McAfee
Together is power.

ENS for Server

Security designed for virtual platforms…

Lehoux Nicolas | Sales Engineer

Challenges in securing virtual environments

Addressing the top security challenges

How can I find virtual machines as and when it comes up?

Connectors

Discovery VM without installing any McAfee agents

How can I secure VM without impacting performance?

Security Designed for VM

Option to Offloaded scanning or running resource intensive tasks based on hypervisor load

How can protect VMs from advance malware?

Adaptive Threat Protection

Behavioral detection& common policies across hybrid datacenter

Virtual Servers: Technology Options

MOVE
(McAfee Optimized for Virtual Environments)

- MOVE Agentless – offloaded scanning for vmware
- MOVE Multi-platform - optimized for virtual environment, supports multiple hypervisors (e.g. VMware, Xen, KVM)
- Antimalware with integrated management & threat intelligence

ENS for Servers & VDI

- NextGen technology optimized for Virtual Servers and VDI
- Optimized for Hypervisor performance, while leveraging all benefits of next generation security solution
- Execute resource intensive tasks such as On-Demand Scanning based on hypervisor load

Virtualization Use Cases

MOVE

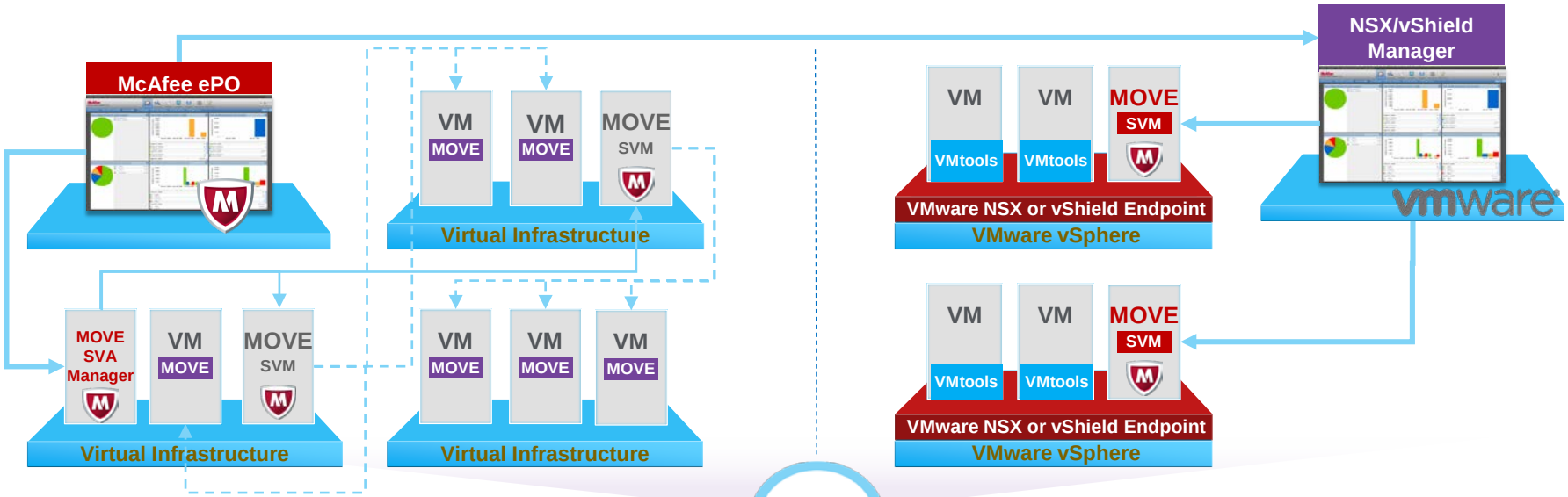
- Scan Storm – benefit from Global Cache
  - E.g.. at 9 AM all employees login to VM causing scan storm
  - Non-persistent VDI created from template everyday
- Prevent performance impact due to DAT and ODS Storm
- Need 2nd layer of security (Primary is perimeter and separate security for data store)
- Smaller footprint – 50 MB Memory, 3 MB Disk
- Agentless scanning in background
- Squeeze VM Density
- Limitations: Only signature based scanning

ENS for Servers & VDI

- Zero day Protection
  - Behavioral protection via Real Protect & DAC (Dynamic Application Containment)
  - IPS Protection – Access Protection & Exploit Prevention
- Prevent performance impact due to DAT and ODS Storm by executing resource intensive when hypervisor is not loaded
- Endpoint Security is primary security (ENS, FW, Web Control, DLP, Encryption, etc.)
- Ease of management – same security across physical & virtual infrastructure
- Supports ENS for Linux
- Limitations: Doesn't prevent scan storm

MOVE

MOVE Security Management



Multi-platform (MP)

- An SVM can protect 200-400 VMs
- 1 SVA Manager for an ePO instance and load balances across the SVM instances

Agentless (AL)

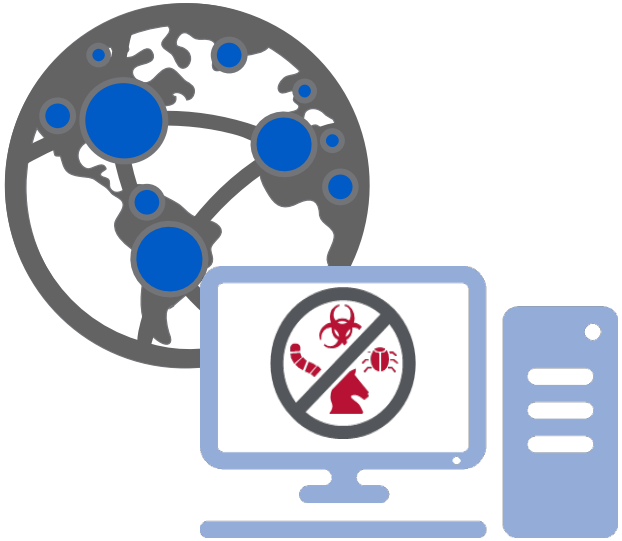
- An SVM protects all the VMs on its hypervisor
- vShield Endpoint can be deployed from ePO
- ePO is tightly integrated with VMware NSX

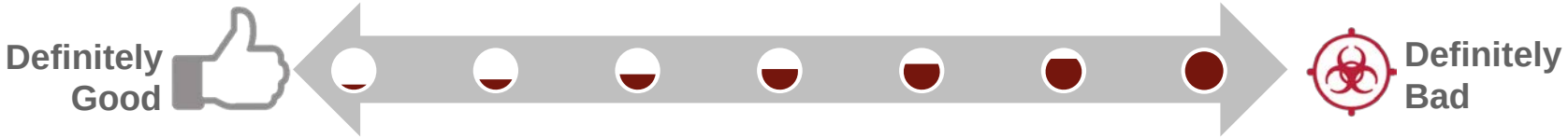
ENS for Servers

Real Protect

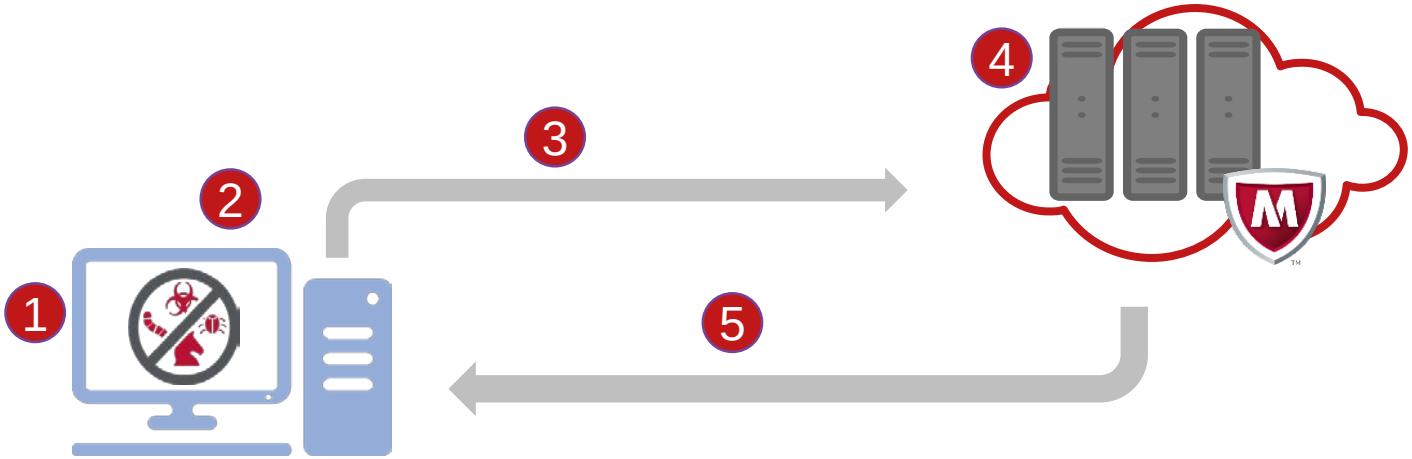
Detects zero-day malware without signatures

- Trace execution in real time to capture behavior
- Catches exploits or legitimate application misuse that static-only methods struggle to detect
- Backed by machine learning analytics
- Uses data analytics in cloud to classify
- Works online and offline with local machine learning





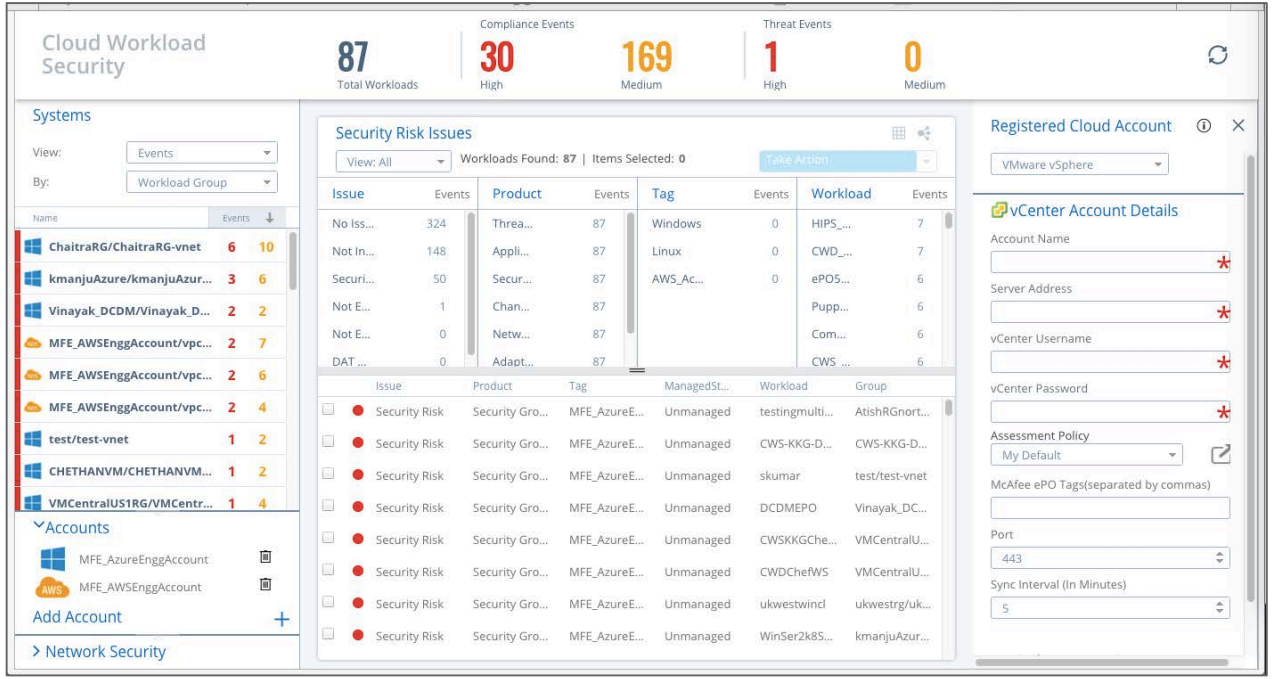
Real Protect in Action



1. A suspicious files gets on the computer
2. If unknown, to the AV scanner and GTI database, Real Protect is triggered to track it's behavior
3. The file's dynamic behavior is recorded and sent to the McAfee cloud
4. In the GTI cloud, the file is analyzed and compared against static and dynamic attributes of known malware
5. The results are sent to the endpoint in real-time and if malicious, it is stopped, removed and remediation begins

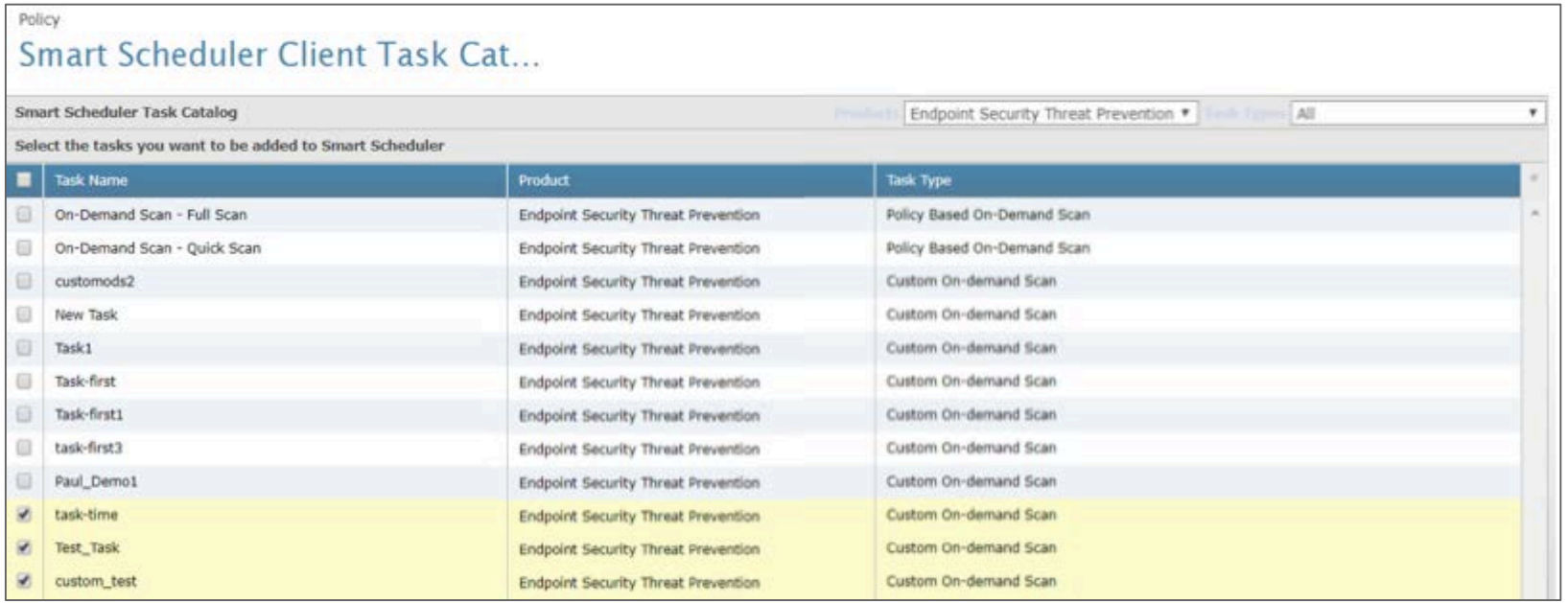
Cloud Workload Security

- Register VMWare Account
- CWS will discover virtual systems running on a hypervisor without agent using vmware API
- CWS will check hypervisor load every 5 min
- New systems will be discovered every 5 min



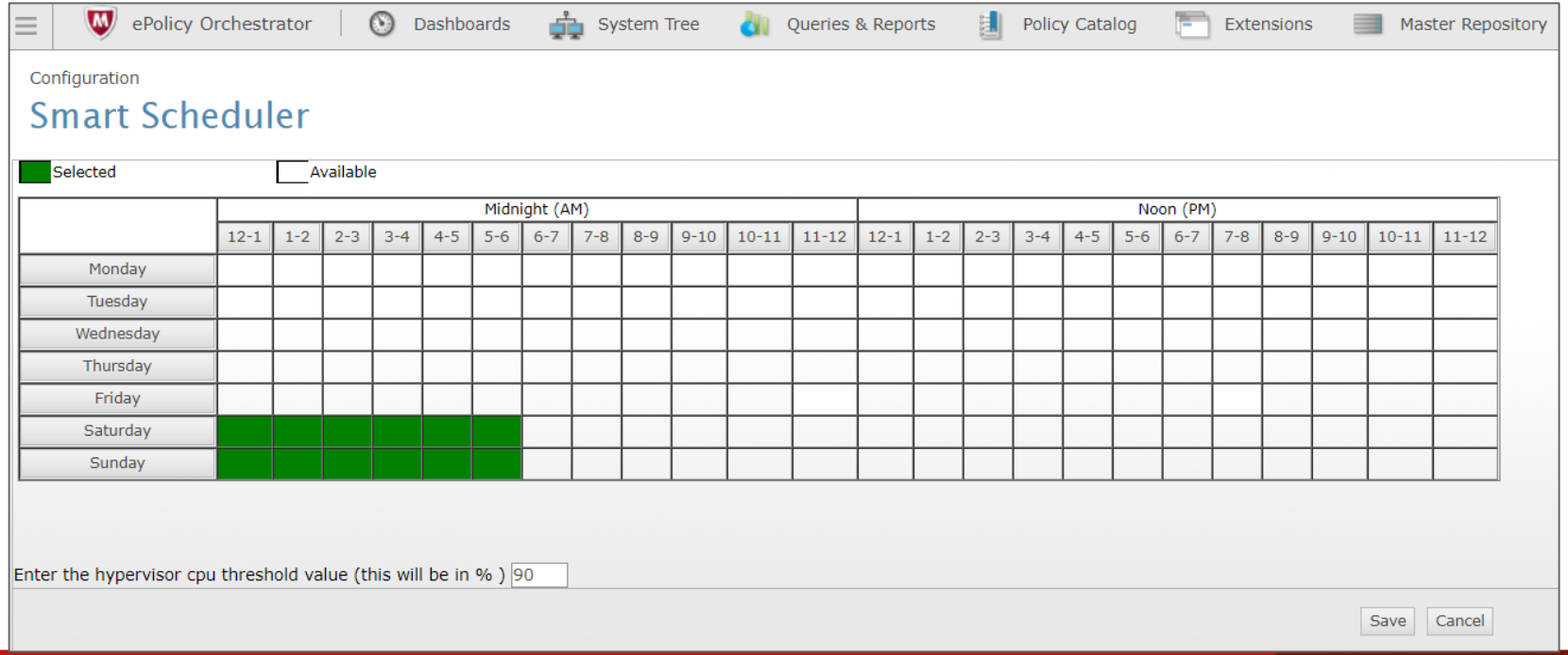
Select Smart Tasks

- Select the tasks to add to Smart Scheduler



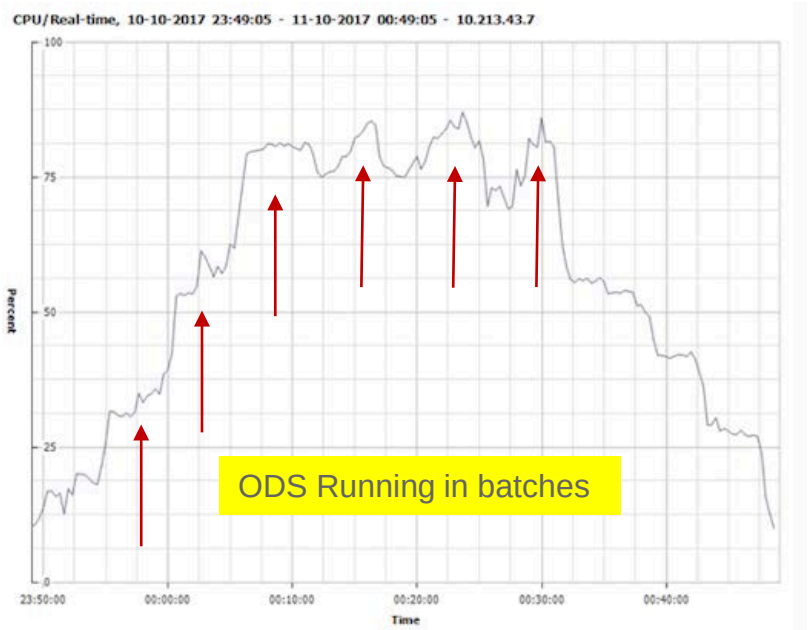
Smart Scheduler

- Schedule task to run during off peak period when the load on hypervisor is below specified limit
- MA executes the task only when hypervisor load is below specified limit



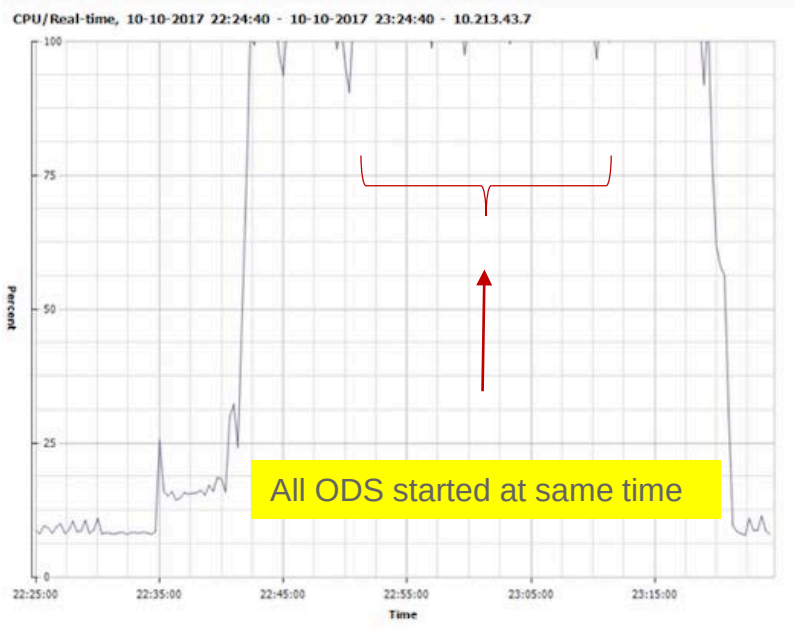
Hypervisor Performance During ODS

With Smart Scan with 75% CPU Limit



Hypervisor CPU never crossed 80%

Without Smart Scan



Hypervisor CPU above 100% during ODS