Trusted Geolocation in The Cloud Technical Demonstration

NIST Interagency Report 7904 - Trusted Geolocation in the Cloud: Proof of Concept Implementation
Trustured Geolocation in the Cloud

- Cloud benefits
  - Agility
  - Flexibility
  - Dynamic Resources
- Cloud Challenges
  - Multi-tenancy and shared hosted infrastructure
  - Lack of physical boundaries
  - Lack of visibility of workloads
  - Integrity of the hosted virtualized compute environment
  - Compliance requirement for restricting workload in a physical location or within a restricted regulated resource pool
  - Technical enforcement mechanism
Trusted Geolocation in the Cloud

Use Case
Trusted Geolocation in the Cloud

- **Trusted resource pool** based on hardware-based secure technical measurement capability
  - **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
  - **Trust-based secure migration** - Provide geolocation measurement and enforcement for the compute nodes
- Workloads instantiation in a trusted resource pool
- Dynamic workloads migration and enforcement between trusted resource pools
- Visibility and transparency in periodic measurement, reporting, and auditing of the workloads to support governance, risk, and compliance requirements
- Industry recommended practices for deploying a secure virtualized infrastructure
Intel® TXT and Hardware Root of Trust

Intel® Trusted Execution Technology (Intel TXT) enforces control of the platform, measures launch components

A hardware based security foundation (Root of Trust) to build and maintain a *chain of trust*, to protect the platform from software based attacks

Trusted and verifiable systems

- Implement policies/controls on top of a foundation of trust beginning in HW and up the stack
- VMware, SUSE, Redhat and others have products that support HW roots of trust and *attestation*

www.intel.com/txt
Trusted Cloud Solution

NIST Reference Design

- Basic Policy Mgt
- Workload Placement & Migration Control
- Basic Trust Attestation
- Basic Geo-Location Attestation

Intel TXT Plug-in (Reference Implementation)

- ConfigMgr Policy Engines
- Verifier/Attestation

VMware vCenter

- RSA
- Archer
- VCenter 4.1
- Intel TXT APIs
- ESX 4.1 U2

VMware vSphere

- Dell Servers (w/ Intel TXT)
- Platform Integrity Measurements (Intel TXT)
- Geo-Tag

Portal and Cloud Mgt

Build

Commercial Solutions In-flight based on this Reference Design.
Trusted Compute Pools – Solution Stacks

- Trusted Policy Management
- Trusted Security Event Monitoring (SIEM)
- Trusted Audit and Compliance (Reporting and Compliance (GRC))

Contact Your Favorite Provider for More Details
Trusted Cloud Architecture

Commercial Solutions

Cloud Portal
Orchestrator/Scheduler (vCloud, OpenStack)
GRC (ex: RSA)
SIEM (ex: McAfee ESM, HP ArcSight)

CUSTOMER A
Citrix Xen
ESXi Host
ESXi Host
VMware vCenter

CUSTOMER B
Linux/KVM
Citrix Xen
ESXi Host
ESXi Host
VMware vCenter

Gather platform status (TCG, XML)

Provide platform Trust & Location Attestation for trusted pools, Compliance, etc

Monitor & Control

RESTful API

Trust Attestation Authority (Virtual Appliance)

HyTrust Policy Enforcement
Permit or Deny Request

Reporting
Logging

Administrator Identity
Administrator Role
Infrastructure Integrity

Virtual Appliance

https
ssl
Trust Cloud Architecture
Commercial Solutions

- Visibility & Monitoring
- Placement policy
- Geo tagging
- PII Compliance Decisions

xStream GRC (xGRC)

Cloud Provider Portal

xStream SIEM (xSIEM)

Cloud Subscriber Portal

- All Syslog/Events
- High/Med/Low

XT Provider
VMWare 5.1 Provider
xSIEM Provider

Trust
Attestation
Authority

vCenter

KVM
ESX

Event Data

Event Data
The Trapezoid® Trust Control Suite addresses hardware level computer attacks, a blind spot in current security defenses.
About Archer

► Award-Winning Enterprise Governance, Risk and Compliance Framework and Solutions
► Flexible GRC Programs to meet unique agency needs
  ► Enabling Federal Continuous Monitoring Initiatives
  ► Automate FISMA Audit and Compliance
    ► Cloud and dedicated environments
► NIST Geolocation Trusted Cloud
Enabling the Cycle of Risk & Compliance

Document Your Control Framework and Identify Risks

Prioritize Deficiencies and Risks

Prioritize Deficiencies and Risks

Remediate Findings and Manage Exceptions

Consolidate and Visualize Compliance Efforts

Automate the remediation process to create an efficient system with accountability

Break information silos and holistically view your environment

Map to any compliance source such as FISMA & NIST 800-53

Make sense of your data: analyze and contextualize to determine where to focus remediation efforts

Identify

Prioritize

Manage

Report
RSA Archer “Core” eGRC Solutions

**Audit Management**
Centrally manage the planning, prioritization, staffing, procedures and reporting of audits to increase collaboration and efficiency.

**Policy Management**
Centrally manage regulations and frameworks (FISMA, NIST, COSO, etc.), policies and control standards, map them to objectives and guidelines, and promote awareness across your agency.

**Business Continuity Management**
Manage the creation, review, testing and activation of business continuity plans to ensure rapid recovery of your business processes.

**Risk Management**
Identify risks to your business, evaluate them through online assessments and metrics, and respond with remediation or acceptance.

**Threat Management**
Track threats through a customizable early warning system to help prevent attacks before they affect your enterprise.

**Compliance Management**
Evaluate the effective design and operation of your internal controls, and respond to issues of non-compliance with remediation or waivers.

**Enterprise Management**
Manage relationships and dependencies within your enterprise hierarchy and infrastructure to support risk and compliance initiatives.

**Vendor Management**
Centralize vendor data, manage relationships, assess vendor risk, and ensure compliance with your policies and controls.

**Incident Management**
Report cyber, physical and other incidents, manage their escalation, track investigations and analyze resolutions.
RSA Archer eGRC Platform

Flexible Platform Enabling Governance, Risk and Compliance

**Integration**
Seamlessly integrate cross-departmental and enterprise data systems with the Archer SmartSuite Framework.

**User Experience**
Brand the interface with your corporate colors, graphics, icons and text to facilitate end-user adoption.

**Application Builder**
Build and tailor on-demand applications and package them into solutions to solve business problems.

**Reports and Dashboards**
Gain a real-time view of your enterprise through actionable reports and graphical dashboards.

**Notifications**
Automatically notify users via email when content changes, tasks enter their queue or deadlines approach.

**Access Control**
Enforce access controls at the system, application, record and field level to ensure a streamlined user experience.

**Business Workflow**
Define and automate business processes to streamline the management of content, tasks, statuses and approvals.
Maximize Compliance Information

Information Security Center

Archer  Data  Feed  Services

Identified System Risks
Foundstone, ETP

Request tools
Policy Exception Requests
Vulnerability Analysis Service Requests

Configuration Compliance
nCircle, ESM

Threat Alerts
Deepsgt, SRT

Ownership Details
SPT, SCPR

Security Documentation
Policies Standards Guidelines

Asset Details
ESL ETP, NeSe Warehouse, etc.
Leverage Agency Information Sources

- Risk Content
- Regulatory Content
- Vulnerability Scanners
- Continuous Controls Monitoring
- Patch Management
- Databases CMDB’s
- Emergency Notifications
- Security Event and Information Management
Holistic & Consistent Views of eGRC
Detailed Agency Dashboard Views
Next Steps

- Engage with the experts in the room
- Understand the capabilities/limitations
- Learn how to participate
- If you haven’t, read NIST IR 7904 (comments by 1/31/13)
- Ask for the technology from COTS providers and integrators
- Give us feedback and help drive standardization
Next Steps

- Engage SDO’s to cover gaps
- Revision 1 of NIST IR 7904: vSphere 5.1 with COTS attestation components (HyTrust Appliance)
- Integrate with other hypervisors, cloud management software, GRCs, etc.
- Extend trust beyond the hypervisor