Intel® Cloud Builders Guide
McAfee Security Management Platform
Trapezoid Trust Control Suite

Intel® Cloud Builders Guide to Cloud Design and Deployment on Intel® Platforms

Integrating Intel® TXT Enabled Clouds with McAfee Security Management Platform leveraging Trapezoid Trust Control Suite

Intel® Xeon® Processor 5500 Series
Intel® Xeon® Processor 5600 Series

Audience and Purpose

This reference architecture describes the security integration of an Intel® Trusted Execution Technology (Intel® TXT[1]) Enabled Cloud infrastructure with the McAfee Security Management Platform leveraging Trapezoid's Trust Control Suite (TCS). Configured to meet Open Data Center Alliance (ODCA) best practices, Trapezoid's Trust Control Suite integrates trust data generated by the cloud infrastructure built on the Intel TXT platform with the McAfee Security Management Platform to audit, monitor, and enforce cloud security policies. This trusted cloud infrastructure is built with VMware vSphere using ESX5.0 on Intel® Xeon® Processor E5-2680 series-based server platforms. McAfee's Secure Management Platform product suite is used to secure the end-user cloud environment and comply with ODCA Platinum Assurance levels.

Trapezoid solutions are focused on the creation of Trust Data Intelligence (TDI) to provide end-to-end hardware-based security for IT infrastructures. The company specializes in the development and integration of hardware security solutions to mitigate risk and attain compliance for enterprise and cloud environments. Trapezoid Trust Control Suite enables organizations to monitor, report, and validate security threats; then dynamically enforce security policies based on hardware trust data.

August 2012

Table of Contents

Executive Summary

Introduction

Trapezoid is a leader in Trust Data Intelligence (TDI), with deep knowledge of the Intel® Trusted Execution Technology (Intel® TXT). Trapezoid's Trust Control Suite ties BIOS level hardware trust data back into the security infrastructure of IT enterprises and Cloud environments. Whether deploying applications in a public, private, or hybrid cloud, a business must ensure that any cloud environment is secure enough for its essential data. Any organization considering a move to cloud computing must carefully assess and continue to monitor its end-to-end security infrastructure.

Trapezoid has surfaced the Intel TXT trust values, which enable enterprises to validate that they are running their applications on both trusted hardware and a trusted hypervisor. As a contributing member in the Open Data Center Alliance (ODCA) Security and Regulatory working groups, Trapezoid is at the forefront of enabling organizations to leverage hardware-based trust data when securing and monitoring their infrastructure and enabling compliance with assurance standards and regulatory compliance.

The Intel® Cloud Builders (ICB) environment was used in implementing this reference architecture which describes the integration of an Intel TXT trust data with the McAfee Security Management Platform, leveraging Trapezoid's Trust Control Suite (TCS). Configured to meet ODCA assurance levels, Trapezoid's TCS integrates trust values and changes in the state of trust generated by the cloud infrastructure. Integrating with McAfee ePolicy Orchestrator, TCS helps audit, monitor, and enforce hardware based security policies in the cloud. This trusted cloud Infrastructure is built with VMware vSphere using ESX 5.0 on Intel® Xeon® Processor E5-2680 series-based server platforms. In addition to enforcing hardware-based security policies based on TCS, McAfee's Secure Management Platform product delivers to the end-user ODCA Provider Assurance compliance.

Intel® Trusted Execution Technology (Intel® TXT)

Designed to help protect against software-based attacks, Intel TXT integrates new security features and capabilities into the processor, chipset, and other platform components. The hardware rooted security enables the ability to increase the confidentiality and integrity of sensitive information from software-based attacks, protect sensitive information without compromising the usability of the platform, and deliver increased security in platform-level solutions through measurement and protection capabilities. It provides a general-purpose safer computing environment capable of running a wide variety of operating systems and applications.

Intel TXT provides hardware rooted trust in which a chain of trust for your execution environment can be built upon. The technology helps protect IT infrastructures against software-based attacks by validating the behavior of key components within a server or PC at startup and checks the consistency in behaviors and launch-time configurations against a verified benchmark called a "known good" sequence.

Each layer of software on a system builds on the previous, and a change or lack of integrity in a lower layer impacts all layers above. For example, if the computer BIOS can be changed by an attacker, then it is possible to report false information to the operating system and countless other types of mischief. Intel TXT provides a mechanism to confirm what code was executed by the server upon boot.

VMware vSphere ESX

Working in concert with industry leaders, VMware is helping enterprises gain the benefits of cloud computing, leveraging existing investments without compromising control. Virtualization is the essential catalyst for cloud computing. VMware builds on this solid foundation with platforms and solutions to power your cloud infrastructure, build and run robust cloud applications, and supply end-user computing as a cloud-based service. A VMware infrastructure has numerous features specifically designed to address security for demanding datacenter or cloud environments such as:

- Custom Roles and Permissions
- Resource Pool Access Control and Delegation
- Real-time Session Management
- Extensive Logging and Audit Trails

Each virtual machine's access to physical resources and physical hardware is mediated through and by the VMkernel and VMM. Technically, virtual machines should not be able to circumvent this level of isolation. Nevertheless, there have been several different reports of malware bypassing this native isolation and affecting an ESX host at the firmware level. Basically, the VMware-based cloud infrastructure must be monitored to validate that virtualization is rooted in hardware trust and maintains desired trust levels as well as identify modifications in the VMkernel.

McAfee Security Management Platform

The McAfee Security Management Platform efficiently handles security through deep integration within the system stack and across the IT environment, allowing global, contextual visibility into changing events and a cross-product command and control core. McAfee's Security Management Platform intelligently connects dynamic context from global threat intelligence, enterprise risk, and system security posture in real time.

This interlacing of threat intelligence and risk management processes allows instant blocking of damaging attacks and adjustments of security postures as risks change. This solution also provides crucial operational intelligence, organizing data and placing it in context for at-a-glance visibility across IT infrastructure. With this implementation of McAfee's Security Management Platform, full ODCA Provider Assurance is met at the Platinum level.

McAfee ePolicy Orchestrator (ePO) is a key component of the McAfee Security Management Platform, and the only enterprise-class software, to provide unified management of endpoint, network, and data security. With end-to-end visibility and powerful automations that slash incident response times, McAfee ePO software dramatically strengthens protection and drives down the cost and complexity of managing risk and security. McAfee ePO is integrated with Trapezoid TCS to surface hardware-based trust data and consolidate it with the rest of the security data being generated by the environment. Together ePO and TCS combine to make intelligent hardware-based policy enforcement decisions.

Trapezoid Trust Control Suite (TCS)

Trapezoid's solutions are focused on the creation of TDI to provide end-to-end hardware based security for IT infrastructures. The company specializes in the development of advanced security solutions to help mitigate risk and attain compliance for enterprise and cloud environments. The Trapezoid TCS enables organizations to monitor, report, and validate potential hardware security threats, then dynamically enforce security policies based on trust data.

TDI is Trapezoid's methodology for the foundation of its products and services. TDI starts with the concept of "trust data," which includes attestable values identified from known good sources, including:

- Intel TXT hardware security status
- Verifiable location values
- Verifiable user identity values
- Verifiable proof of life values
- Measurable software, mathematical fingerprints, or hash values

Trust data doesn't just originate from known "good" sources – it also includes data generated by sources that are known to be "potentially good" or "trustable," "potentially bad" or "non-trustable," and "bad" or "untrusted." Trapezoid combines this trust data with data generated by traditional security event monitoring tools and other elements in a company's infrastructure; establishing end-to-end TDI to provide an intelligent view of an enterprise's security posture.

TDI enables Trapezoid to create an interconnected ecosystem among traditionally independent infrastructure elements, such as servers, network elements, security devices, clients, and applications. The Trapezoid ecosystem operates in a coordinated, contextual manner to provide the first ever actionable and reportable hardware-centric security posture. As TDI is reported to the ecosystem its elements can automatically respond to threats with dynamic policy enforcement as defined by administrators or Trapezoid's published rule sets. More specifically, Trapezoid's approach enables each element to respond with relevant actions independently while detecting and contributing to the TDI of the entire environment.

This granular system of checks and balances enables the enterprise technology infrastructure to communicate and react intelligently to potential security threats. The Trapezoid security ecosystem recognizes changes in the state of the infrastructure and responds to potential threats through the synchronized, dynamic enforcement of security policies. By understanding what is "trusted" and ensuring all systems maintain that status, Trapezoid helps minimize risk, protect sensitive data, and enable business continuity.

Test Bed Blueprint

This section describes the hardware components, network topology, minimum storage, and server requirements needed to execute the reference architecture and test cases described in this document.

System	Detailed Configuration
Management Server (x1)	Microsoft Windows 2008, IIS, .NET 2.0, VMware vCenter Server 5.0, and vSphere Web Services* SDK
Management Client	Microsoft Windows 7, .Net 2.0, and VMware vCenter Client 5.0
ESXi 5 Host Trusted (x3)	Form Factor: 2U Rack Mount Server Intel® Xeon® Processor E5-2680 @2.70GHz, 20MB Cache, 8.0GT/s QPI 8-Core, Sandy Bridge-EP Memory: 24 GB RAM storage: 5x 100GB HDD 2x Ethernet network
ESXi 5 Host NOT Trusted (x2)	Form Factor: 2U Rack Mount Server Intel® Xeon® Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM storage: 5x 100GB HDD 2x Ethernet network
iSCSI Data Store Server	Form Factor: 2U Rack Mount Server Processor: Intel Xeon Processor X5600 @2.93 GHz, 2-socket x 6 cores = 12 cores Memory: 24 GB RAM storage:10x 100GB HDD Ethernet network

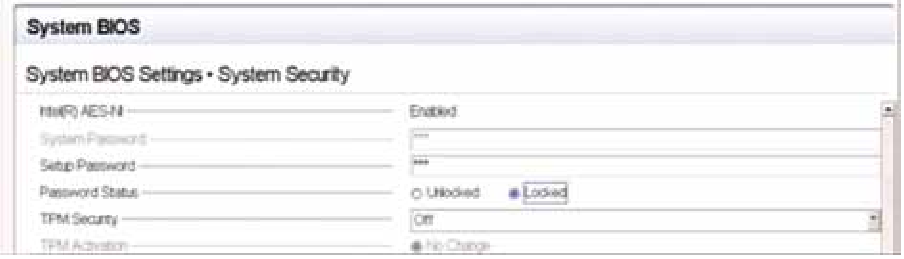
Table 1: Hardware requirements

Intel TXT Server Provisioning

The following changes are required in the BIOS settings of each physical server being deployed in a trusted cloud infrastructure. Intel TXT settings and other security settings must be configured prior to hypervisor installation. Immediately after the provisioning of Intel TXT in the BIOS, the hypervisor installation must be performed. If any BIOS settings are changed after provisioning Intel TXT, the TPM Trust Values will not be properly reflected and the hypervisor kernel will cease to be part of the server's trusted boot state.

Step 1: Boot Server and Enable Password Security

1. Boot server and enter BIOS setup [F2]
2. System Setup-> [System Bios]
3. System Bios -> [System Security]
4. System Security -> System Bios Password status -> [Enable BIOS passwords]



System BIOS

System BIOS Settings • System Security

Intel(R) AES-NI: Enabled

System Password: ***

Setup Password: ***

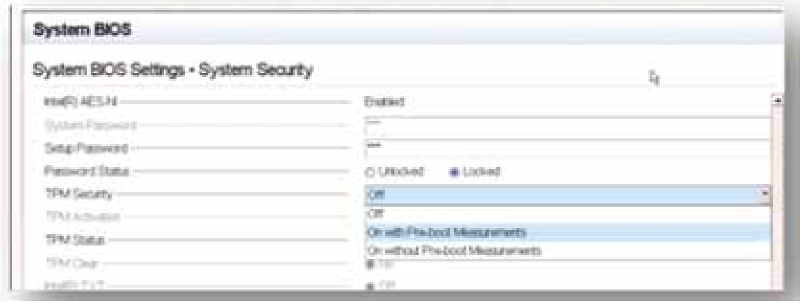
Password Status: ○ Unlocked ● Locked

TPM Security: Off

TPM Activation: ● No Change

Step 2: Enable TPM Settings

1. After reboot at the initial prompt, press F2 key to enter BIOS setup
2. Enter BIOS setup password
3. System Setup-> [System Bios]
4. System Bios -> [System Security]
5. System Security -> TPM Security -> [Enable]



System BIOS

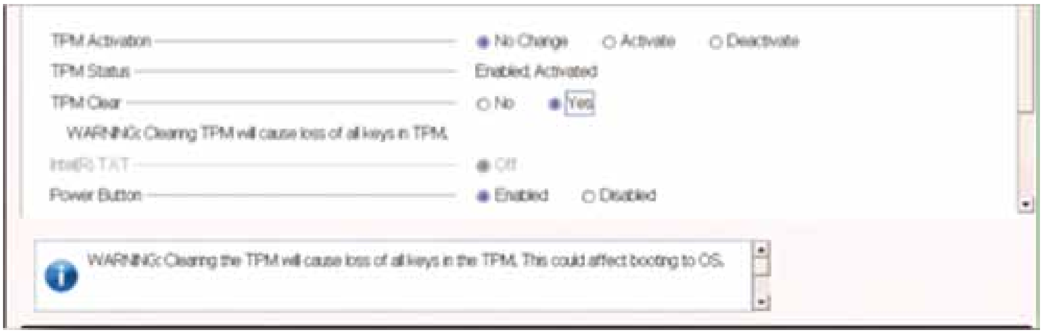
System BIOS Settings • System Security

Intel(R) AES-NI — Enabled
System Password — ***
Setup Password — ***
Password Status — ○ Unlocked ● Locked
TPM Security — Off
TPM Activation
TPM Status
TPM Clear

Off
On with Pre-boot Measurements
On without Pre-boot Measurements

Step 3: Clear TPM

1. After reboot at the initial prompt, press F2 key to enter BIOS setup
2. Enter BIOS setup password
3. System Setup-> [System Bios]
4. System Bios -> [System Security]
5. System Security -> [TPM Security]
6. TPM Security -> [TPM Clear] -> YES

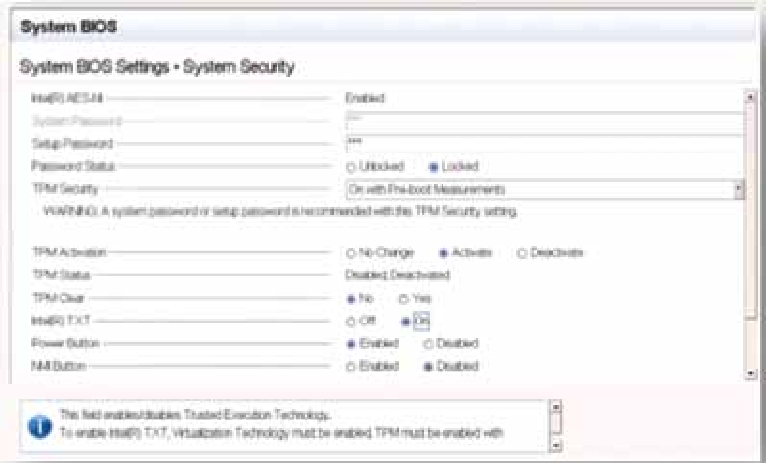


TPM Activation — ● No Change ○ Activate ○ Deactivate
TPM Status — Enabled, Activated
TPM Clear — ○ No ● Yes
WARNING: Clearing TPM will cause loss of all keys in TPM.
Intel(R) TXT — ● Off
Power Button — ● Enabled ○ Disabled

WARNING: Clearing the TPM will cause loss of all keys in the TPM. This could affect booting to OS.

Step 4: TPM and TXT Attribute Changes

1. After reboot at the initial prompt, press F2 key to enter BIOS setup
2. Enter BIOS setup password
3. System Setup-> [System Bios]
4. System Bios -> [System Security]
5. System Security -> [Intel TXT]-> Change to ON



System BIOS

System BIOS Settings • System Security

Intel(R) AES-NI Enabled
System Password
Setup Password ***
Password Status ○ Unlocked ● Locked
TPM Security On with Pre-boot Measurements
WARNING: A system password or setup password is recommended with this TPM Security setting.

TPM Activation ○ No Change ● Activate ○ Deactivate
TPM Status Disabled, Deactivated
TPM Clear ● No ○ Yes
Intel(R) TXT ○ Off ● On
Power Button ● Enabled ○ Disabled
NMI Button ○ Enabled ● Disabled

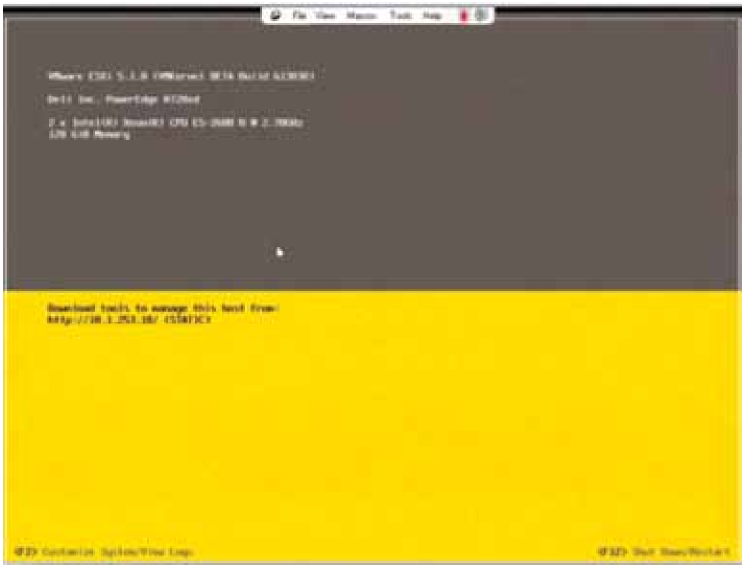
This field enables/disables Trusted Execution Technology.
To enable Intel(R) TXT, Virtualization Technology must be enabled, TPM must be enabled with

NOTE: The server hardware is now prepared for hypervisor installation rooted in trust by Intel TXT.

VMware ESX TPM Attestation

After installing the hypervisor (in this case VMware ESX 5.0) on a server with Intel TXT enabled in the BIOS, the new ESX Host will need to be added to VMware vCenter for management. When a new ESX Host is added to vCenter, the Intel TXT trust values can be validated by querying the vSphere Web API. Intel TXT Trust Values can also be queried from the server directly if no vCenter is available.

Perform a VMware ESX hypervisor trusted installation immediately after the Intel TXT process above.

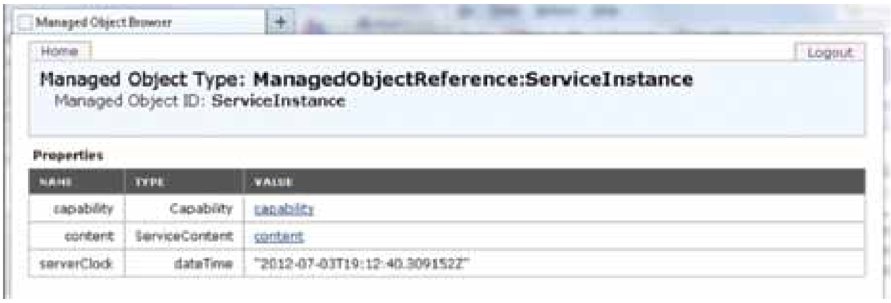


```
VMware ESXi 5.1.0 (VMKernel BETA Build [illegible])

Dell Inc. PowerEdge R720xd

2 x Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
128 GiB Memory

Download tools to manage this host from:
http://10.1.253.18/ (STATIC)

<F2> Customize System/View Logs                    <F12> Shut Down/Restart
```

After the VMware ESX installation to run a VMware host ”TPM Attestation Report” using the vSphere Web API, you must connect to the vSphere API browser running directly on your vCenter server. Using the vSphere Web API, drill down into the ”Values” of the following “Processes” as designated by the syntax: “PROCESS:TYPE--> VALUE”:

Use the following steps to validate Intel TXT Trust using the vSphere Web API 5.0:

1. ServiceContent --> content

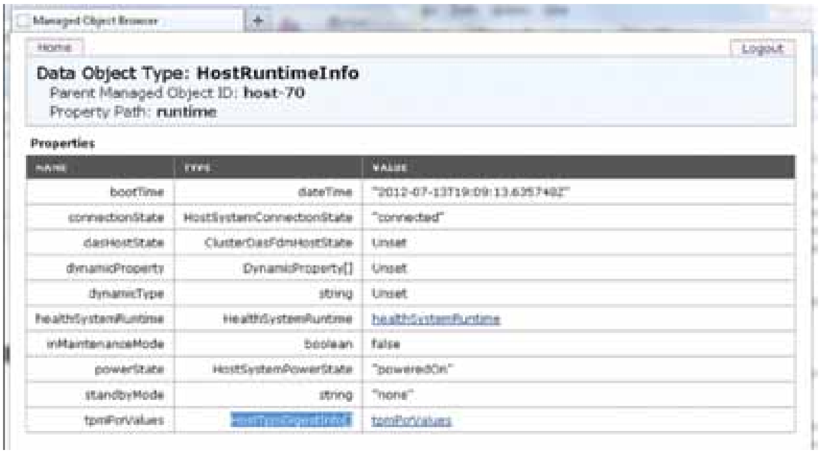


Managed Object Type: ManagedObjectReference:ServiceInstance
Managed Object ID: **ServiceInstance**

Properties

NAME	TYPE	VALUE
capability	Capability	capability
content	ServiceContent	content
serverClock	dataTime	"2012-07-03T19:12:40.309152Z"

2. ManagedObjectReference:Folder --> group-d1 (Datacenters)
3. ManagedObjectReference:ManagedEntity[] --> datacenter-2 (DCName)
4. ManagedObjectReference:Folder --> group-h4 (host)
5. ManagedObjectReference:ManagedEntity[]--> domain-c60 (ClusterName)
6. ManagedObjectReference:HostSystem[]--> host-70 (HostIP)

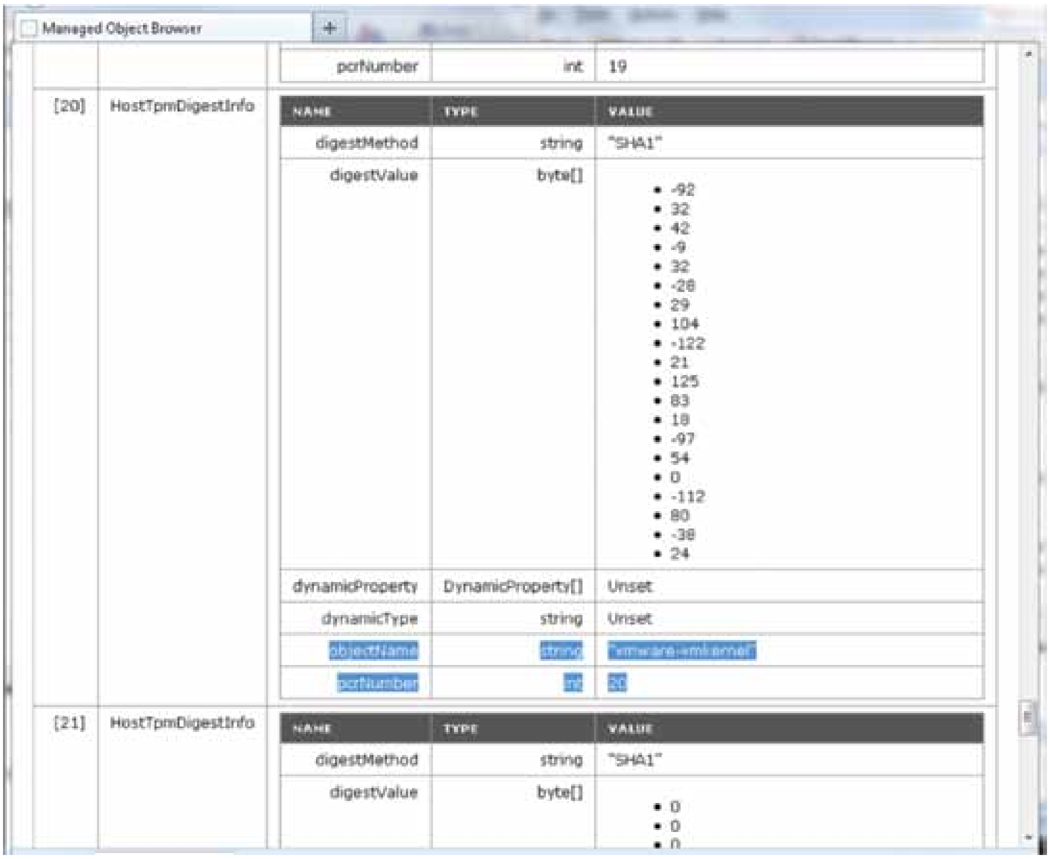


Data Object Type: HostRuntimeInfo
Parent Managed Object ID: **host-70**
Property Path: **runtime**

Properties

NAME	TYPE	VALUE
bootTime	dateTime	"2012-07-13T19:09:13.635740Z"
connectionState	HostSystemConnectionState	"connected"
dasHostState	ClusterDasFdmHostState	Unset
dynamicProperty	DynamicProperty[]	Unset
dynamicType	string	Unset
healthSystemRuntime	HealthSystemRuntime	healthSystemRuntime
inMaintenanceMode	boolean	false
powerState	HostSystemPowerState	"poweredOn"
standbyMode	string	"none"
tpmPcrValues	HostTpmDigestInfo[]	tpmPcrValues

7. HostRuntimeInfo --> runtime
8. HostTpmDigestInfo[]-->tpmPcrValues
9. Search for ”vmware-vmkernel” (Should be under: **pcrNumber int 20**)



pcrNumber	int	19

[20] HostTpmDigestInfo

NAME	TYPE	VALUE
digestMethod	string	"SHA1"
digestValue	byte[]	• -92 • 32 • 42 • -9 • 32 • -28 • 29 • 104 • -122 • 21 • 125 • 83 • 18 • -97 • 54 • 0 • -112 • 80 • -38 • 24
dynamicProperty	DynamicProperty[]	Unset
dynamicType	string	Unset
objectName	string	"vmware-vmkernel"
pcrNumber	int	20

[21] HostTpmDigestInfo

NAME	TYPE	VALUE
digestMethod	string	"SHA1"
digestValue	byte[]	• 0 • 0 • 0

ICB Trusted Cloud Deployment

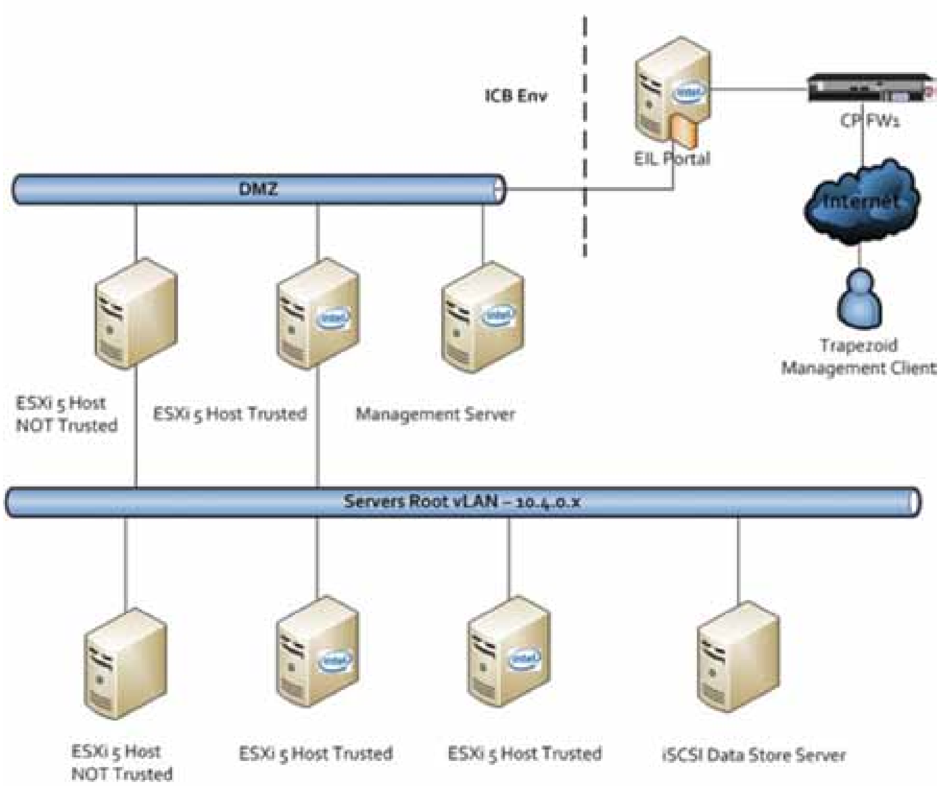


Figure 1: Physical cloud infrastructure

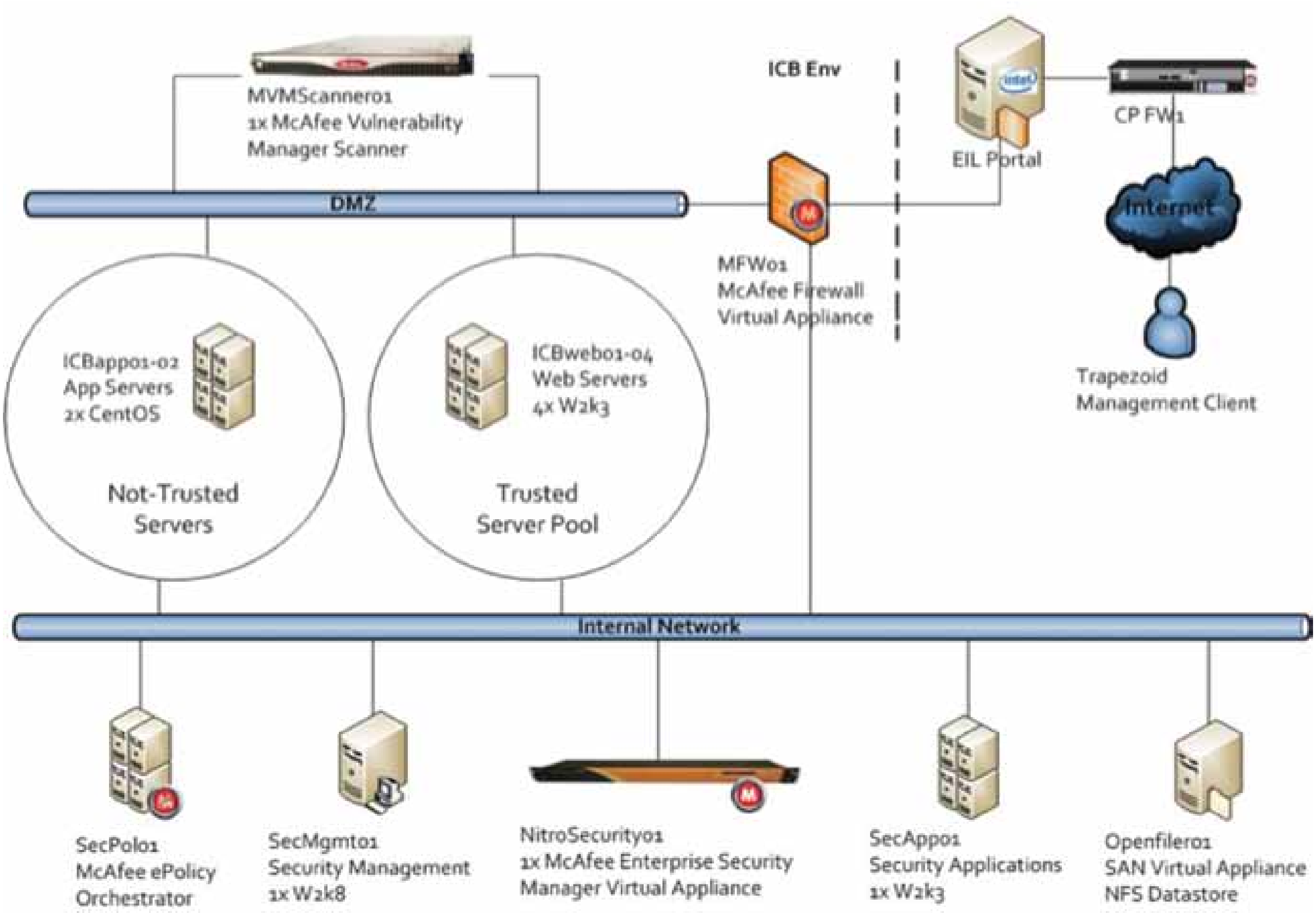


Figure 2: Virtual cloud infrastructure

McAfee Security Management Platform

McAfee's Security Management Platform suite of products enable security administrators to manage and protect without boundaries and gain visibility into the security posture across your entire infrastructure. Get risk-aware visibility and rapid response across your entire IT environment, and assess changing risk through real-time correlation of evolving threats correlated to events, users, systems, data, and countermeasures within your organization. With the complete McAfee security suite, administrators can create a security command and control core that spans devices, applications, networks, and databases.

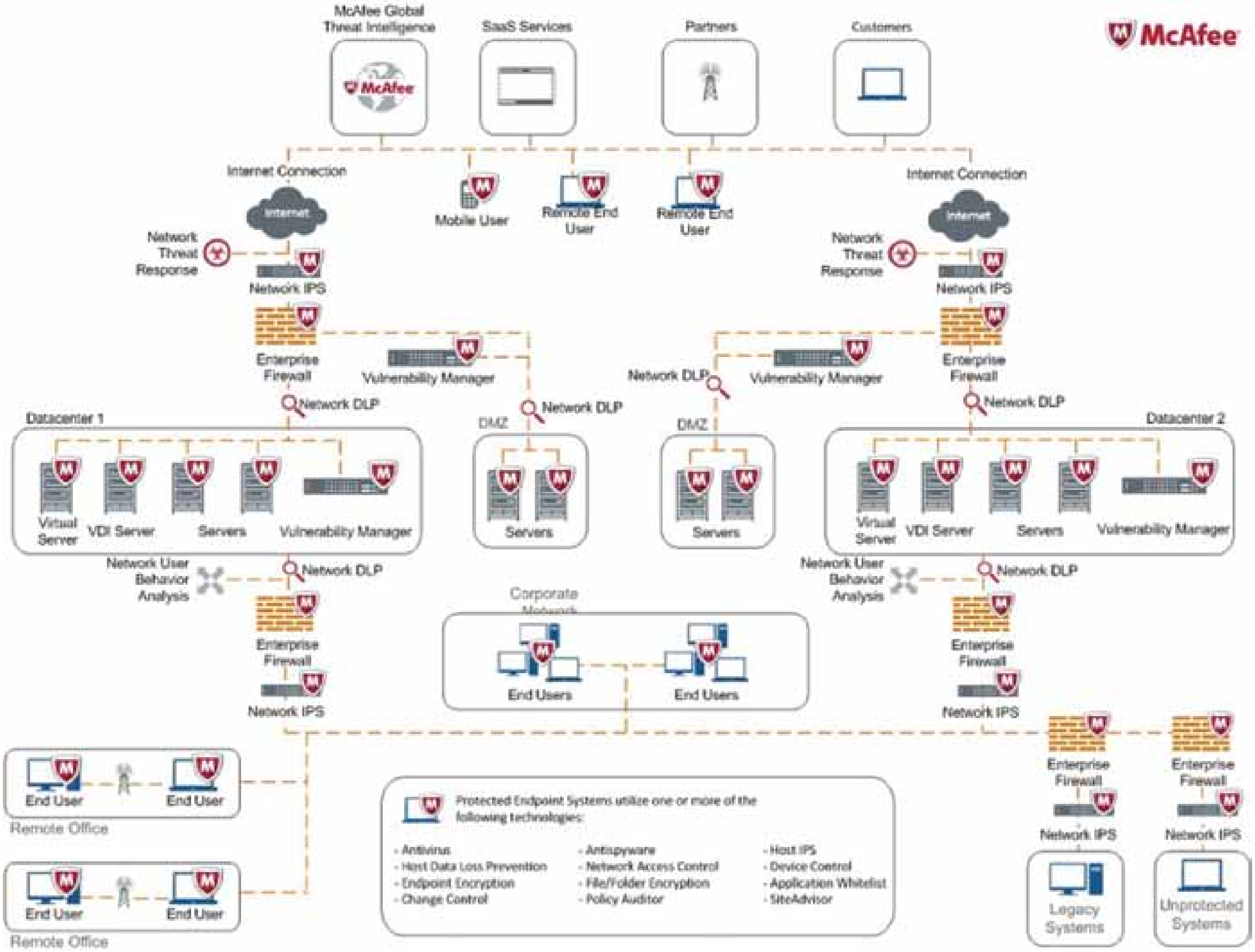


Figure 3: McAfee Security Management Platform suite of products

McAfee ePolicy Orchestrator

The McAfee ePolicy Orchestrator (ePO) server is at the heart the McAfee solution, delivering a coordinated, proactive defense against malicious threats and attacks for the enterprise. As the distributed component of ePolicy Orchestrator, the ePO management agent or "Common Framework" is the autonomous link between the security manager and point solutions on every managed host. As its name implies, the Common Framework allows for a single ePO agent to effectively manage, monitor, and update multiple complementary security products, including those from other vendors. The ePO agent is a vehicle of information and enforcement between the ePolicy Orchestrator Security Manager and each managed system. For each of the managed systems, the agent retrieves updates, executes scheduled tasks, enforces policies, and forwards properties and events to the Security Manager. With scalability in mind, the independent nature of the ePO agent (security manager does not need to regulate/initiate contact with the agent) allows the ePolicy Orchestrator Security Manager Solution to scale for use in large enterprise environments, with up to 250,000 individual managed hosts reporting to a single security manager.

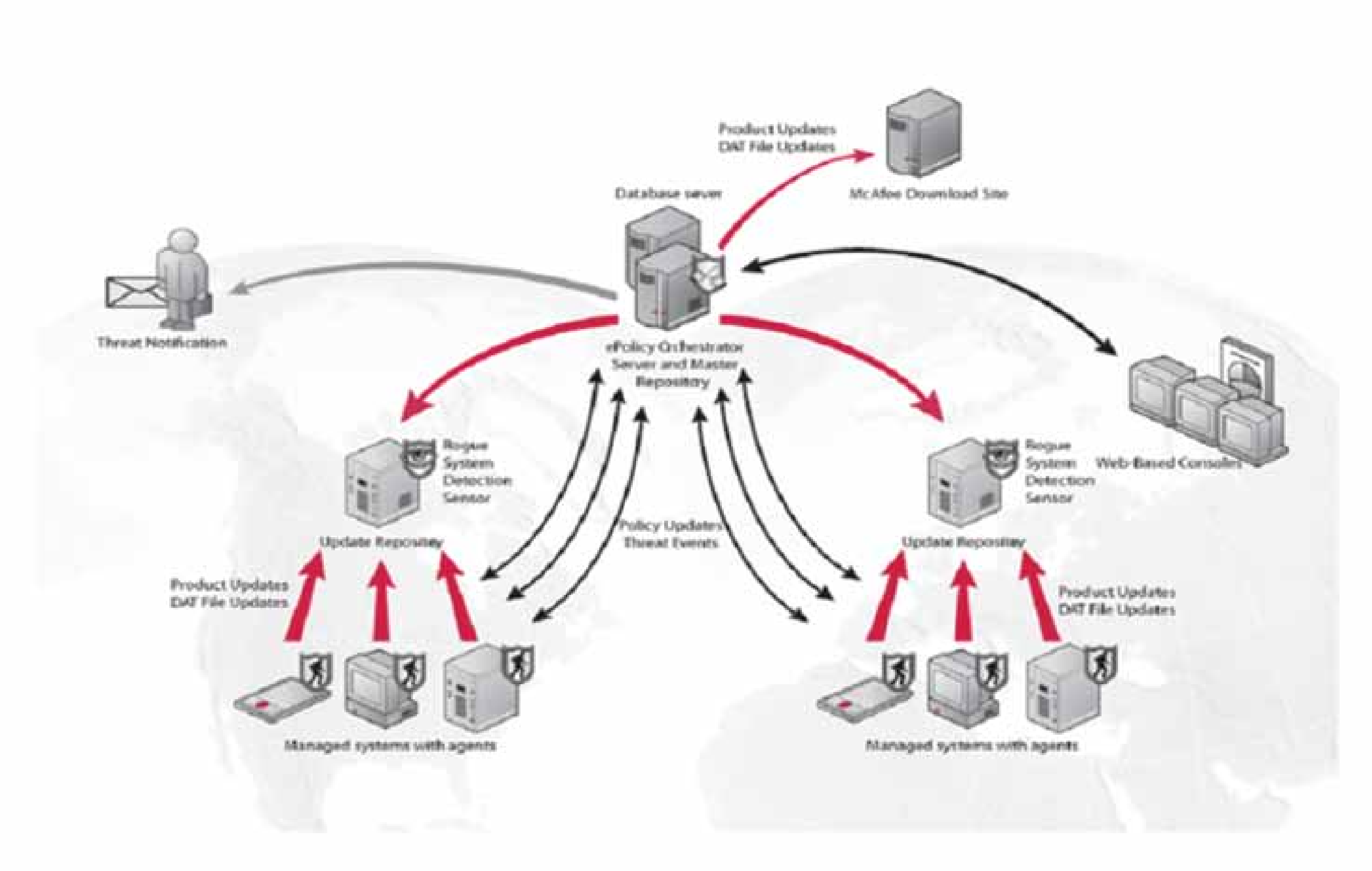


Figure 4: McAfee ePolicy Orchestrator

McAfee Vulnerability Manager

McAfee Vulnerability Manager finds and prioritizes security vulnerabilities and policy violations on your network. It balances asset criticality with vulnerability severity, enabling you to focus protection on your most important assets. McAfee Vulnerability Manager provides fast, precise, and complete insights into vulnerabilities on all of your networked assets. Easy-to-implement Vulnerability Manager readily scales to suit networks from hundreds to millions of nodes. Nonstop global research helps you stay ahead of evolving threats and new vulnerabilities. A single, actionable, correlated view of your weaknesses and the patented FoundScore risk formula helps you direct remediation efforts where they are needed most. Vulnerability Manager features include:

- Priority-based auditing and remediation — Combines vulnerability, severity, and asset criticality information to quickly identify, rank, and address violations and vulnerabilities on networked systems and devices.
- Proof of “not vulnerable” — A major requirement of auditors is to prove that you’re not vulnerable to threats, which is a significant attribute of McAfee Vulnerability Manager.
- New threat identification and correlation — Automatically ranks the risk potential of new threats by correlating events to your asset and vulnerability data.
- Policy auditing and compliance assessments — Defines values of policy checks and determines whether your organization complies with major regulations. An easy-to-use wizard gives you templates for SOX, FISMA, HIPAA, PCI, and more.
- Flexible reporting — Categorizes data by asset or network, and uses powerful filters to select and organize results in your reports. You can even create reports while scans are running.
- Broad and deep content coverage — Performs authenticated and unauthenticated checks, automatically updated 24/7 by McAfee Labs, one of the world’s top threat research center. This helps you delve deep into operating systems and network devices to find vulnerabilities and policy violations.

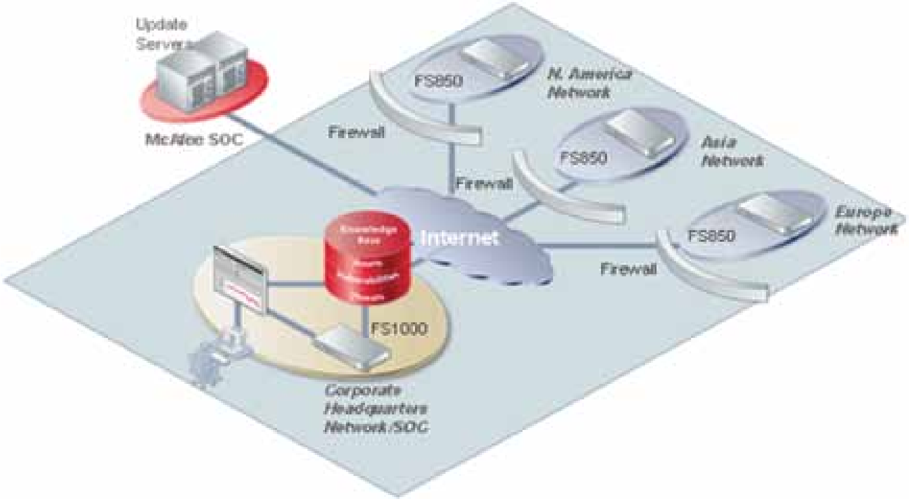


Figure 4: McAfee Vulnerability Manager

McAfee Enterprise Security Manager (ESM)

McAfee Enterprise Security Manager (ESM) provides the speed and rich context required to identify critical threats, respond quickly, and easily address compliance requirements. Continuous global threat and enterprise risk feeds deliver adaptive and autonomous risk management, allowing remediation of threats and compliance reporting in minutes instead of hours. The McAfee Security Information and Event Management (SIEM) system consists of several integrated components. All McAfee SIEM systems require at least one McAfee Enterprise Security Manager for information analysis and reporting, and one McAfee Event Receiver for information collection. Additional optional components may be added to the McAfee SIEM system as needed, including the McAfee Enterprise Log Manager (ELM) for long-term log retention, McAfee Application Data Monitor (ADM) for application session analysis and monitoring, McAfee Database Event Monitor (DEM) for database transaction monitoring and auditing, McAfee Advanced Correlation Engine (ACE) to provide dedicate correlation logic, and McAfee Intrusion Prevention System (IPS) for active network protection.

McAfee Advanced Correlation Engine (ACE)

McAfee ACE provides advanced event correlation to any McAfee ESM deployment. McAfee ACE appliances supplement McAfee ESM's existing event correlation capabilities by providing two dedicated correlation engines. McAfee ACE can be deployed in either real-time or historical modes. When operating in real-time mode, events are analyzed as they are collected for immediate threat and risk detection. In historical mode, any available data collected by McAfee SIEM can be "replayed" through either or both correlation engines, for recursive threat and risk detection. McAfee ACE provides the necessary processing horsepower to support this new level of correlation across an entire enterprise, and can easily scale to accommodate even the largest networks. And because McAfee ACE is a standalone appliance, there's no performance impact on the SIEM in terms of event collection and event management – allowing you to fully utilize all of McAfee ACE's correlation capabilities without compromise.

McAfee Database Event Monitor (DEM)

McAfee DEM is a complete database protection solution that delivers non-intrusive, detailed security logging by monitoring all access to sensitive corporate and customer data. McAfee DEM's pre-defined rules and reports, privacy-friendly logging features and encrypted, time-stamped files make it easy to comply with the specific data access regulations required by PCI-DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX and others. McAfee Event Receivers cache event and flow data locally to ensure uninterrupted data collection in the event that there is a network failure between the Receiver and one or more ESM appliances.

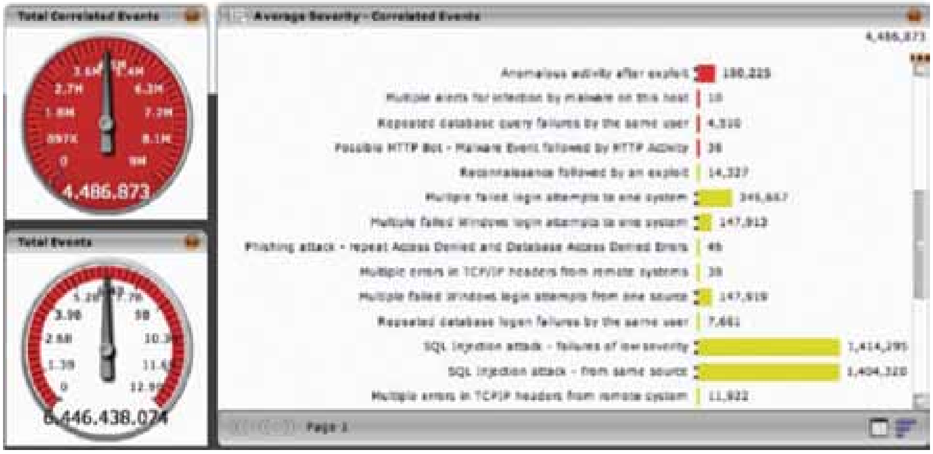

Total Correlated Events
0
897K
1.8M
2.7M
3.6M
4.5M
5.4M
6.3M
7.2M
8.1M
9M
4.486.873
Total Events
0
1.3B
2.6B
3.9B
5.2B
7.7B
9B
10.3B
11.6B
12.9B
6.446.438.074
Average Severity - Correlated Events
4,486,873
Anomalous activity after exploit
190,223
Multiple alerts for infection by malware on this host
10
Repeated database query failures by the same user
4,310
Possible HTTP Bot - Malware Event followed by HTTP Activity
38
Reconnaissance followed by an exploit
14,327
Multiple failed login attempts to one system
345,667
Multiple failed Windows login attempts to one system
147,912
Phishing attack - repeat Access Denied and Database Access Denied Errors
46
Multiple errors in TCP/IP headers from remote systems
39
Multiple failed Windows login attempts from one source
147,919
Repeated database logon failures by the same user
7,661
SQL Injection attack - failures of low severity
1,414,295
SQL Injection attack - from same source
1,404,320
Multiple errors in TCP/IP headers from remote system
11,922
Page 1

Figure 5: McAfee Enterprise Security Manager

Trapezoid Trust Control Suite (TCS)

Trapezoid TCS provides real-time events and associated metadata to a variety of platform, networking, and security devices. TCS events and data enable connected environments to have visibility and make intelligent decisions by providing more information than is available in standalone environment. For supported environments that utilize Intel TXT as a component of the computer platform, TCS provides data on the BIOS, flash-able platform code, hypervisor, and loadable kernel modules. Any changes in the code are immediately communicated. TCS also provides information on which virtual systems are running on Intel TXT hardware and real-time notification events for changes in trust status.

TCS provides information and platform trust data that is updated in real time and on a regular periodic basis in bulk. The combination provides status and change events which can be used for reporting and automated responses. Once installed and configured, the TCS McAfee ePO Extension establishes a trusted connection to the TCS server. Administrators can send alerts, open trouble tickets, run queries, update policies, etc. Used in conjunction with a security monitoring platform like McAfee's ePO or SIEM products, TCS can serve as a robust monitoring tool to validate, alert, and proactively block activities based on any changes in Intel TXT values.

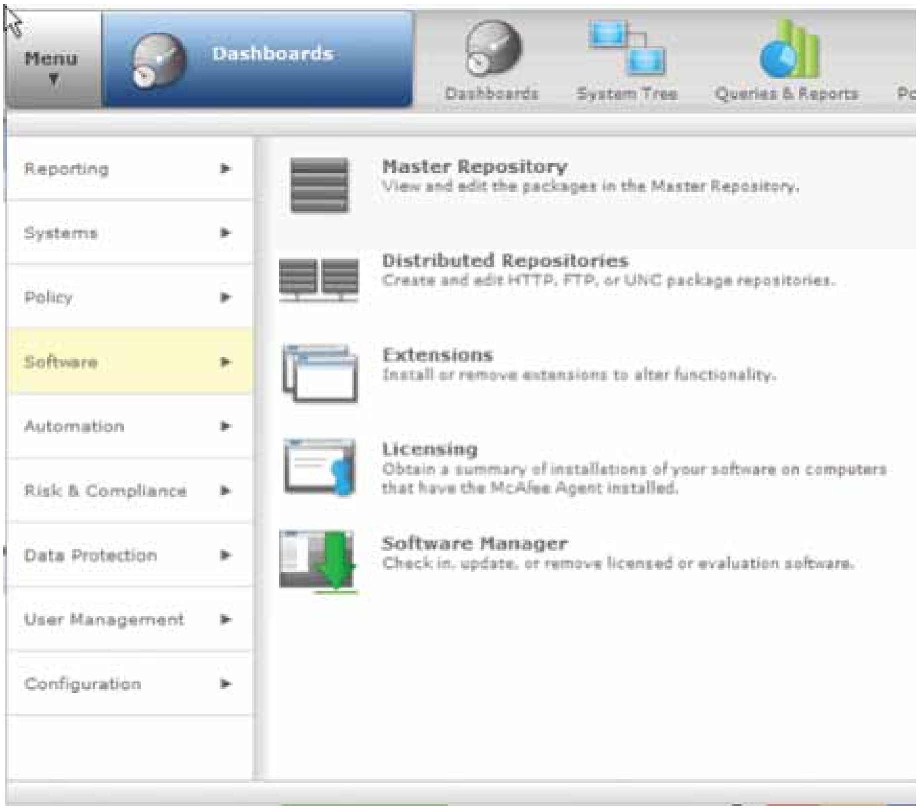
TCS Virtual Appliance

TCS Virtual Appliance installation and configuration steps:

1. Deploy TCS Virtual Appliance from the OVF template.
2. Download the TCS Virtual Appliance OVF to the vSphere client machine.
3. Launch the vSphere client and connect to the vCenter. In the VI Client, select "File" > "Virtual Appliance" > "Import" or in vSphere Client, select "File" > "Deploy OVF Template" and in the wizard, select the location to install/import the TCS OVF file.
4. Once the import is complete, TCS Virtual Appliance appears in the VMware vSphere Client inventory hierarchy for the selected VMware vCenter or ESX host.
5. In order to power-on the TCS virtual machine, from the vSphere Client Summary tab display, click the "Power on" command. Once the boot process is completed, the management network interface for TCS (eth0) will be set to DHCP by default or it can be manually configured.
6. At the console window, login as the user "tcsadmin" with the password "tcsadmin".
7. Change directories to the /tcs/vSphereagent: cd /tcs/vSphereagent
8. Edit the Config.xml file which requires the following configuration settings: vi config.xml
   a. vSphere Server IP and credentials
   b. McAfee ePO Server IP and credentials
   c. SIEM Server IP address as a Syslog destination
9. Save and exit text editor once the IP address and credential information has been updated in the TCS Config.xml file
10. Executive the TCS server from the current directory: java -jar trapezoidService.jar

McAfee ePO TCS Plug-in Configuration

1. Log into the ePO Web console using either the hostname or IP address of the server and the ports configured during installation (i.e.: https://10.x.x.x:8443).
2. Install the necessary components and extensions by going to the Menu > Software > and choosing either Master Repository or Extensions depending on the component being installed.



Master Repository
View and edit the packages in the Master Repository.

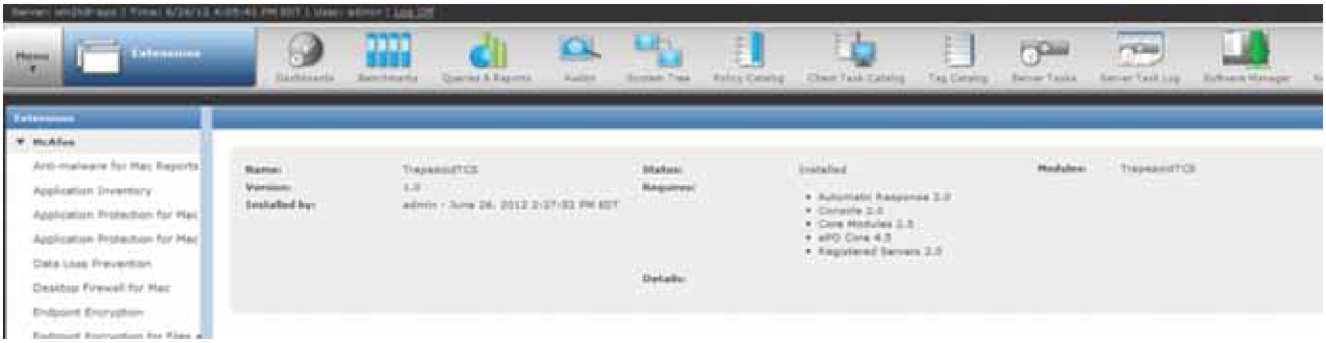
Distributed Repositories
Create and edit HTTP, FTP, or UNC package repositories.

Extensions
Install or remove extensions to alter functionality.

Licensing
Obtain a summary of installations of your software on computers that have the McAfee Agent installed.

Software Manager
Check in, update, or remove licensed or evaluation software.

3. The following packages and corresponding extensions should be installed using the respective installation instructions from the McAfee website:
   a. Trapezoid TCS



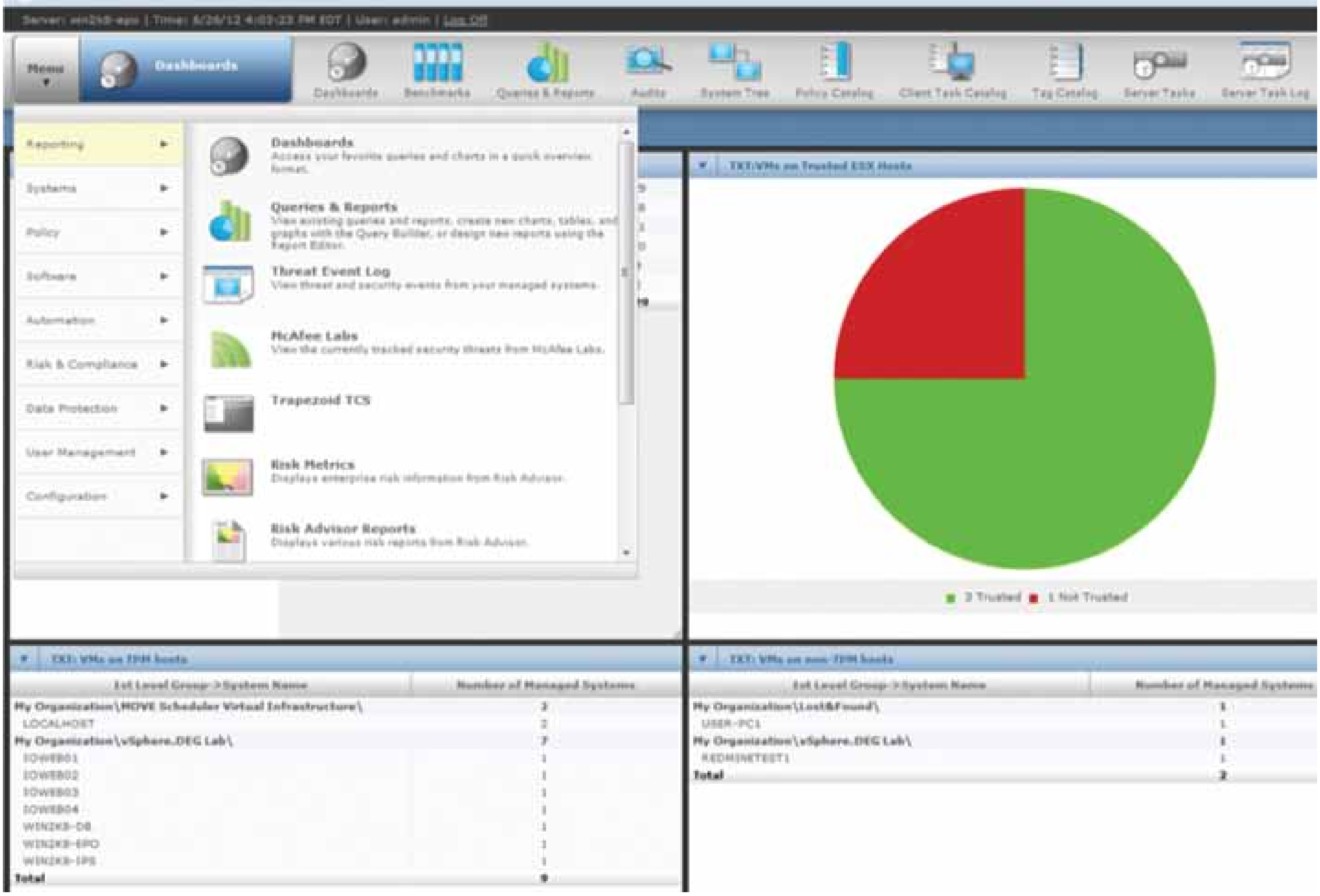
Name: TrapezoidTCS
Version: 1.0
Installed by: admin - June 26, 2012 2:27:51 PM EDT
Status: Installed
Requires:
- Automatic Response 2.0
- Console 2.0
- Core Modules 2.3
- ePO Core 4.5
- Registered Servers 2.0

Modules: TrapezoidTCS
Details:

   b. McAfee Agent
   c. McAfee VirusScan
   d. McAfee Host Intrusion Prevention
   e. McAfee Policy Auditor
   f. McAfee NAC Client
   g. McAfee Date Lost Prevention

4. The following are optional components depending on the type of PoC / Service-level being offered:
   a. McAfee Endpoint Encryption
   b. McAfee File & Folder Encryption
   c. McAfee Deep Defender
   d. Move Scheduler Agent

5. Verify proper Trapezoid TCS plug-in installation by clicking the Menu dropdown and selecting Trapezoid TCS.


Server: win2k8-epo | Time: 6/26/12 4:03:23 PM EDT | User: admin | Log Off
Menu
Dashboards
Dashboards
Benchmarks
Queries & Reports
Audits
System Tree
Policy Catalog
Client Task Catalog
Tag Catalog
Server Tasks
Server Task Log
Reporting
Systems
Policy
Software
Automation
Risk & Compliance
Data Protection
User Management
Configuration
Dashboards
Access your favorite queries and charts in a quick overview format.
Queries & Reports
View existing queries and reports, create new charts, tables, and graphs with the Query Builder, or design new reports using the Report Editor.
Threat Event Log
View threat and security events from your managed systems.
McAfee Labs
View the currently tracked security threats from McAfee Labs.
Trapezoid TCS
Risk Metrics
Displays enterprise risk information from Risk Advisor.
Risk Advisor Reports
Displays various risk reports from Risk Advisor.
TXT: VMs on Trusted ESX Hosts
🟩 3 Trusted 🟥 1 Not Trusted

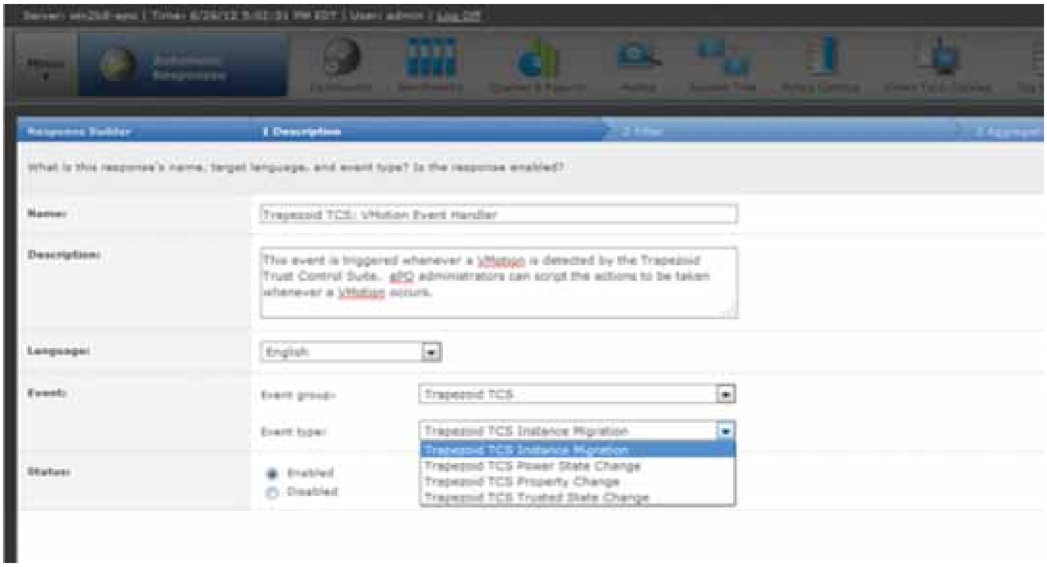
TXT: VMs on TPM hosts

1st Level Group->System Name	Number of Managed Systems
My Organization\MOVE Scheduler Virtual Infrastructure\	2
LOCALHOST	2
My Organization\vSphere.DEG Lab\	7
IOWEB01	1
IOWEB02	1
IOWEB03	1
IOWEB04	1
WIN2K8-DB	1
WIN2K8-EPO	1
WIN2K8-IPS	1
Total	9

TXT: VMs on non-TPM hosts

1st Level Group->System Name	Number of Managed Systems
My Organization\Lost&Found\	1
USER-PC1	1
My Organization\vSphere.DEG Lab\	1
REDMINETEST1	1
Total	2

6. Set up different types of Automated Responses and Alerts with Trapezoid TCS plug-in.


Server: win2k8-epo | Time: 6/26/12 5:02:31 PM EDT | User: admin | Log Off
Menu
Automatic Responses
Response Builder
1 Description
2 Filter
3 Aggregation

What is this response's name, target language, and event type? Is the response enabled?

Name: Trapezoid TCS: VMotion Event Handler

Description: This event is triggered whenever a VMotion is detected by the Trapezoid Trust Control Suite. ePO administrators can script the actions to be taken whenever a VMotion occurs.

Language: English

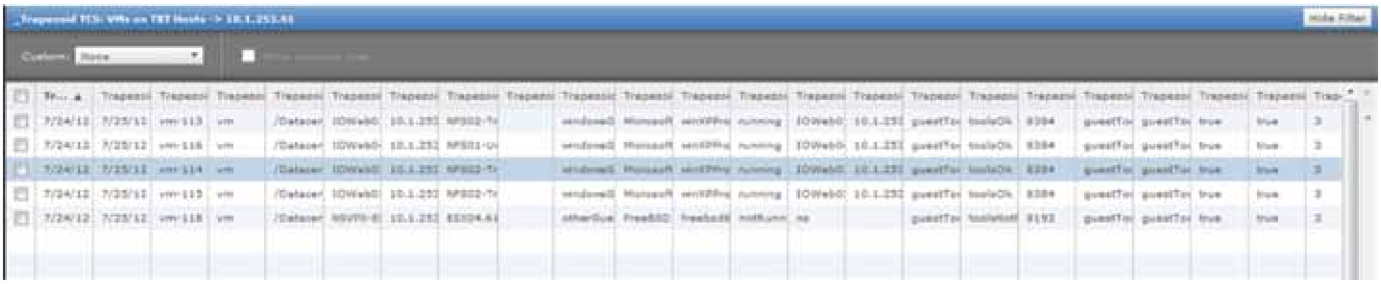
Event: Event group: Trapezoid TCS

Event type: Trapezoid TCS Instance Migration

- Trapezoid TCS Instance Migration
- Trapezoid TCS Power State Change
- Trapezoid TCS Property Change
- Trapezoid TCS Trusted State Change

Status: ● Enabled ○ Disabled

7. Drill down into the trust status of individual VMs, ESX Hosts, or Data Stores.



_Trapezoid TCS: VMs on TXT Hosts -> 10.1.253.41

Custom: None

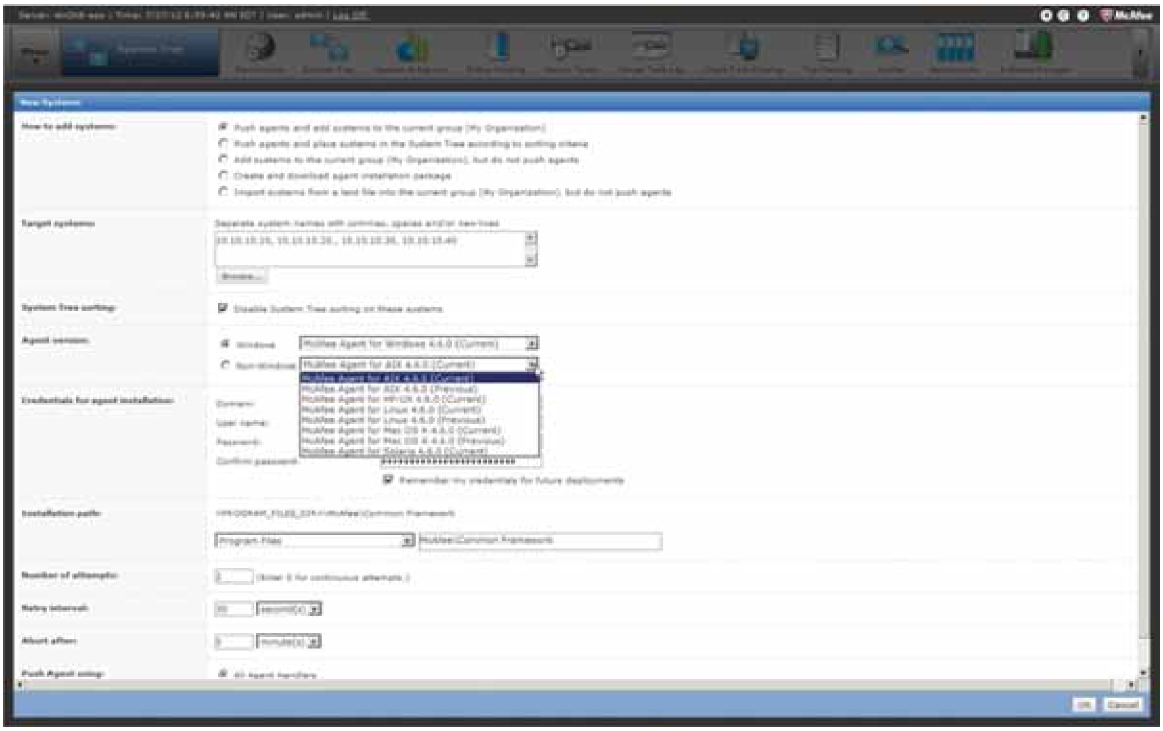
□	Tr... ▲	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trapezoi	Trap-
□	7/24/12	7/25/12	vm-113	vm	/Datacer	IOWeb0	10.1.25	NFS02-T		windowsG	Microsoft	winXPPro	running	IOWeb0	10.1.25	guestTo	toolsOk	8384	guestTo	guestTo	true	true	3
□	7/24/12	7/25/12	vm-116	vm	/Datacer	IOWeb0	10.1.25	NFS01-U		windowsG	Microsoft	winXPPro	running	IOWeb0	10.1.25	guestTo	toolsOk	8384	guestTo	guestTo	true	true	3
□	7/24/12	7/25/12	vm-114	vm	/Datacer	IOWeb0	10.1.25	NFS02-T		windowsG	Microsoft	winXPPro	running	IOWeb0	10.1.25	guestTo	toolsOk	8384	guestTo	guestTo	true	true	3
□	7/24/12	7/25/12	vm-115	vm	/Datacer	IOWeb0	10.1.25	NFS02-T		windowsG	Microsoft	winXPPro	running	IOWeb0	10.1.25	guestTo	toolsOk	8384	guestTo	guestTo	true	true	3
□	7/24/12	7/25/12	vm-118	vm	/Datacer	NSVM-E	10.1.25	ESXi04.6		otherGue	FreeBSD	freebsd	notRunn	no		guestTo	toolsNot	8192	guestTo	guestTo	true	true	3

NOTE: Some products may require several components depending on the OS types used in the environment.

McAfee ePO Agent Configuration

In order to prepare the environment, the next step will be to prepare the systems that will be monitored including the ePO server by deploying agents and installing the required components.

1. Go to Menu > Systems > System Tree and at the bottom left hand side of the page go to System Tree Actions >New Systems.
2. You may choose the option you prefer to deploy but the easiest way when there is only a handful of servers is to add the IP address of the server separated by server type (i.e. all Windows systems first, then Linux, etc).


New Systems

How to add systems:
- ● Push agents and add systems to the current group (My Organization)
- ○ Push agents and place systems in the System Tree according to sorting criteria
- ○ Add systems to the current group (My Organization), but do not push agents
- ○ Create and download agent installation package
- ○ Import systems from a text file into the current group (My Organization), but do not push agents

Target systems: Separate system names with commas, spaces and/or new lines
10.10.10.25, 10.10.10.30, , 10.10.10.35, 10.10.10.40
Browse...

System Tree sorting: ☑ Disable System Tree sorting on these systems

Agent version:
- ● Windows: McAfee Agent for Windows 4.6.0 (Current)
- ○ Non-Windows: McAfee Agent for AIX 4.6.0 (Current)

McAfee Agent for AIX 4.6.0 (Current)
McAfee Agent for AIX 4.6.0 (Previous)
McAfee Agent for HP-UX 4.6.0 (Current)
McAfee Agent for Linux 4.6.0 (Current)
McAfee Agent for Linux 4.6.0 (Previous)
McAfee Agent for Mac OS X 4.6.0 (Current)
McAfee Agent for Mac OS X 4.6.0 (Previous)
McAfee Agent for Solaris 4.6.0 (Current)

Credentials for agent installation:
Domain:
User name:
Password:
Confirm password: ••••••••••••••••••••••••
☑ Remember my credentials for future deployments

Installation path: <PROGRAM_FILES_DIR>\McAfee\Common Framework
Program Files | McAfee\Common Framework

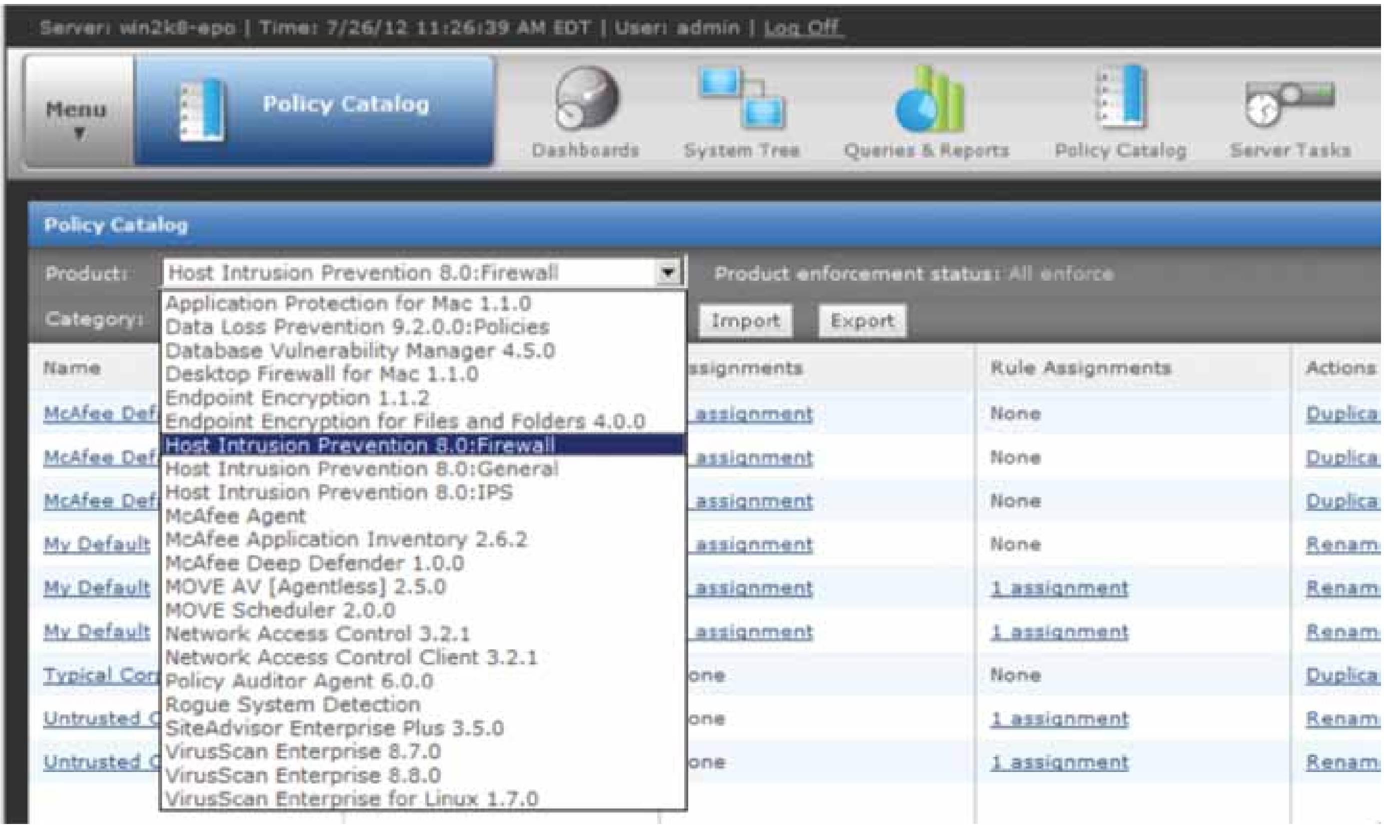
Number of attempts: 1 (Enter 0 for continuous attempts.)

Retry interval: 30 second(s)

Abort after: 5 minute(s)

Push Agent using: ● All Agent Handlers

3. You will need to configure the policies either by going to Menu > Policies > Policy Catalog or you may click the Policy Catalog in the top menu bar. From the drop down list choose the component you want to configure and click in the specific policy you want to change or you may import a previously exported policy.



Menu ▼
Policy Catalog
Dashboards
System Tree
Queries & Reports
Policy Catalog
Server Tasks
Import
Export
Application Protection for Mac 1.1.0
Data Loss Prevention 9.2.0.0:Policies
Database Vulnerability Manager 4.5.0
Desktop Firewall for Mac 1.1.0
Endpoint Encryption 1.1.2
Endpoint Encryption for Files and Folders 4.0.0
Host Intrusion Prevention 8.0:Firewall
Host Intrusion Prevention 8.0:General
Host Intrusion Prevention 8.0:IPS
McAfee Agent
McAfee Application Inventory 2.6.2
McAfee Deep Defender 1.0.0
MOVE AV [Agentless] 2.5.0
MOVE Scheduler 2.0.0
Network Access Control 3.2.1
Network Access Control Client 3.2.1
Policy Auditor Agent 6.0.0
Rogue System Detection
SiteAdvisor Enterprise Plus 3.5.0
VirusScan Enterprise 8.7.0
VirusScan Enterprise 8.8.0
VirusScan Enterprise for Linux 1.7.0

Server: win2k8-epo | Time: 7/26/12 11:26:39 AM EDT | User: admin | Log Off

Policy Catalog

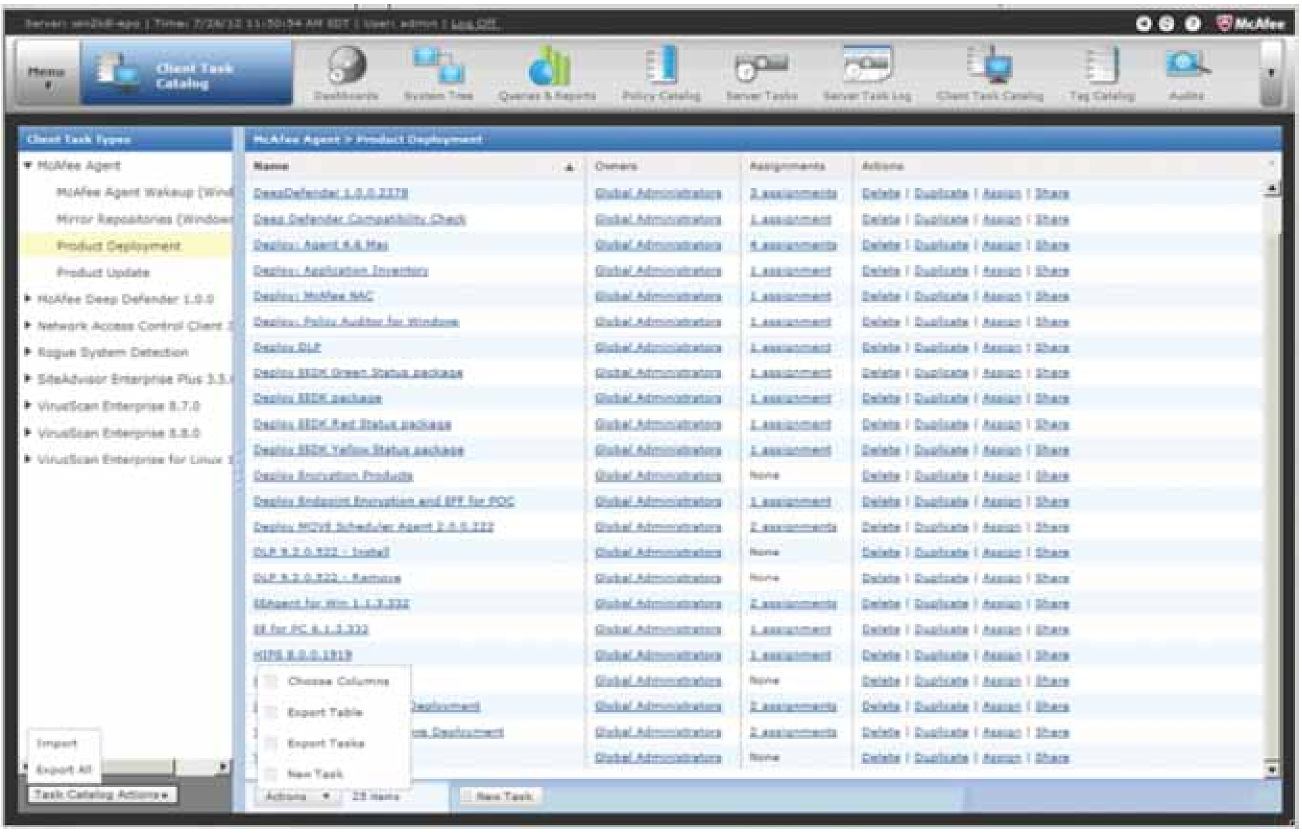
Product: Host Intrusion Prevention 8.0:Firewall

Product enforcement status: All enforce

Category:

Name	ssignments	Rule Assignments	Actions
McAfee Def	assignment	None	Duplica
McAfee Def	assignment	None	Duplica
McAfee Def	assignment	None	Duplica
My Default	assignment	None	Renam
My Default	assignment	1 assignment	Renam
My Default	assignment	1 assignment	Renam
Typical Cor	one	None	Duplica
Untrusted C	one	1 assignment	Renam
Untrusted C	one	1 assignment	Renam

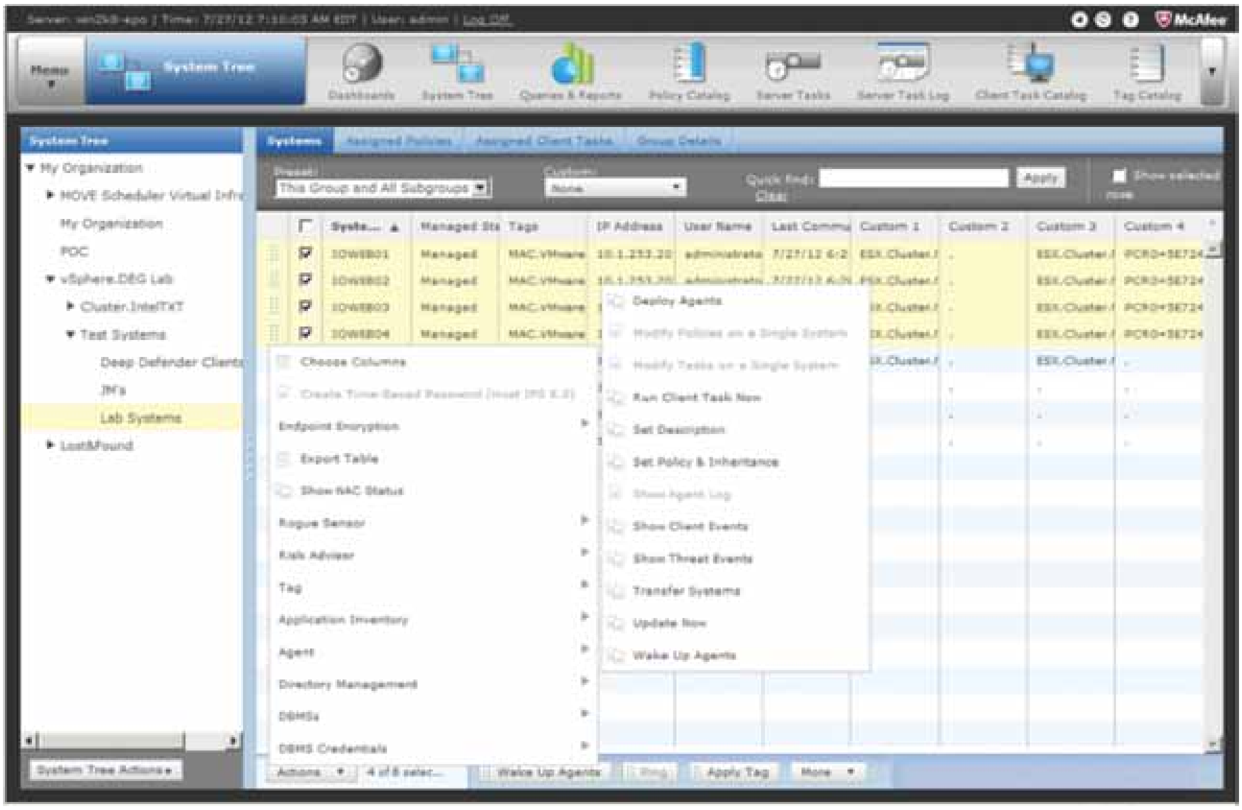
4. Go to Client Task Catalog from Menu > Policy > Client Task Catalog and configure the new policies or import a previously exported catalog.



McAfee Agent > Product Deployment

Name	Owners	Assignments	Actions
DeepDefender 1.0.0.2278	Global Administrators	3 assignments	Delete | Duplicate | Assign | Share
Deep Defender Compatibility Check	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy: Agent 4.6 Mac	Global Administrators	4 assignments	Delete | Duplicate | Assign | Share
Deploy: Application Inventory	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy: McAfee NAC	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy: Policy Auditor for Windows	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy DLP	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy EEDK Green Status package	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy EEDK package	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy EEDK Red Status package	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy EEDK Yellow Status package	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy Encryption Products	Global Administrators	None	Delete | Duplicate | Assign | Share
Deploy Endpoint Encryption and EFF for POC	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
Deploy MOVE Scheduler Agent 2.0.0.222	Global Administrators	2 assignments	Delete | Duplicate | Assign | Share
DLP 9.2.0.322 - Install	Global Administrators	None	Delete | Duplicate | Assign | Share
DLP 9.2.0.322 - Remove	Global Administrators	None	Delete | Duplicate | Assign | Share
EEAgent for Win 1.1.3.332	Global Administrators	2 assignments	Delete | Duplicate | Assign | Share
EE for PC 6.1.3.332	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
HIPS 8.0.0.1919	Global Administrators	1 assignment	Delete | Duplicate | Assign | Share
[illegible]	Global Administrators	None	Delete | Duplicate | Assign | Share
[illegible] Deployment	Global Administrators	2 assignments	Delete | Duplicate | Assign | Share
[illegible] ne Deployment	Global Administrators	2 assignments	Delete | Duplicate | Assign | Share
[illegible]	Global Administrators	None	Delete | Duplicate | Assign | Share

5. After the Client Task Catalog, go to the System Tree and click on the Assigned Client Tasks tab to configure the Deployment task for all the components. Ensure you have chosen My Organization on the left hand side panel as the starting point.



□	Syste... ▲	Managed Sta	Tags	IP Address	User Name	Last Commu	Custom 1	Custom 2	Custom 3	Custom 4
☑	IOWEB01	Managed	MAC.VMware	10.1.253.20	administrato	7/27/12 6:2	ESX.Cluster.I	-	ESX.Cluster.I	PCR0=5E724
☑	IOWEB02	Managed	MAC.VMware	10.1.253.20	administrato	7/27/12 6:N	ESX.Cluster.I	-	ESX.Cluster.I	PCR0=5E724
☑	IOWEB03	Managed	MAC.VMware				X.Cluster.I	-	ESX.Cluster.I	PCR0=5E724
☑	IOWEB04	Managed	MAC.VMware				X.Cluster.I	-	ESX.Cluster.I	PCR0=5E724

6. Choose the correct task (i.e. McAfee Agent > Product Deployment > HIPS 8.x) and Run the Client Task.

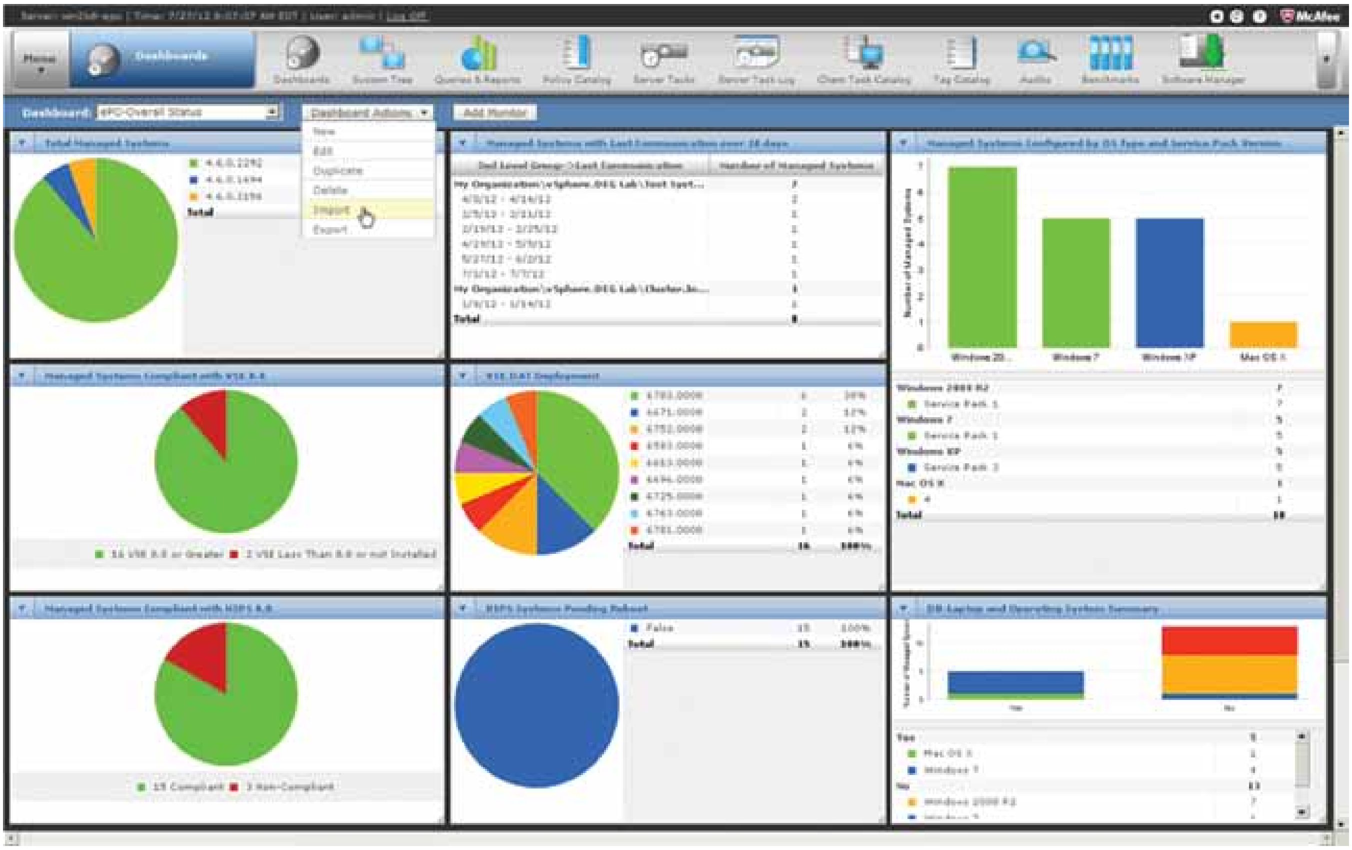
McAfee ePO Advanced Configuration

After the agents have been deployed, the software components installed, and the systems are tagged accordingly, you may start the creating or importing the different dashboards, reports and tasks.

1. You may create or import new dashboards and reports by going to Menu > Reporting > Queries and Reporting.

NOTE: Queries are the basis for the basis for both reports and dashboards. Whenever you export either a dashboard or a report, the corresponding queries will be exported.

2. You may add or import new dashboards under the Dashboard window > Dashboard Actions.

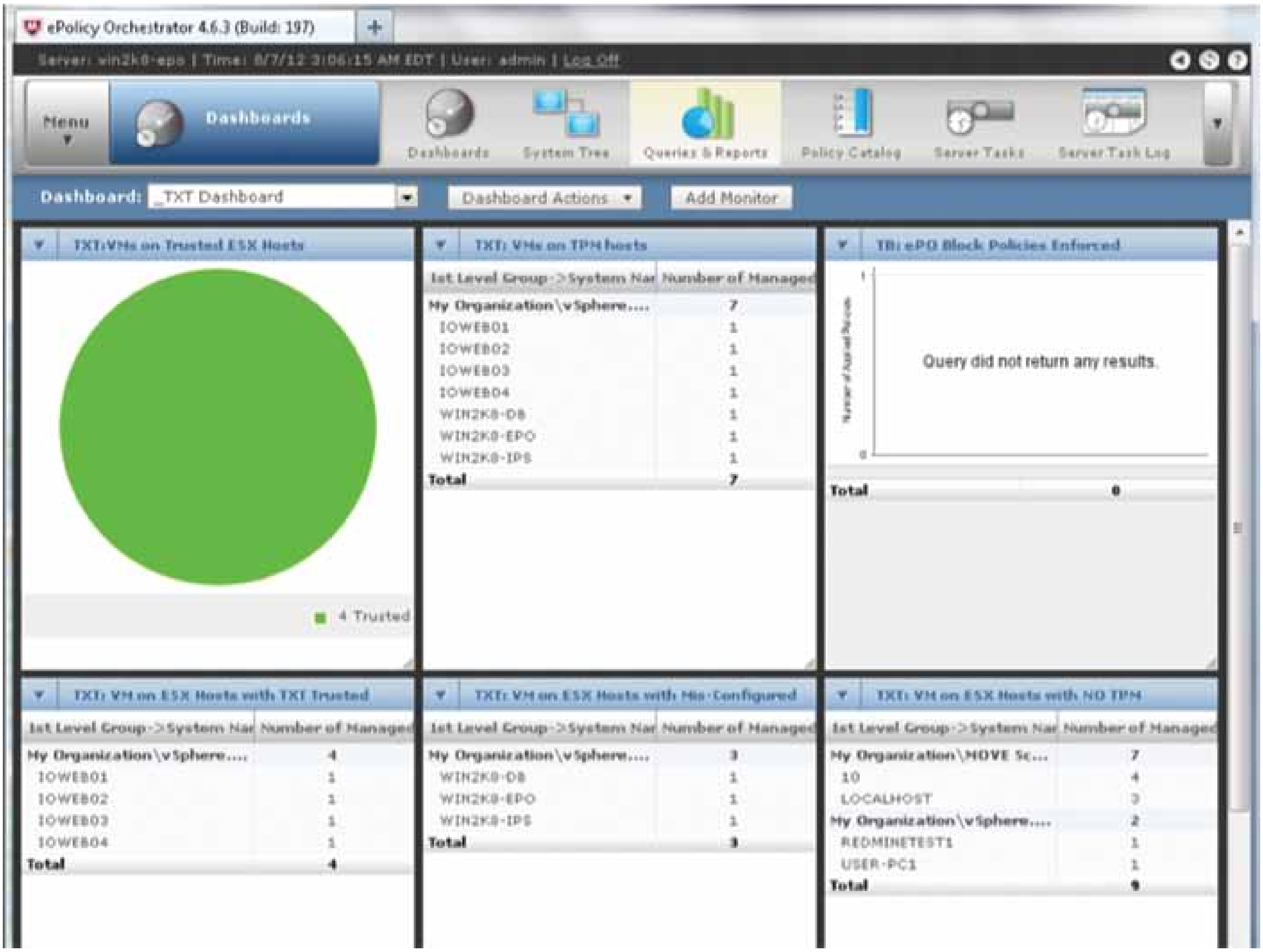


TCS Implementation Scenarios

Scenario 1 - Intel TXT Trusted Server Pool Validation

Trapezoid's TCS validates server hardware trust and integrity at the BIOS level leveraging Intel TXT, VMware ESX 5.0 vSphere API, and McAfee ePO. Intel TXT is a hardware security solution that protects IT infrastructures against attacks by validating the behavior of key components within a server during startup. Each time VMware ESXi boots, it measures the VMkernel with a subset of values and stores the measurements of the Trusted Platform Module. Verifying these measurements confirms a secure boot and ensures the integrity of the VMkernel and other components. TCS enables the administrator to enforce security policies based on a Trusted Server Pool and can alert when a Guest VM is vMotioned outside of the Trusted Server Pool.

1. Log into McAfee ePO with your browser.
2. Click on Dashboards and select the following ePO Dashboards:
   a. Trapezoid TCS
   b. TXT Dashboard



Server: win2k8-epo | Time: 8/7/12 3:06:15 AM EDT | User: admin | Log Off

Dashboard: _TXT Dashboard

TXT:VMs on Trusted ESX Hosts

TXT: VMs on TPM hosts

1st Level Group->System Nar	Number of Managed
My Organization\vSphere....	7
IOWEB01	1
IOWEB02	1
IOWEB03	1
IOWEB04	1
WIN2K8-DB	1
WIN2K8-EPO	1
WIN2K8-IPS	1
Total	7

TB: ePO Block Policies Enforced

Query did not return any results.

Total	0

TXT: VM on ESX Hosts with TXT Trusted

1st Level Group->System Nar	Number of Managed
My Organization\vSphere....	4
IOWEB01	1
IOWEB02	1
IOWEB03	1
IOWEB04	1
Total	4

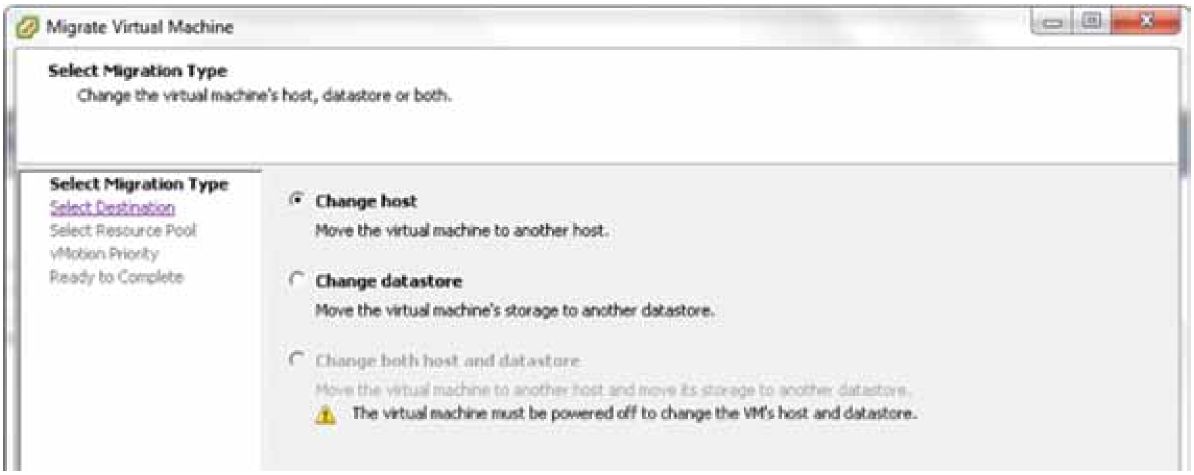
TXT: VM on ESX Hosts with Mis-Configured

1st Level Group->System Nar	Number of Managed
My Organization\vSphere....	3
WIN2K8-DB	1
WIN2K8-EPO	1
WIN2K8-IPS	1
Total	3

TXT: VM on ESX Hosts with NO TPM

1st Level Group->System Nar	Number of Managed
My Organization\MOVE Sc...	7
10	4
LOCALHOST	3
My Organization\vSphere....	2
REDMINETEST1	1
USER-PC1	1
Total	9

3. Validate which virtual machines have Intel TXT trusted boot enforced, which ones reside on an Intel TXT trusted server, and which systems are out of compliance.
4. vMotion a Guest VM from a Trusted ESX Host to Non-Trusted ESX Host.



Migrate Virtual Machine

Select Migration Type

Change the virtual machine's host, datastore or both.

● **Change host**

Move the virtual machine to another host.

○ **Change datastore**

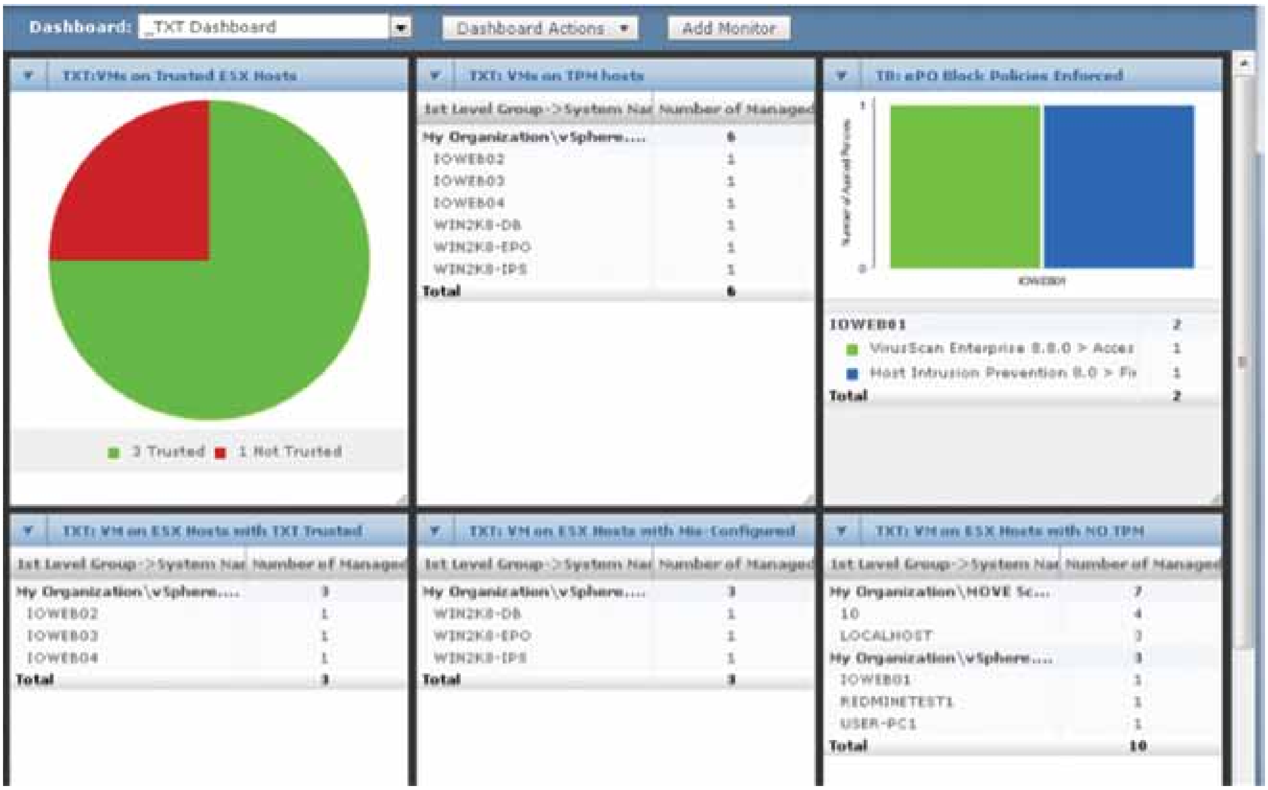
Move the virtual machine's storage to another datastore.

○ Change both host and datastore

Move the virtual machine to another host and move its storage to another datastore.

⚠ The virtual machine must be powered off to change the VM's host and datastore.

5. Return to the TCS and Intel TXT dashboards and validate which virtual machines have moved outside of the Trusted Server Pool and are currently running on a Non-Trusted server.



Dashboard: _TXT Dashboard
Dashboard Actions
Add Monitor
TXT:VMs on Trusted ESX Hosts
🟩 3 Trusted 🟥 1 Not Trusted
TB: ePO Block Policies Enforced
Number of Applied Policies
1
0
IOWEB01

TXT: VMs on TPM hosts

1st Level Group->System Nai	Number of Managed
My Organization\vSphere....	6
IOWEB02	1
IOWEB03	1
IOWEB04	1
WIN2K8-DB	1
WIN2K8-EPO	1
WIN2K8-IPS	1
Total	6

TB: ePO Block Policies Enforced

IOWEB01	2
🟩 VirusScan Enterprise 8.8.0 > Acces	1
🟦 Host Intrusion Prevention 8.0 > Fi	1
Total	2

TXT: VM on ESX Hosts with TXT Trusted

1st Level Group->System Nai	Number of Managed
My Organization\vSphere....	3
IOWEB02	1
IOWEB03	1
IOWEB04	1
Total	3

TXT: VM on ESX Hosts with Mis-Configured

1st Level Group->System Nai	Number of Managed
My Organization\vSphere....	3
WIN2K8-DB	1
WIN2K8-EPO	1
WIN2K8-IPS	1
Total	3

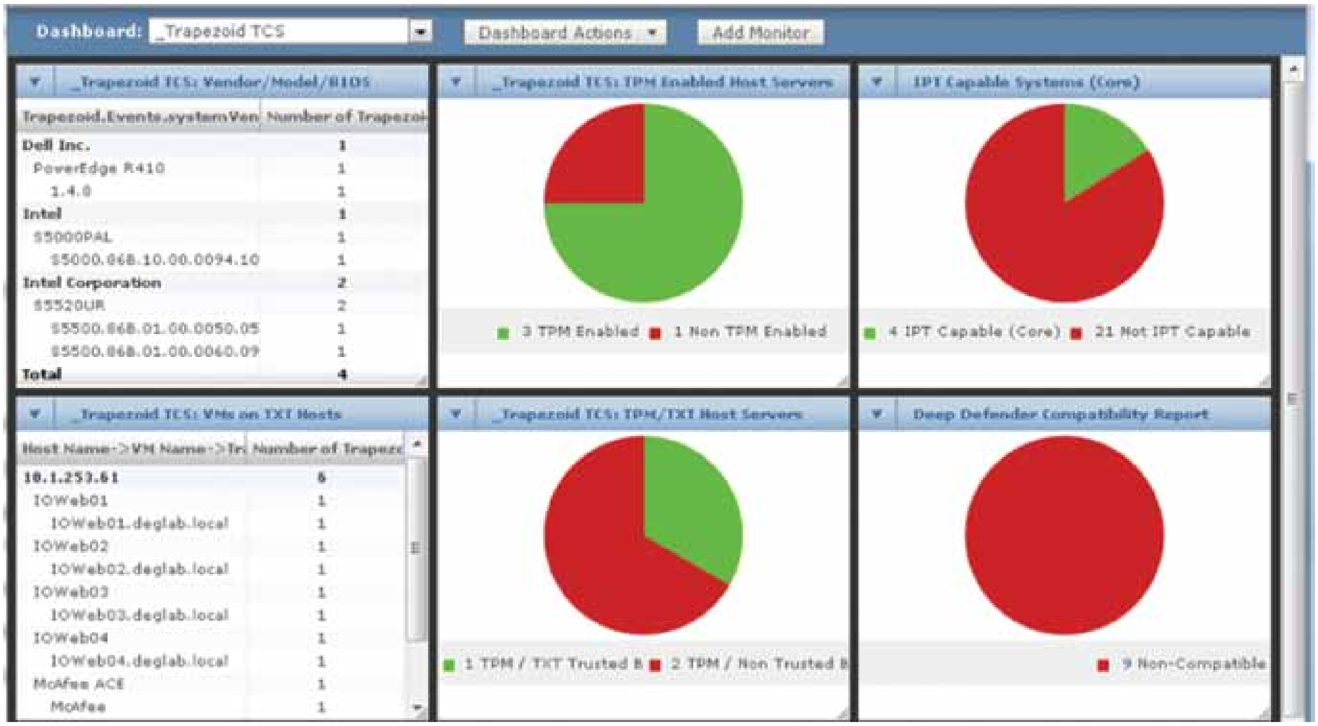
TXT: VM on ESX Hosts with NO TPM

1st Level Group->System Nai	Number of Managed
My Organization\MOVE Sc...	7
10	4
LOCALHOST	3
My Organization\vSphere....	3
IOWEB01	1
REDMINETEST1	1
USER-PC1	1
Total	10

Scenario 2 - Network Security Policy Enforcement

Trapezoid's TCS integrates with the McAfee ePO security agent to enforce HIPS, Firewall, and NAC policies on clients and servers based on Deep Defender hardware-assisted security and Intel TXT hardware trust values.

1. Log into McAfee ePO with your browser.
2. Click on Dashboards and select the following ePO Dashboards:
   a. Trapezoid TCS Dashboard



Dashboard: _Trapezoid TCS

_Trapezoid TCS: Vendor/Model/BIOS

Trapezoid.Events.systemVen	Number of Trapezoi
Dell Inc.	1
PowerEdge R410	1
1.4.0	1
Intel	1
S5000PAL	1
S5000.868.10.00.0094.10	1
Intel Corporation	2
S5520UR	2
S5500.868.01.00.0050.05	1
S5500.868.01.00.0060.09	1
Total	4

_Trapezoid TCS: VMs on TXT Hosts

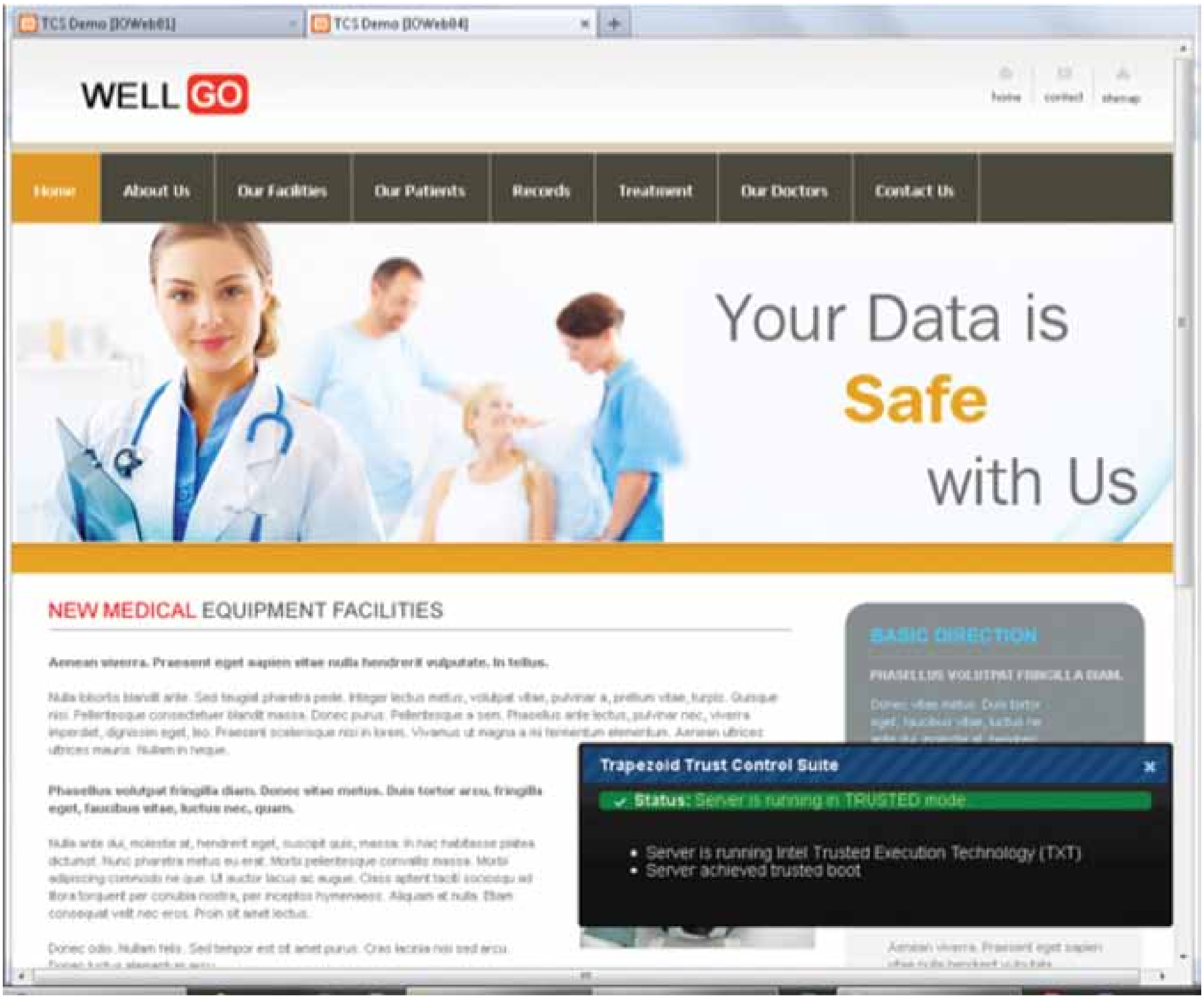
Host Name->VM Name->Tr	Number of Trapezc
10.1.253.61	6
IOWeb01	1
IOWeb01.deglab.local	1
IOWeb02	1
IOWeb02.deglab.local	1
IOWeb03	1
IOWeb03.deglab.local	1
IOWeb04	1
IOWeb04.deglab.local	1
McAfee ACE	1
McAfee	1

   b. TXT DD Dashboard
3. Verify the McAfee Security Agent is installed and running on each client HIPS/Firewall.
4. Connect to the sample web application running on a server that is within the Trusted Server Pool (those servers with Intel TXT enabled) i.e. ICBWeb01: http://10.x.x.x:4444/
5. vMotion Web server from an Trusted host to a Non-Trusted host.
6. Attempt to connect once again to the Web application when the Guest VM has been moved outside of the Trusted Server Pool.
7. The HIPS/Firewall Policy will be enforced and block the communications from the server-side.

Scenario 3 - Application Trust Awareness

Trapezoid's TCS integrates with Web applications that can be made aware of the underlying Intel TXT hardware-based trust status of the host the application server is running on. The application can implement security measures based on the level of trust a client or the server itself is determined to have. Lesser degrees of trust limit the output of the Web application based on awareness of client-side hardware security status and trusted server status.

1. Connect to the sample Web application running on ICBWeb01: http://10.x.x.x/med
2. Validate the Web application trust status with the TCS pop-up message showing a red, yellow, or green status based on the trusted boot status of the application server.



NEW MEDICAL EQUIPMENT FACILITIES

Aenean viverra. Praesent eget sapien vitae nulla hendrerit vulputate. In tellus.

Nulla lobortis blandit ante. Sed feugiat pharetra pede. Integer lectus metus, volutpat vitae, pulvinar a, pretium vitae, turpis. Quisque nisi. Pellentesque consectetuer blandit massa. Donec purus. Pellentesque a sem. Phasellus ante lectus, pulvinar nec, viverra imperdiet, dignissim eget, leo. Praesent scelerisque nisi in lorem. Vivamus ut magna a mi fermentum elementum. Aenean ultrices ultrices mauris. Nullam in neque.

Phasellus volutpat fringilla diam. Donec vitae metus. Duis tortor arcu, fringilla eget, faucibus vitae, luctus nec, quam.

Nulla ante dui, molestie at, hendrerit eget, suscipit quis, massa. In hac habitasse platea dictumst. Nunc pharetra metus eu erat. Morbi pellentesque convallis massa. Morbi adipiscing commodo ne que. Ut auctor lacus ac augue. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam et nulla. Etiam consequat velit nec eros. Proin sit amet lectus.

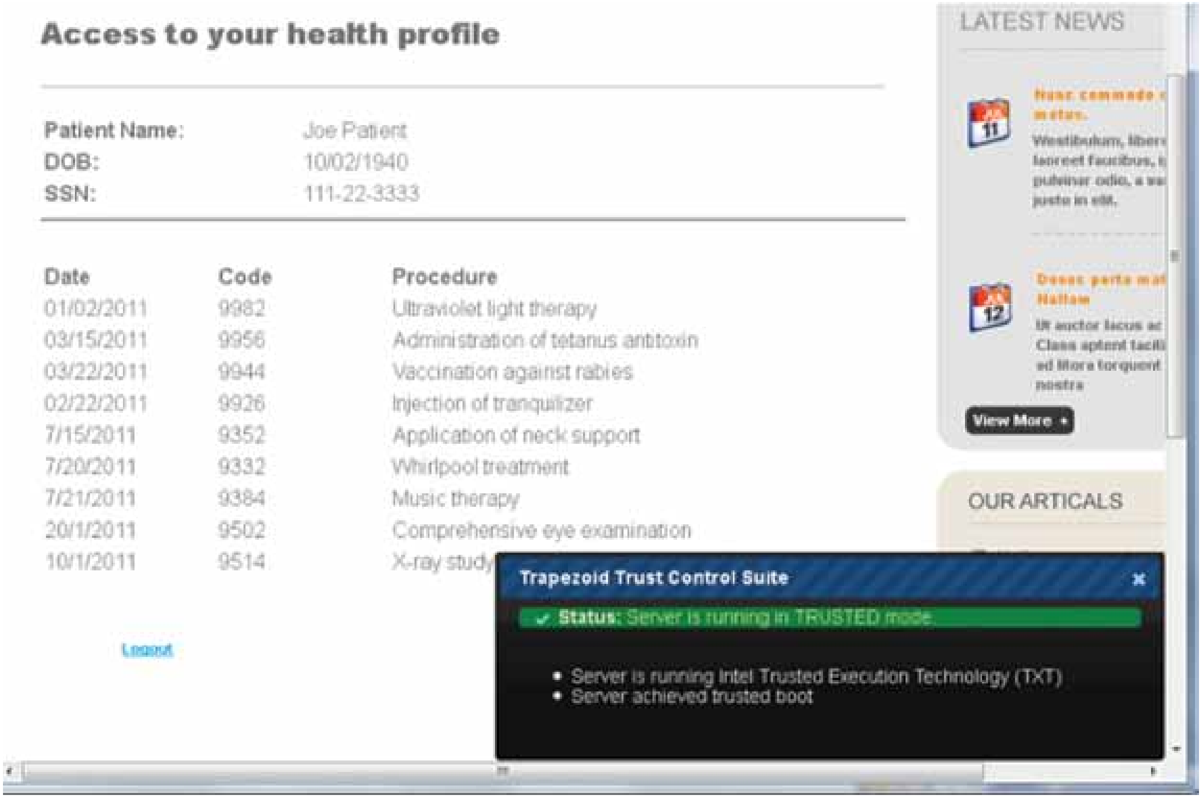
Donec odio. Nullam felis. Sed tempor est sit amet purus. Cras lacinia nisi sed arcu.

Trapezoid Trust Control Suite

✓ **Status:** Server is running in TRUSTED mode

- Server is running Intel Trusted Execution Technology (TXT)
- Server achieved trusted boot

3. Go to Records and log in to see all medical procedures performed on a fictitious patient records file.



Access to your health profile

Patient Name:	Joe Patient
DOB:	10/02/1940
SSN:	111-22-3333

Date	Code	Procedure
01/02/2011	9982	Ultraviolet light therapy
03/15/2011	9956	Administration of tetanus antitoxin
03/22/2011	9944	Vaccination against rabies
02/22/2011	9926	Injection of tranquilizer
7/15/2011	9352	Application of neck support
7/20/2011	9332	Whirlpool treatment
7/21/2011	9384	Music therapy
20/1/2011	9502	Comprehensive eye examination
10/1/2011	9514	X-ray study

Logout

LATEST NEWS

Nunc commodo metus.

Westibulum, liber laoreet faucibus, pulvinar odio, a va justo in elit.

Donec porta ma Nallam

Ut auctor lacus ac Class aptent tacit ad litora torquent nostra

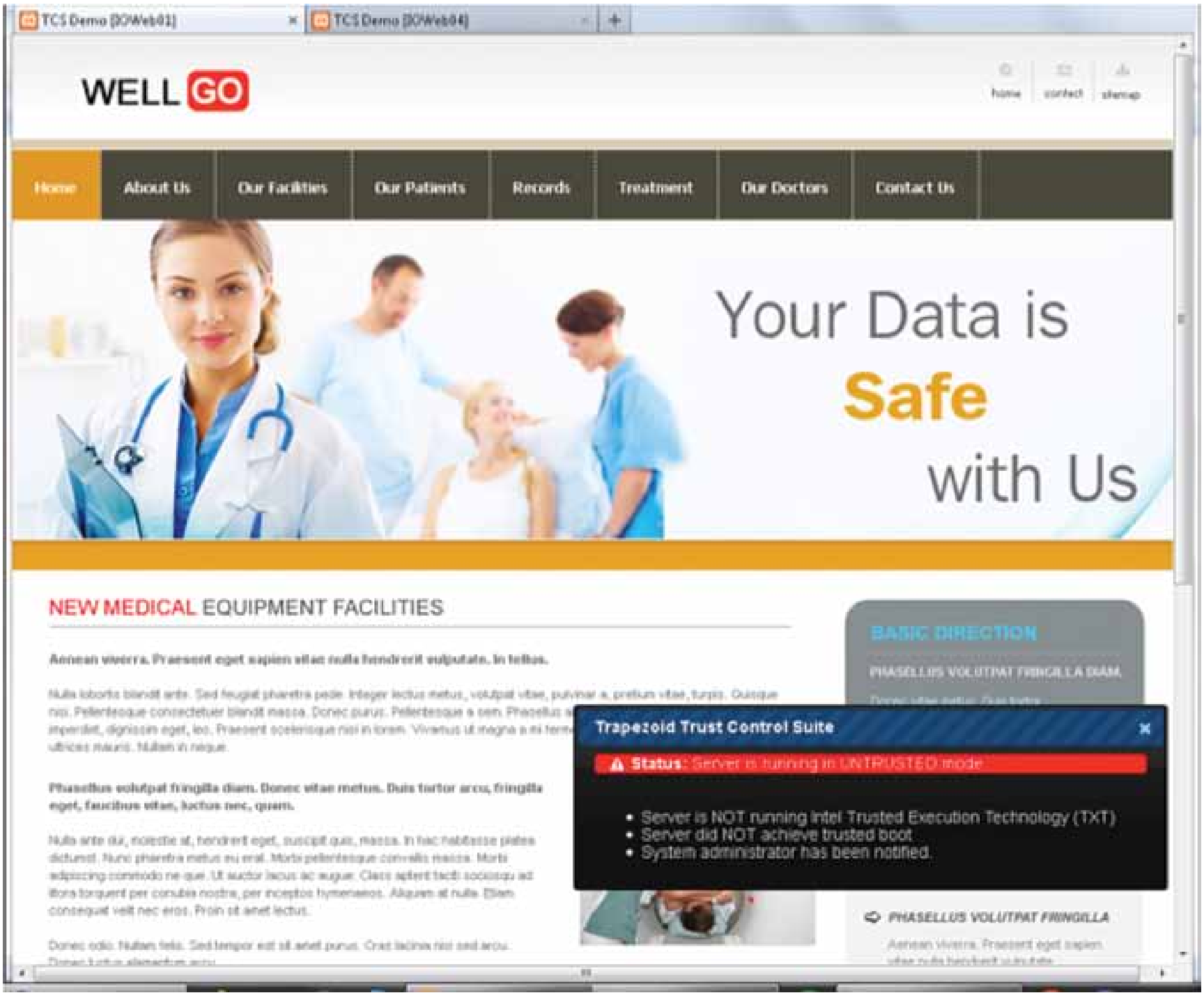
OUR ARTICALS

Trapezoid Trust Control Suite

✓ Status: Server is running in TRUSTED mode.

- Server is running Intel Trusted Execution Technology (TXT)
- Server achieved trusted boot

4. vMotion the application from an Trusted host to a Non-Trusted host.
5. Reconnect to the fictitious medical website and validate the Web application trust status with the TCS pop-up message showing a red, yellow, or green status based on the trusted boot status of the application server.



Trapezoid Trust Control Suite

Status: Server is running in UNTRUSTED mode

- Server is NOT running Intel Trusted Execution Technology (TXT)
- Server did NOT achieve trusted boot
- System administrator has been notified.

6. The sample medical Web application will not allow any logins because it is running in reduced functionality due to hardware-based trust awareness built into the application based on TCS trust data intelligence.

Open Data Center Usage Model Alignment

Open Data Center Alliance Overview

The Open Data Center Alliance (ODCA) was formed in 2010 as a consortium of global IT organizations to deliver a unified voice for emerging data center and cloud computing requirements. ODCA's mission is "to speed the migration to cloud computing by enabling the solution and service ecosystem to address IT requirements with the highest level of interoperability and standards."

The goal is to Identify customer requirements for corporate adoption and deployment of cloud computing. Defining usage models for these requirements based on open, industry-standard, multi-vendor solutions that support a vision of secure federation, automation, common management, and transparency. ODCA published eight usage models in June 2011 and since this time has delivered enhancements to existing usage models as well as published new usage models addressing additional customer requirements for the cloud. These member-defined requirements document the most pressing challenges and needed solutions for cloud deployment in four categories: Secure Federation, Automation, Common Management and Policy, and Transparency. In this reference architecture, we address two of the cornerstone Secure Federation usage models – Provider Assurance and Security Monitoring. The Provider Assurance and Security Monitoring usage models are used as a standards assurance of cloud security compliance.

ODCA Provider Assurance Usage Model

This usage model seeks to define requirements for standardized definitions of security levels within the cloud. Used with the companion ODCA usage model for Security Monitoring, it will enable cloud subscribers to make more informed choices on the levels of security they may want to adopt, based on the confidentiality, integrity, and availability requirements of their hosted solutions.

The intent for this usage model is to define the security requirements for cloud computing and implement a framework to assure against them. To do this, the usage model seeks to define minimum levels for cloud security within tiers. These tiers will provide offerings with increasing levels of security to meet the requirements of organizations that subscribe to cloud services.

These levels are:

- Bronze – Basic security
- Silver – Enterprise security equivalent
- Gold – Financial organization security equivalent
- Platinum – Military organization security equivalent

These usage model security requirements are mapped in the table below to the ODCA Test Cases and the McAfee Security Platform reference architecture.

Provider Assurance Usage Model Requirement	ODCA Test Case ID	Assurance Level	Security Platform
Antivirus and malware protection (with definition updates within 24 hours)	1. Vulnerability Management	Bronze	McAfee ePolicy Orchestrator (ePO)
Vulnerability management process exists and is fully tested to ensure no impact to target or application	1. Vulnerability Management	Bronze	McAfee Vulnerability Manager & McAfee ePolicy Orchestrator
Network and firewall isolation of Cloud-Subscriber systems with management	2. Network and Firewall Isolation	Bronze	McAfee Firewall / RHEL Firewall / SIEM
Physical access control into cloud data center	7. Integrity and Trust	Bronze	Policy Document Repository
Secure protocols used for remote administration (e.g., SSL, SSH, RDP, etc.)	1. Vulnerability Management	Bronze	McAfee Vulnerability Manager & McAfee ePolicy Orchestrator
All default passwords and guest access removed	1. Vulnerability Management 3. Identity Management	Bronze	McAfee Vulnerability Manager & McAfee ePolicy Orchestrator
Mandatory use of non-disclosure agreements (NDAs) for cloud provider staff	6. Confidentiality	Bronze	Policy Document Repository
Mandatory use of Information Technology Infrastructure Library (ITIL) processes for change, incident, and configuration management	7. Integrity and Trust	Bronze	Policy Document Repository
Identity management for subscriber assets	3. Identity Management 4. Security Information and Event Management	Bronze	McAfee Enterprise Security Manager
Data retention and deletion management	5. Data Retention and Deletion	Bronze	Policy Document Repository
Security incident and event monitoring	4. Security Information and Event Management	Bronze	McAfee Enterprise Security Manager
Network intrusion prevention; updates applied within 48 hours	2. Network and Firewall Isolation	Silver	McAfee ePolicy Orchestrator - Host Intrusion Prevention
Event logging for all administration-level events (requires controlled access to logs)	4. Security Information and Event Management	Silver	McAfee Enterprise Security Manager
Four-eye principle for key administrator changes	7. Integrity and Trust	Silver	Policy Document Repository
Cloud provider has an implemented and tested technical continuity plan	8. Availability	Silver	Policy Document Repository
Fully documented and controlled network	2. Network and Firewall Isolation	Silver	Policy Document Repository
Systems must be developed using Secure Software Development Lifecycle Coding Standards	7. Integrity and Trust	Silver	Policy Document Repository
Option to perform penetration testing on hosted systems and applications	1. Vulnerability Management	Gold	Policy Document Repository
Physical segmentation of hardware (server, storage, network, etc.) to ensure isolation from all other systems	2. Network and Firewall Isolation	Gold	Policy Document Repository
Encrypted communication between cloud provider and Cloud-Subscriber	1. Vulnerability Management 3. Identity Management	Gold	McAfee Vulnerability Manager
Multi-factor authentication	3. Identity Management	Gold	McAfee Enterprise Security Manager

Ability for Cloud-Subscriber to define geographic limits for hosting	5. Data Retention and Deletion 7. Integrity and Trust	Gold	Intel TXT Trust Data and VMware ESX
Storage encryption at logical unit number (LUN) level	6. Confidentiality	Gold	Policy Document Repository
No administrative access for cloud provider staff	3. Identity Management 4. Security Information and Event Management	Platinum	McAfee Enterprise Security Manager
Strong encryption mandatory for all data in-flight and at rest	6. Confidentiality	Platinum	Policy Document Repository

ODCA Security Monitoring Usage Model

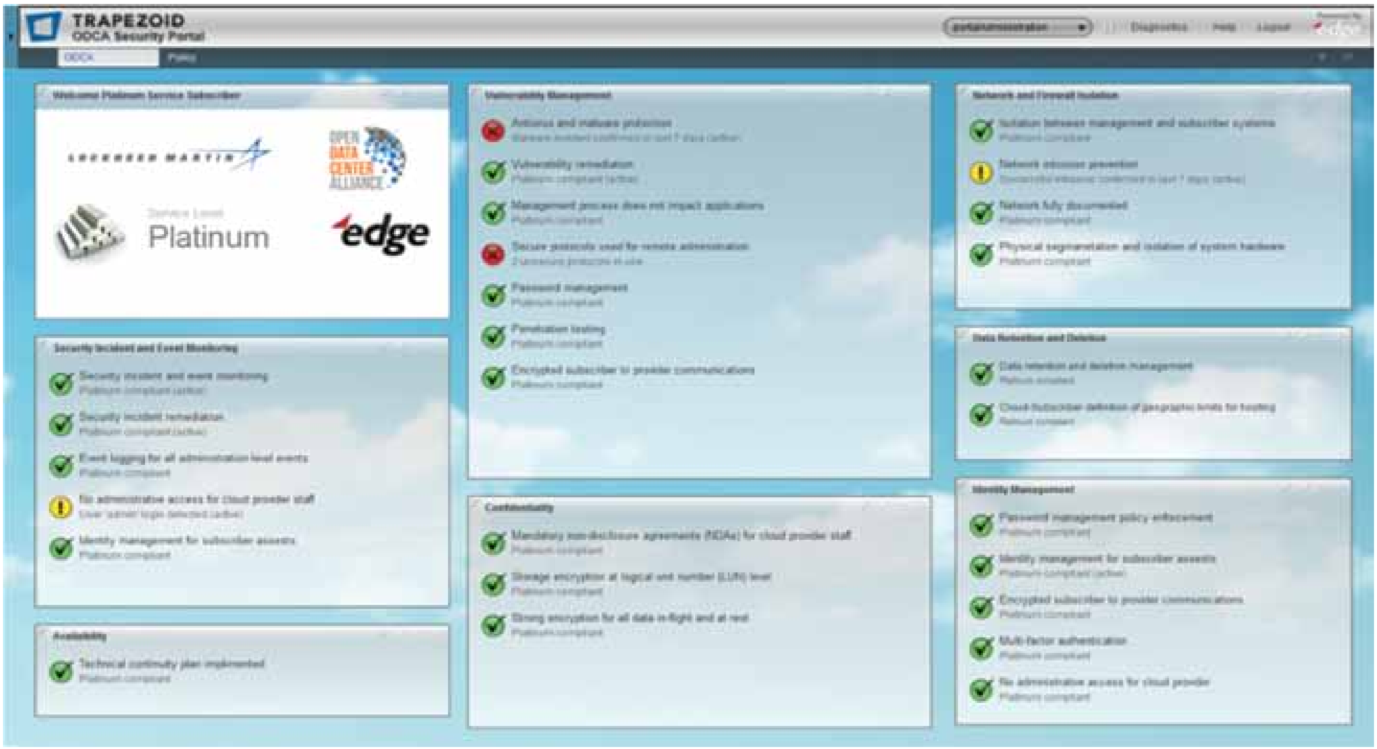
The ODCA Security Monitoring usage model relies heavily on the proper implementation of the Provider Assurance usage model and evaluates the transparency and ease with which the Cloud Subscriber can query and report on the Cloud Provider's infrastructure and security controls. There are two scenarios offered by the ODCA Security Usage Model, a Full Success Scenario and a Partial Success Scenario, both with a goal to "provide a standardized monitoring framework, format and syntax for monitoring the standards defined in the Provider Security Assurance Usage Model, plus provide a view of the actual status of assets that exist in the cloud."

Some of the critical API sets or mechanisms that will be required by the Security Monitoring usage model include features that enhance the control, management, reporting and audit of the security environment. According to the 2011 specificaition, the model should span:

- Patch management and version control APIs, with audit/query function
- Identity management services and APIs for consolidation and federation of access control
- Platform Trust APIs (system trust, identity and geographic position/ platform location established by the root of trust can be consumed by control, monitor and audit functions)
- API for import/export to Cloud-Subscriber log systems from cloud SIEM systems
- Audit/Query APIs for platform attributes (CPU, memory, chipset security, virtualization features, BIOS revisions)
- Cryptographic Key Management APIs for the deployment, use and escrow of cryptographic keys in cloud and enterprise infrastructures
- Facilities and resource management APIs for dynamic data and access to static and offline data (such as facilities control logs)
- "Peer service" monitor APIs to verify that Cloud-Subscriber workload is not on shared resources with specific list of blacklisted peers or being negatively impacted by oversubscribing peer service (e.g. "noisy neighbor")
- Network traffic and threat analysis services and APIs for controlling and reporting on the infrastructure to mitigate malware and denial-of-service (DoS) attacks

Success Scenario 1 (full): Cloud-Providers provide a secure Web-based interface, which allows the Cloud-Subscriber to get a report of the actual status of the cloud services that they purchase.

For example, the Web interface would allow the Cloud-Subscriber to get anti-virus definition status, IPS events and firewall logs. **NOTE**: This usage model is for information gathering only. Active actions such as remediation and performing more vulnerabilities scans will not be performed using this tool.



Welcome Platinum Service Subscriber

Security Incident and Event Monitoring

- ✓ Security incident and event monitoring
  Platinum compliant (active)
- ✓ Security incident remediation
  Platinum compliant (active)
- ✓ Event logging for all administration level events
  Platinum compliant
- ⚠ No administrative access for cloud provider staff
  User 'admin' login detected (active)
- ✓ Identity management for subscriber assets
  Platinum compliant

Availability

- ✓ Technical continuity plan implemented
  Platinum compliant

Vulnerability Management

- ✗ Antivirus and malware protection
  Malware incident confirmed in last 7 days (active)
- ✓ Vulnerability remediation
  Platinum compliant (active)
- ✓ Management process does not impact applications
  Platinum compliant
- ✗ Secure protocols used for remote administration
  2 unsecure protocols in use
- ✓ Password management
  Platinum compliant
- ✓ Penetration testing
  Platinum compliant
- ✓ Encrypted subscriber to provider communications
  Platinum compliant

Confidentiality

- ✓ Mandatory non-disclosure agreements (NDAs) for cloud provider staff
  Platinum compliant
- ✓ Storage encryption at logical unit number (LUN) level
  Platinum compliant
- ✓ Strong encryption for all data in-flight and at rest
  Platinum compliant

Network and Firewall Isolation

- ✓ Isolation between management and subscriber systems
  Platinum compliant
- ⚠ Network intrusion prevention
  Successful intrusion confirmed in last 7 days (active)
- ✓ Network fully documented
  Platinum compliant
- ✓ Physical segmentation and isolation of system hardware
  Platinum compliant

Data Retention and Deletion

- ✓ Data retention and deletion management
  Platinum enabled
- ✓ Cloud-Subscriber definition of geographic limits for hosting
  Platinum compliant

Identity Management

- ✓ Password management policy enforcement
  Platinum compliant
- ✓ Identity management for subscriber assets
  Platinum compliant (active)
- ✓ Encrypted subscriber to provider communications
  Platinum compliant
- ✓ Multi-factor authentication
  Platinum compliant
- ✓ No administrative access for cloud provider
  Platinum compliant

Failure Conditions 1:

- Inconsistent, incomplete, or tampered reporting (e.g. gaps in heartbeats or health checks, out-of-band values without documented remediation action, integrity check does not match).
- Unacceptable delays in gathering and preparing the reporting data, or having out-of-date data, without sufficient notification to the Cloud-Subscriber.

Success Scenario 2 (partial): Cloud-Providers provide a standard interface (such as Cloud Audit A6 API) that permits the Cloud-Subscriber to query security status of the purchased assets in order to get a real-time security status. Cloud-Providers should present this interface through a web-based monitoring facility to Cloud-Subscribers and to the Cloud-Compliance-Agency. Cloud-Subscribers should implement their own cloud monitoring infrastructure.

Failure Conditions 2:

- Cloud-Providers supply the service, but fail to allow real-time access to the data (e.g. authorization issues or other access problems).
- A Cloud-Provider's web-monitoring application does not comply with the monitoring standard as defined by the Cloud-Standards-Body.
- The Cloud-Provider's data is falsified and so incorrectly represents the status of the service.
- Delays or failure to respond to queries due to the Cloud-Provider having insufficient service capacity to handle volume of real-time monitoring.

Failure Handling: Security issues and other failure scenarios would be addressed by the contractual agreements between the Cloud-Subscriber and Cloud-Provider. It is envisioned that, depending on the nature of the failure, there would be progressively increasing penalties.

ODCA Test Cases

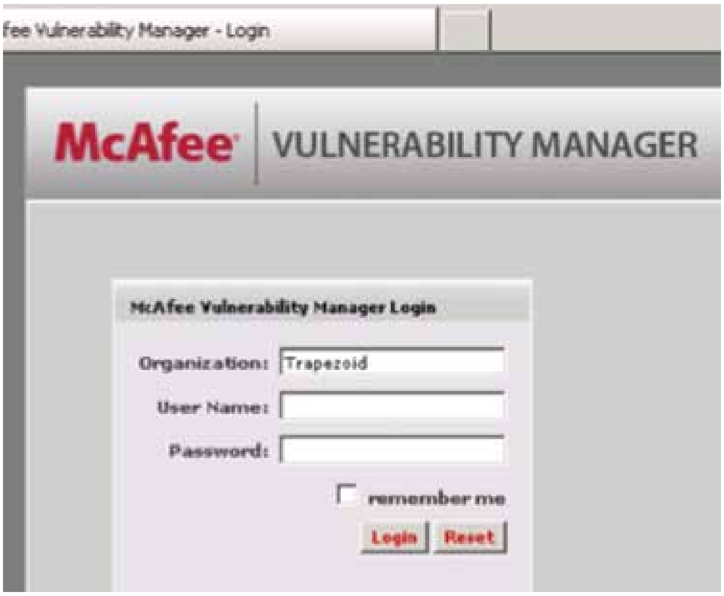
Test Case 1 - Vulnerability Management

This test case references the following ODCA Provider Assurance usage model security requirements:

- Requirement 1: Antivirus Updates Within 24hrs
- Requirement 2: Vulnerability Management
- Requirement 5: Secure Remote Administration
- Requirement 6: Authentication and Password Auditing
- Requirement 18: Penetration Test of Hosts and Applications
- Requirement 20: Physical Hardware Segmentation

McAfee Vulnerability Manager

1. Open the Web browser and click on the McAfee Vulnerability Manager (MVM) favorites link or navigate to: https://win2k8mvm.inteleil.com/ or https://10.x.x.x
2. Log in with credentials provided by Security Provider.



McAfee Vulnerability Manager Login

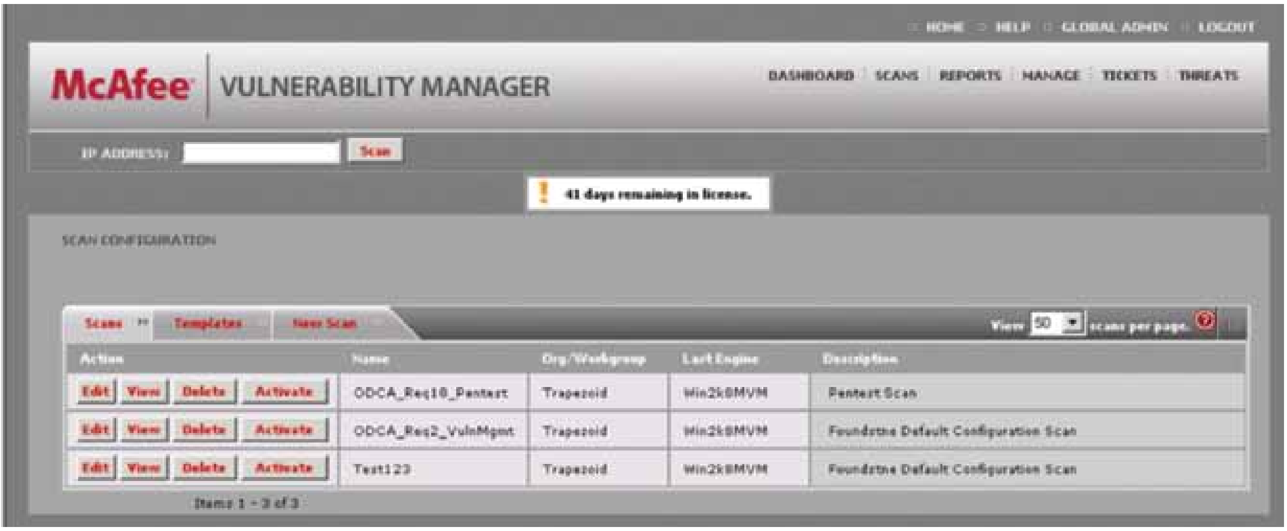
Organization: Trapezoid

User Name:

Password:

□ remember me

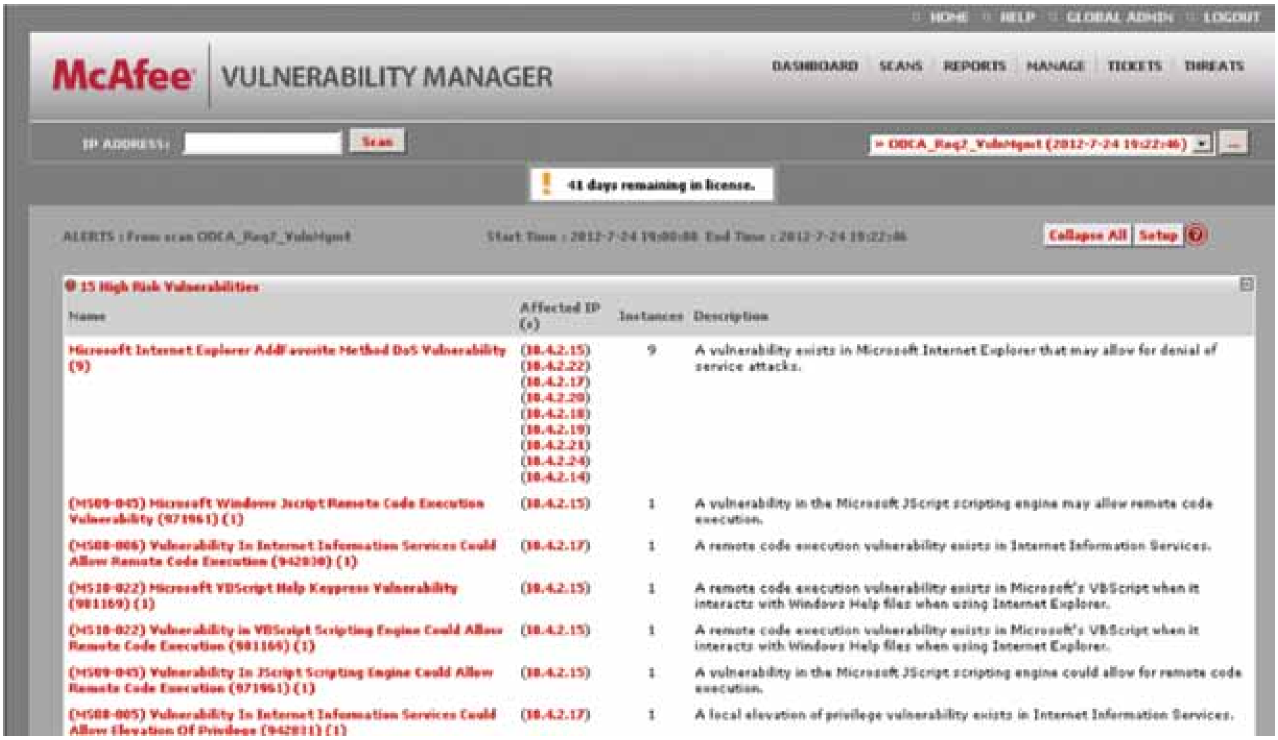
3. ODCA Provider Assurance usage model security requirements are met by the following scheduled vulnerability scans:
    a. ODCA Requirement 2: Vulnerability Management
    b. ODCA Requirement 18: Penetration Test of Hosts and Applications



Action	Name	Org/Workgroup	Last Engine	Description
Edit View Delete Activate	ODCA_Req18_Pentest	Trapezoid	Win2k8MVM	Pentest Scan
Edit View Delete Activate	ODCA_Req2_VulnMgmt	Trapezoid	Win2k8MVM	Foundstone Default Configuration Scan
Edit View Delete Activate	Test123	Trapezoid	Win2k8MVM	Foundstone Default Configuration Scan

Items 1 - 3 of 3

4. After logging into MVM click on Scans > Edit Status to view the configured scans.
5. The Scan Status link under Scans will show the current progress of vulnerability scans and provide a historical view of scans performed.
6. Under the Report link, click on Alerts and it will show the scan statistics and a summary of vulnerability information.

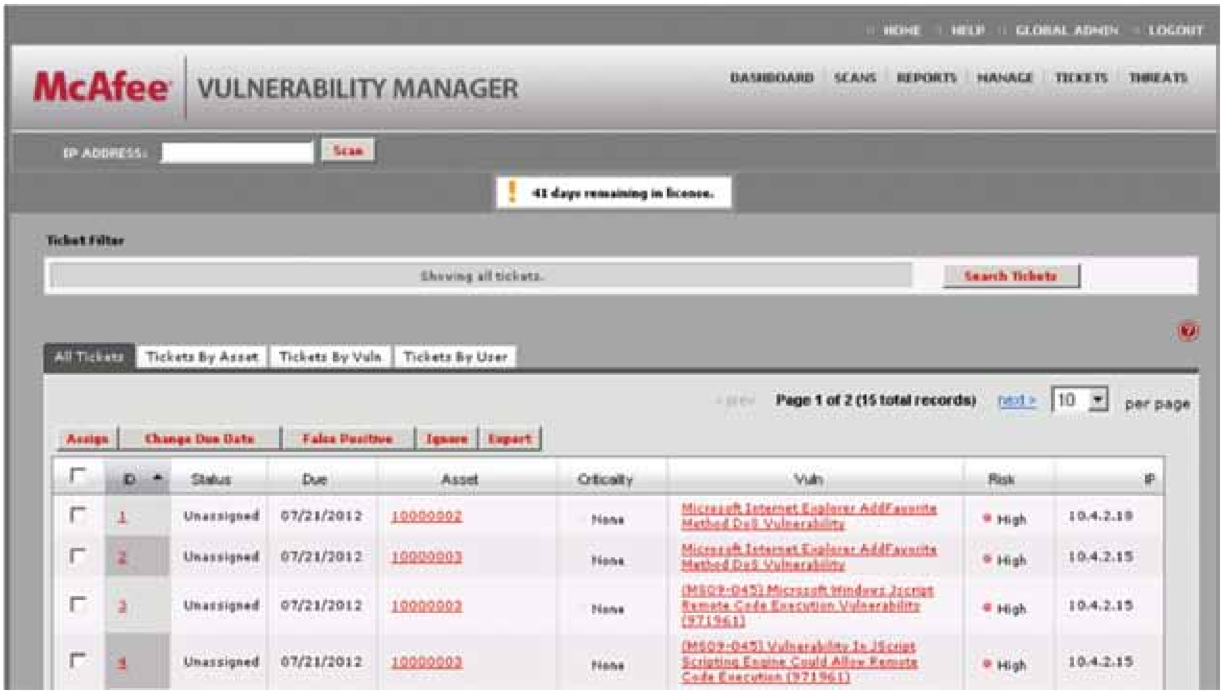


ALERTS : From scan ODCA_Req2_VulnMgmt Start Time : 2012-7-24 19:00:08 End Time : 2012-7-24 19:22:46

15 High Risk Vulnerabilities

Name	Affected IP (s)	Instances	Description
Microsoft Internet Explorer AddFavorite Method DoS Vulnerability (9)	(10.4.2.15) (10.4.2.22) (10.4.2.17) (10.4.2.20) (10.4.2.18) (10.4.2.19) (10.4.2.21) (10.4.2.24) (10.4.2.14)	9	A vulnerability exists in Microsoft Internet Explorer that may allow for denial of service attacks.
(MS09-045) Microsoft Windows Jscript Remote Code Execution Vulnerability (971961) (1)	(10.4.2.15)	1	A vulnerability in the Microsoft JScript scripting engine may allow remote code execution.
(MS08-006) Vulnerability In Internet Information Services Could Allow Remote Code Execution (942830) (1)	(10.4.2.17)	1	A remote code execution vulnerability exists in Internet Information Services.
(MS10-022) Microsoft VBScript Help Keypress Vulnerability (981169) (1)	(10.4.2.15)	1	A remote code execution vulnerability exists in Microsoft's VBScript when it interacts with Windows Help files when using Internet Explorer.
(MS10-022) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169) (1)	(10.4.2.15)	1	A remote code execution vulnerability exists in Microsoft's VBScript when it interacts with Windows Help files when using Internet Explorer.
(MS09-045) Vulnerability In JScript Scripting Engine Could Allow Remote Code Execution (971961) (1)	(10.4.2.15)	1	A vulnerability in the Microsoft JScript scripting engine could allow for remote code execution.
(MS08-005) Vulnerability In Internet Information Services Could Allow Elevation Of Privilege (942831) (1)	(10.4.2.17)	1	A local elevation of privilege vulnerability exists in Internet Information Services.

7. Click on Tickets > All Tickets to view all currently reported vulnerability issues found from the scans meeting the ODCA Gold Subscriber Test Case 1 Requirement (Vulnerability Remediation).



41 days remaining in license.

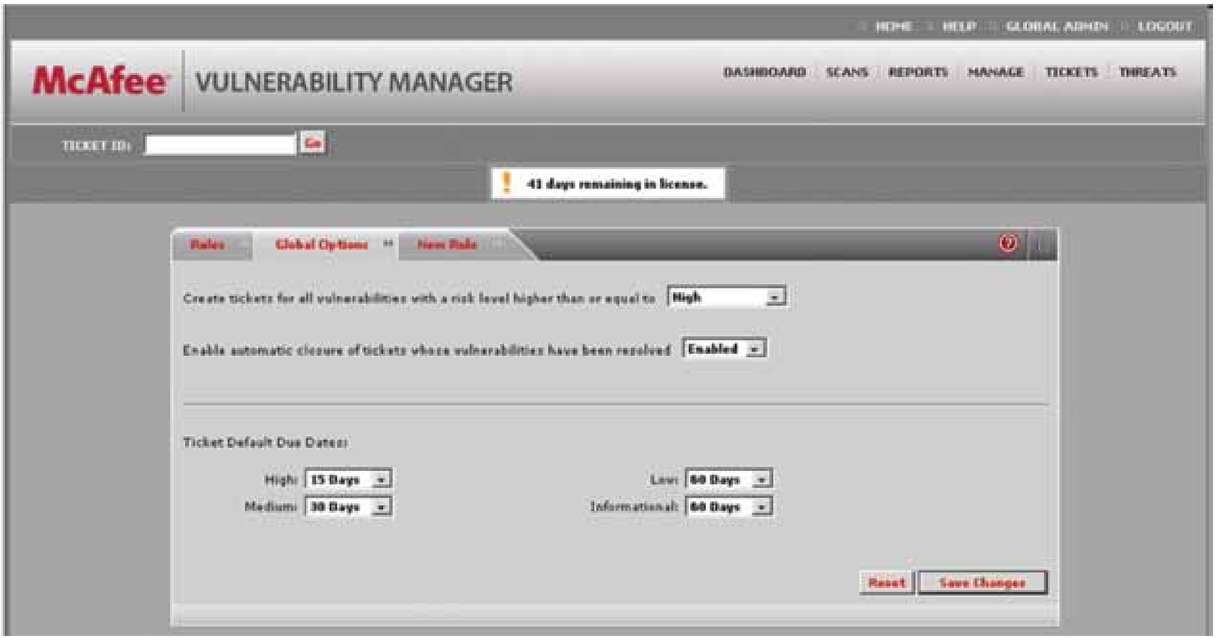
Ticket Filter

Showing all tickets.

Page 1 of 2 (15 total records) 10

☐	ID	Status	Due	Asset	Criticality	Vuln	Risk	IP
☐	1	Unassigned	07/21/2012	10000002	None	Microsoft Internet Explorer AddFavorite Method DoS Vulnerability	● High	10.4.2.18
☐	2	Unassigned	07/21/2012	10000003	None	Microsoft Internet Explorer AddFavorite Method DoS Vulnerability	● High	10.4.2.15
☐	3	Unassigned	07/21/2012	10000003	None	(MS09-045) Microsoft Windows Jscript Remote Code Execution Vulnerability (971961)	● High	10.4.2.15
☐	4	Unassigned	07/21/2012	10000003	None	(MS09-045) Vulnerability In JScript Scripting Engine Could Allow Remote Code Execution (971961)	● High	10.4.2.15

8. These tickets are opened and emailed to recipients of our choosing to report the patch and critical level score per asset.
9. Click on Manage > Ticketing > Global Options and New Rule sections to specify whom the tickets are assigned, due dates, and criteria that are used to match tickets to rules.



41 days remaining in license.

Create tickets for all vulnerabilities with a risk level higher than or equal to: High

Enable automatic closure of tickets whose vulnerabilities have been resolved: Enabled

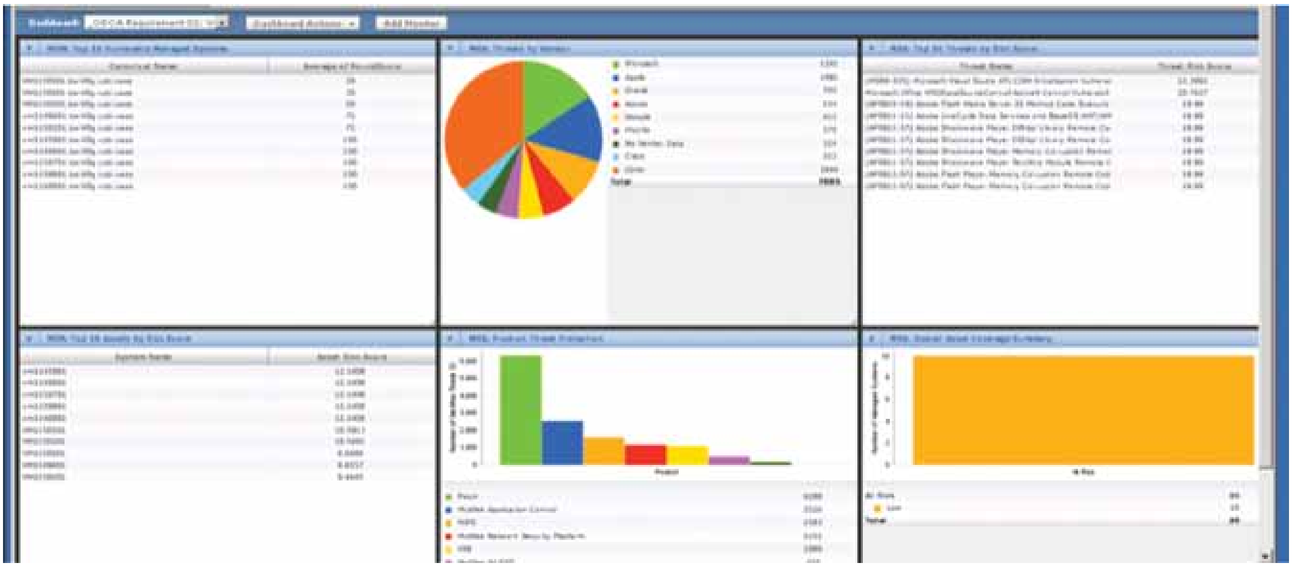
Ticket Default Due Dates:

High: 15 Days
Medium: 30 Days
Low: 60 Days
Informational: 60 Days

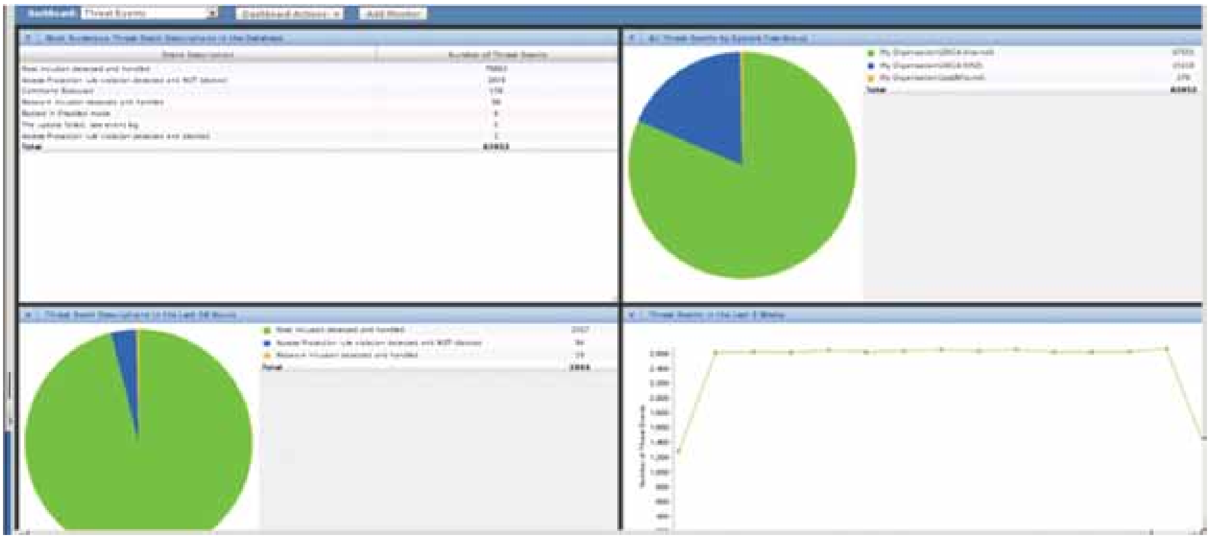
10. Log off of MVM.

McAfee ePolicy Orchestrator

1. Open the Web browser and then click on McAfee ePO favorites link or navigate to: https://10.x.x.x:8443
2. ODCA Provider Assurance usage model security requirements are met by the following real-time dashboards:
   a. ODCA Requirement 1: Antivirus Updates Within 24hrs
   b. ODCA Requirement 2: Vulnerability Management



   c. ODCA Requirement 6: Authentication and Password Auditing
   d. ODCA Requirement 5: Secure Remote Administration
3. ODCA Gold Subscriber Test Case 1 Requirement (Vulnerability Management) real-time dashboards:
   a. PA: MS Patch Status Summary to view all assets and vulnerabilities found in the scanned environment.
   b. MRA: Threat Dashboard and this will show you Risk Advisors dashboard showing all vulnerable applications and threats found in the environment.



Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page, click on the ODCA Gold Subscriber Project > Activity.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
   a. ODCA Requirement 2: Vulnerability Management
   b. ODCA Requirement 18: Penetration Testing Policy
   c. ODCA Requirement 20: Physical Hardware Segmentation

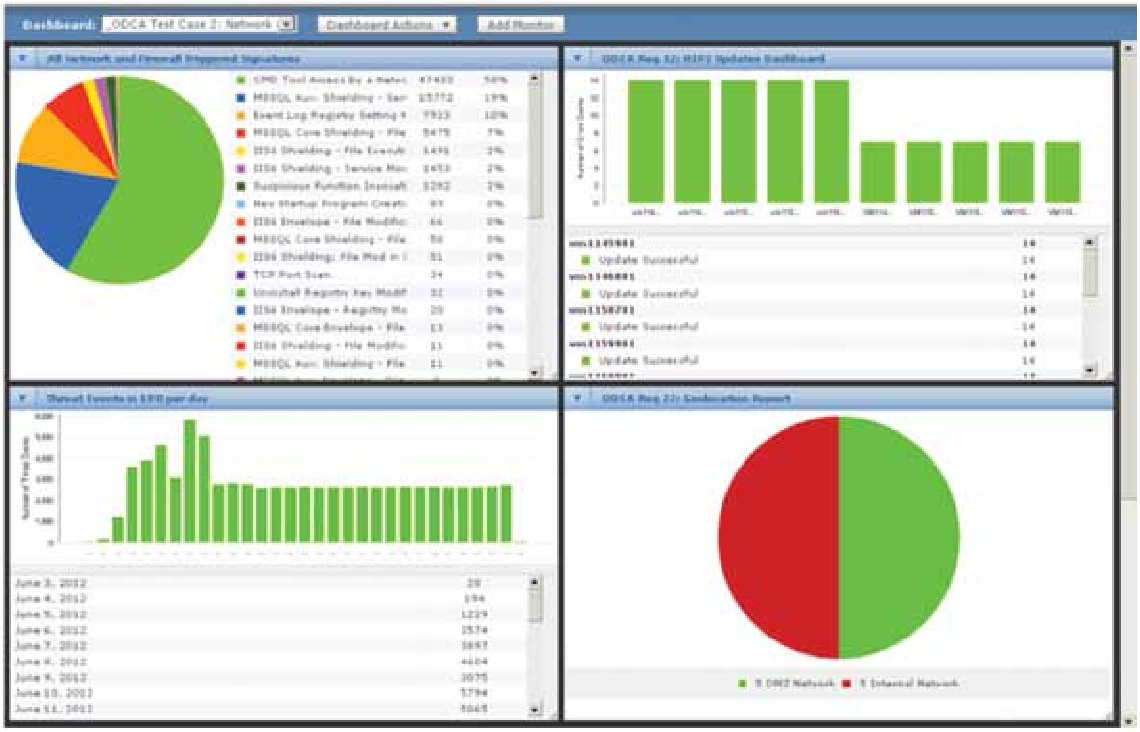
Test Case 2 - Network and Firewall Isolation

This test case references the following ODCA Provider Assurance usage model security requirements:

- Requirement 3: Network Firewalls
- Requirement 12: Intrusion Prevention
- Requirement 16: Fully documented and controlled network
- Requirement 19: Physical segmentation of hardware

McAfee ePolicy Orchestrator

1. Open the Web browser and then click on McAfee ePO favorites link or navigate to: https://10.x.x.x:8443
2. Log in with credentials provided by Security Provider.
3. ODCA Provider Assurance usage model security requirements are met by the following real-time dashboards:
   a. ODCA Requirement 3: Network Firewalls
   b. ODCA Requirement 12: Intrusion Prevention


Dashboard:
_ODCA Test Case 2: Network
Dashboard Actions
Add Monitor
All Network and Firewall Triggered Signatures
ODCA Req 12: HIPS Updates Dashboard
Threat Events in EPO per day
ODCA Req 22: Geolocation Report
DMZ Network
Internal Network

🟩 CMD Tool Access By a Networ	47433	58%
🟦 MSSQL Aux. Shielding - Ser	15772	19%
🟧 Event Log Registry Setting	7933	10%
🟥 MSSQL Core Shielding - File	5475	7%
🟨 IIS6 Shielding - File Executi	1495	2%
🟪 IIS6 Shielding - Service Mo	1453	2%
■ Suspicious Function Invocati	1292	2%
🟦 New Startup Program Creati	89	0%
🟧 IIS6 Envelope - File Modific	66	0%
🟥 MSSQL Core Shielding - File	58	0%
🟨 IIS6 Shielding: File Mod in I	51	0%
🟪 TCP Port Scan	34	0%
🟩 Uninstall Registry Key Modif	32	0%
🟦 IIS6 Envelope - Registry Mo	20	0%
🟧 MSSQL Core Envelope - File	13	0%
🟥 IIS6 Shielding - File Modific	11	0%
🟨 MSSQL Aux. Shielding - File	11	0%

wm1145901	14
🟩 Update Successful	14
wm1146801	14
🟩 Update Successful	14
wm1150701	14
🟩 Update Successful	14
wm1159901	14
🟩 Update Successful	14

June 3, 2012	28
June 4, 2012	194
June 5, 2012	1229
June 6, 2012	2574
June 7, 2012	3657
June 8, 2012	4604
June 9, 2012	3075
June 10, 2012	5794
June 11, 2012	5065

4. On the same EPO console, select on Queries & Reports then click on the reports tab and select the last run results.

Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page click on the ODCA Gold Subscriber Project.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
   a. ODCA Requirement 16: Fully documented and controlled network
   b. ODCA Requirement 19: Physical segmentation of hardware

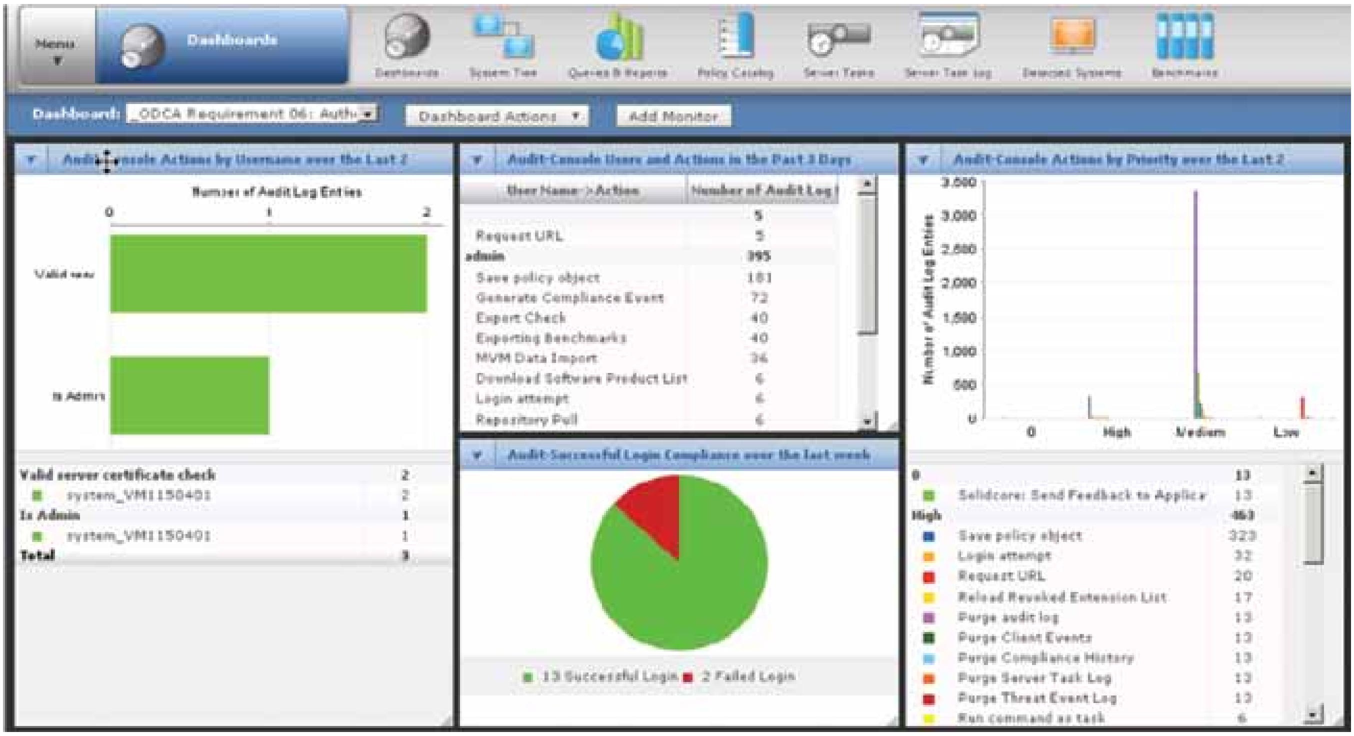
Test Case 3 - Identity Management

This test case references the following ODCA Provider Assurance usage model security requirements:

- Requirement 6: All default passwords and guest access removed
- Requirement 9: Identity management for subscriber assets
- Requirement 20: Encrypted communication between cloud provider and Cloud-Subscriber
- Requirement 21: Multi-factor authentication

McAfee ePolicy Orchestrator

1. Open the Web browser and then click on McAfee ePO favorites link or navigate to: https://10.x.x.x:8443
2. ODCA Provider Assurance usage model security requirements are met by the following real-time dashboards:
   a. ODCA Requirement 6: All default passwords and guest access removed


Menu
Dashboards
Dashboards
System Tree
Queries & Reports
Policy Catalog
Server Tasks
Server Task Log
Detected Systems
Benchmarks
Dashboard:
ODCA Requirement 06: Auth
Dashboard Actions
Add Monitor
Audit-Console Actions by Username over the Last 2
Number of Audit Log Entries
0
1
2
Valid serv
Is Admin
Audit-Console Users and Actions in the Past 3 Days
Audit-Console Actions by Priority over the Last 2
Number of Audit Log Entries
3,500
3,000
2,500
2,000
1,500
1,000
500
0
0
High
Medium
Low
Audit-Successful Login Compliance over the last week
🟩 13 Successful Login 🟥 2 Failed Login

Valid server certificate check	2
🟩 system_VM1150401	2
Is Admin	1
🟩 system_VM1150401	1
Total	3

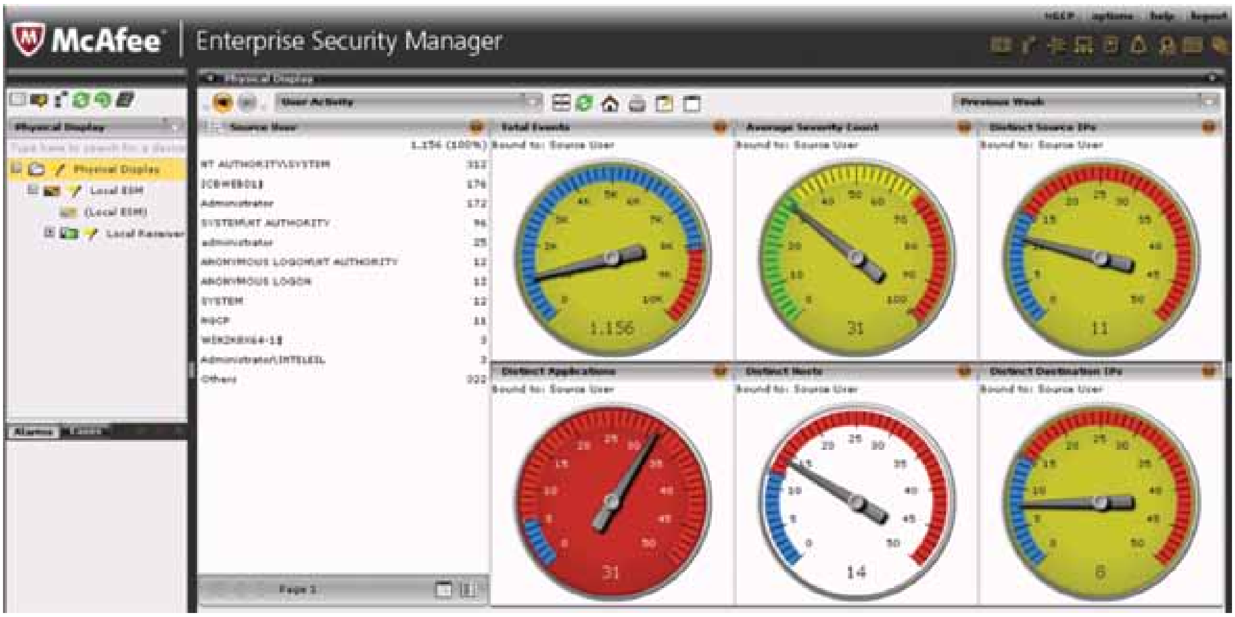
User Name->Action	Number of Audit Log I
	5
Request URL	5
admin	395
Save policy object	181
Generate Compliance Event	72
Export Check	40
Exporting Benchmarks	40
MVM Data Import	36
Download Software Product List	6
Login attempt	6
Repository Pull	6

0		13
🟩	Solidcore: Send Feedback to Applica	13
High		463
🟦	Save policy object	323
🟧	Login attempt	32
🟥	Request URL	20
🟨	Reload Revoked Extension List	17
🟪	Purge audit log	13
🟩	Purge Client Events	13
🟦	Purge Compliance History	13
🟧	Purge Server Task Log	13
🟥	Purge Threat Event Log	13
🟨	Run command as task	6

   b. ODCA Requirement 9: Identity management for subscriber assets

McAfee Enterprise Security Manager

1. Open the Web browser and then click on ESM favorites link or navigate to: https://10.x.x.x/ and click in the Login option.
2. Log in with credentials provided by Security Provider.
3. ODCA Provider Assurance usage model security requirements for Requirement 24 are met by the McAfee Enterprise Security Manager dashboard under the dropdown option > Dashboard Views > User Activity:
    a. 01 authentication
    b. 02 login AND succeeded
    c. 03 login



Source User	1,156 (100%)
NT AUTHORITY\SYSTEM	312
ICBWEB01$	176
Administrator	172
SYSTEM\NT AUTHORITY	96
administrator	25
ANONYMOUS LOGON\NT AUTHORITY	12
ANONYMOUS LOGON	12
SYSTEM	12
NGCP	11
WIN2K8X64-1$	3
Administrator\INTELEIL	3
Others	322

Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page click on the ODCA Gold Subscriber Project.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
    a. ODCA Requirement 20: Encrypted communication between Provider and Subscriber
    b. ODCA Requirement 21: Multi-factor authentication

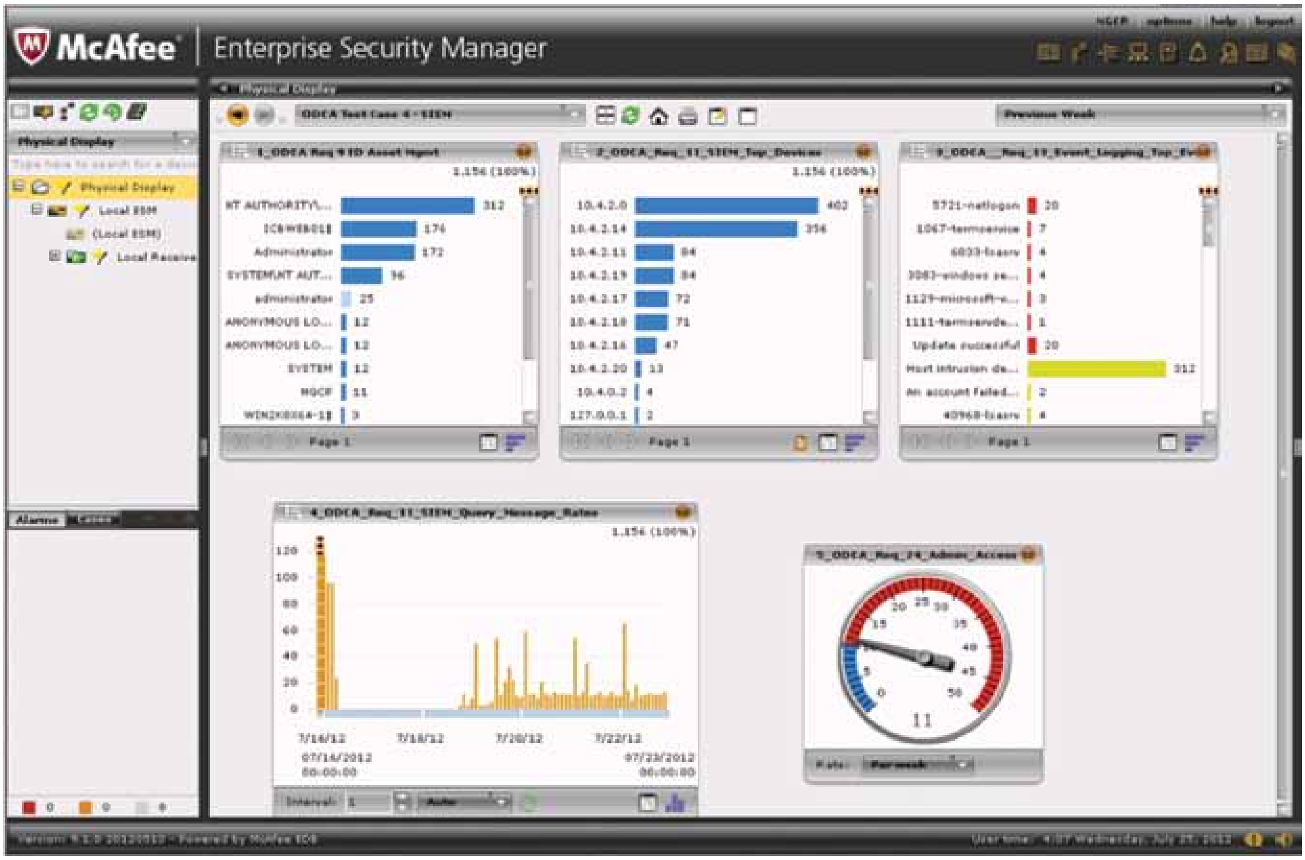
Test Case 4 - Security Incident and Event Monitoring (SIEM)

This test case references the following ODCA Provider Assurance usage model security requirements:

- Requirement 9: Identity management for subscriber assets
- Requirement 11: Security incident and event monitoring
- Requirement 13: Event logging for all administration-level events (controlled access to logs)
- Requirement 24: No administrative access for cloud provider staff

McAfee Enterprise Security Manager

1. Open the Web browser and then click on ESM favorites link or navigate to: http://10.x.x.x
2. Log in with credentials provided by Security Provider.
3. ODCA Provider Assurance usage model security requirements are met by the following McAfee Enterprise Security Manager ODCA Test Case 4 Dashboards:
   a. ODCA Requirement 9: Identity management for subscriber assets
   b. ODCA Requirement 11: Security incident and event monitoring
   c. ODCA Requirement 13: Event logging for all administration-level events (requires controlled access to logs)
   d. ODCA Requirement 24: No administrative access for cloud provider staff



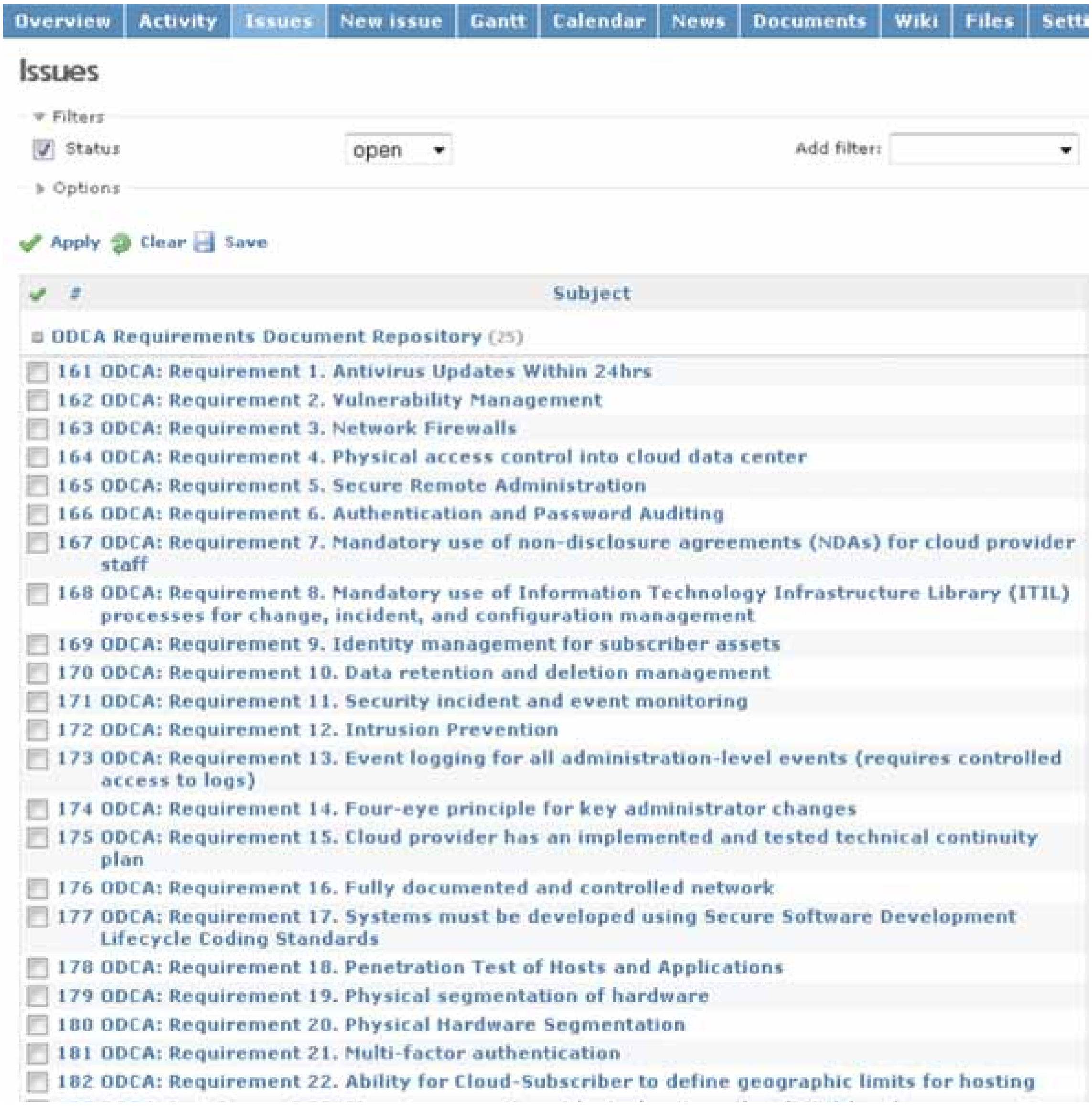
Test Case 5 - Data Retention and Deletion

This test case references the following ODCA requirements:

- Requirement 10: Data retention and deletion management
- Requirement 22: Ability for Cloud-Subscriber to define geographic limits for hosting

Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page click on the ODCA Gold Subscriber Project.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
   a. ODCA Requirement 10: Data retention and deletion management
   b. ODCA Requirement 22: Ability for Cloud-Subscriber to define geographic limits for hosting



Issues

☑ Status: open

✓	#	Subject
		ODCA Requirements Document Repository (25)
□	161	ODCA: Requirement 1. Antivirus Updates Within 24hrs
□	162	ODCA: Requirement 2. Vulnerability Management
□	163	ODCA: Requirement 3. Network Firewalls
□	164	ODCA: Requirement 4. Physical access control into cloud data center
□	165	ODCA: Requirement 5. Secure Remote Administration
□	166	ODCA: Requirement 6. Authentication and Password Auditing
□	167	ODCA: Requirement 7. Mandatory use of non-disclosure agreements (NDAs) for cloud provider staff
□	168	ODCA: Requirement 8. Mandatory use of Information Technology Infrastructure Library (ITIL) processes for change, incident, and configuration management
□	169	ODCA: Requirement 9. Identity management for subscriber assets
□	170	ODCA: Requirement 10. Data retention and deletion management
□	171	ODCA: Requirement 11. Security incident and event monitoring
□	172	ODCA: Requirement 12. Intrusion Prevention
□	173	ODCA: Requirement 13. Event logging for all administration-level events (requires controlled access to logs)
□	174	ODCA: Requirement 14. Four-eye principle for key administrator changes
□	175	ODCA: Requirement 15. Cloud provider has an implemented and tested technical continuity plan
□	176	ODCA: Requirement 16. Fully documented and controlled network
□	177	ODCA: Requirement 17. Systems must be developed using Secure Software Development Lifecycle Coding Standards
□	178	ODCA: Requirement 18. Penetration Test of Hosts and Applications
□	179	ODCA: Requirement 19. Physical segmentation of hardware
□	180	ODCA: Requirement 20. Physical Hardware Segmentation
□	181	ODCA: Requirement 21. Multi-factor authentication
□	182	ODCA: Requirement 22. Ability for Cloud-Subscriber to define geographic limits for hosting

Test Case 6 - Confidentiality

This test case references the following ODCA requirements:

- Requirement 7: Mandatory use of non-disclosure agreements (NDAs) for cloud provider staff
- Requirement 23: Storage encryption at logical unit number (LUN) level
- Requirement 25: Strong encryption mandatory for all data in-flight and at rest

Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page click on the ODCA Gold Subscriber Project.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
   a. ODCA Requirement 7: Mandatory use of non-disclosure agreements (NDAs) for cloud provider staff
   b. ODCA Requirement 23: Storage encryption at logical unit number (LUN) level
   c. ODCA Requirement 25: Strong encryption mandatory for all data in-flight and at rest

Test Case 7 - Integrity and Trust

This test case references the following ODCA requirements:

- Requirement 4: Physical access control into cloud data center
- Requirement 8: Mandatory use of Information Technology Infrastructure Library (ITIL) processes for change, incident, and configuration management
- Requirement 14: Four-eye principle for key administrator changes
- Requirement 17: Systems must be developed using Secure Software Development Lifecycle Coding Standards
- Requirement 22: Ability for Cloud-Subscriber to define geographic limits for hosting

Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page click on the ODCA Gold Subscriber Project.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
   a. ODCA Requirement 4: Physical access control into cloud data center
   b. ODCA Requirement 8: Mandatory use of Information Technology Infrastructure Library (ITIL) processes for change, incident, and configuration management
   c. ODCA: Requirement 14: Four-eye principle for key administrator changes
   d. ODCA Requirement 17: Systems must be developed using Secure Software Development Lifecycle Coding Standards
   e. ODCA Requirement 22 Ability for Cloud-Subscriber to define geographic limits for hosting

Test Case 8 - Availability

This test case references the following ODCA requirements:

- Requirement 15: Cloud provider has an implemented and tested technical continuity plan

Redmine Document Repository

1. Open the Web browser and then click on the Redmine favorites link or navigate to: http://10.x.x.x/redmine
2. Log in with credentials provided by Security Provider and from the home page click on the ODCA Gold Subscriber Project.
3. ODCA Provider Assurance usage model security requirements are met by the following Cloud Provider Policy Documents:
   a. ODCA Requirement 15: Cloud provider has an implemented and tested technical continuity plan

Things to Consider

During the design and implementation of this reference architecture there were several things that needed to be considered. Because this reference architecture consists of building blocks that need to be provisioned and deployed in a secure and trusted manner, the entire infrastructure needs to be carefully architected. From the ground up, starting with server provisioning, through the security stack, and up to regulatory compliance, here are some things to consider when attempting to rebuild a similar architecture:

- Intel TXT Trusted Platform Module (TPM) hardware chips must be purchased and provisioned on all hardware before the hypervisor installation.
- Licensing for software platforms including McAfee, Trapezoid, and other commercial solutions deployed as part of this reference architecture all require licensing provided by the corresponding vendors
- This reference architecture is built using VMware and VSphere. Trapezoid TCS will be adding support for other hypervisors such as Xen and Hyper-V.

- TCS virtual appliance beta version 3 is the currently vetted solution and tested to work in this reference architecture. TCS version 1 will be released later this year with enhanced trust integration, SIEM, and added hypervisor support.
- ODCA Network and Firewall compliance was met using McAfee ePO's host-based security agents in this implementation, not network-based firewalls. The ePO agents include firewall, HIPS, and data leakage protection.
- The McAfee Security Management Platform consists of ePO, MVM, and SEM virtual appliances or servers. Other components such as Risk Advisor and Policy Auditor were not implemented but would also play key roles in protecting a production infrastructure.
- The ODCA Platinum Assurance Security Monitoring portal implemented in this reference architecture is for demonstration purposes only and does not query the security platforms directly. In a production environment the security portal uses APIs wherever possible and Single Sign-On technology to present a unified view of the entire security infrastructure.
- Support for Cisco UCS, VCE, and other private and public cloud hardware solutions is expected in the TCS production release.

Conclusion

This reference architecture describes the integration of an Intel TXT trust data with the McAfee Security Management Platform, leveraging Trapezoid's TCS to monitor and maintain trust of the cloud infrastructure and all the virtual machines deployed within. Configured to meet ODCA assurance levels, Trapezoid's TCS integrates trust values and changes in the state of trust generated by the cloud infrastructure. Integrating with McAfee ePO, TCS helps audit, monitor, and enforce hard-ware based security policies in the cloud. This Trusted Cloud Infrastructure is built with VMware vSphere using ESX5.0 on Intel® Xeon® Processor E5-2680 series-based server platforms. In addition to enforcing hardware-based security policies based on TCS, McAfee's Secure Management Platform product delivers to the end-user ODCA Provider Assurance compliance.

Trapezoid's goal is to provide a standardized monitoring framework, format, and syntax for monitoring the standards defined in the Provider Security Assurance usage model, plus provide a view of the actual status of assets that exist in the cloud. Trapezoid enabled cloud subscribers and providers alike to integrate trust and security throughout their entire infrastructure. In today's complex computing environment and demanding IT industry it's not enough to implement security, it is also necessary to be sure you can trust your security implementation and monitor changes in the trust level of the organization's assets.

Disclaimers

∆ Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which

have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

[1] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/technology/security. In addition, Intel TXT requires that the original equipment manufacturer provides TPM functionality, which requires a TPM-supported BIOS. TPM functionality must be initialized and may not be available in all countries.