Audience and Purpose

This reference architecture describes the security integration of an Intel® Trusted Execution Technology (Intel® TXT®) 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.
# Table of Contents

Executive Summary ................................................................. 4
Introduction ............................................................................ 4
Intel® TXT ................................................................................ 4
VMware vSphere ESX ............................................................... 4
McAfee Security Management Platform .................................... 4
Trapezoid Trust Control Suite .................................................. 5

Test Bed Blueprint .................................................................. 6
Hardware Requirements .......................................................... 6
Intel TXT Server Provisioning ................................................... 6
VMware ESX TPM Attestation .................................................. 8
ICB Trusted Cloud Deployment ................................................ 11
Physical Cloud Infrastructure .................................................. 11
Virtual Cloud Infrastructure ..................................................... 12

McAfee Security Management Platform ................................... 13
McAfee ePolicy Orchestrator ................................................... 14
McAfee Vulnerability Manager ................................................ 15
McAfee Enterprise Security Manager ....................................... 16
McAfee Advanced Correlation Engine (ACE) ......................... 16
McAfee Database Event Monitor (DEM) ................................. 16

Trapezoid Trust Control Suite .................................................. 17
TCS Virtual Appliance ............................................................ 17
TCS McAfee ePO Plug-in ........................................................ 18
TCS McAfee ePO Agent Configuration ..................................... 21
TCS McAfee ePO Advanced Configuration ................................ 25

TCS Implementation Scenarios ................................................ 26
Scenario 1 - Intel TXT Trusted Server Pool Validation ............... 26
Scenario 2 - Network Security Policy Enforcement ................. 28
Scenario 3 - Application Trust Awareness ............................... 29

ODCA Usage Model Alignment ............................................... 32
Open Data Center Alliance Overview ...................................... 32
ODCA Provider Assurance Usage Model ................................. 32
ODCA Security Monitoring Usage Model ............................... 34

ODCA Test Cases ................................................................. 36
Test Case 1 - Vulnerability Management ................................. 36
Test Case 2 - Network and Firewall Isolation ........................... 40
Test Case 3 - Identity Management ......................................... 41
Test Case 4 - Security Incident and Event Monitoring (SIEM) .... 43
Test Case 5 - Data Retention and Deletion ............................... 44
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.

<table>
<thead>
<tr>
<th>System</th>
<th>Detailed Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Server (x1)</td>
<td>Microsoft Windows 2008, IIS, .NET 2.0, VMware vCenter Server 5.0, and vSphere Web Services* SDK</td>
</tr>
<tr>
<td>Management Client</td>
<td>Microsoft Windows 7, .Net 2.0, and VMware vCenter Client 5.0</td>
</tr>
<tr>
<td>ESXi 5 Host Trusted (x3)</td>
<td>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</td>
</tr>
<tr>
<td>ESXi 5 Host NOT Trusted (x2)</td>
<td>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</td>
</tr>
<tr>
<td>iSCSI Data Store Server</td>
<td>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</td>
</tr>
</tbody>
</table>

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]
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]

![Image of BIOS settings]

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

![Image of TPM settings]
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

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.
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

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

The McAfee ePolicy Orchestrator (ePO) server is at the heart of 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](image)
**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 centers. 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.

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. Execute 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.

3. The following packages and corresponding extensions should be installed using the respective installation instructions from the McAfee website:
   a. Trapezoid TCS
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.
6. Set up different types of Automated Responses and Alerts with Trapezoid TCS plug-in.

![Image of Trapezoid TCS interface]

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

![Image of trust status interface]

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

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
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.

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

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

**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 specification, 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.
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.inteleli.com/ or https://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 scheduled vulnerability scans:
   a. ODCA Requirement 2: Vulnerability Management
   b. ODCA Requirement 18: Penetration Test of Hosts and Applications

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.
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).

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.

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

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
   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

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
**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

**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 hardware-based security policies in the cloud. This Trusted Cloud Infrastructure is built with VMware vSphere using ESXi 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.

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.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, Xeon, Xeon inside, and Intel Intelligent Power Node Manager are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

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.