

Trusted Geolocation in The Cloud Technical Demonstration

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



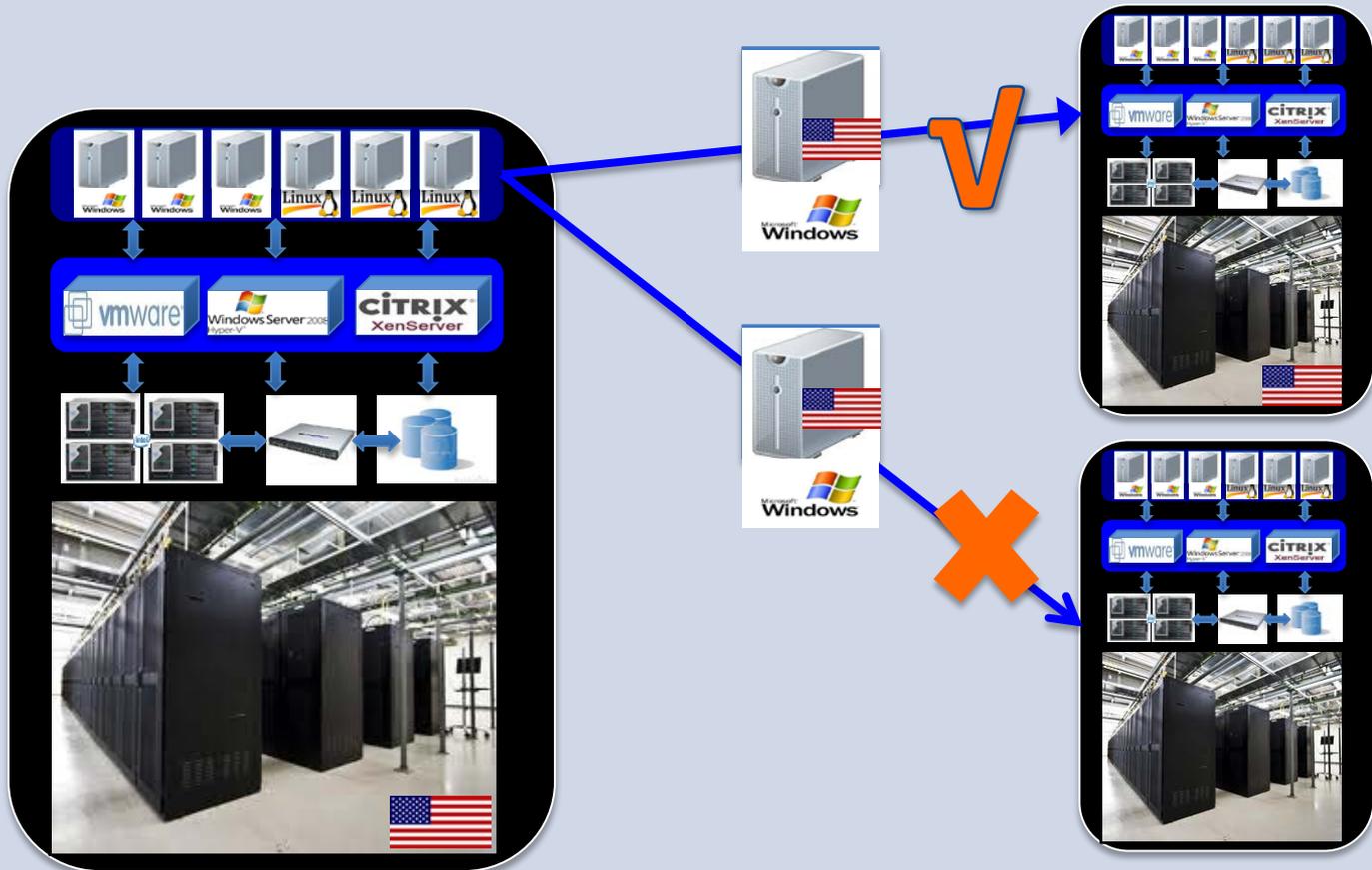
Trusted Geolocation in the Cloud

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

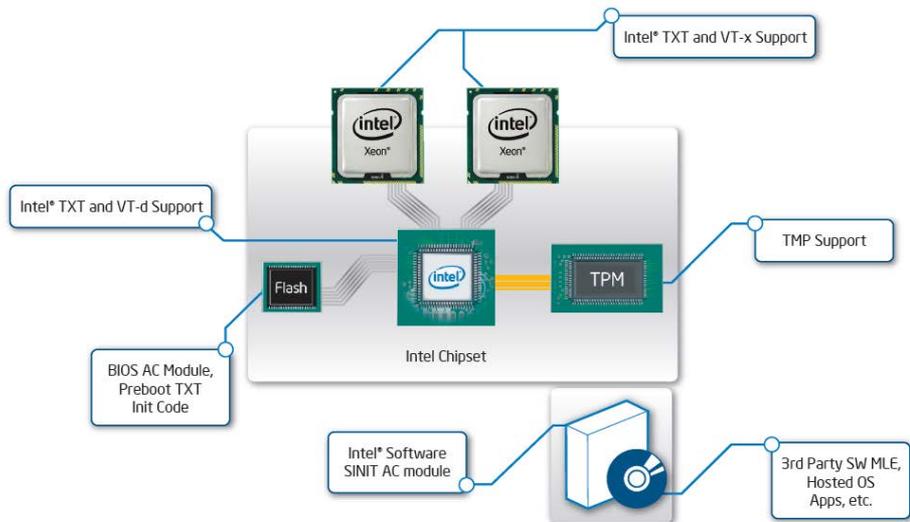
Security Requirements

- **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

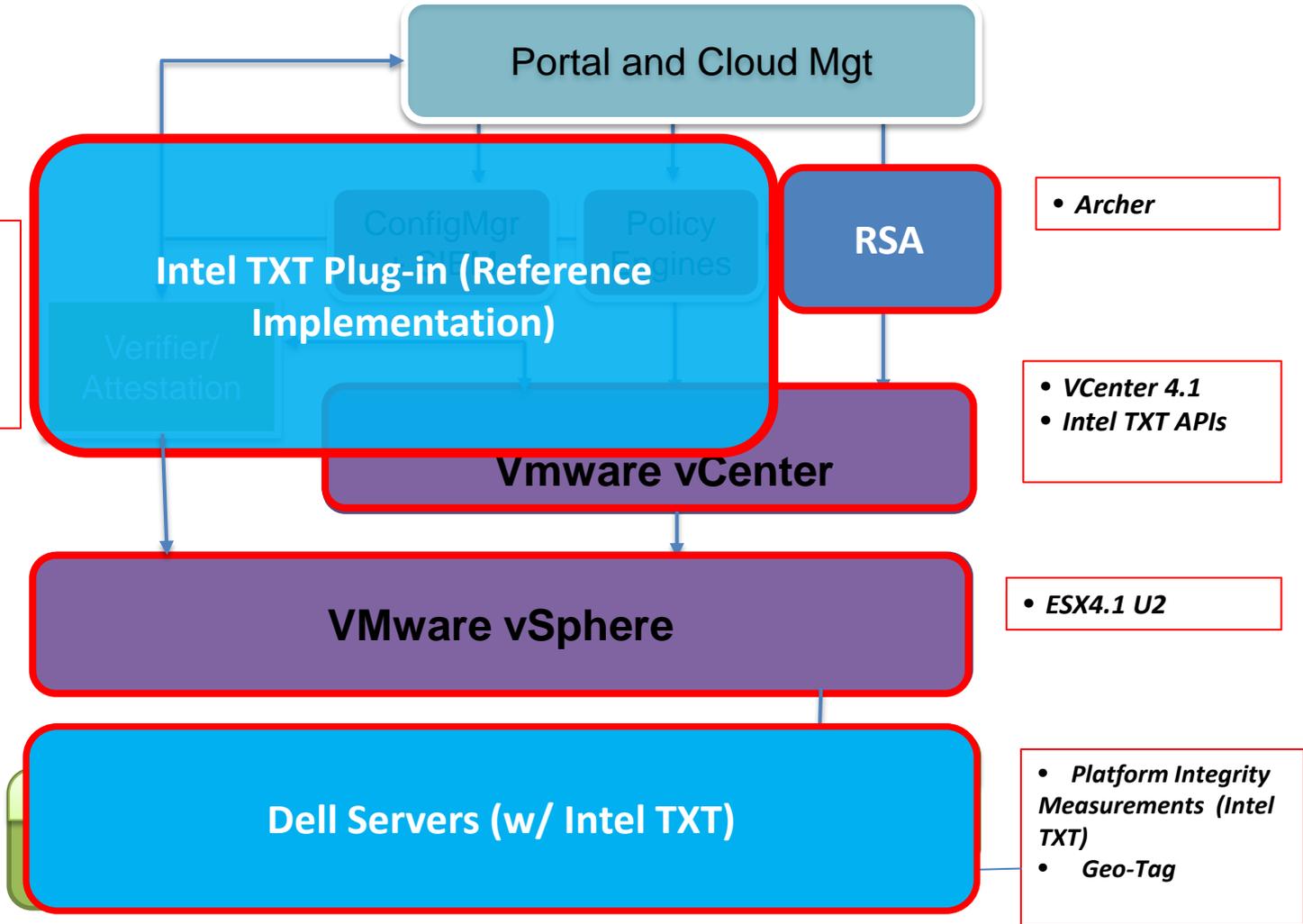
A hardware based security foundation (Root of Trust) to build and maintain a chain of trust, to protect the platform from software based attacks



Trusted and verifiable systems

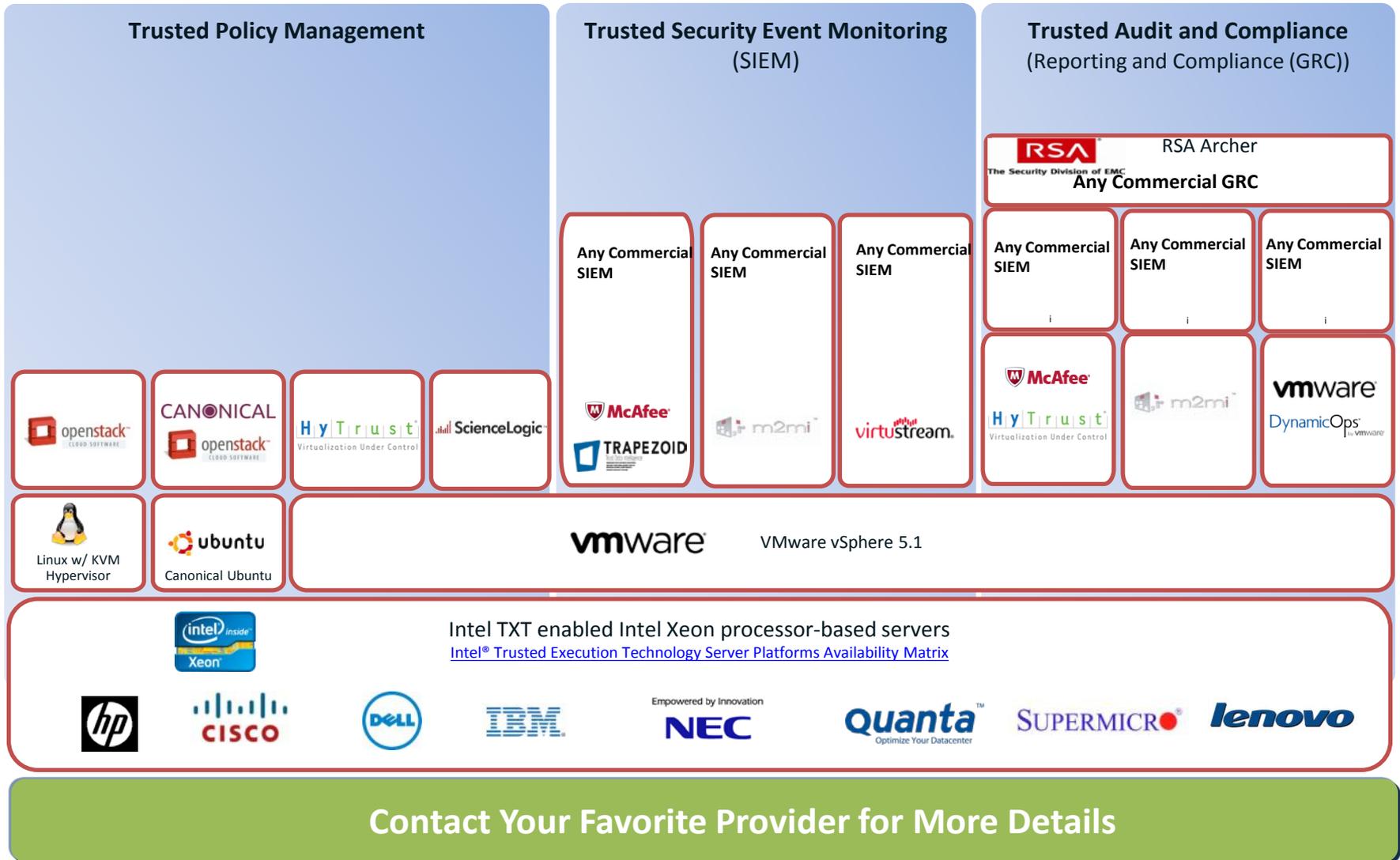
- Implement policies/controls on top of a foundation of trust beginning in HW and up the stack
- VMware, SUSE, Redhat and others have products that support HW roots of trust and attestation

Trusted Cloud Solution NIST Reference Design

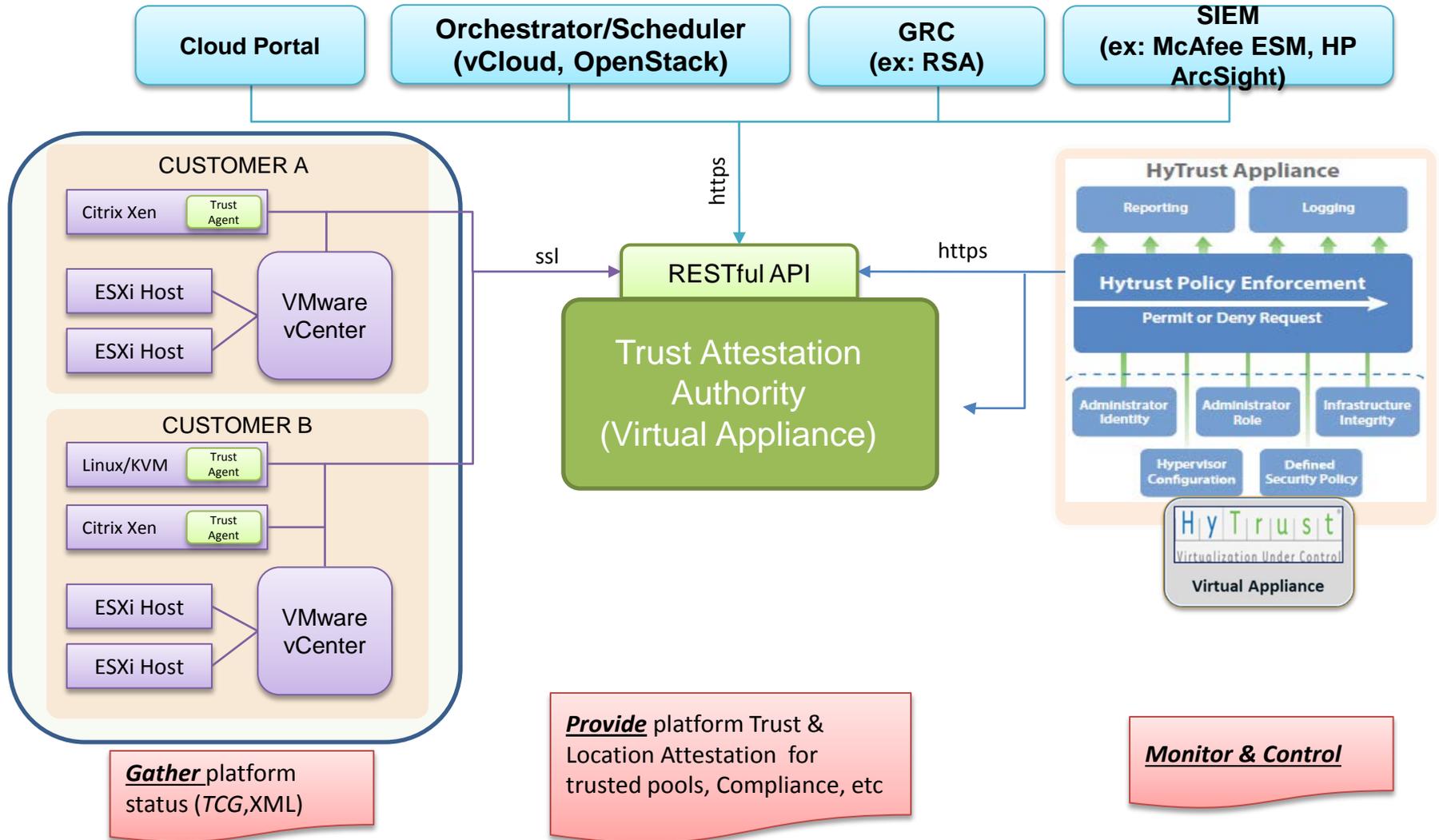


Commercial Solutions In-flight based on this Reference Design.

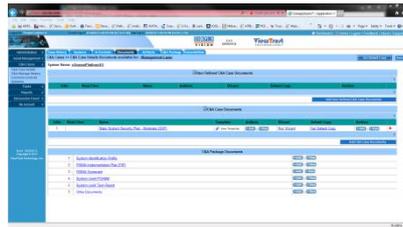
Trusted Compute Pools – Solution Stacks



Trusted Cloud Architecture Commercial Solutions



Trust Cloud Architecture Commercial Solutions



xStream GRC (xGRC)

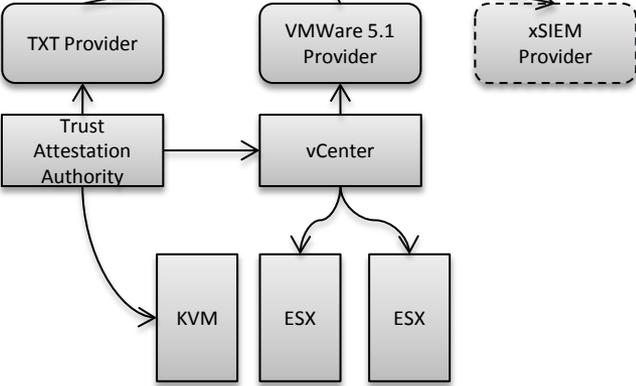


Cloud Provider Portal

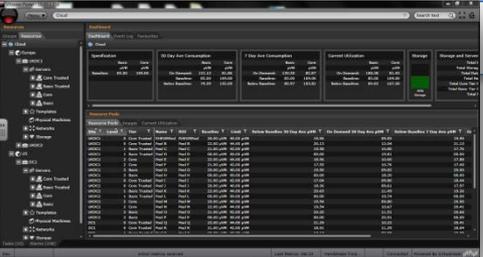
xStream SIEM (xSIEM)



Cloud Subscriber Portal



All Syslog/Events
High/Med/Low

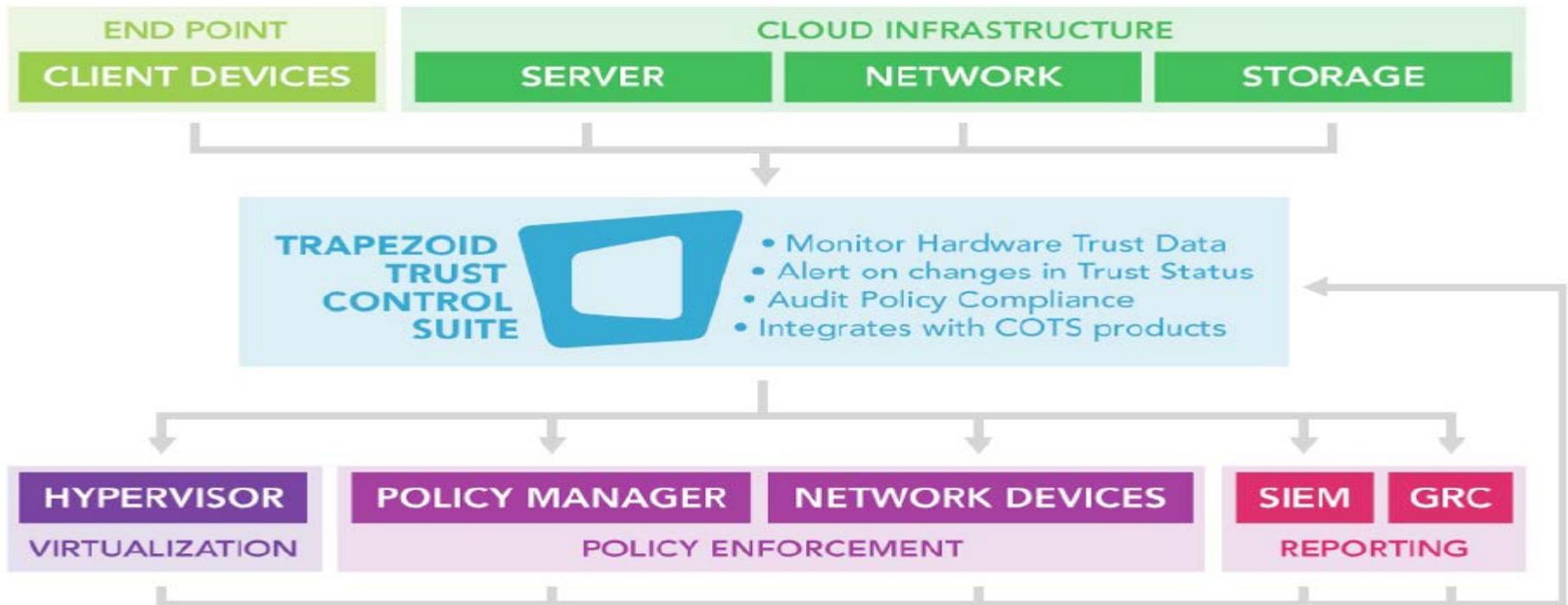


- Visibility & Monitoring
- Placement policy
- Geo tagging
- PII Compliance Decisions

Trusted Cloud Infrastructure Commercial Solutions



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

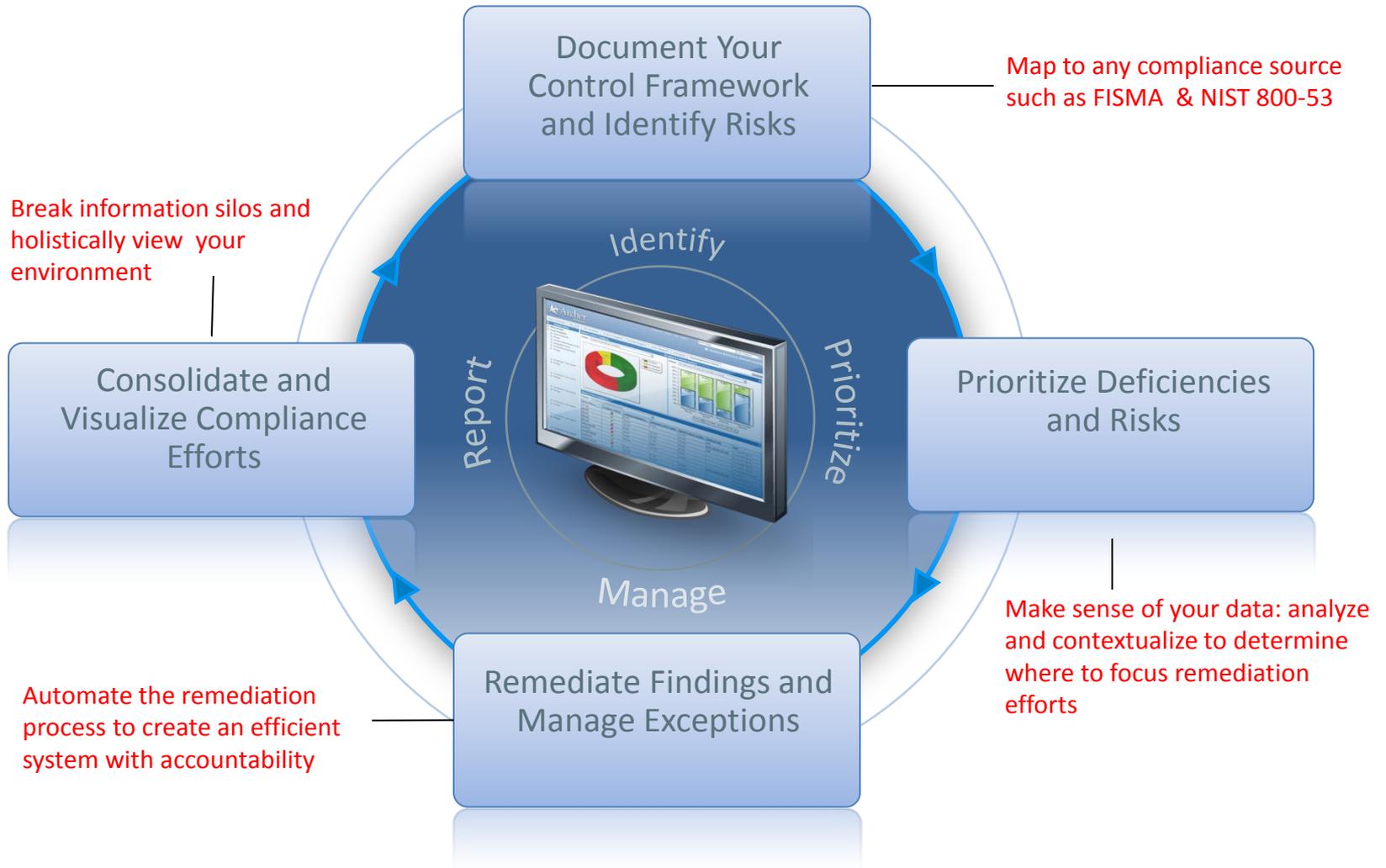


About Archer

- ▶ 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.

Threat Management

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

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

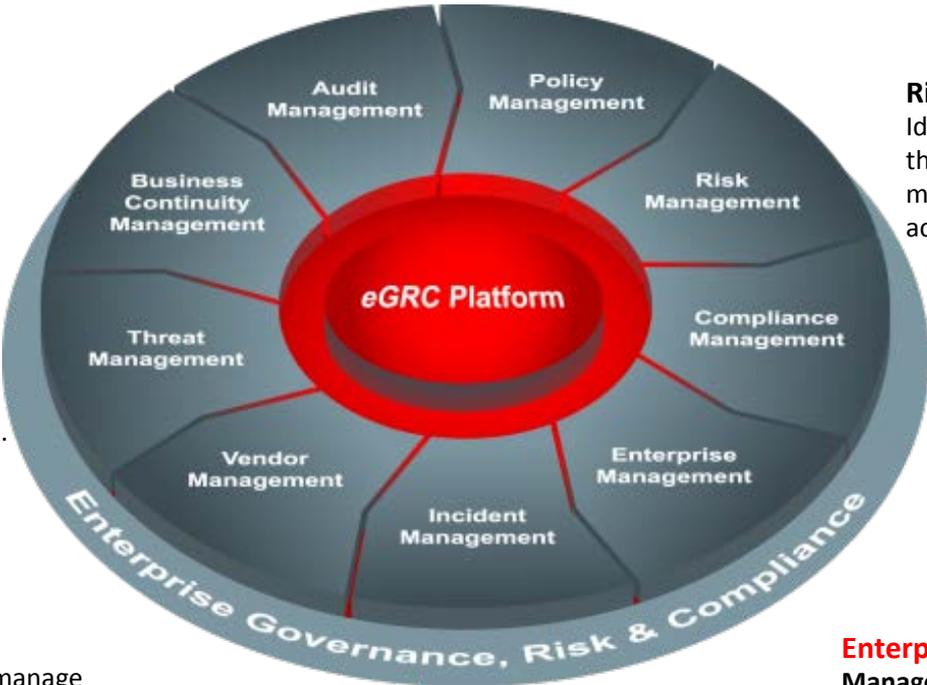
Manage relationships and dependencies within your enterprise hierarchy and infrastructure to support risk and compliance initiatives.

Risk Management

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

Compliance Management

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



RSA Archer eGRC Platform

Flexible Platform Enabling Governance, Risk and Compliance

User Experience

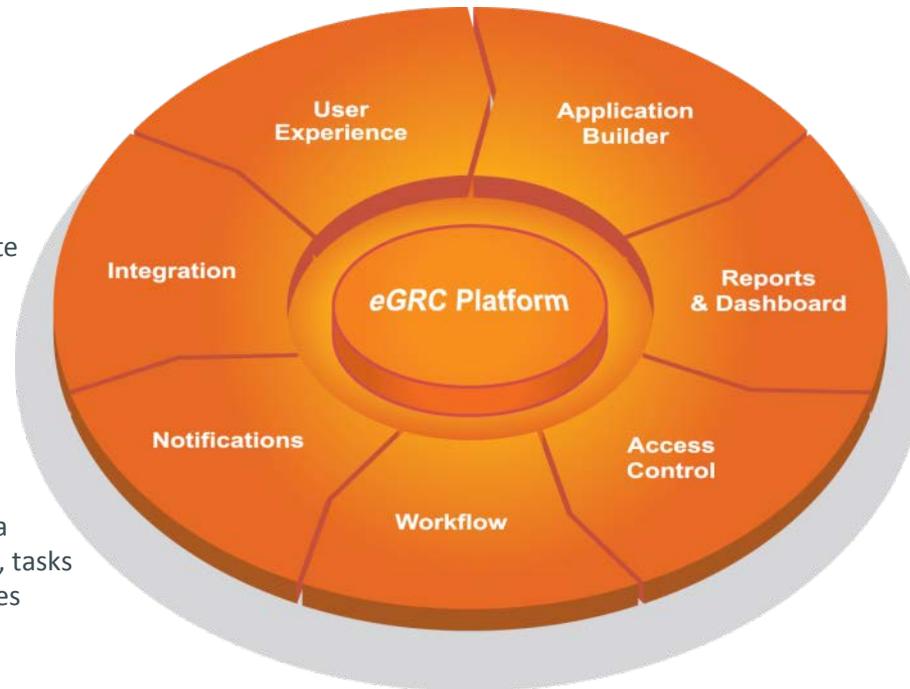
Brand the interface with your corporate colors, graphics, icons and text to facilitate end-user adoption.

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.

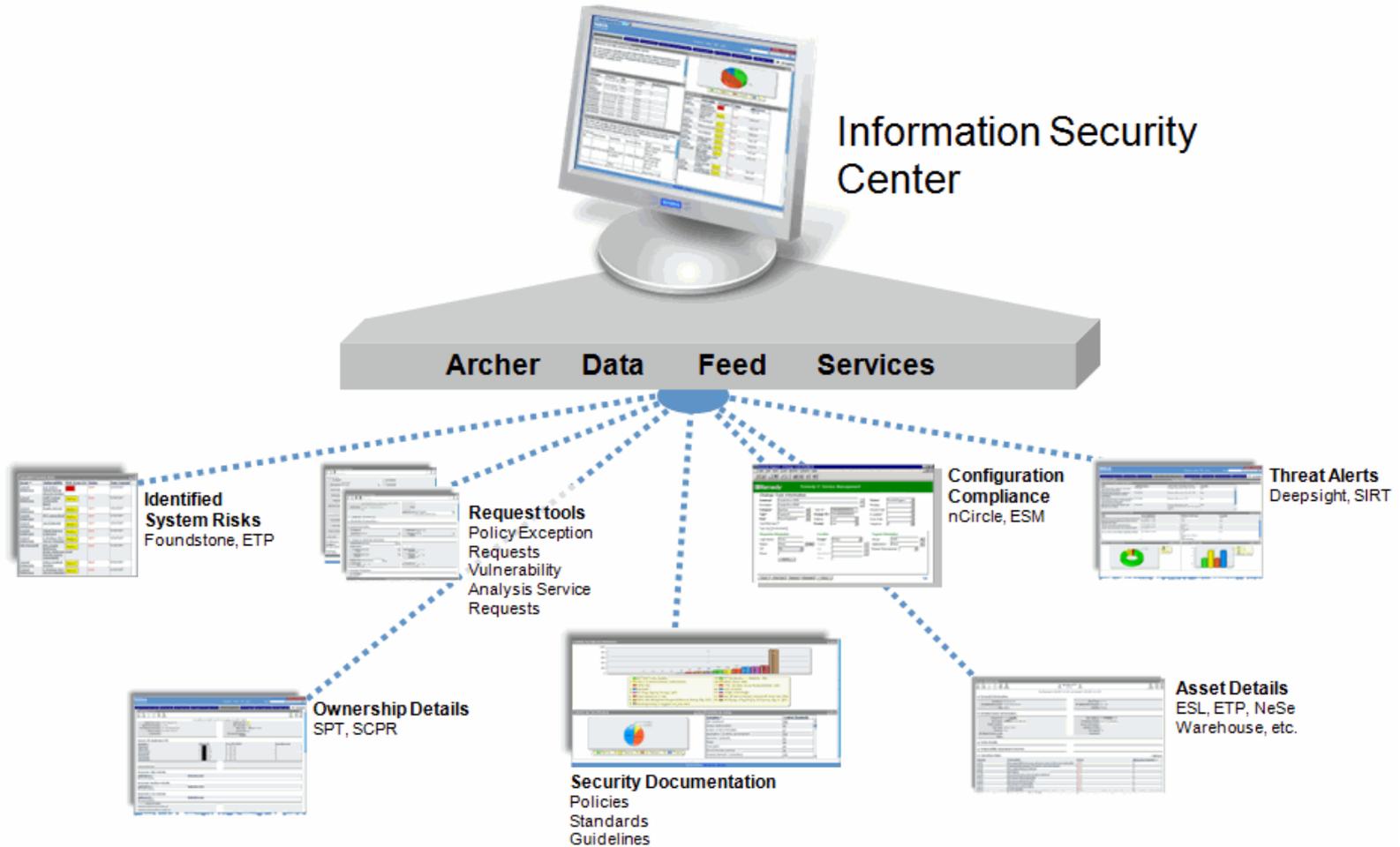
Access Control

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



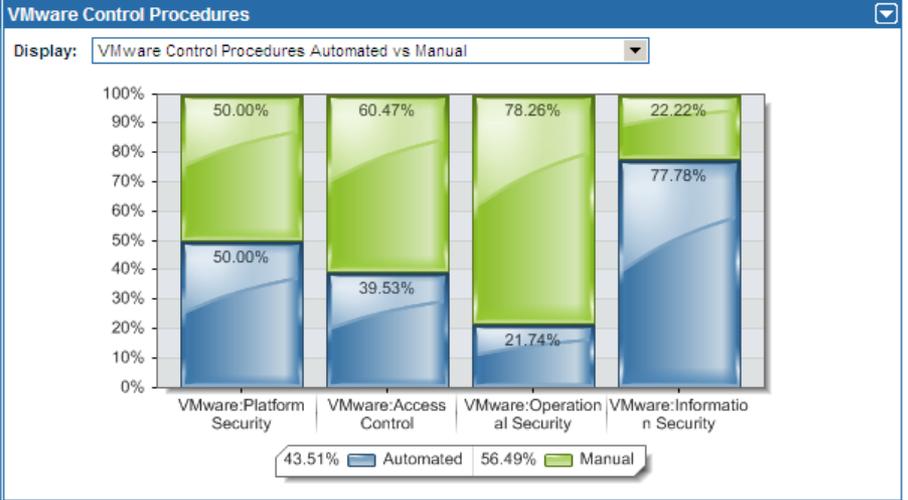
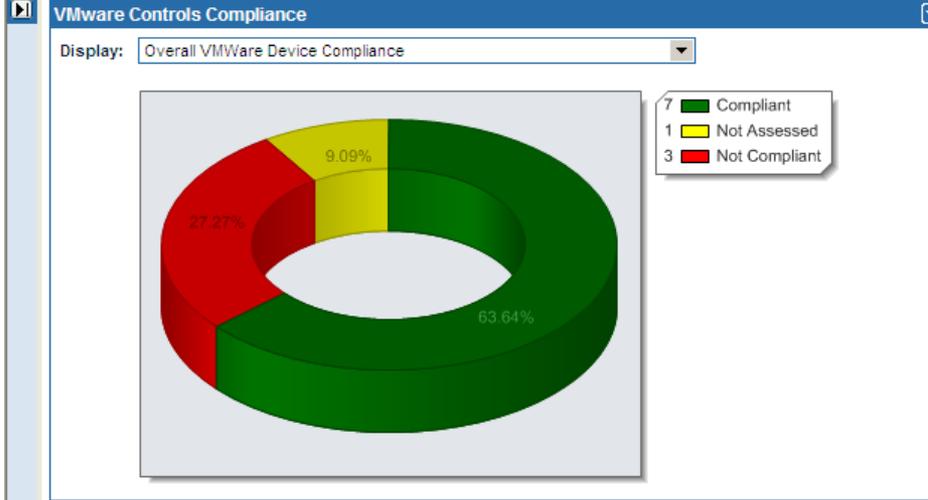
Holistic & Consistent Views of eGRC

The screenshot displays the RSA Archer eGRC dashboard interface. At the top, the header includes the RSA Archer eGRC logo, navigation links (Preferences, Reports, Help, Logout), a search bar for 'Risk Management', and the tagline 'Enterprise Governance, Risk and Compliance'. Below the header is a main navigation bar with tabs for Policy Management, Risk Management, Compliance Management, Enterprise Management, Incident Management, Vendor Management, Threat Management, Business Continuity Management, Audit Management, Task Management, and More. A secondary navigation bar offers actions like Search Risks, Add a Risk, Add a Loss Event, Add a Metric, and Metrics - All.

The dashboard content is organized into several sections:

- Navigation Menu:** A sidebar on the left provides access to Administration, Risk Management, Risk Register, Metrics, Loss Events, Risk Project, Question Library, Risk Assessments, Quarterly Risk Reviews, Risk Assessment, Application Assessment, and Device Assessment.
- Dashboard:** The main area features a 'Welcome, System Administrator' message and a 'Risk Register' section. A prominent bar chart, 'Risks by Residual Rating', shows the distribution of risks across five categories: High (12), Medium High (13), Medium (7), Medium Low (6), and Low (6).
- Exception Requests Trending (by Month Submitted):** A line chart showing the number of exception requests from January 2010 to January 2011. The data points are: Jan 2010 (17), Feb 2010 (7), Mar 2010 (9), Apr 2010 (11), May 2010 (12), Jun 2010 (10), Jul 2010 (11), Aug 2010 (6), Sep 2010 (6), Oct 2010 (6), Nov 2010 (6), Dec 2010 (6), and Jan 2011 (6).
- Risk Metrics Management:** A pie chart titled 'Metrics by Current Status' shows that 81.33% of metrics are in a green state, while 13.25% are in a red state.
- Risk Project Summary:** A section for 'Open Risk Projects by Management Sponsor' lists projects managed by Karrer, Mason (5), Robertson, Army (5), and P-hif, Isaac (4).
- Net Total Losses By Business Unit By Month:** A bar chart showing net total losses, with a peak of 9,000,000 in one month.

Virtual Compliance Dashboards & Reports



VMware Device Compliance

Display: VMware Device Compliance Overview

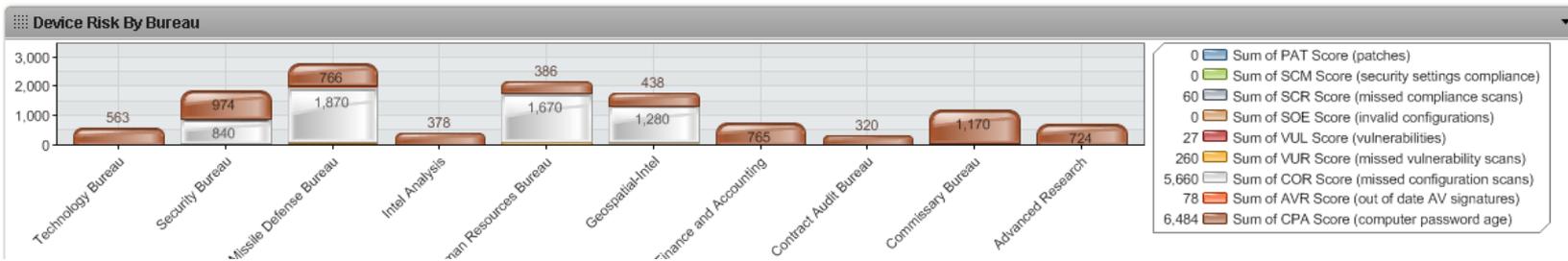
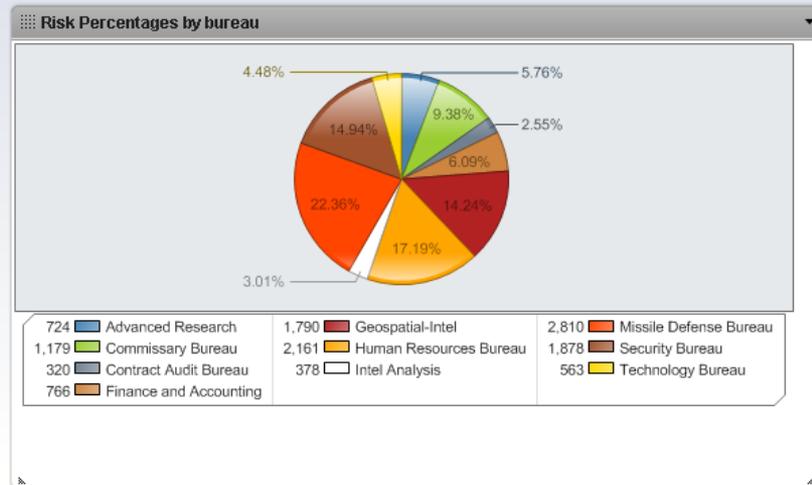
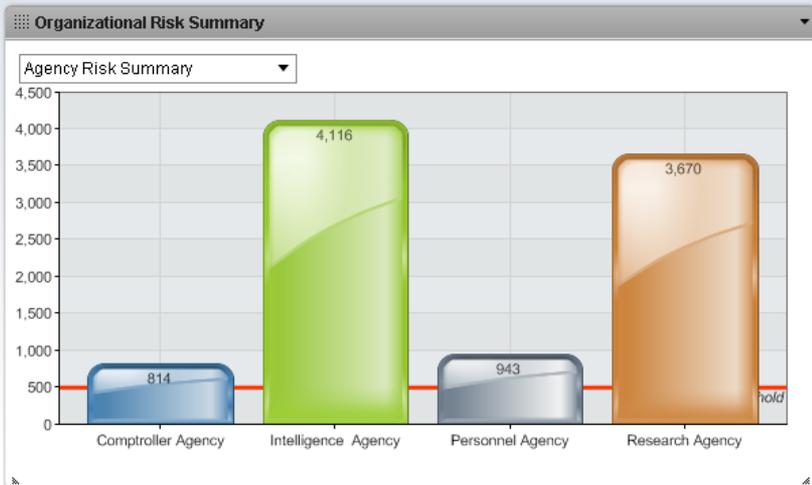
Device Name	Compliance Rating	Combined Compliance	Automated Control Compl...	Manual Control Complia...	Business Unit	Type
ESX 080	✓	100.00%	100.00%	100.00%	Asia	VMware ESX Server
ESX 100	✓	100.00%	100.00%	100.00%	North American Services	VMware ESX Server
ESX 241	✓	100.00%	100.00%	100.00%	Asia	VMware 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



Navigation Menu <<

- Administration
- Continuous Monitoring
 - Devices
 - Users
 - Vulnerability Scan Results
 - Configuration Checks
 - Configuration Check Results
 - Exception Requests
 - Remediation Plans
 - Authoritative Sources



- 0 Sum of PAT Score (patches)
- 0 Sum of SCM Score (security settings compliance)
- 60 Sum of COR Score (missed compliance scans)
- 0 Sum of SOE Score (invalid configurations)
- 27 Sum of VUL Score (vulnerabilities)
- 260 Sum of VUR Score (missed vulnerability scans)
- 5,660 Sum of COR Score (missed configuration scans)
- 78 Sum of AVR Score (out of date AV signatures)
- 6,484 Sum of CPA Score (computer password age)

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