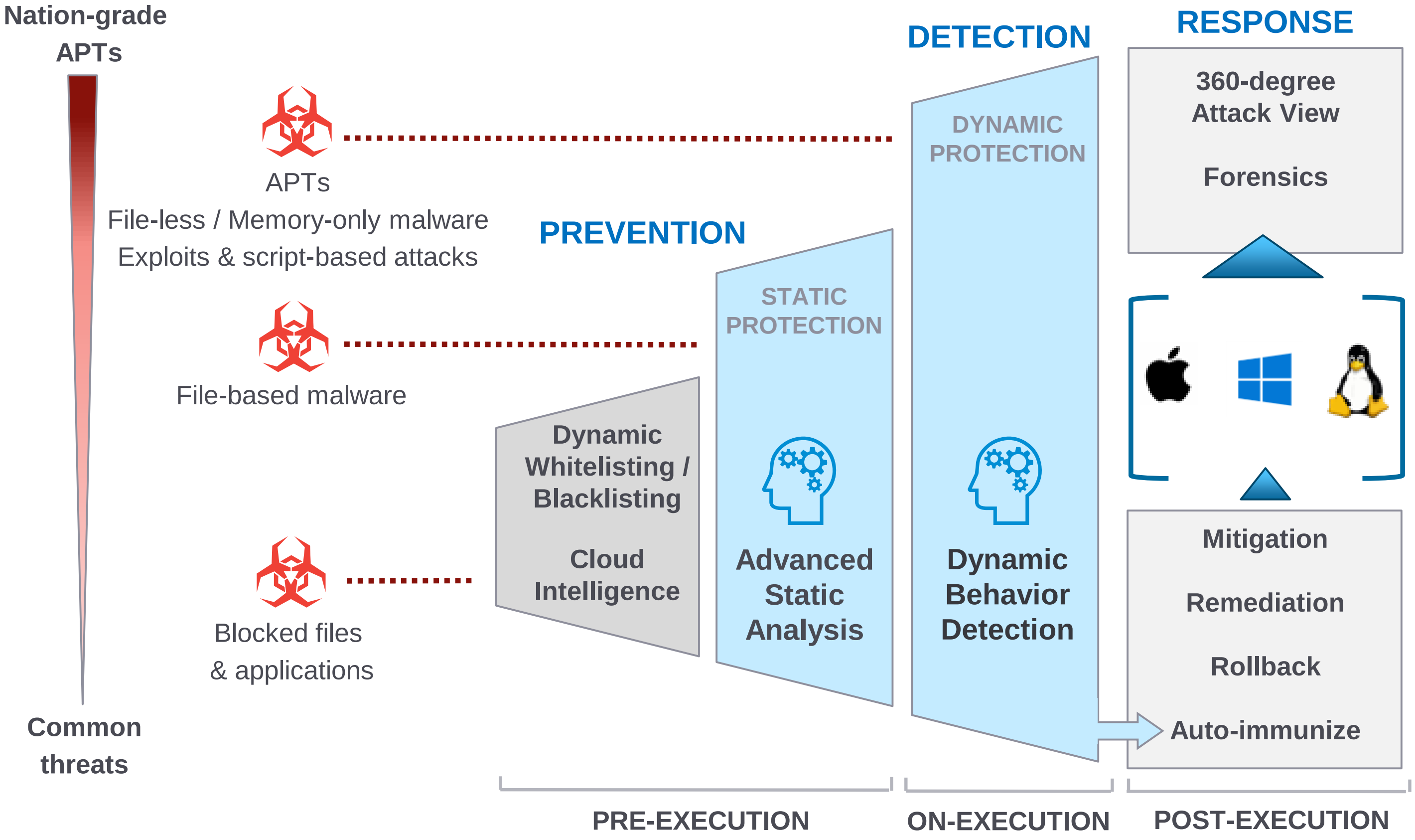
Post-Execution

Mitigation

Remediation

Forensics

The SentinelOne Endpoint Protection Platform



Single Autonomous Agent

70MB

Memory Footprint

Single Management Console

Supports up to

25,000

Endpoints

Cloud or On-Premise Deployment

Multi-layered Protection Across Major Threat Vectors

Dynamic Whitelisting / Blacklisting

- Reduce overall attack surface by blocking known bad programs

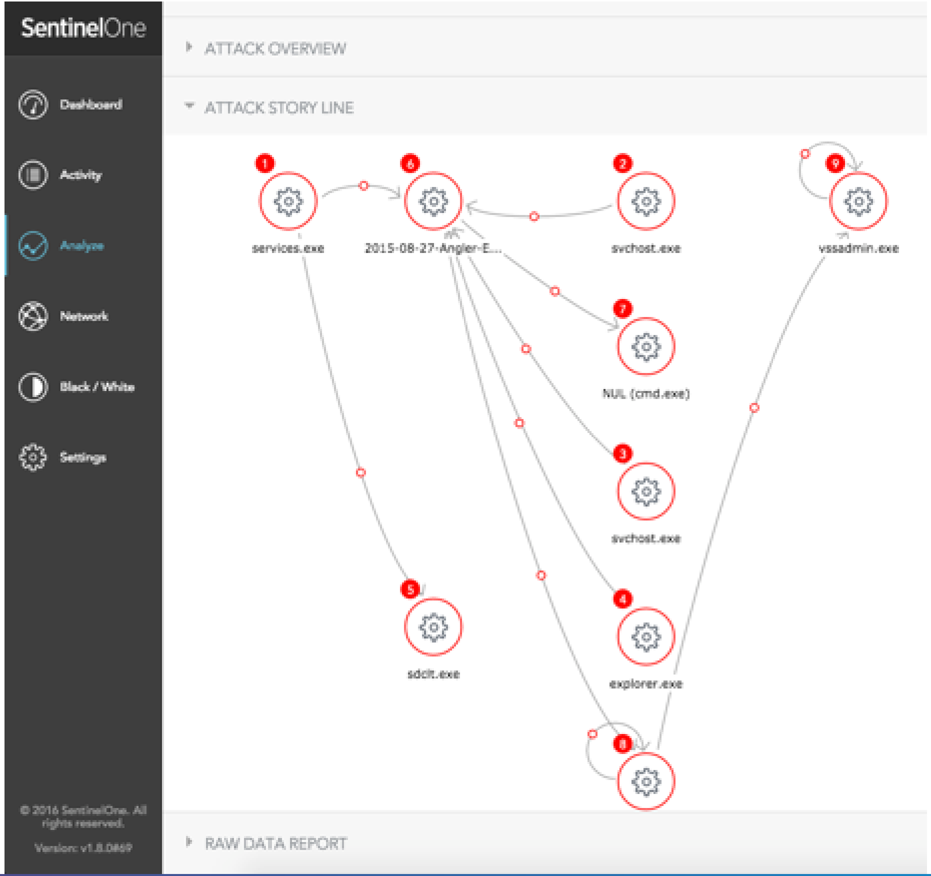
Advanced Static Prevention

- Deep File Inspection engine uncovers known and unknown malware-- upfront

Behavior-based Threat Detection

- Dynamically detect the most advanced attacks across any vector

Deep Endpoint Visibility and 360º View of Attacks



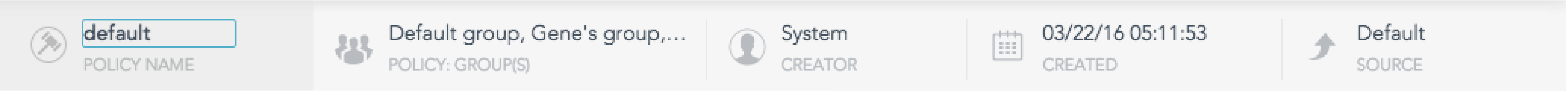
Lightweight, autonomous agent

- ✦ Continuously monitors all user/kernel activity on the user endpoint or server, online or offline
- ✦ Server agents sit out-of-band, preserving performance

Full-context forensics in real time

- ✦ 360-degree view of threats, from inception to termination

Fully Automated, Policy-driven Response



POLICY NAME: default

POLICY: GROUP(S): Default group, Gene's group,...

CREATOR: System

CREATED: 03/22/16 05:11:53

SOURCE: Default

Zero-touch mitigation

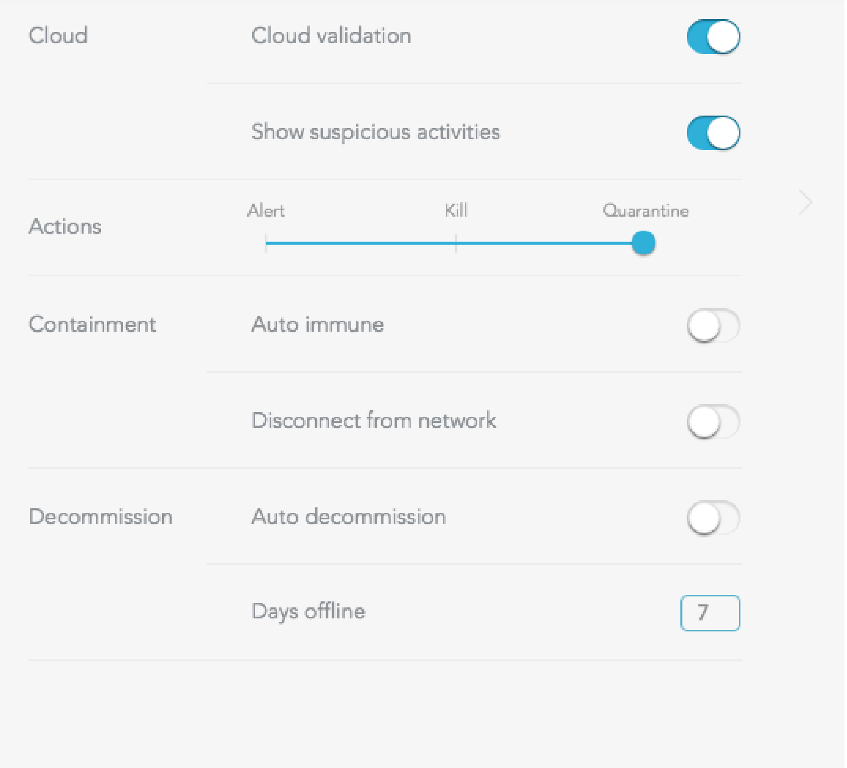
- Policy-based; covers all endpoints for decisive incident response

Robust containment

- Stops lateral threat movement by disconnecting the infected device from the network

Full remediation & rollback

- Reverse malware-driven system and file modifications



Cloud
- Cloud validation: ● on
- Show suspicious activities: ● on

Actions: Alert — Kill — Quarantine (Quarantine selected)

Containment
- Auto immune: ○ off
- Disconnect from network: ○ off

Decommission
- Auto decommission: ○ off
- Days offline: 7

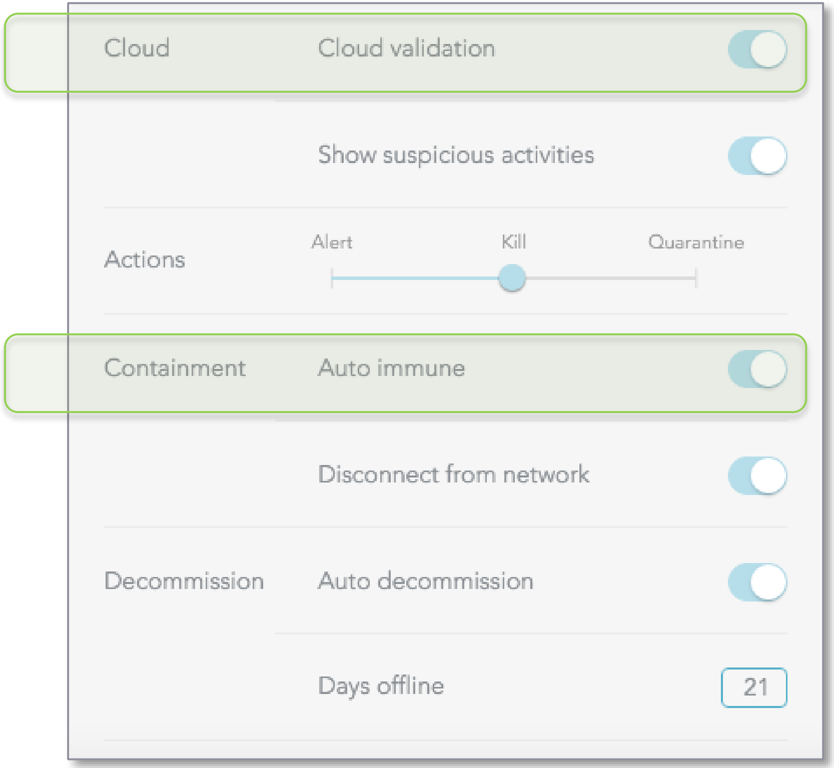
Adaptive Defenses

Cloud Intelligence

- ✦ Extend protection by leveraging threat intelligence from select reputation services

Auto-Immunization

- ✦ Notify all Agents on the network when a new threat is detected



Cloud	Cloud validation	●
	Show suspicious activities	●
Actions	Alert — Kill — Quarantine	Kill
Containment	Auto immune	●
	Disconnect from network	●
Decommission	Auto decommission	●
	Days offline	21

SentinelOne Benefits

- ✓ Superior protection against advanced threats without performance overhead
- ✓ Automated threat mitigation at machine speed
- ✓ Visualize attacks with real-time forensics

- ✓ Seamlessly adapt against the latest threats
- ✓ Cut TCO by up to 5x over multi-solution approaches
- ✓ Protect user endpoints and data center servers with a single platform
- ✓ Easily deployable across enterprise-scale environments

Protection from Ransomware. Guaranteed.

CYBER SentinelOne GUARANTEE

- SentinelOne detects and remediates ransomware attacks **AND** financially backs its products

- With the SentinelOne Cyber Guarantee:
  - **Customers will be compensated for any successful ransomware attack**
    - Up to $1,000 per affected endpoint
    - Up to $1M total

Other Companies Who Rely On SentinelOne

VISA

eShares

NETFLIX

TIME

FORTUNE

RED TAPE

GANNETT

salesforce

DELTA DENTAL

MARY KAY

Walmart

rackspace

NASDAQ

Taboola

Content You May Like.

Dodge & Cox Funds

Certified

SentinelOne is a certified replacement for Antivirus

AV-TEST av-test.org 06/2015 APPROVED CORPORATE ENDPOINT PROTECTION

AV-TEST av-test.org 12/2016 CERTIFIED MACOS SIERRA

HIPAA

PCI

DEMO

Netsurion

EventTracker

Actionable Security Intelligence

What is SIEM?

- What devices in your network have logs?
- Is there valuable security related data in the logs?
- Do you monitor them?
    - Real-time
    - Hourly
    - Daily
    - Weekly
    - Monthly
    - Yearly

What is SIEM?

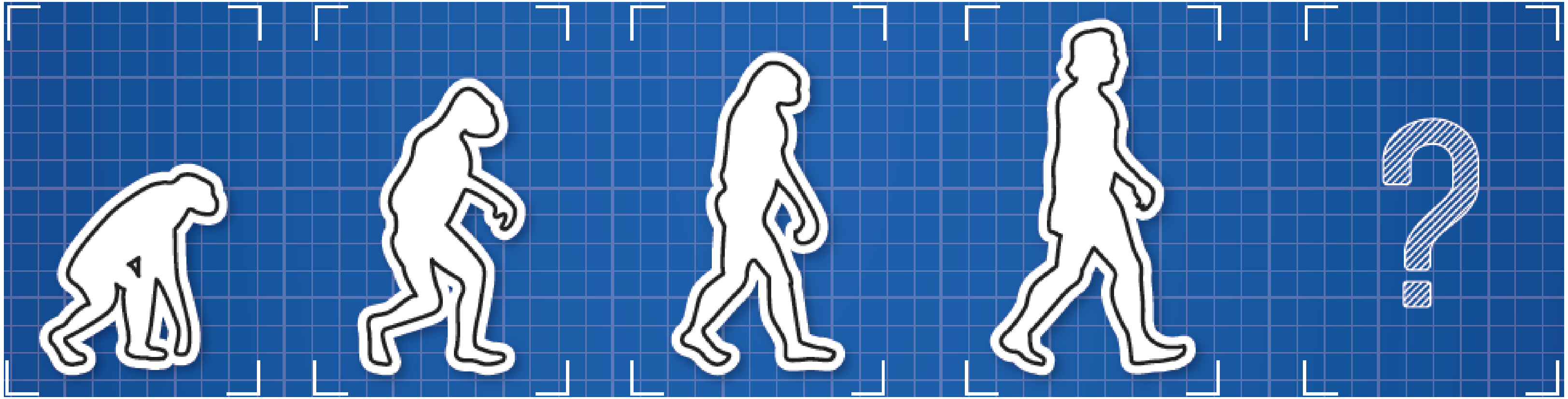
- Even a small network can generate millions of log records daily generating dozens or hundreds of “alerts”
- Each of these logs has a unique format
- Maybe you have implemented a syslog server and tried to monitor for specific lines of activity
- Now how do you leverage it?

This is where SIEM begins and basic log management ends!

What is SIEM?

- Security and Event Management (SIEM)
  - Coined by Gartner in 2005
- An approach that combines:
  - SIM (Security Information Management)
    - Collecting, monitoring and analyzing security related data from logs
  - SEM (Security Event Management)
    - Alerting on specific triggers in log data
- Pronounced “sim” with a silent e

The Evolution of SIEM?



Centralized Log Management

Centralized log collection and storage is used to fulfill an operational need.

SIEM

The technology began to extract intelligence from logs to meet a compliance or security need.

SIEM ++

SIEM vendors add adjacent technologies like VAS, IDS, flow analysis and deception (honeynet), for greater security and compliance

SIEM-As-A-Service

With greater intelligence comes the need for more monitoring and analysis, but a skills shortage creates a market for managed or co-managed options that help provide a better SIEM ROI.

SIEM-As-A-Utility (future)

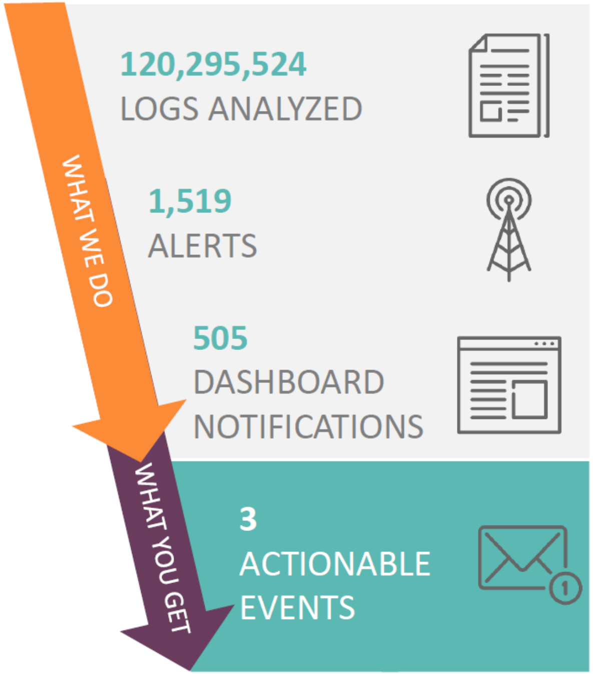
In the future, security will be built into the foundation of the network devices.

The Questions We Must Answer

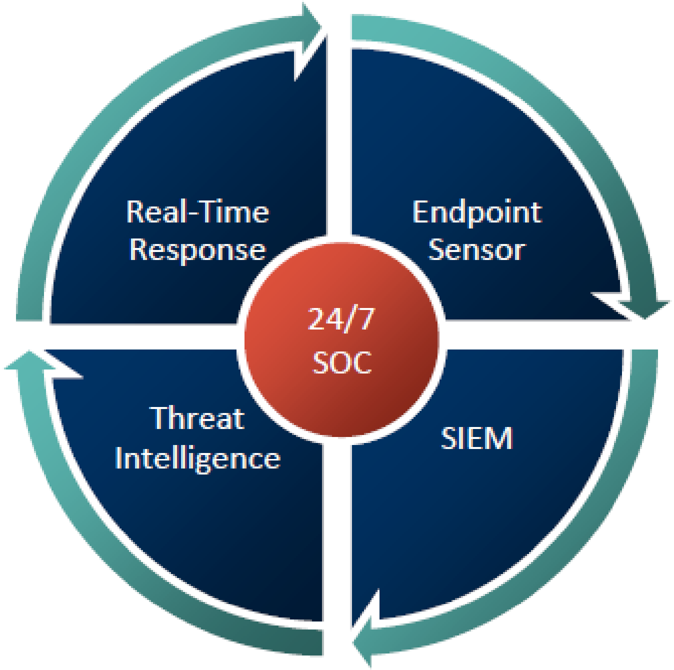
- The 4 W’s
  - Who
    - Who is being attacked?
  - What
    - What is it trying to do?
  - Where
    - Where is the attack coming from?
  - When
    - When did it happen?

Netsurion
EventTracker
Actionable Security Intelligence

- ✓ Routers
- ✓ Firewalls
- ✓ Servers
- ✓ Laptops
- ✓ Desktops
- ✓ Switches



Netsurion EventTracker
Actionable Security Intelligence



- ✓ No Hardware Required
- ✓ Over 2,100 Log Types / Sources
- ✓ Threat Response Capabilities

Alerts (Monitored by Hi-Link/SOC/EventTracker)

A new TCP port started listening
Active directory: group policy changed
Admin interactive/remote login success
Administrative logon success
Critical potential breach by unknown process from low reputation IP
Critical potential breach from low reputation IP
Critical service is not running
Disc space is critically low
Excessive logon failures due to bad password/username
Excessive logon (id 4625) failures from an IP address
Media insert alert
New Windows audit policy and account management activity
New Windows software install activity
New Windows user location affinity activity
Out of ordinary IP address activity

Out of ordinary Windows interactive logon activity
Out of ordinary Windows process activity
Runaway CPU process - A process or system consuming high CPU
Runaway memory process - A process or system is taking too much memory
Terminated connection to reputed bad IP
Unknown or unsafe MD5 hash detected
User account disabled
User added or deleted
Users added to domain admin or local admin group
User password set to never expire
Windows: Audit log cleared

Level 1=Automated termination of process and/or connection, and security operations center response

Default Reports for All Systems

Multiple logon failures by user(s)

Multiple logon failures from multiple remote IP addresses

New process connected to site or IP address with a bad reputation

New service started

New software has been installed on your network

New TCP entry point opened

Out of ordinary activities from IP address(es)

Out of ordinary activities from multiple process(es)

Out of ordinary activities from multiple users

Terminated connections to reputed bad IP addresses

Terminated process(es) having black listed hash

USB activities

User(s) added to admin group

User(s) created

User location affinity

Unsafe process or DLL executed

Pricing

SentinelOne

Advanced Endpoint Security

Workstation:	$4 - $8 per month
Server:	$9 - $30 per month

EventTracker

Managed SIEM for MSPs

Firewall/Switch/Server:	$50 - $90 per month
Workstation:	$5 - $9 per month
One-Time Setup Fee:	$499 - $1199