Trusted Geolocation in The Cloud Technical Demonstration

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST National Institute of Standards and Technology

intel

RSA The Security Division of EMC | Archer technologies

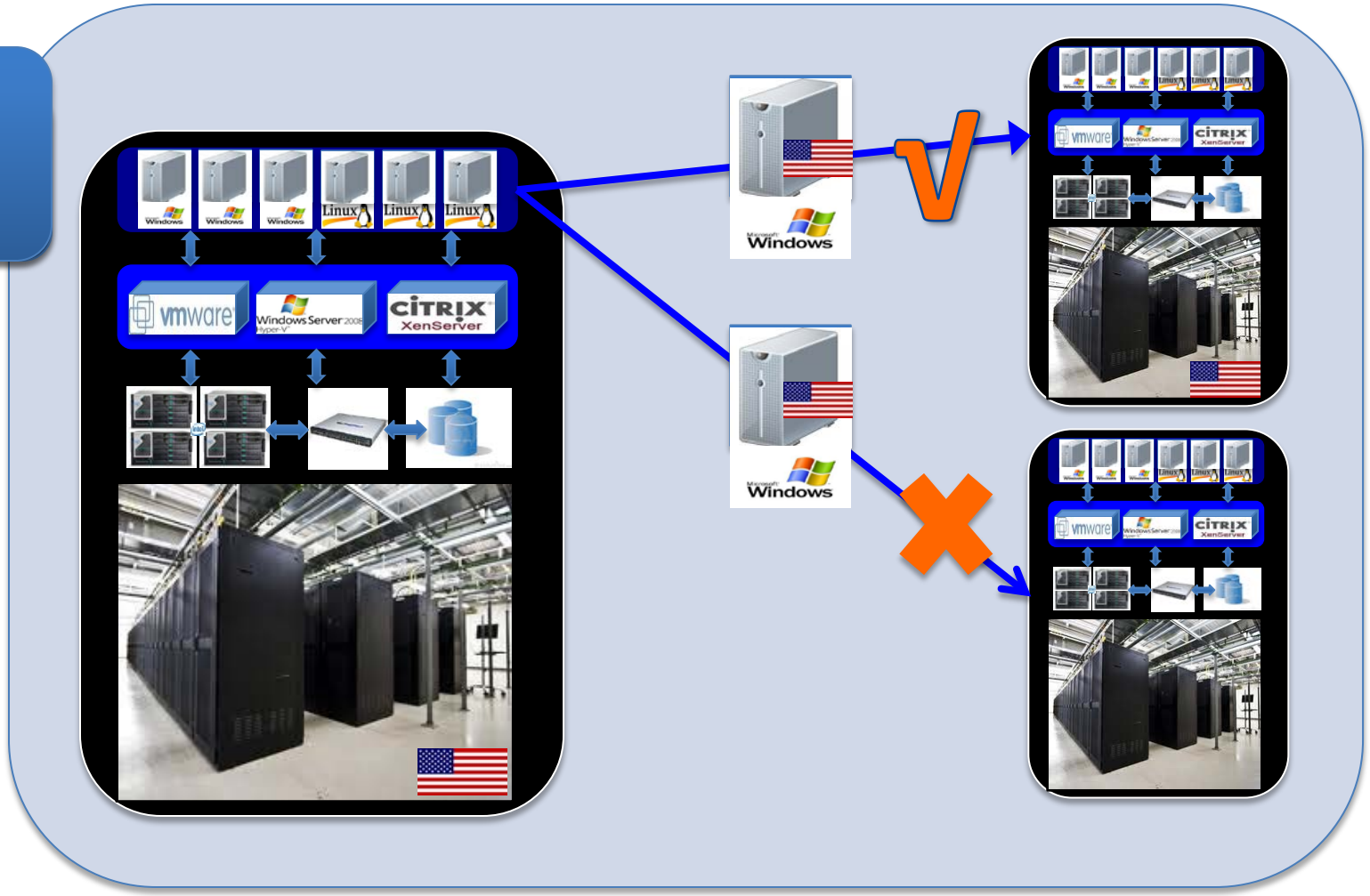
Trusted Geolocation in the Cloud

Business Opportunities

- 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

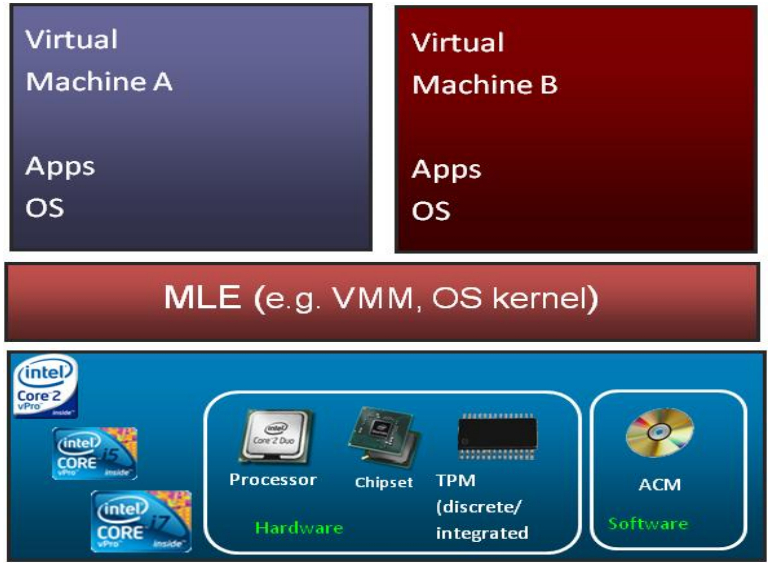
Security Requirements

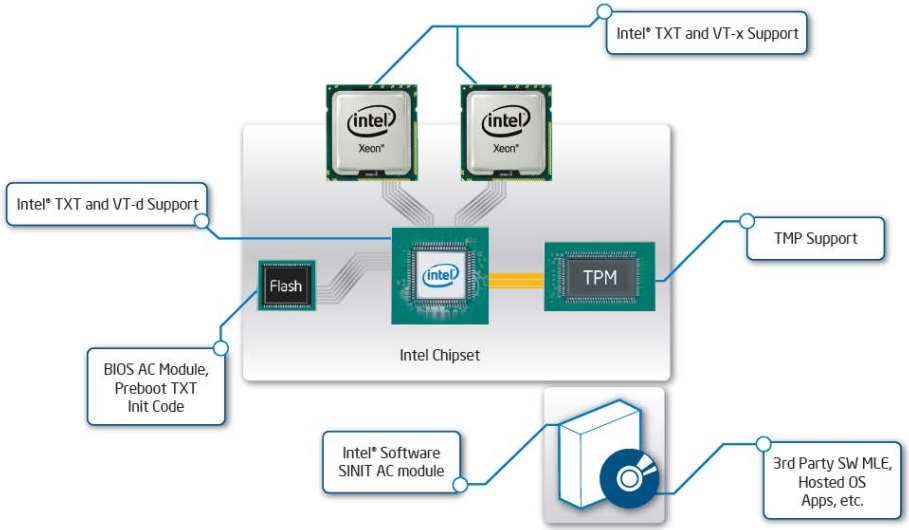
- **Trusted resource pool** based on hardware-based secure technical measurement capability
  - **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
  - **Trust-based secure migration** - Provide geolocation measurement and enforcement 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*

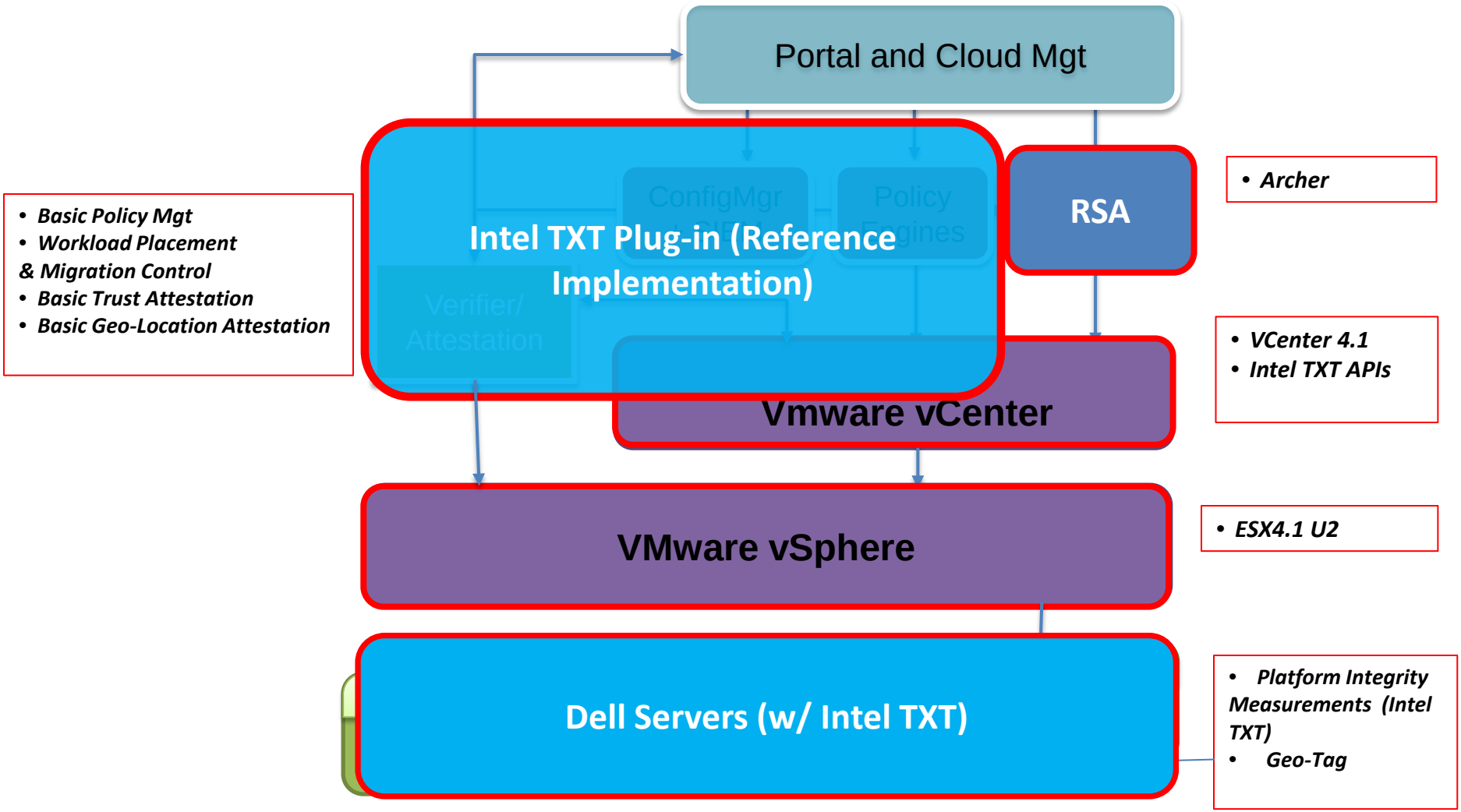
www.intel.com/txt

Trusted Cloud Solution

Solution Architecture

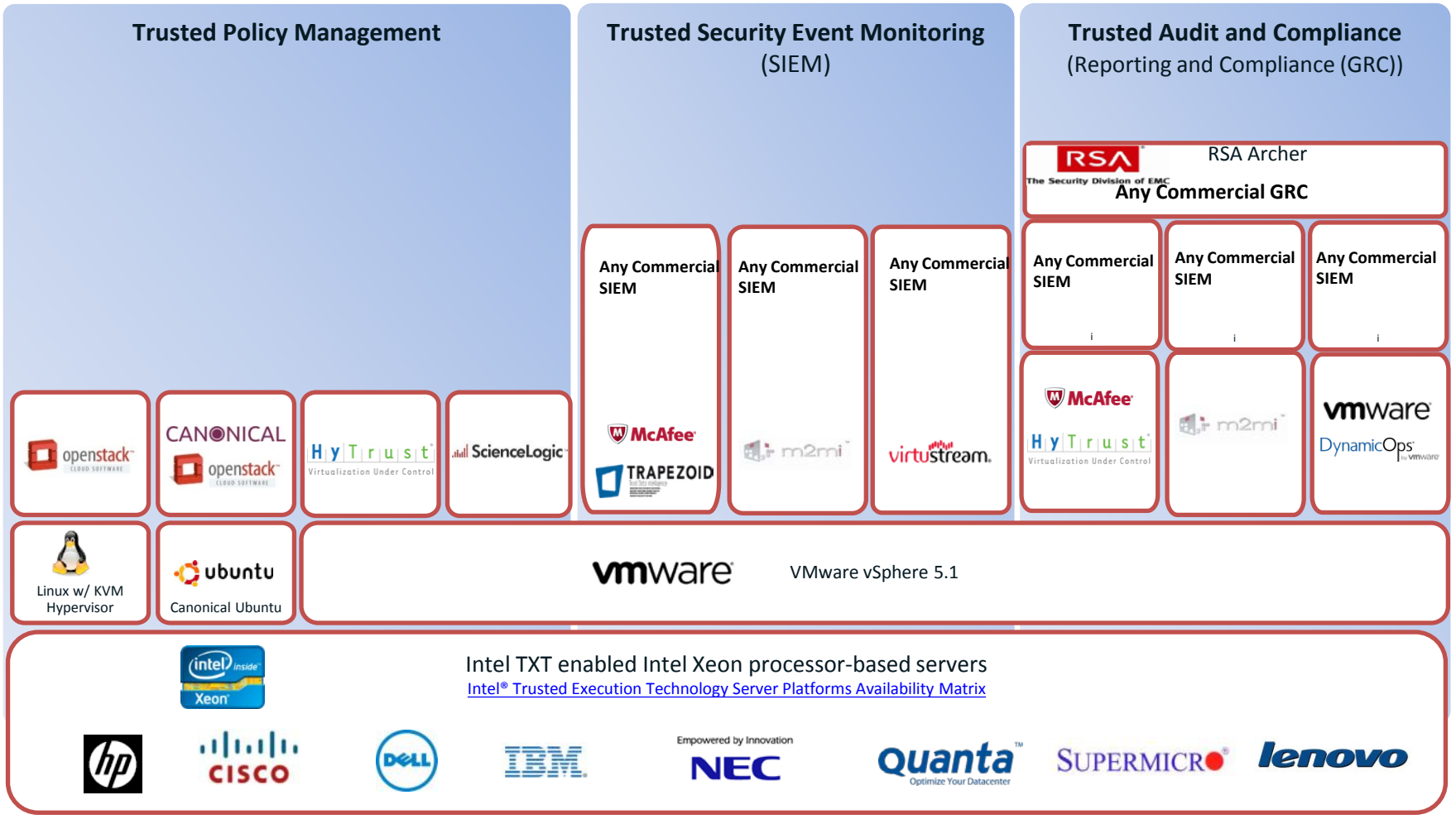
Trusted Cloud Solution

NIST Reference Design



Commercial Solutions In-flight based on this Reference Design.

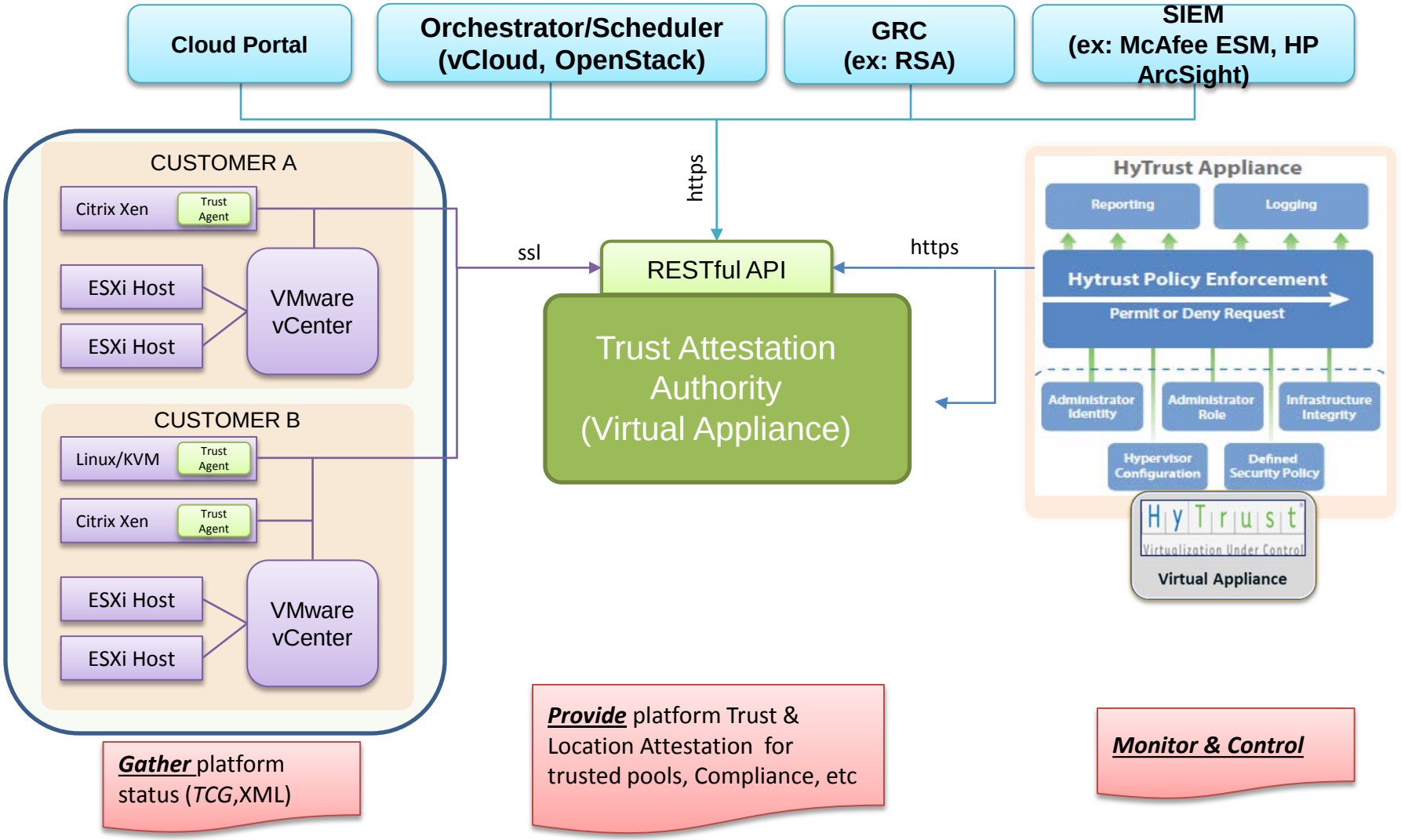
Trusted Compute Pools – Solution Stacks



Contact Your Favorite Provider for More Details

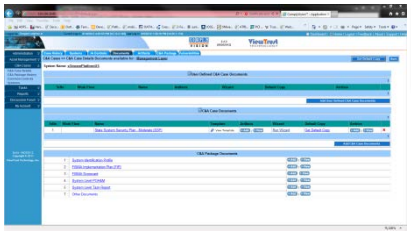
Trusted Cloud Architecture

Commercial Solutions



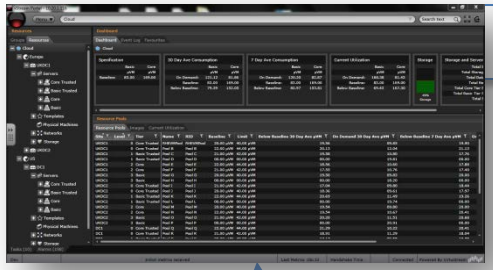
Trust Cloud Architecture
Commercial Solutions

virtustream

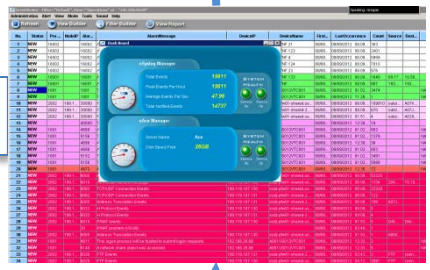


xStream GRC (xGRC)

Event Data



Cloud Provider Portal



xStream SIEM (xSIEM)

Cloud Subscriber Portal

Event Data

xStream

TXT Provider

VMWare 5.1 Provider

xSIEM Provider

Event Data

All Syslog/Events
High/Med/Low

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

Trust Attestation Authority

vCenter

KVM

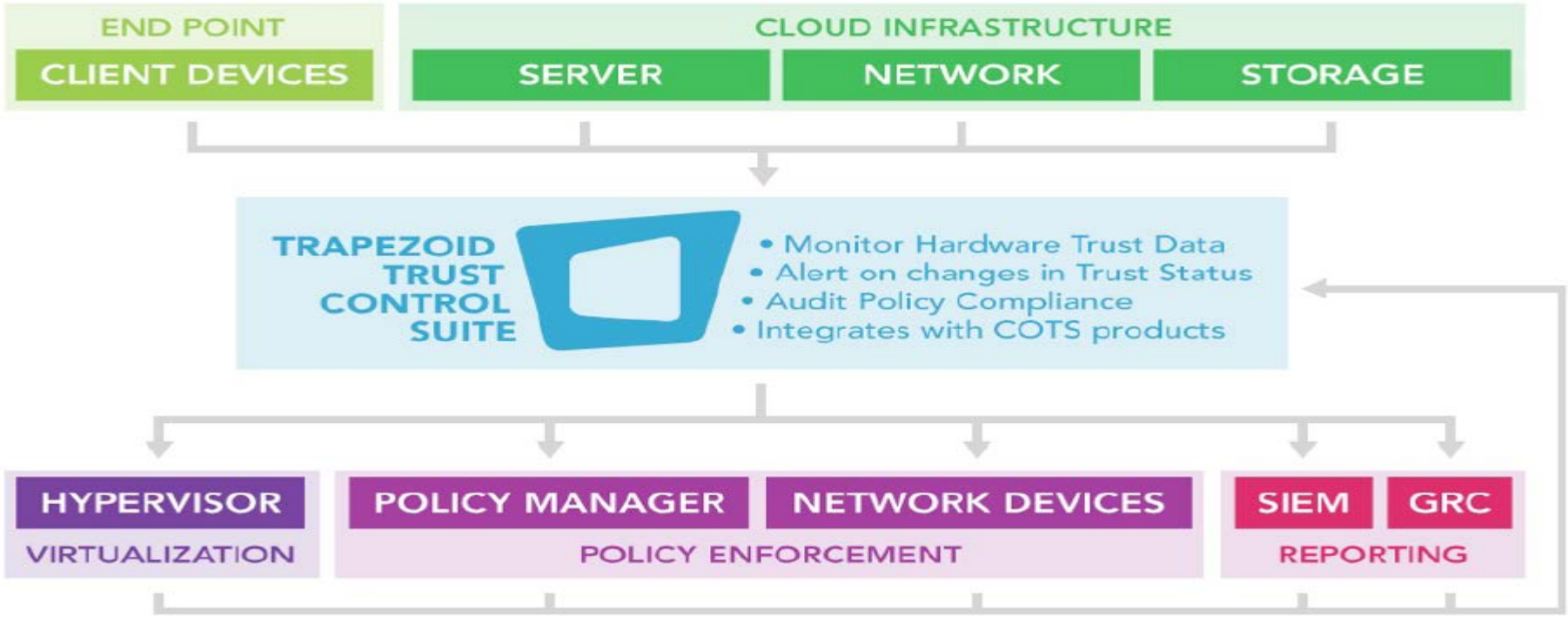
ESX

ESX

Trusted Cloud Infrastructure Commercial Solutions

TRAPEZOID TRUST CONTROL SUITE

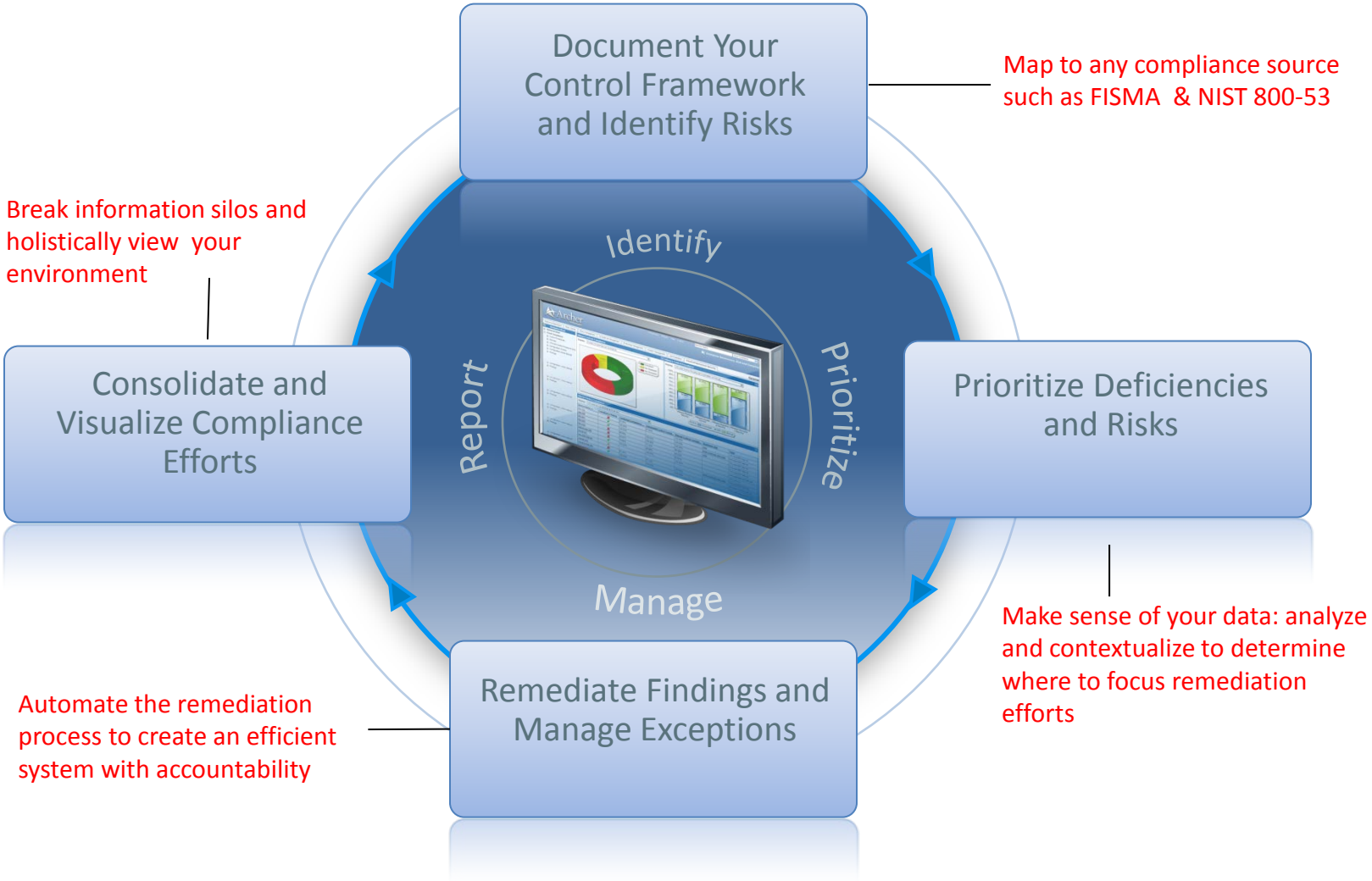
The Trapezoid® Trust Control Suite addresses hardware level computer attacks, a blind spot in current security defenses.



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



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.

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.

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

RSA Archer eGRC Platform

Flexible Platform Enabling Governance, Risk and Compliance

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.

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

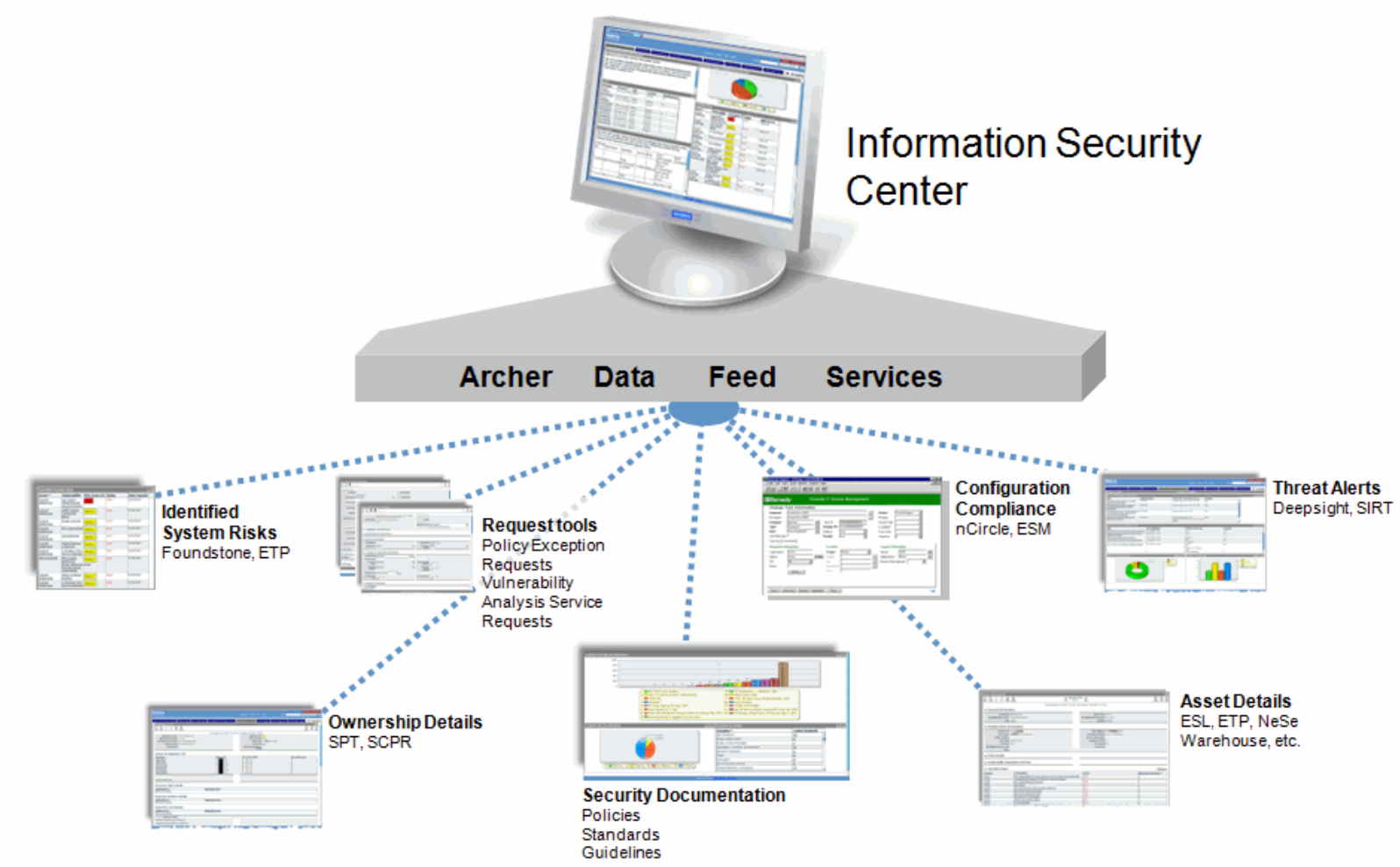
Reports and Dashboards
Gain a real-time view of your enterprise through actionable reports and graphical dashboards.

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.

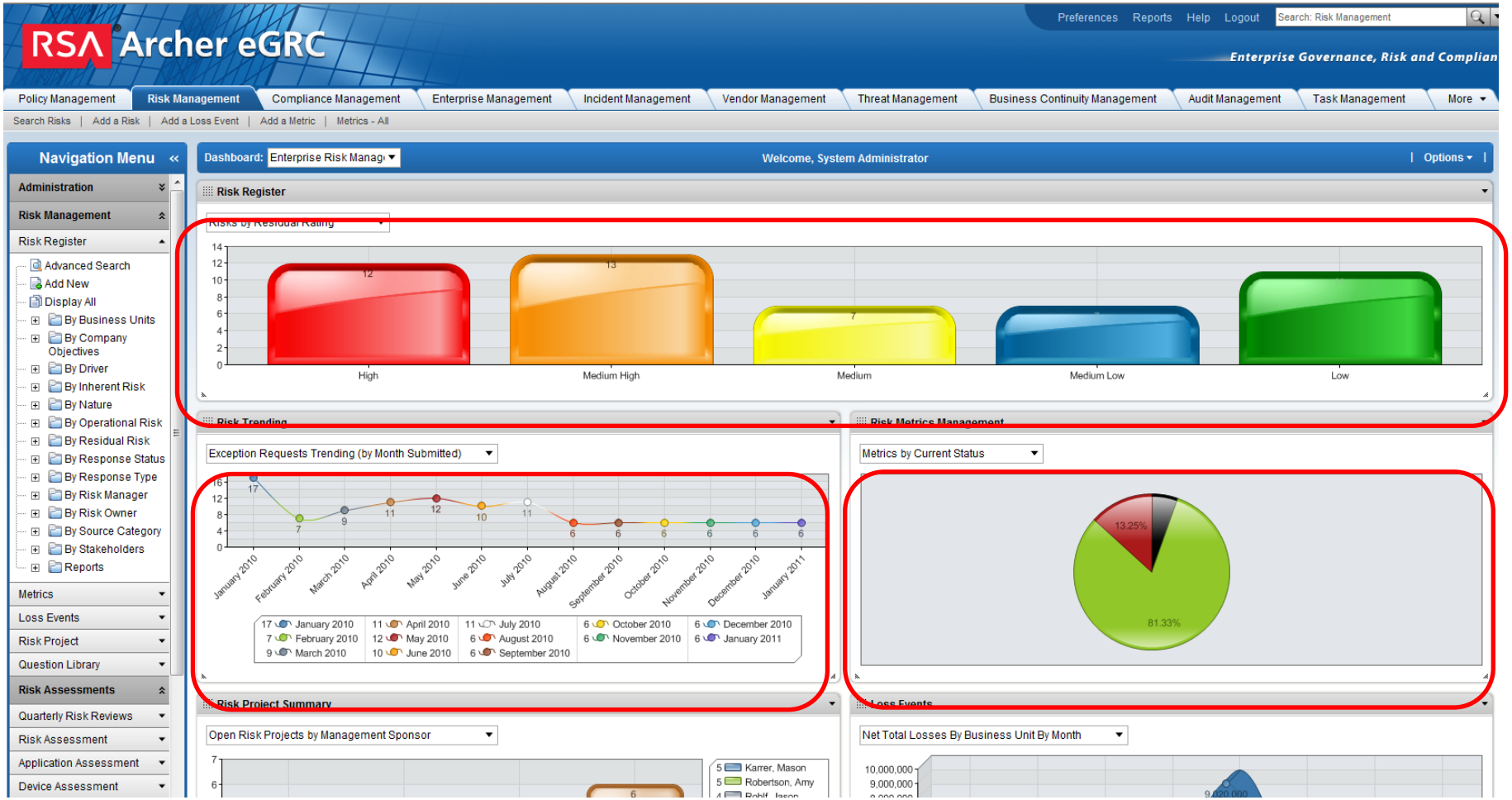
Maximize Compliance Information



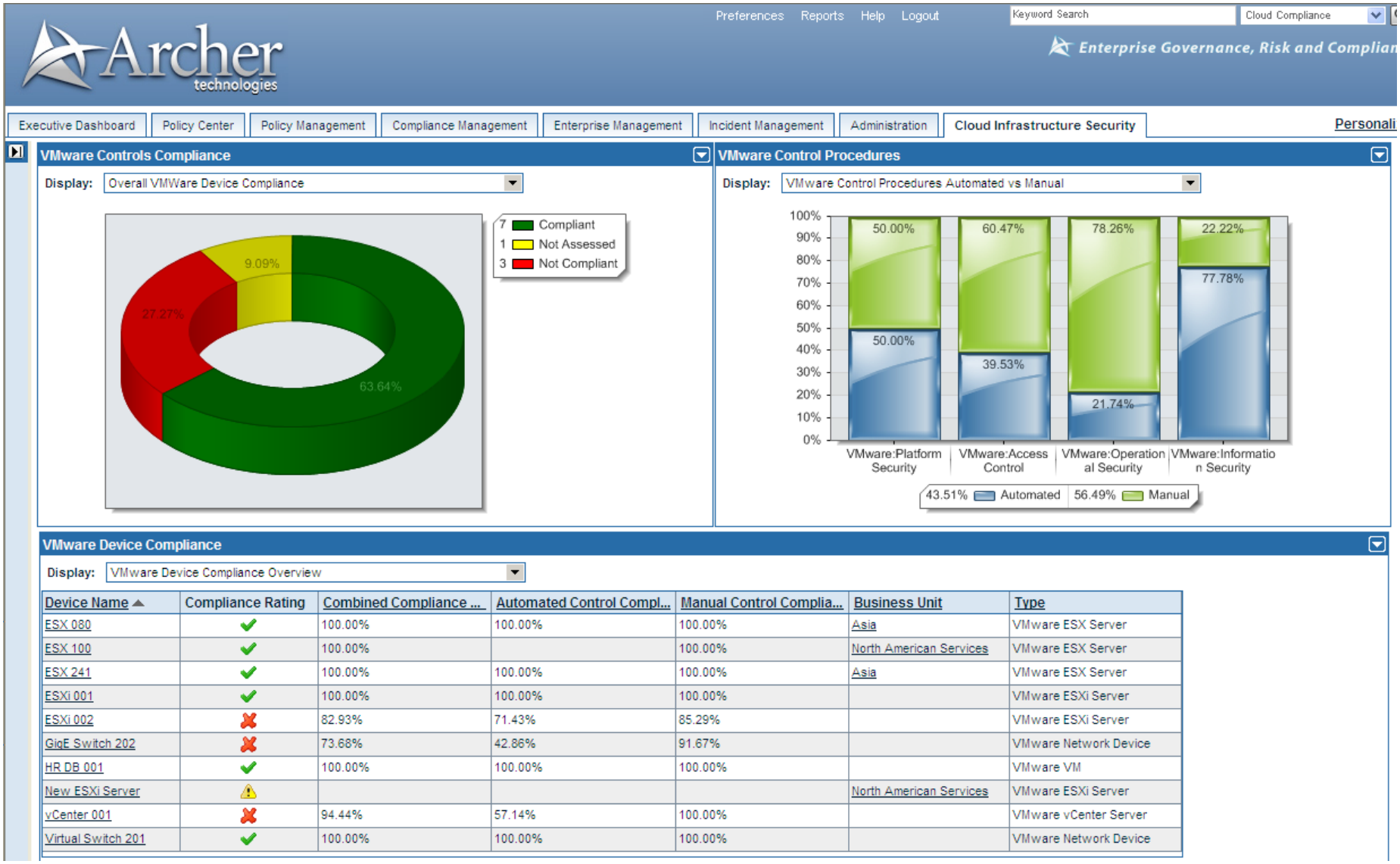
Leverage Agency Information Sources

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



Virtual Compliance Dashboards & Reports



Device Name	Compliance Rating	Combined Compliance ...	Automated Control Compl...	Manual Control Complia...	Business Unit	Type
ESX 080	✔	100.00%	100.00%	100.00%	Asia	VMware ESX Server
ESX 100	✔	100.00%		100.00%	North American Services	VMware ESX Server
ESX 241	✔	100.00%	100.00%	100.00%	Asia	VMware ESX Server
ESXi 001	✔	100.00%	100.00%	100.00%		VMware ESXi Server
ESXi 002	✘	82.93%	71.43%	85.29%		VMware ESXi Server
GigE Switch 202	✘	73.68%	42.86%	91.67%		VMware Network Device
HR DB 001	✔	100.00%	100.00%	100.00%		VMware VM
New ESXi Server	⚠				North American Services	VMware ESXi Server
vCenter 001	✘	94.44%	57.14%	100.00%		VMware vCenter Server
Virtual Switch 201	✔	100.00%	100.00%	100.00%		VMware Network Device

Detailed Agency Dashboard Views

Trusted Geolocation in the Cloud

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

Trusted Geolocation in the Cloud

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