McAfee
An Intel Company

McAfee Virtualization Solutions

Securing the Virtual World

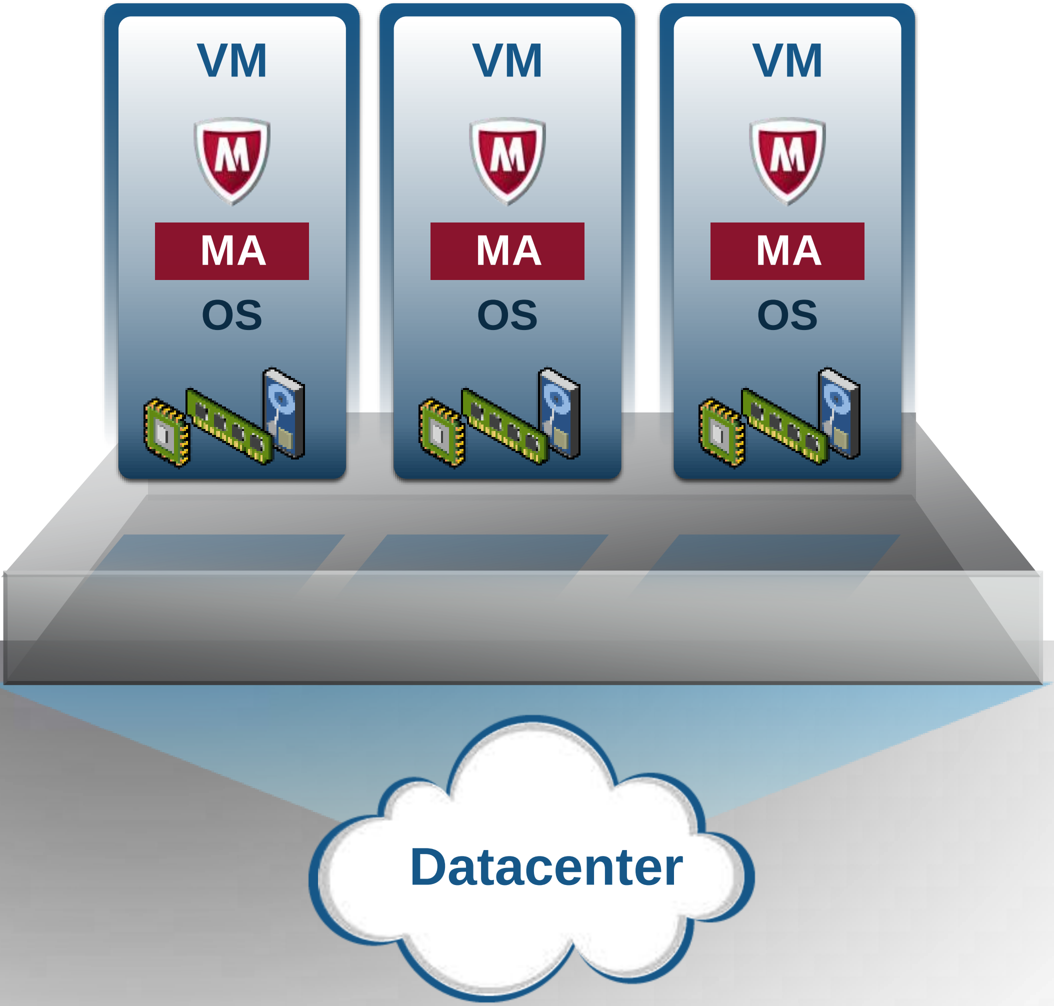
SAFE NEVER SLEEPS.

Agenda

- Challenges with Virtualization
- Virtualization Solutions
- Summary

Security Must Evolve as the Data Center Evolves

- AV storms
- Large AV footprint
- Security tied to hypervisor
- Managing hypervisor load
- Lack of DAT updates on offline virtual machines
- Streaming Technologies
- Single Security Console for physical and virtual infrastructure



Agenda

- Challenges with Virtualization
- **Virtualization Solutions**
- Summary

McAfee Solutions for Virtualization

MOVE AV for Virtual Desktops

- Offloads On Access Scan (OAS)
- Memory protection (w/Host IPS or MAC)
- Licensed per node

MOVE AV for Virtual Servers

- Offloads On Access Scan (OAS) **OR**
- Hypervisor-aware (ODS) scheduling
- Offline security for virtual servers
- Licensed per hypervisor

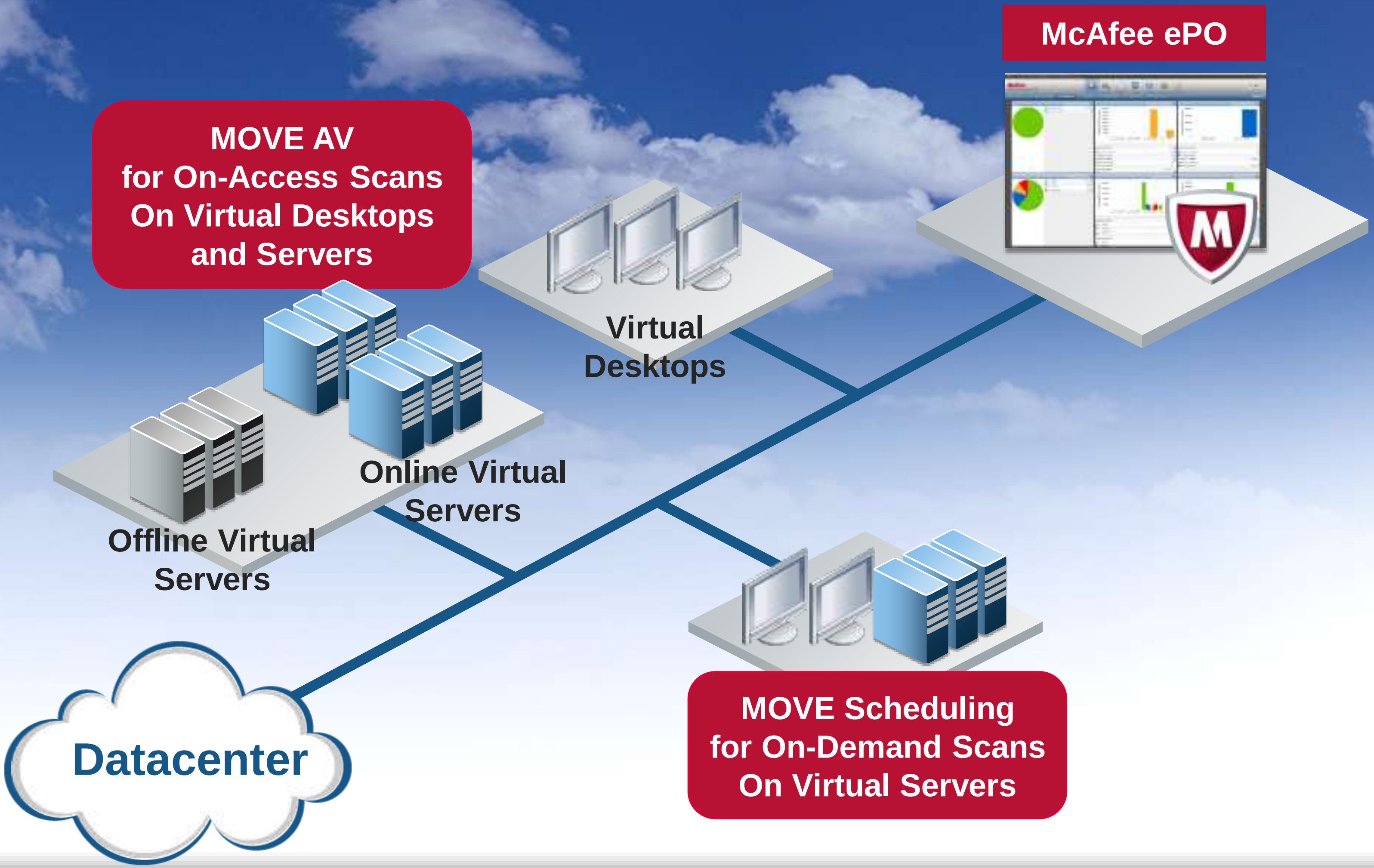
Application Control

- Dynamic local white-listing
- Blocks all unwanted/unauthorized changes
- Licensed per node

VSE for Storage

- Continually provides malware protection to shared storage resources of virtualized and physical systems
- Licensed per AV scanner

McAfee MOVE in the Datacenter


McAfee ePO

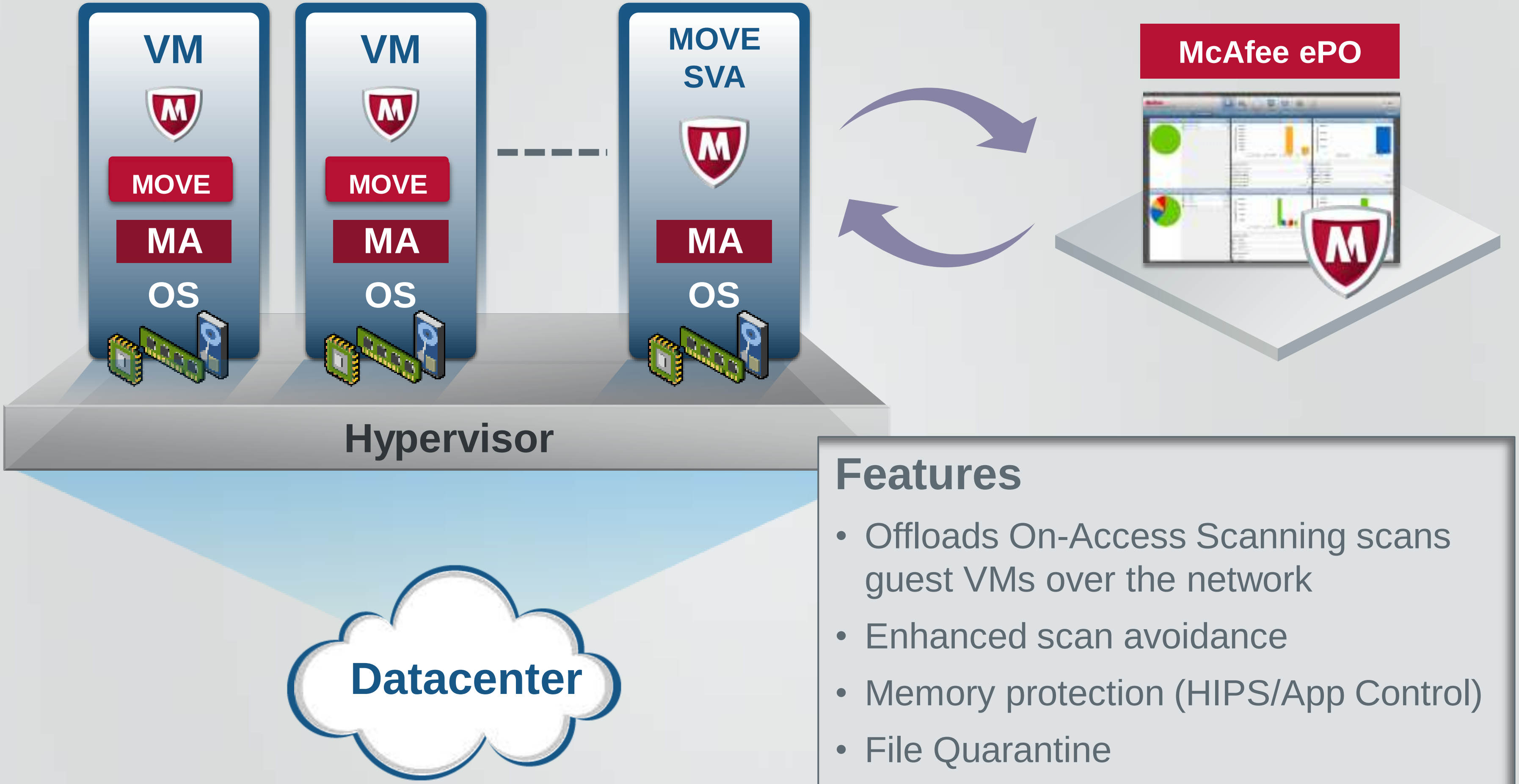
MOVE AV
for On-Access Scans
On Virtual Desktops
and Servers

MOVE Scheduling
for On-Demand Scans
On Virtual Servers

MOVE AV Deployment Options

Feature	Multi-Platform deployment	Agentless deployment
Anti-Virus Features		
On-Access Scanning	✓	✓
On-Demand Scanning	✓	✓
GTI File Reputation	✓	✓
File Quarantine Action	✓ Per file	✗ (Per VM – optional using vShield App)
Architecture		
Hypervisor / Platform Support	Supports major Hypervisors	VMware only
Security Virtual Appliance (SVA) Platform	Windows 2008	Linux
Deployment scalability	450 VMs per SVA	One SVA per ESX host
Scan Method from SVA to VMs	Network	VMware vShield: private channel

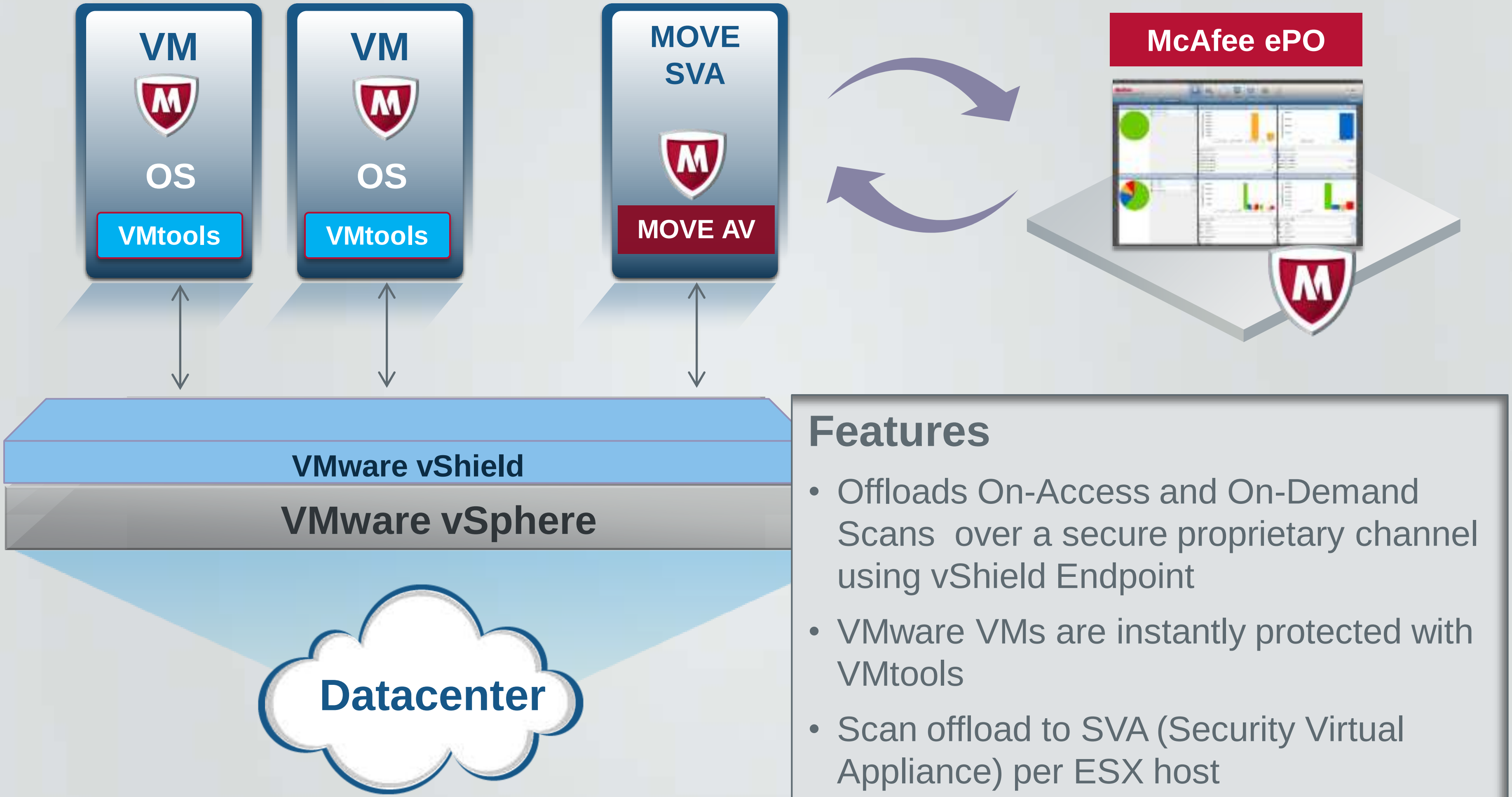
MOVE AV – Multi-Platform Deployment option



Features

- Offloads On-Access Scanning scans guest VMs over the network
- Enhanced scan avoidance
- Memory protection (HIPS/App Control)
- File Quarantine
- GTI file reputation
- VirusScan Enterprise license

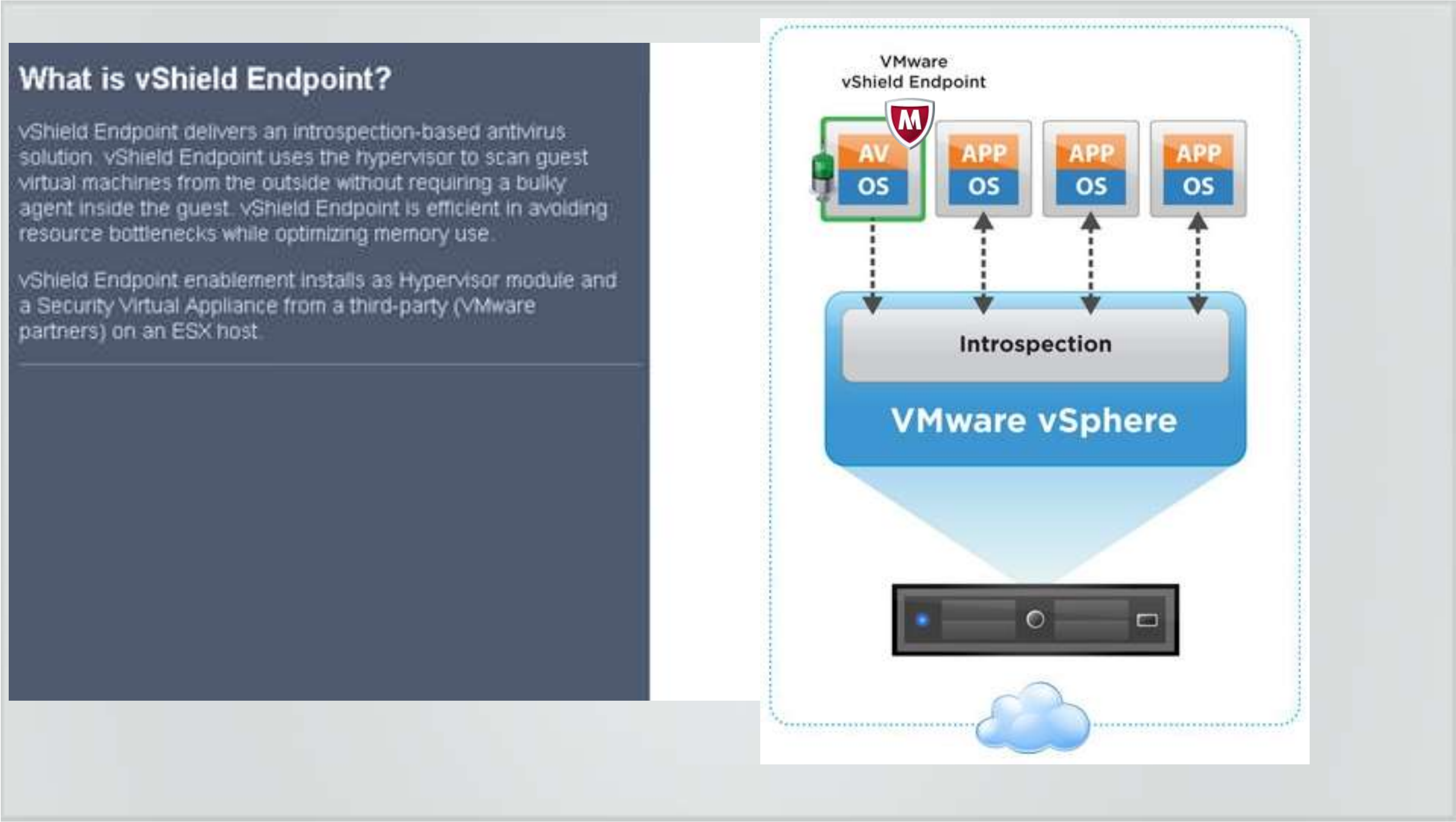
MOVE AV – Agentless Deployment option



Features

- Offloads On-Access and On-Demand Scans over a secure proprietary channel using vShield Endpoint
- VMware VMs are instantly protected with VMtools
- Scan offload to SVA (Security Virtual Appliance) per ESX host
- Protection is vMotion-aware

VMware vShield Endpoint



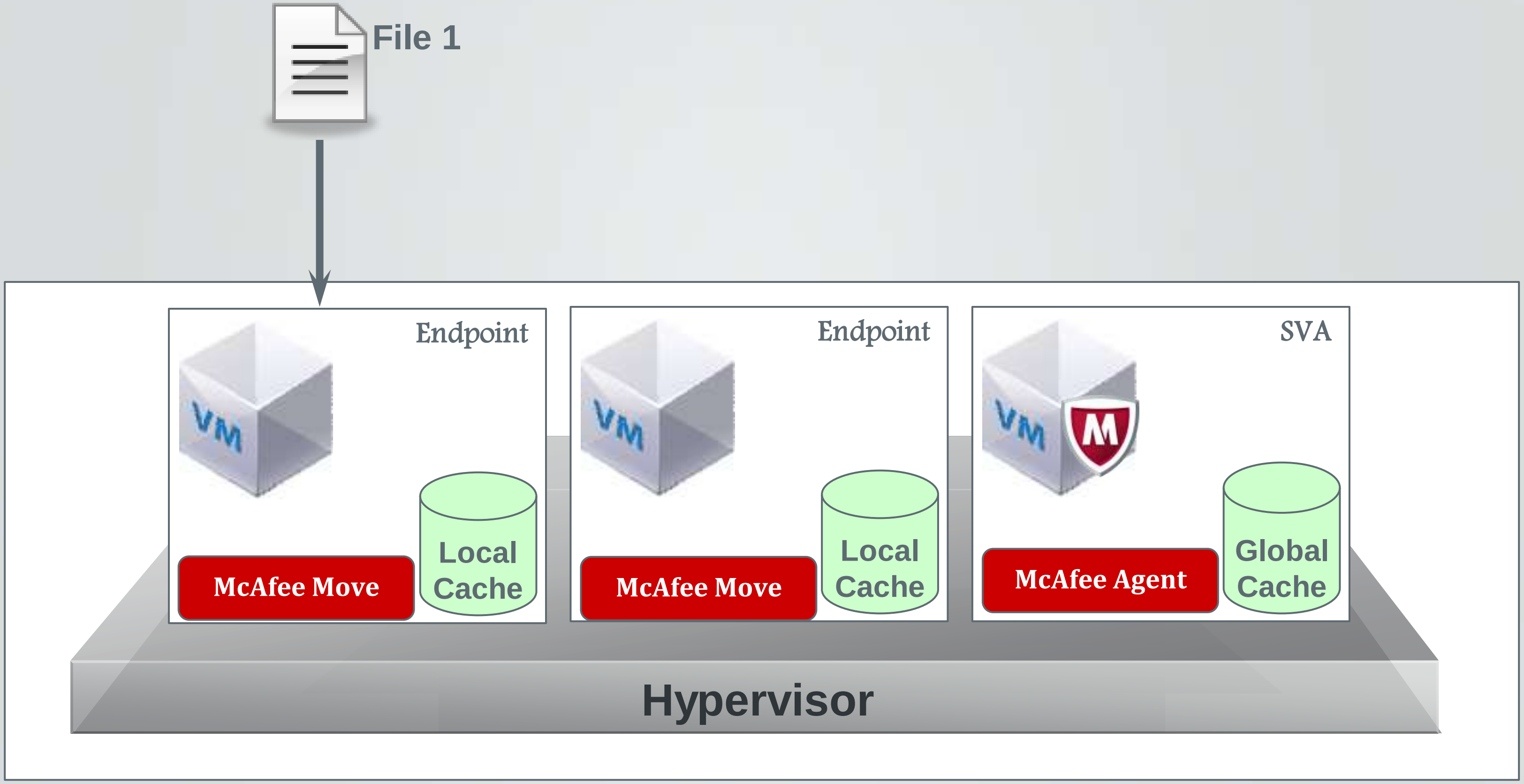
What is vShield Endpoint?

vShield Endpoint delivers an introspection-based antivirus solution. vShield Endpoint uses the hypervisor to scan guest virtual machines from the outside without requiring a bulky agent inside the guest. vShield Endpoint is efficient in avoiding resource bottlenecks while optimizing memory use.

vShield Endpoint enablement installs as Hypervisor module and a Security Virtual Appliance from a third-party (VMware partners) on an ESX host.

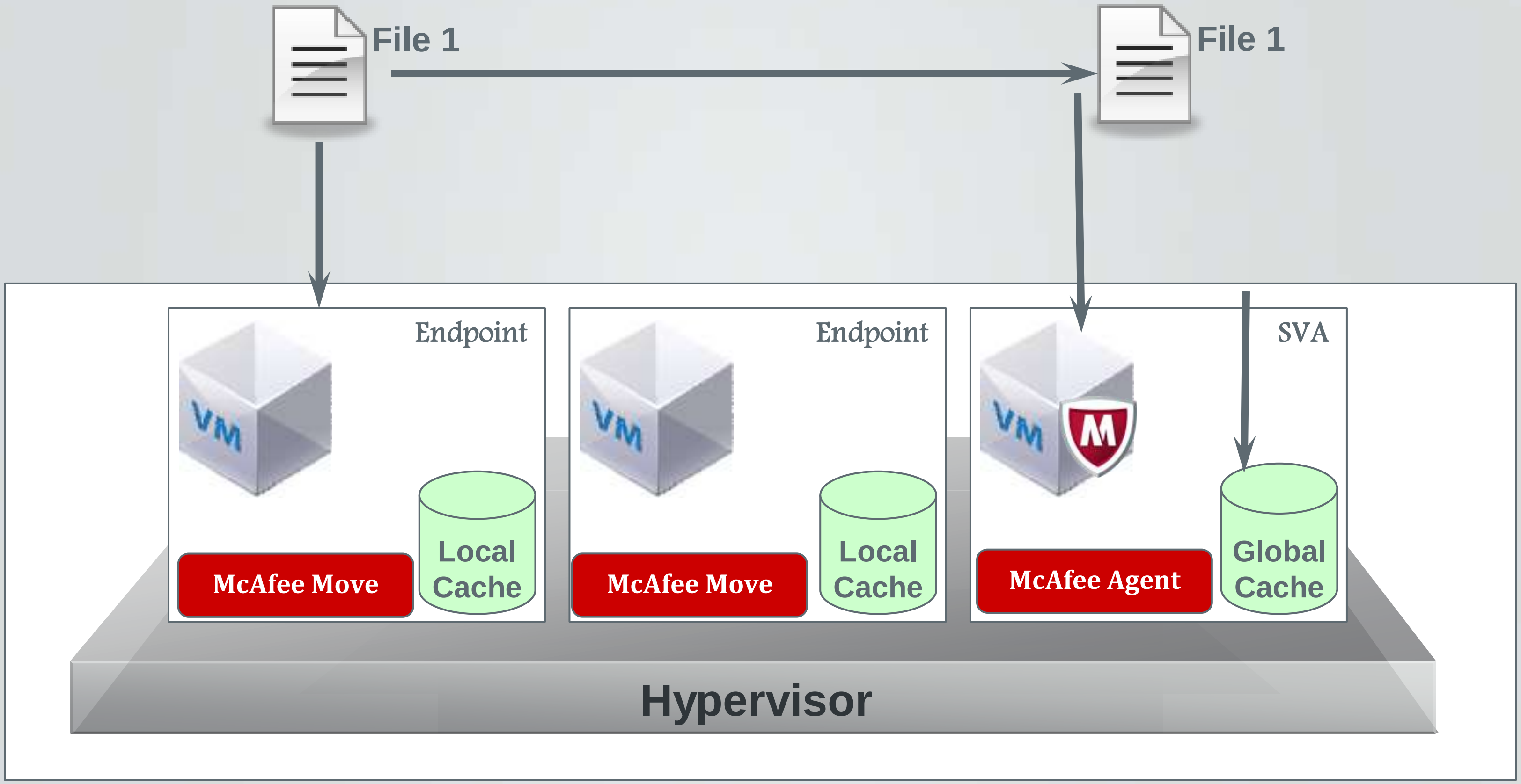
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

A virtual machine accesses a file…



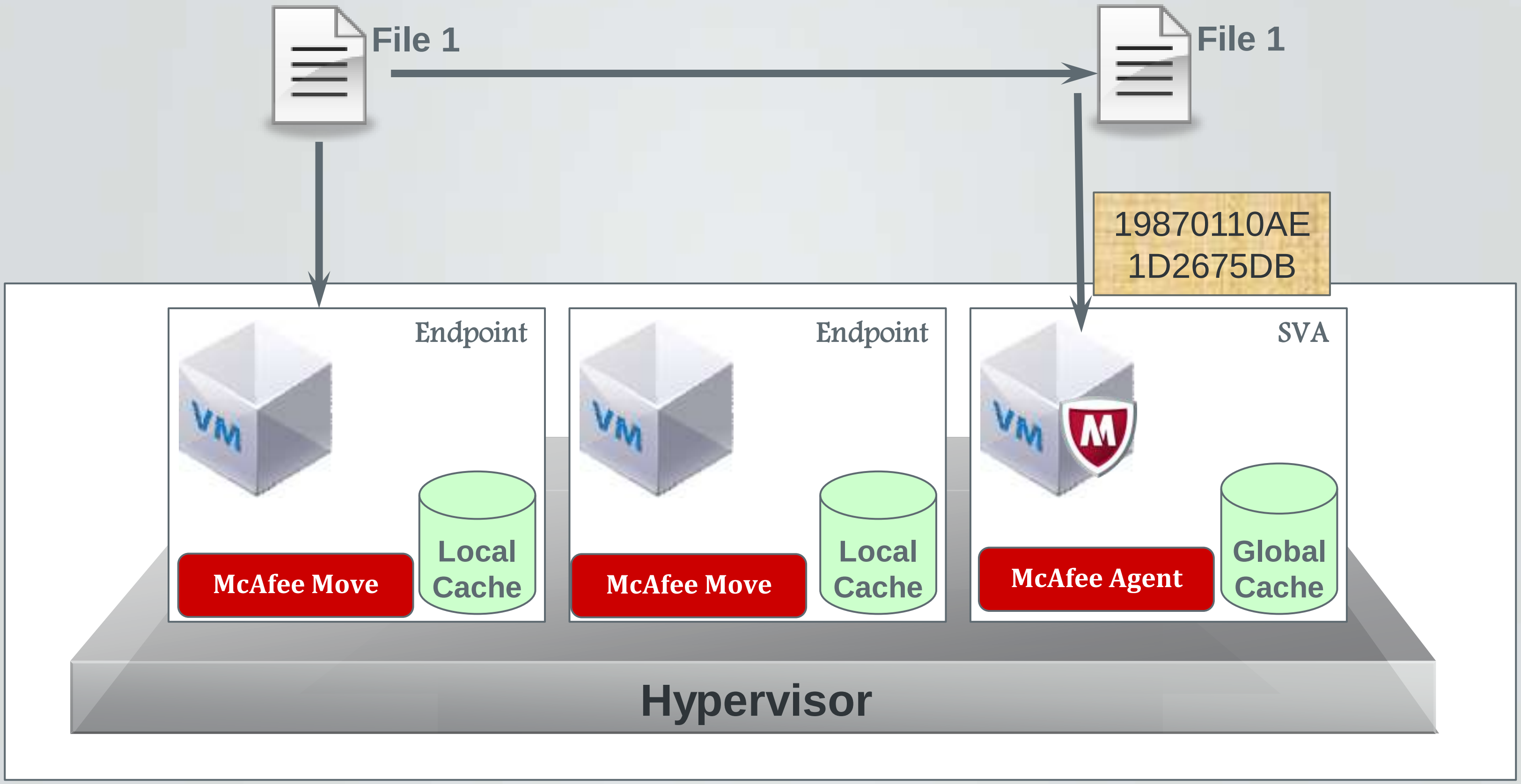
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

The file is checked against the Local Endpoint Cache.
If not in the Local Cache, MOVE requests the entire file.



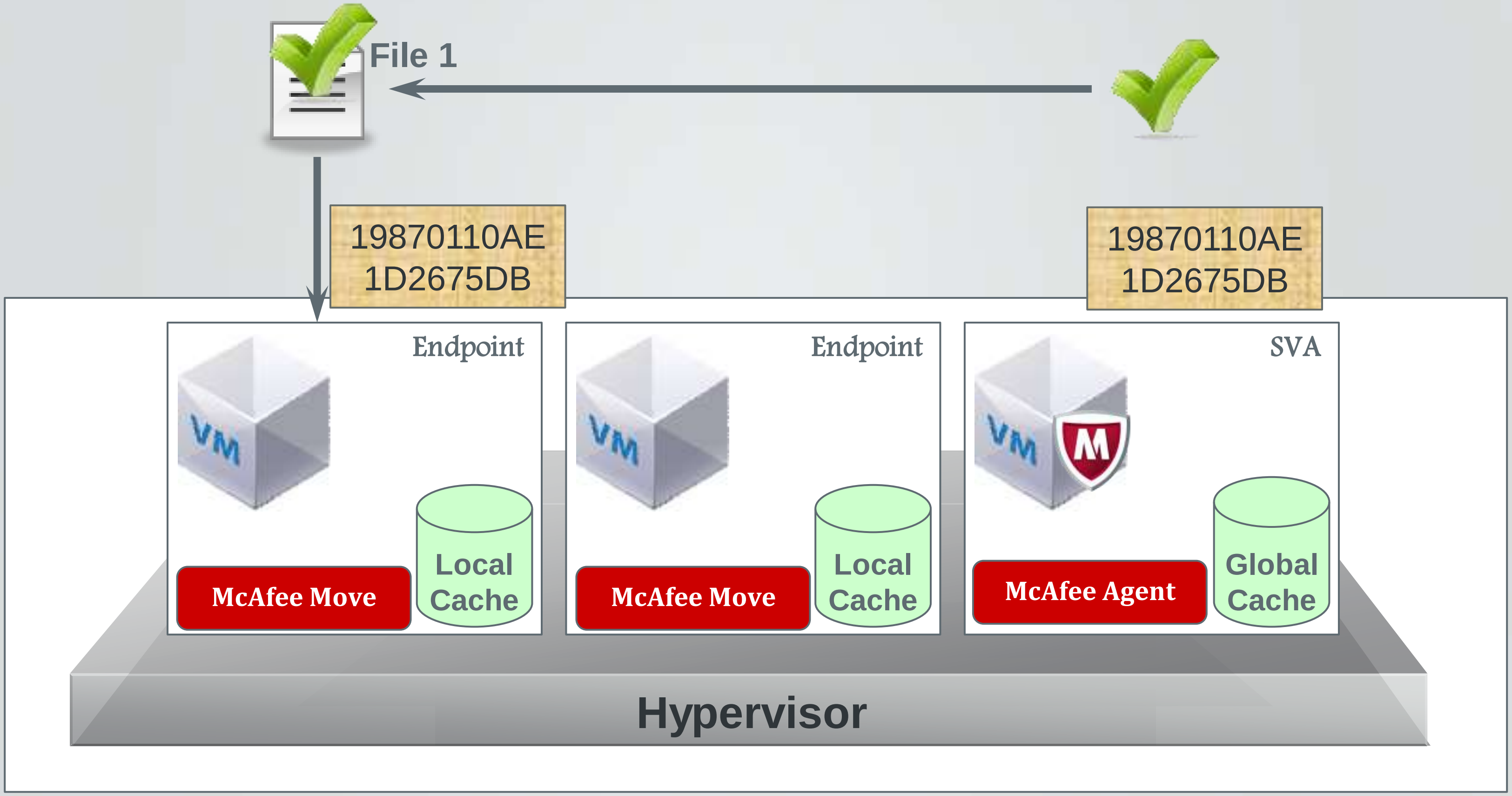
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

As the file is received, MOVE AV creates an MD5 of the file contents, then checks it against the Global Cache.



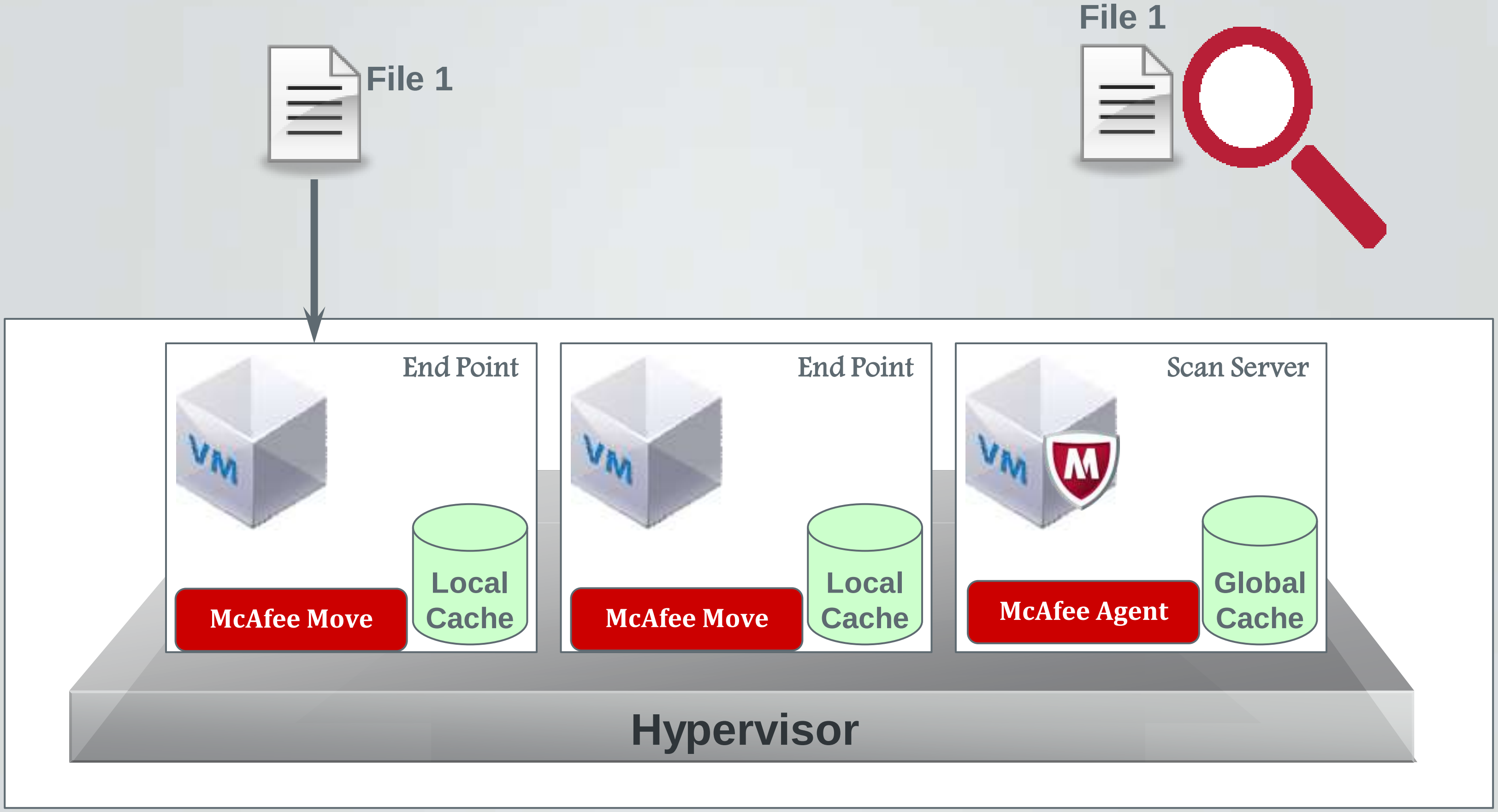
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

MD5 - IN the Global Cache, no scanning occurs. MOVE AV informs MOVE Endpoint to cache the file, access is granted.



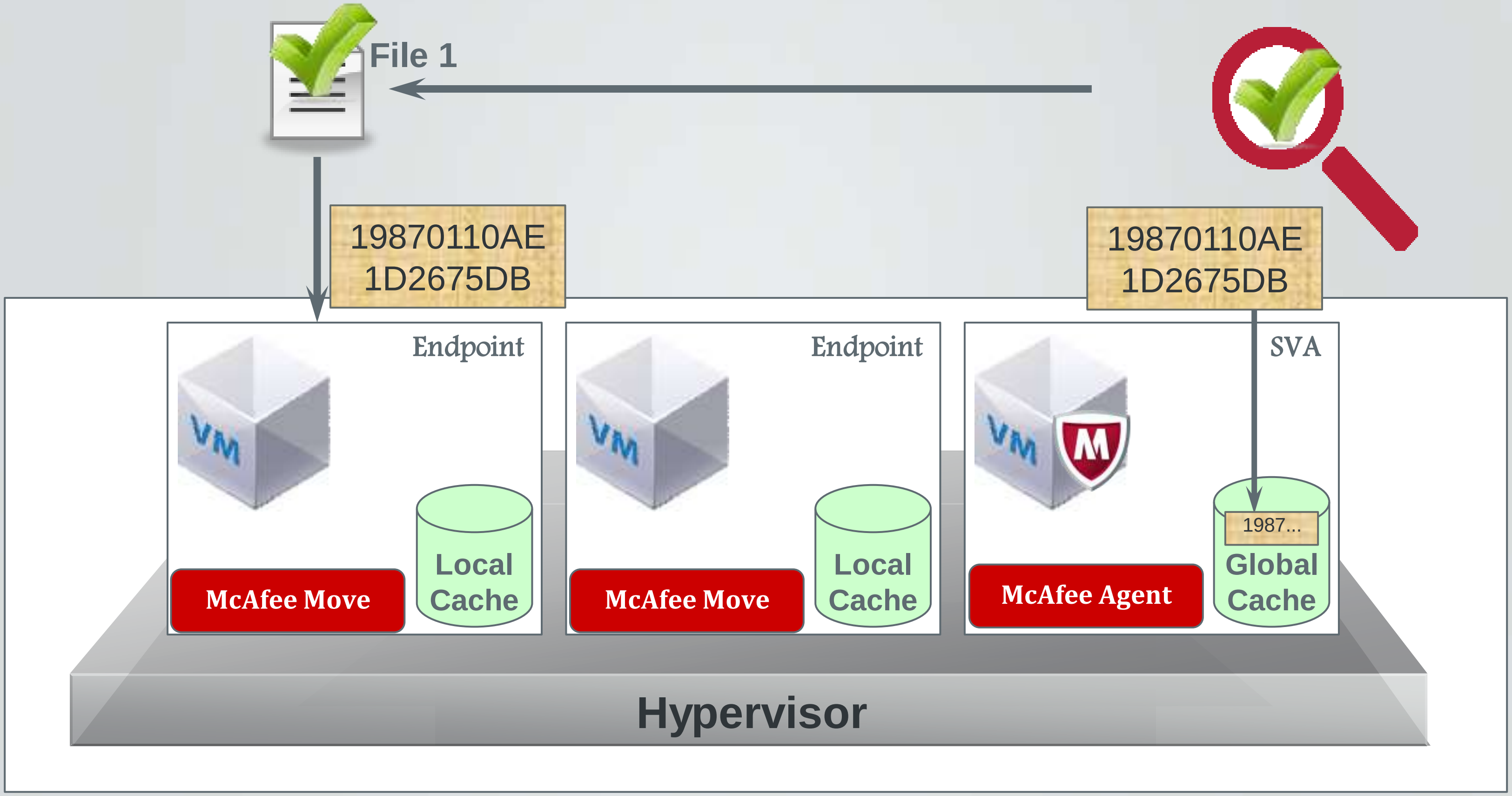
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

MD5 - NOT in the Global Cache, the File is analysed for Malware using both Signature and GTI technologies.



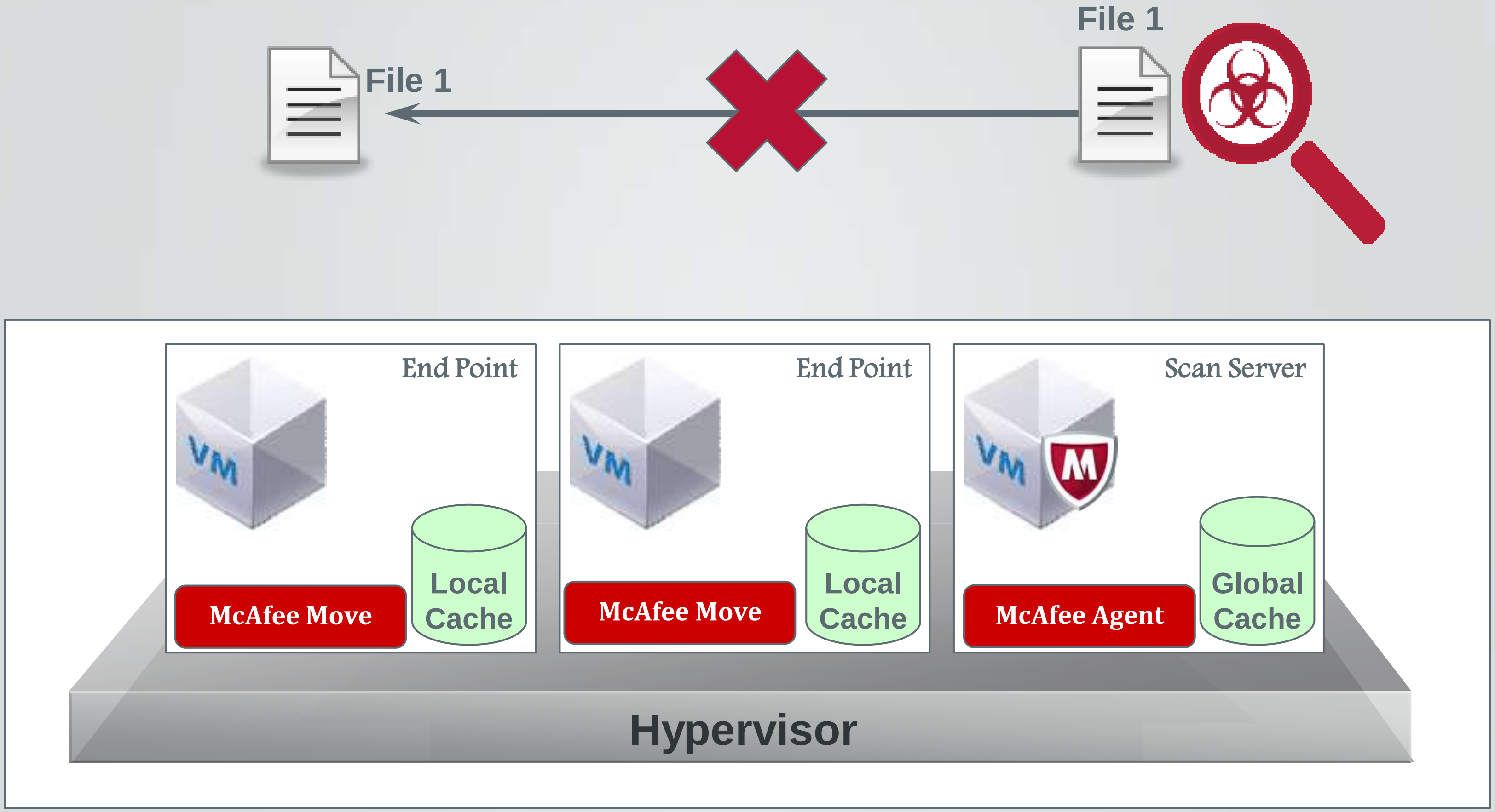
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

If the File is GOOD, the MD5 is added to the Global Cache, File access is granted



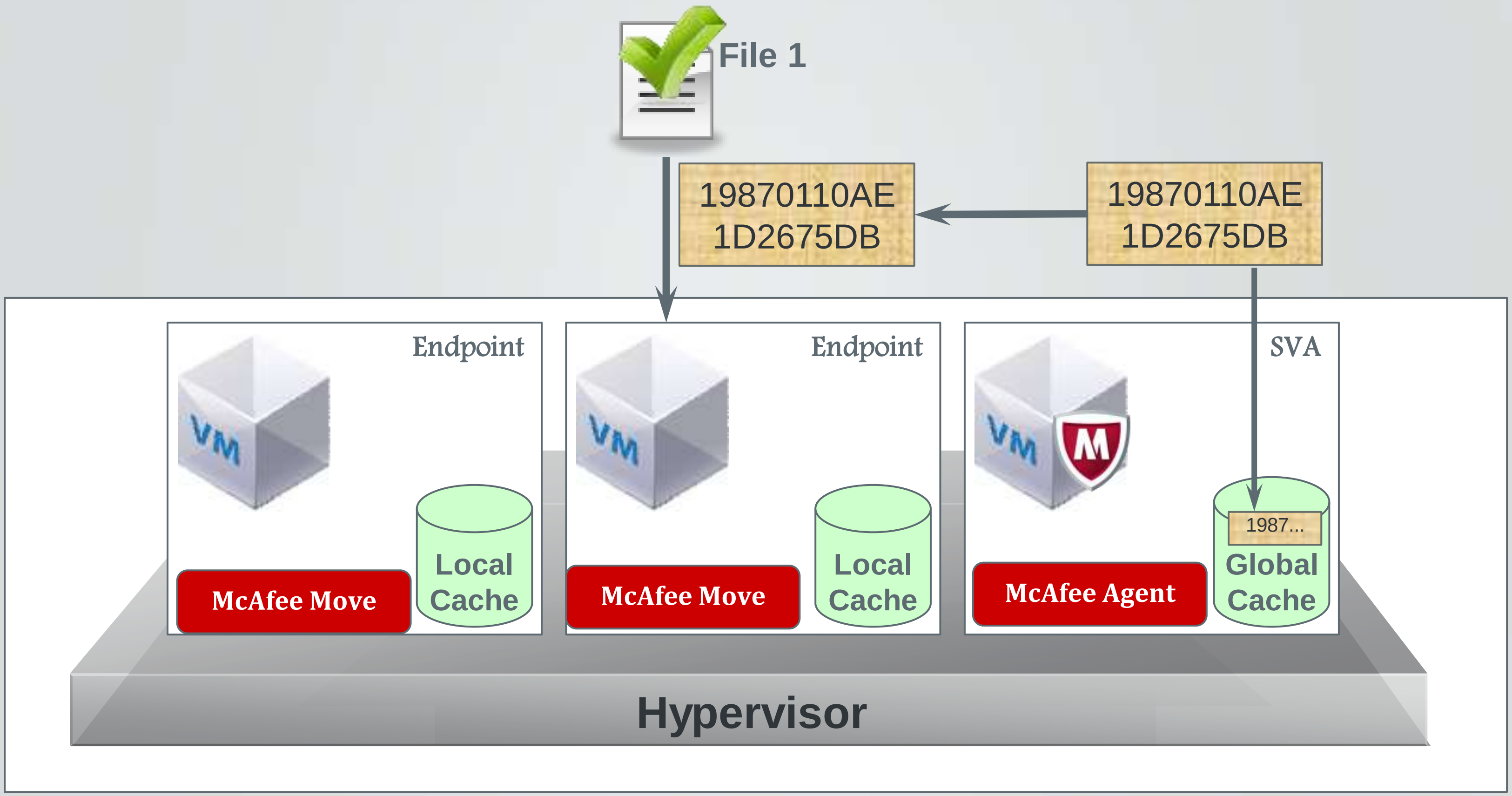
MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

If the File is MALICIOUS, MOVE AV will inform MOVE Endpoint to delete/deny access to the File based on policy.



MOVE AV 2.5 Agentless – Files up to 1MB (40MB with Multi-Platform)

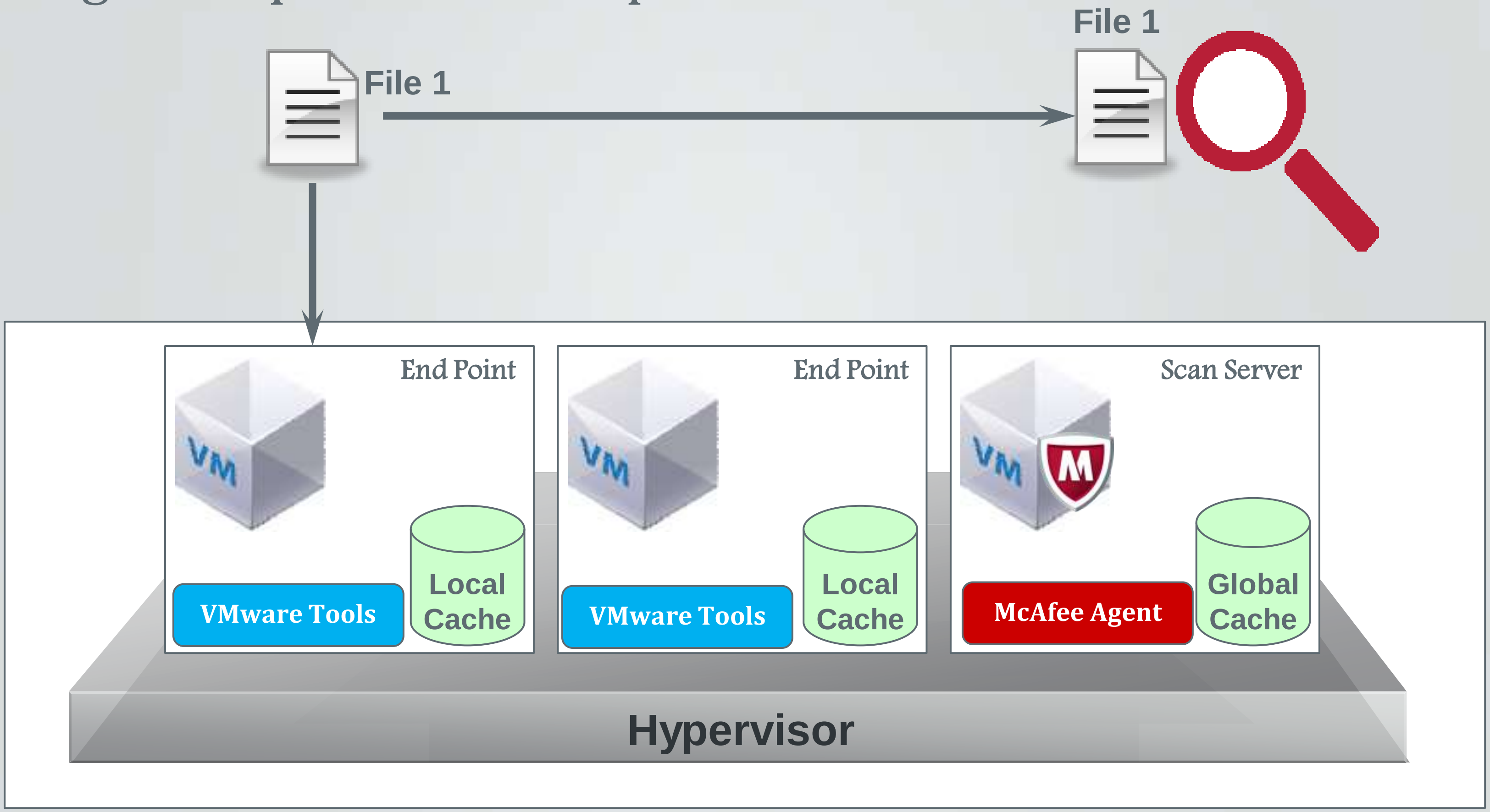
When the File is accessed from a different endpoint, the Global cache is leveraged, that file has been seen and need not be scanned again



The information contained in this document is for informational purposes only and should not be deemed an offer by McAfee or create an obligation on McAfee. McAfee reserves the right to discontinue products at any time, add or subtract features or functionality, or modify its products, at its sole discretion, without notice and without incurring further obligations.

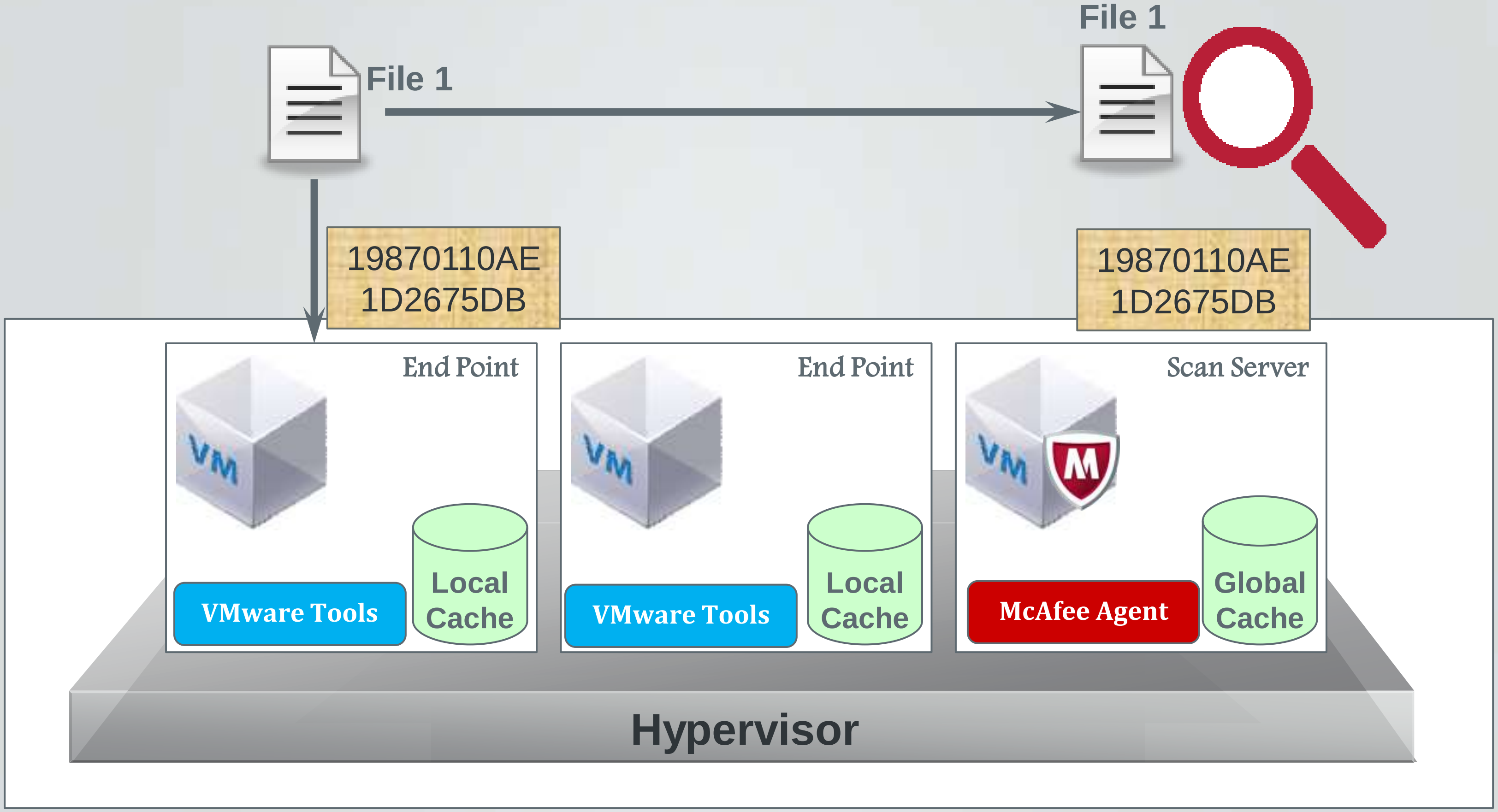
MOVE AV 2.5 Agentless – Files > 1MB

The file handle tells the engine to look at the file, the engine requests needed portions of the file.



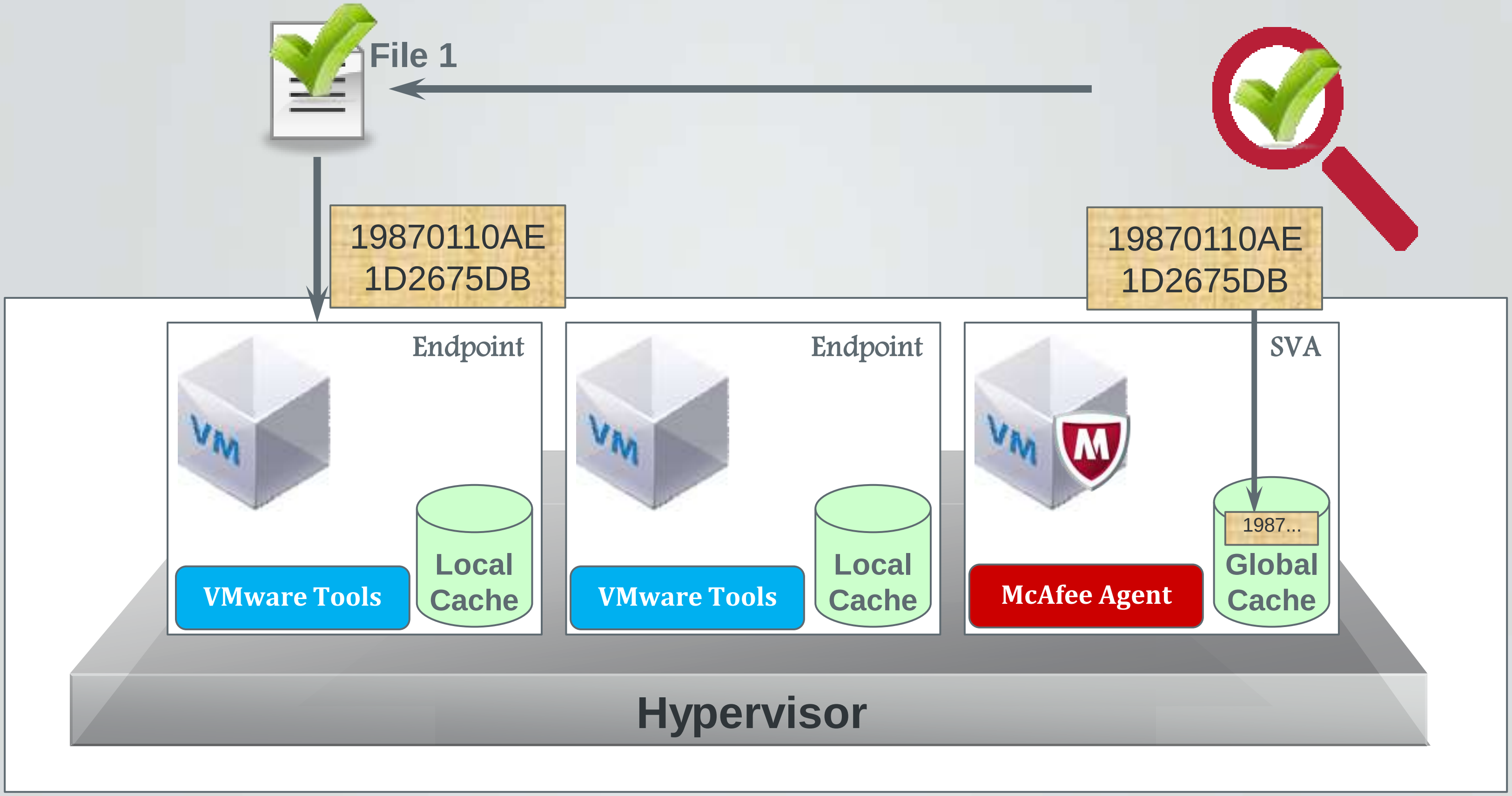
MOVE AV 2.5 Agentless – Files > 1MB

The File is analysed for Malware using both Signature and Cloud technologies, and may reach out for additional bits.



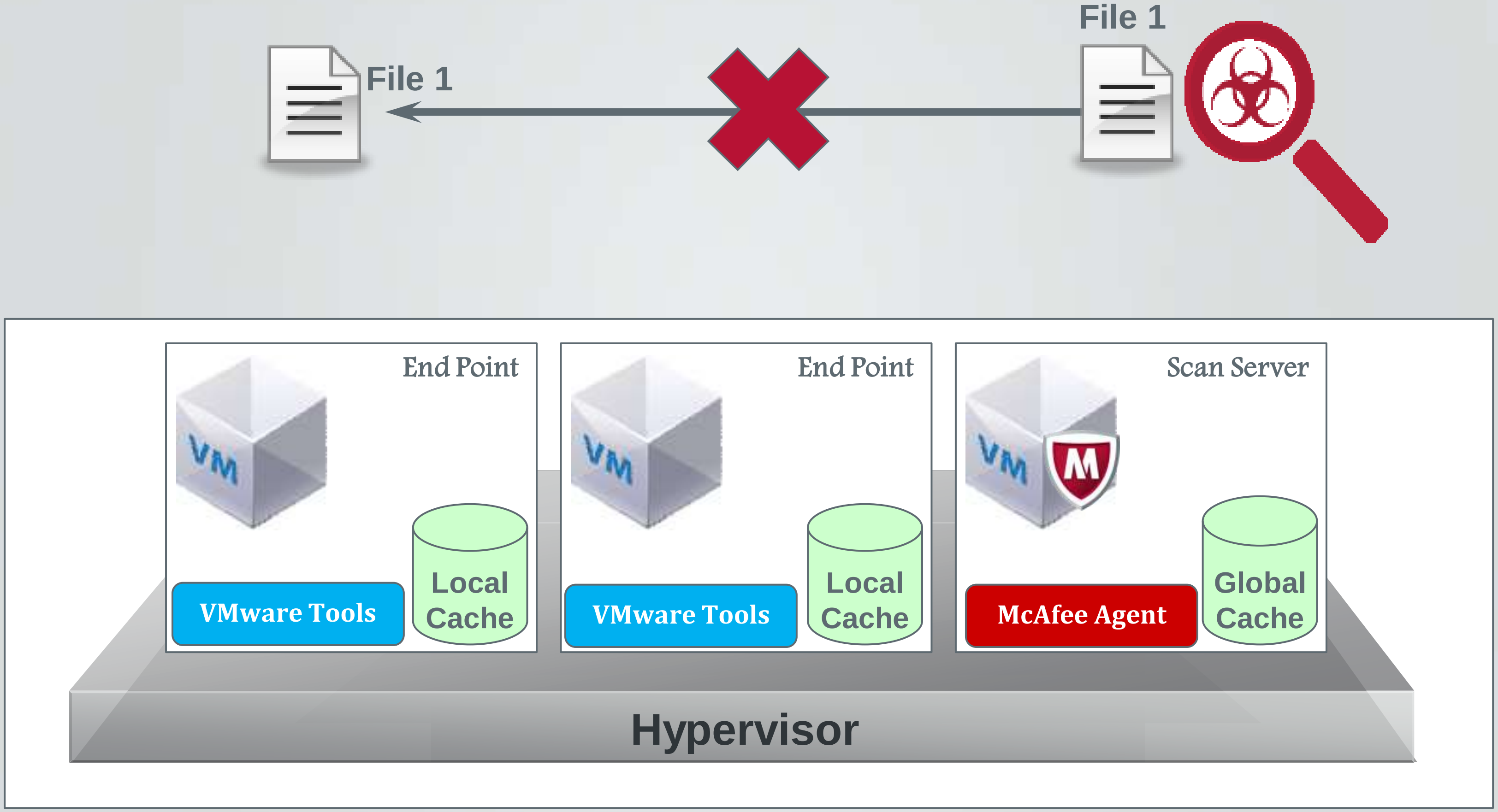
MOVE AV 2.5 Agentless – Files > 1MB

If the File is GOOD, MOVE AV informs vShield Endpoint to cache the file, File access is granted



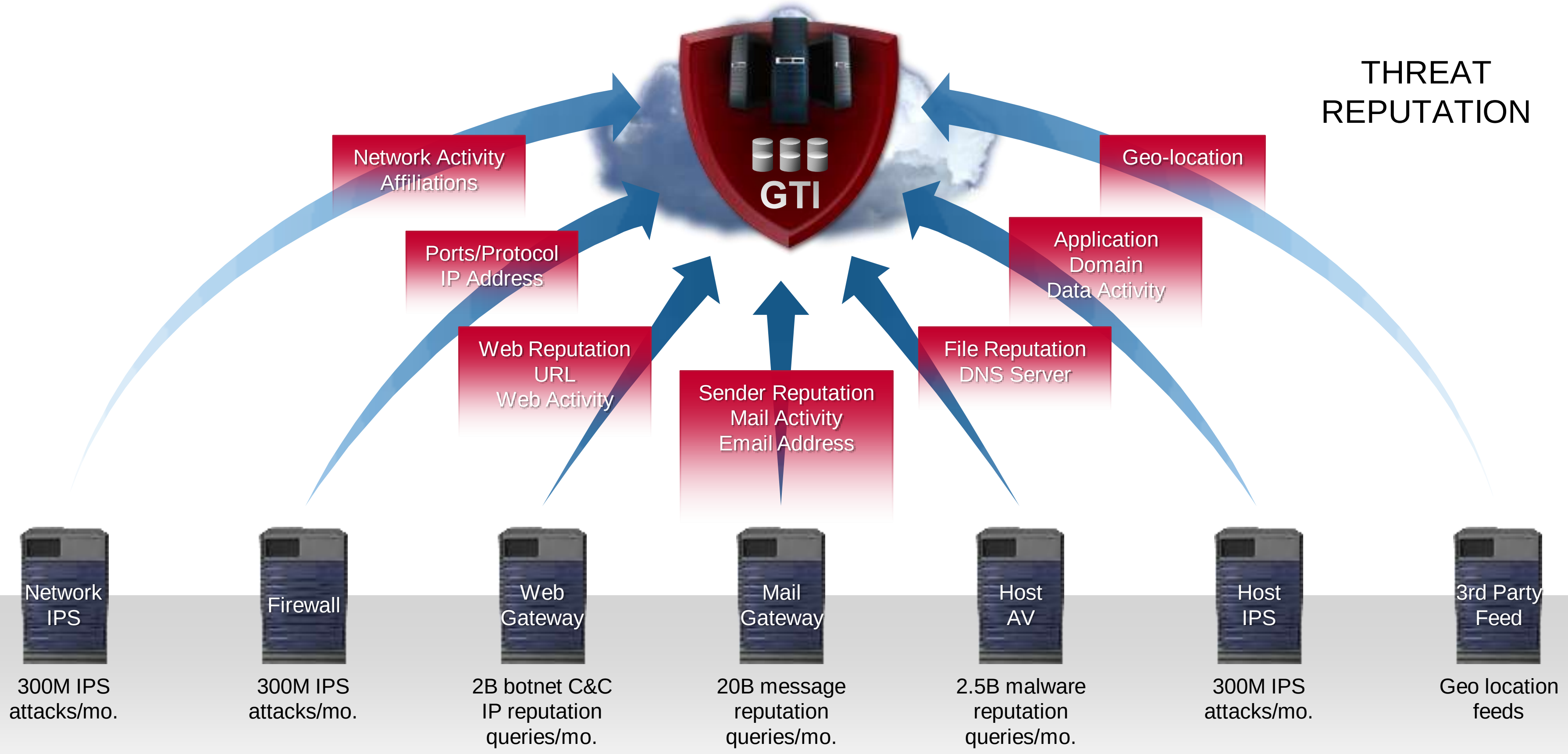
MOVE AV 2.5 Agentless – Files > 1MB

If the File is MALICIOUS, MOVE AV will inform vShield Endpoint to delete/deny access to the File based on policy.



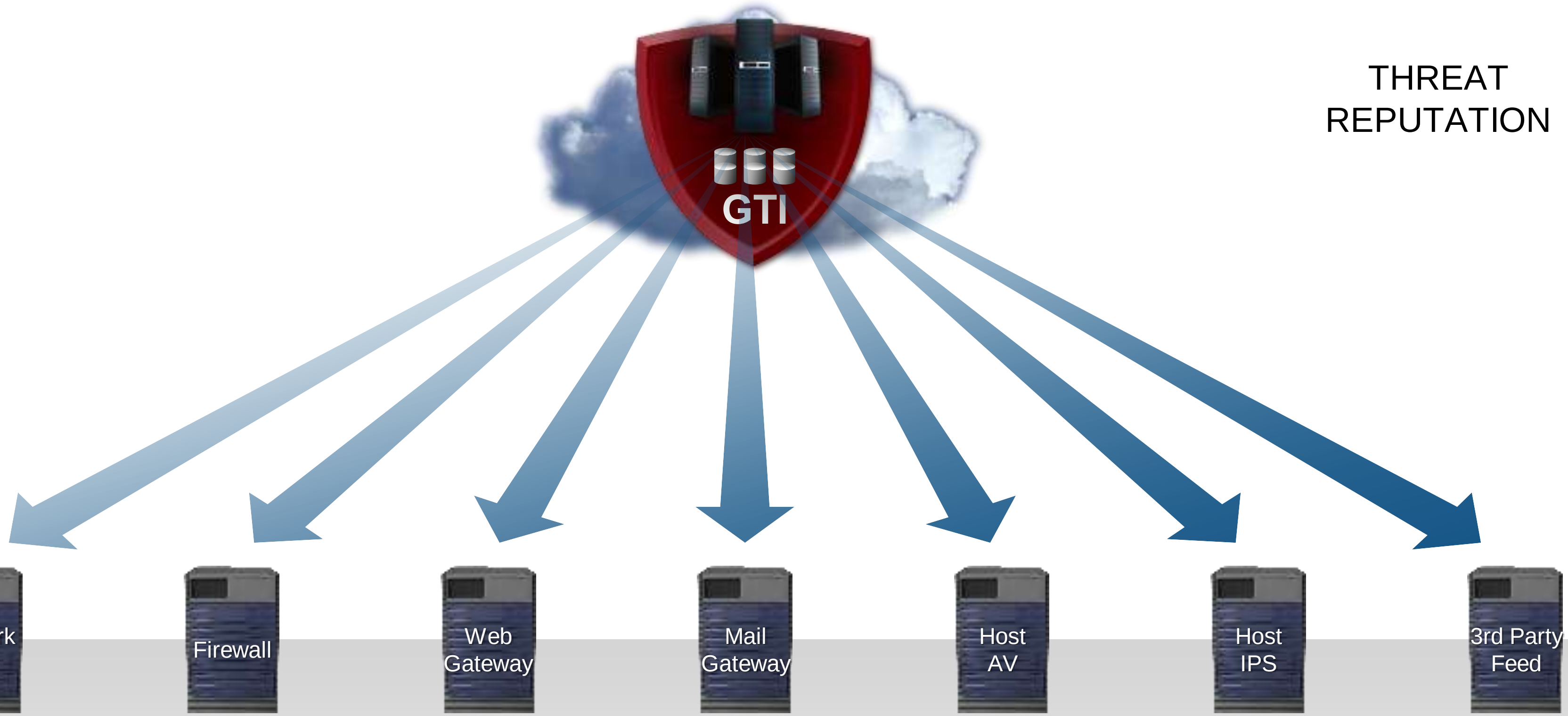
Global Threat Intelligence

What it takes to make your organization safe



Global Threat Intelligence

What it takes to make your organization safe



THREAT REPUTATION

300M IPS attacks/mo.

300M IPS attacks/mo.

2B botnet C&C IP reputation queries/mo.

20B message reputation queries/mo.

2.5B malware reputation queries/mo.

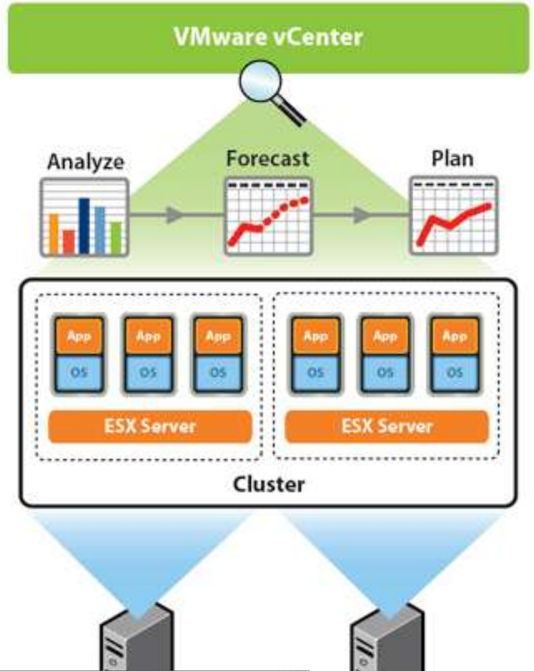
300M IPS attacks/mo.

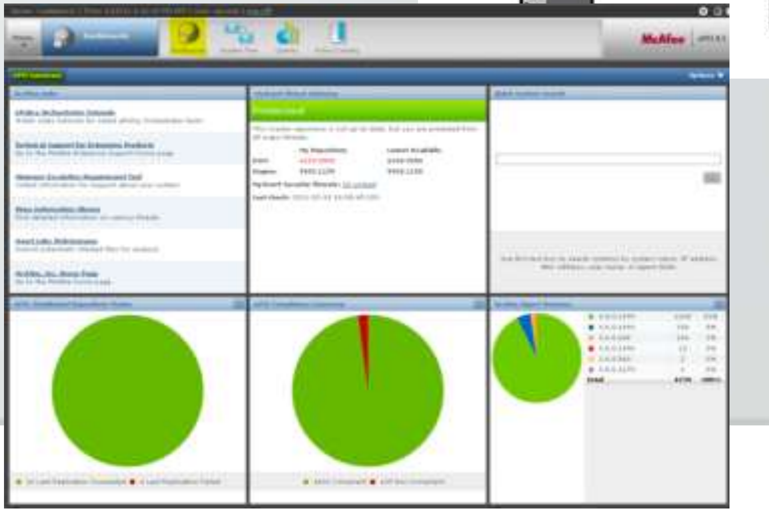
Geo location feeds

Intelligent Security Management

McAfee
An Intel Company

- vShield Manager/vCenter maintain constant communications of their connected VMs
- ePO constantly queries vCenter to maintain a map of VM UUID's other associated identifying information
- When we detect a virus, we know the UUID and we map that to the hostname
- ePO notifies vShield (via vCenter) know the file is infected and vShield implements assigned policy
- ePO maintains policy and delivers content updates to the McAfee SVA





MOVE Demo

DEMO

Application Control and Virtualization

McAfee
An Intel Company

Ensures only trusted applications run on servers and endpoints

- Dynamic whitelisting trust model reduces cost of ownership
- Zero day threat protection reduces patching cycles
- Blocks unwanted applications and their risks
- Extend the lifespan of legacy systems

Application Control

Virtualization Benefits

Minimal endpoint impact on Virtual Desktop and Virtualized Application Servers
Consumes less than 10MB of RAM and minimal CPU
No online scanning
No Signature Updates
Minimal Disk footprint

McAfee Application Control

Multi-layered Security Solution

McAfee
An Intel Company

Dynamic Whitelisting

Prevent all unauthorized code from running

Memory Protection

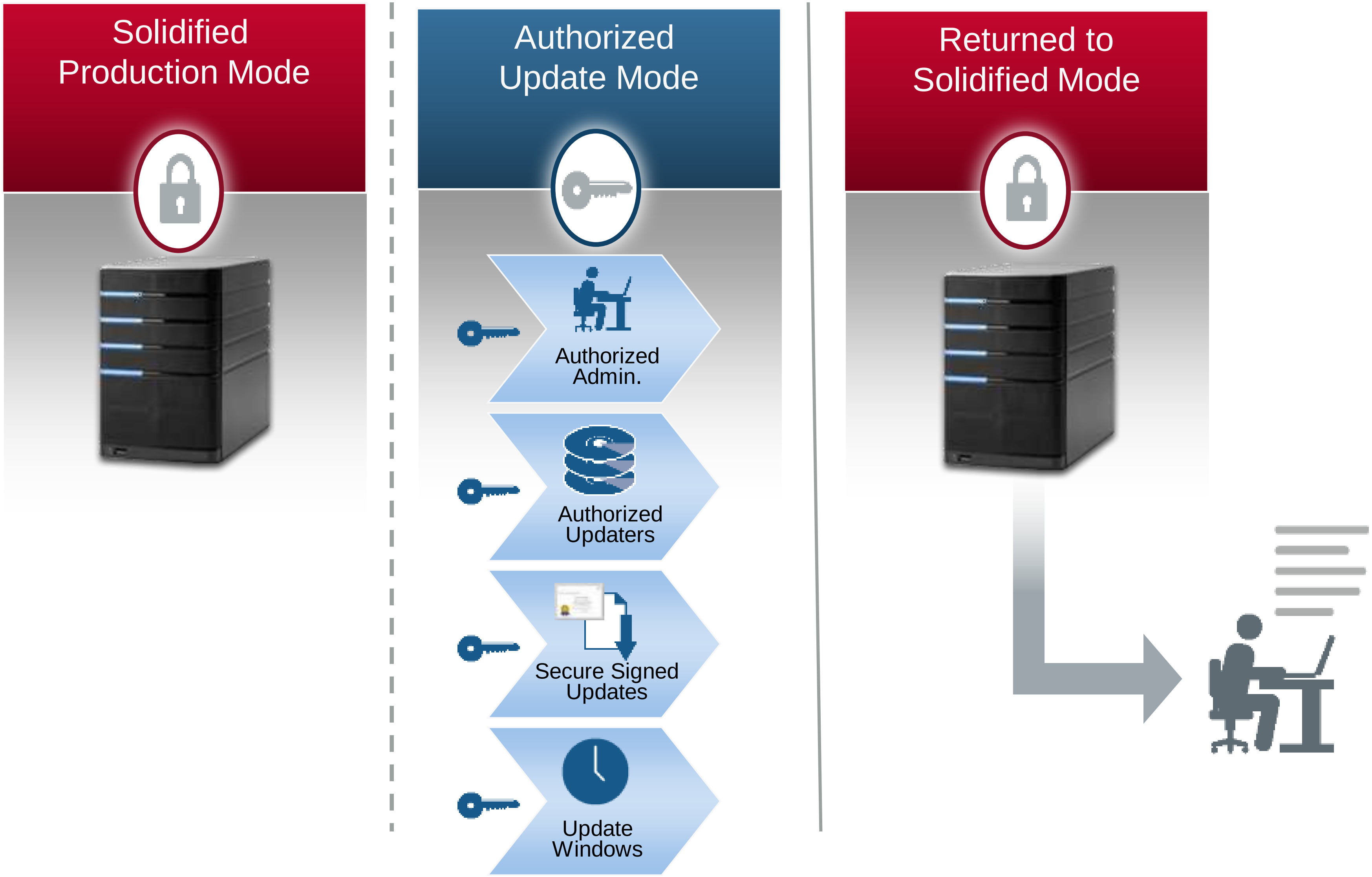
Protect against memory-based attacks, and application tampering

Image Deviation

Compare deployed system images to desired standard images with on-demand reporting

McAfee Dynamic Trust Model

Supporting Security and Operations through Trust



Solidified Production Mode

Authorized Update Mode

Returned to Solidified Mode

Enforce Policy and Monitor Change

- Enforce policies
  - *Real-time change monitoring of files, apps, databases, and networking devices*
- Deny unauthorized changes
  - *Prevent compliance drift*
  - *Integrated with change management systems like BMC Remedy and HP Service Center*

- Keep the bad stuff out
  - *Dynamic application whitelisting secures systems*
  - *0-day protection with no DAT files at all*
  - *Protection from memory-based attacks*
  - *Protection for embedded systems and constrained devices*
  - *Broad platform support*
- Stop unauthorized apps
  - *Only trusted applications/sources can execute*

Optimized

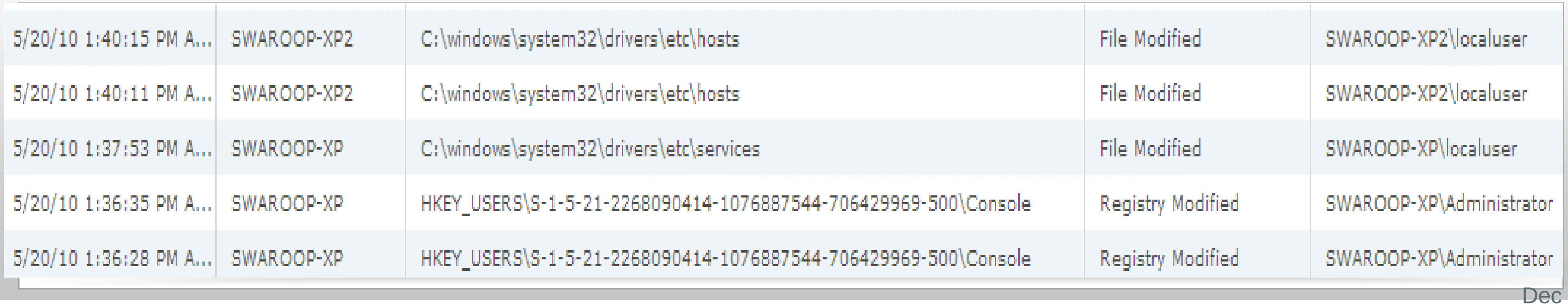
Change Control

Change Accountability

Application Control

Controlled Change
Maximizing Server Uptime

- Real-time change tracking of files, directories & registry keys
- Gives the Who? When? What? Why?
  - Username
  - Time of change
  - Program name
  - File/registry content
- Out of the box policies track critical resources by default
- Special alerting mechanisms for critical changes



5/20/10 1:40:15 PM A...	SWAROOP-XP2	C:\windows\system32\drivers\etc\hosts	File Modified	SWAROOP-XP2\localuser
5/20/10 1:40:11 PM A...	SWAROOP-XP2	C:\windows\system32\drivers\etc\hosts	File Modified	SWAROOP-XP2\localuser
5/20/10 1:37:53 PM A...	SWAROOP-XP	C:\windows\system32\drivers\etc\services	File Modified	SWAROOP-XP\localuser
5/20/10 1:36:35 PM A...	SWAROOP-XP	HKEY_USERS\S-1-5-21-2268090414-1076887544-706429969-500\Console	Registry Modified	SWAROOP-XP\Administrator
5/20/10 1:36:28 PM A...	SWAROOP-XP	HKEY_USERS\S-1-5-21-2268090414-1076887544-706429969-500\Console	Registry Modified	SWAROOP-XP\Administrator

Agenda

- Challenges with Virtualization
- Virtualization Solutions
- **Summary**

Thank You

Q&A

www.McAfee.com/Virtualization