Operating Highly Secure Enterprise Hybrid Cloud

Safely operating Systems of Record

GLOBAL PRODUCT DATA
INTEROPERABILITY
SUMMIT
2016

ELYSIUM

Parker | Aerospace

NORTHROP GRUMMAN

BOEING

virtustream®

Speaker

Kaus Phaltankar

President, Virtustream Security Solutions

- Chair, Sub-committee for Big Data, AFCEA International
- Publication – Implementing Secure Intranets and Extranets
- Patents – Network Engineering
- Adjunct faculty – University of Miami

ELYSIUM Parker NORTHROP GRUMMAN BOEING GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

# About Virtustream

A Dell Technologies Company

- 2,000+ employees
- 20+ data centers
- Major operations in 10 countries
- One of the fastest growing EMC companies

Technology Leadership

- IP Leader in cloud enterprise app assurance and security
- Inventor of the µVM™ cloud technology
- Developer of xStream® Management Software
- Operator of leading enterprise-class cloud IaaS
- One of the world's largest storage platforms

The shift in cloud adoption
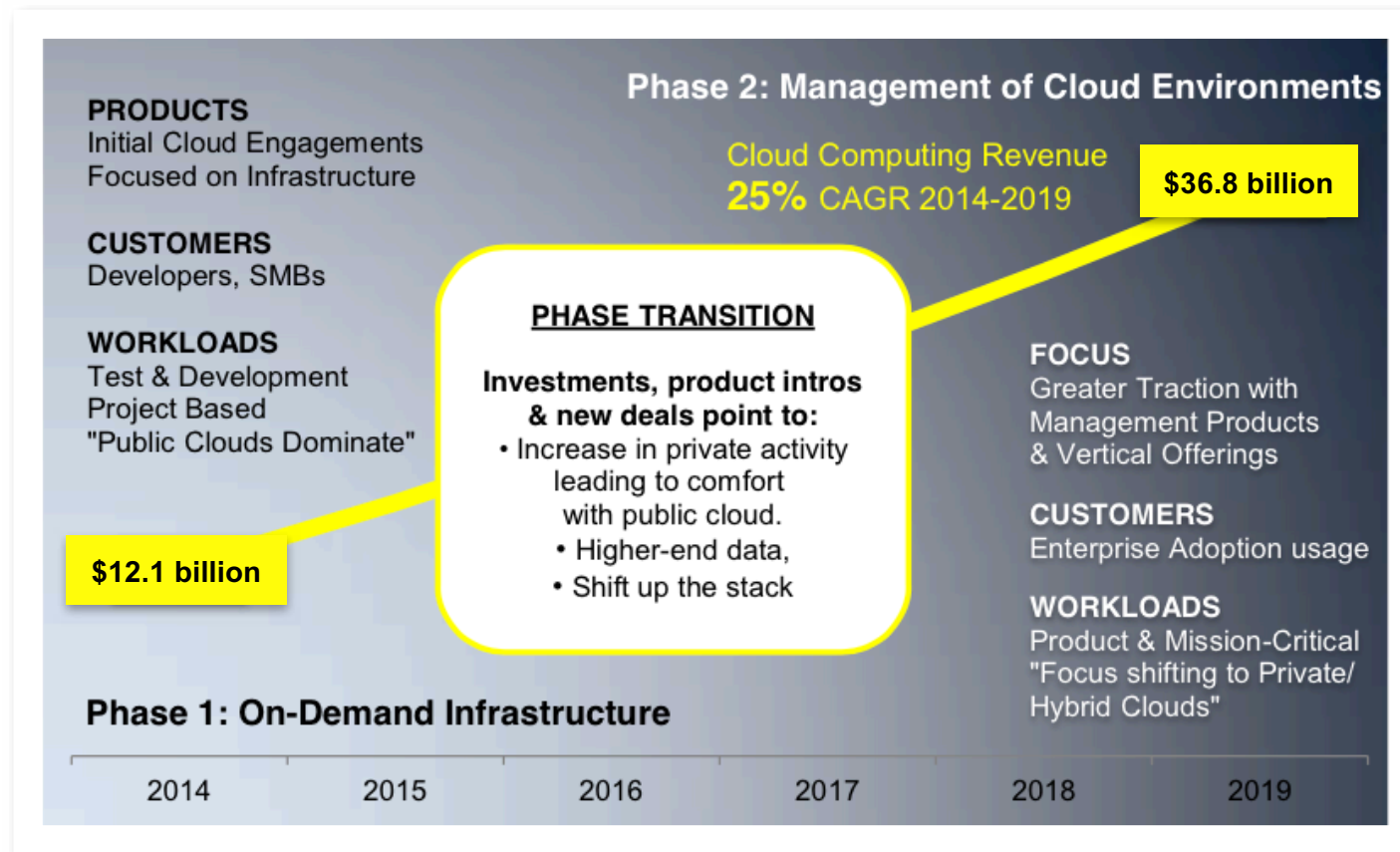
Source: 451 Research Cloud Computing Market Overview, May 2015

Key Priorities

Application Transformation
Cloud-enable traditional apps; provide platform for cloud-native

Operational Automation
Bring cloud automation and agility to enterprise apps & ops

Infrastructure Modernization
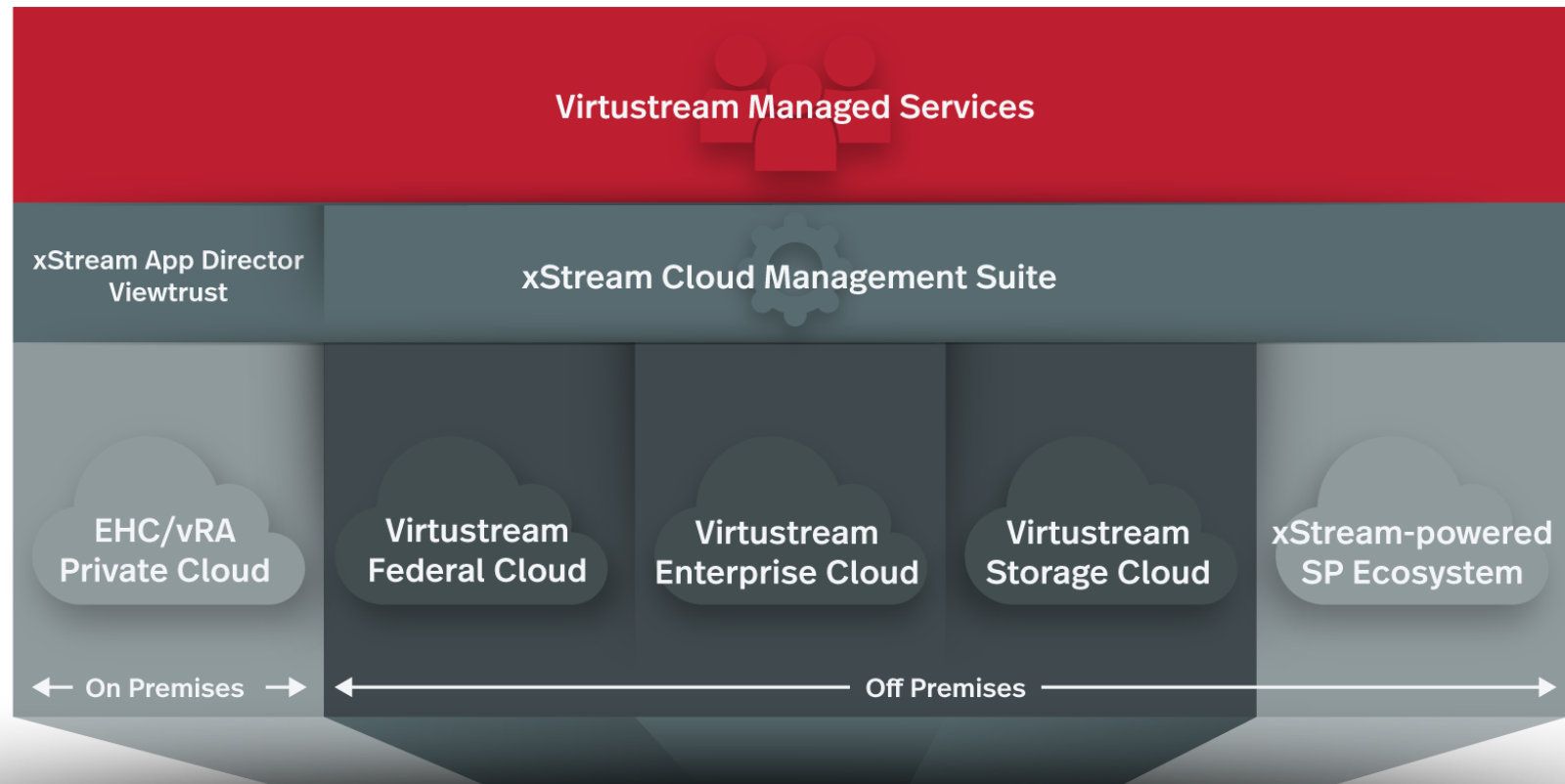Platform to assure efficiency, resiliency, performance & agility

ELYSIUM   Parker   NORTHROP GRUMMAN   BOEING   GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

A changing conversation

Public vs. Private	Hybrid
Infrastructure	Applications
Server Deployment	Service Delivery
Self-Service	Managed Services
Supply Utility	**Deliver Business Value**

ELYSIUM   Parker   NORTHROP GRUMMAN   BOEING   GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

Built for the Enterprise

Virtustream Enterprise Cloud

Built for Mission-Critical Systems of Record

- Designed and tuned for mission-critical, I/O-intensive apps
- SLAs for application performance
- Planning and migration services
- Full suite of managed services including application expertise
- Also available for government organizations

Flexible, hybrid deployments

- Virtual private or public architecture
- Federate with on-premises private clouds & global footprint of xStream-powered service provider clouds

xStream-powered Cloud

- Greater efficiency & automation
- Consumption-based pricing
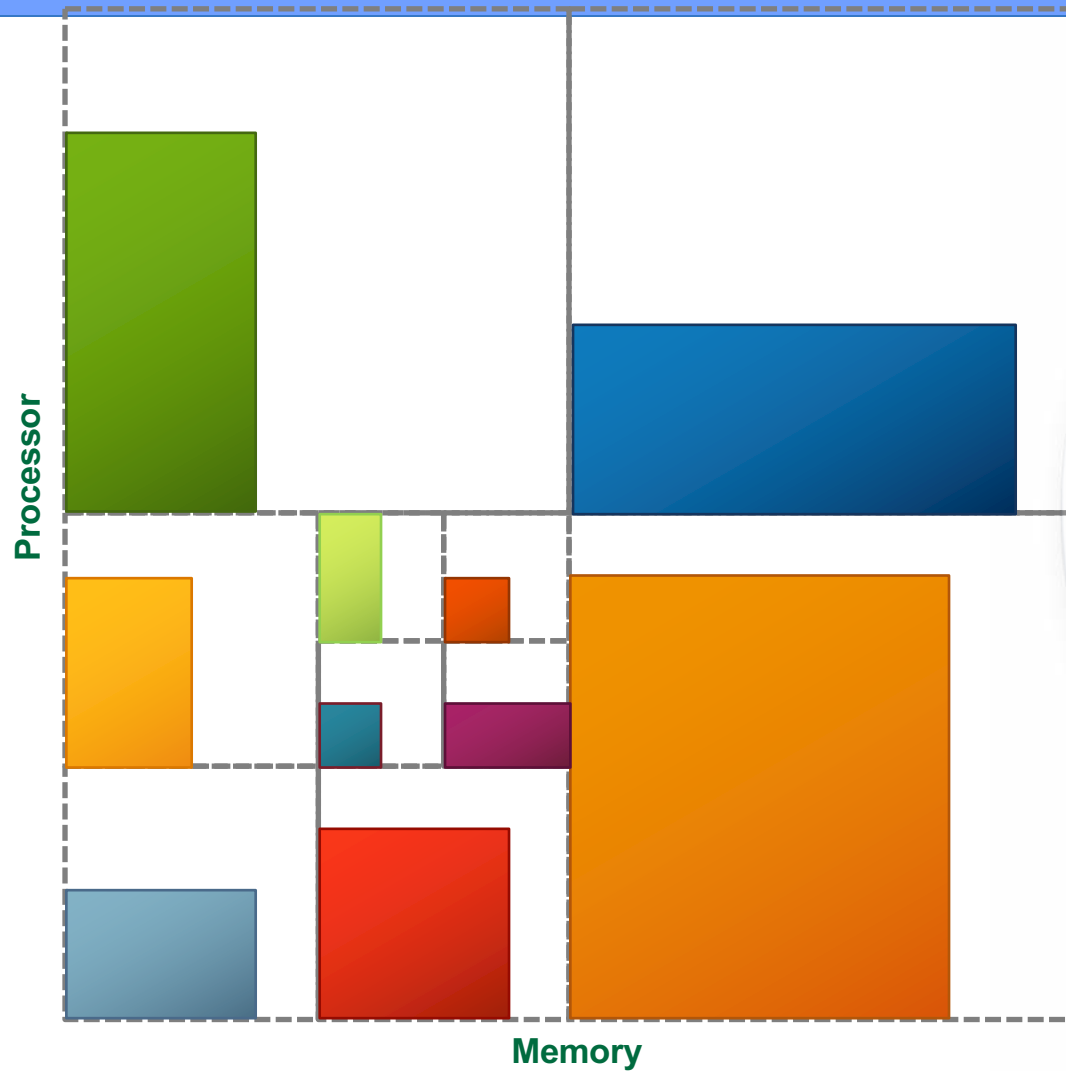
µVM: The cloud kilowatt
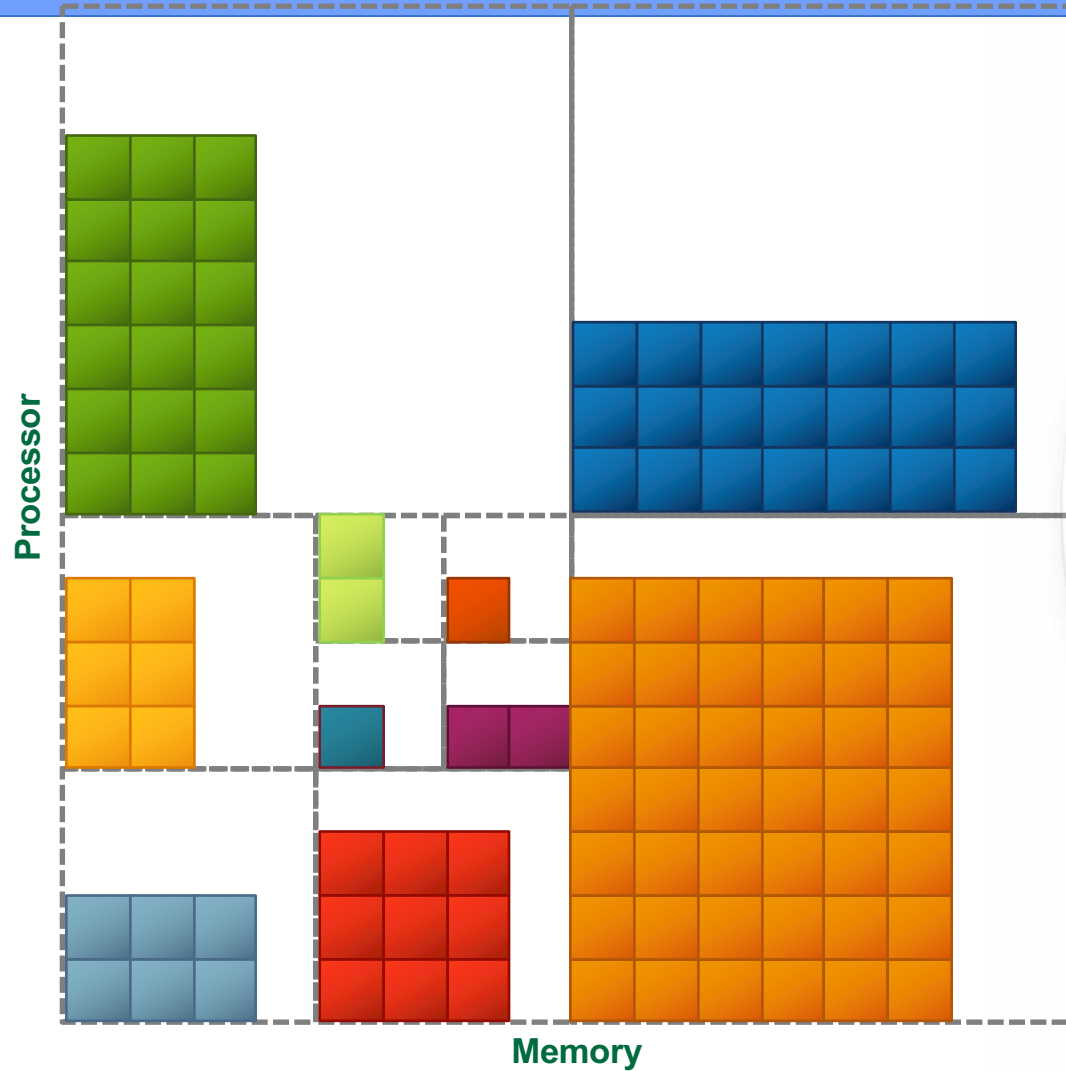
Assurance, Economics & Optimization

- Consumption-based billing

- Usage analytics

- Intelligent workload placement

- Proactive infrastructure optimization

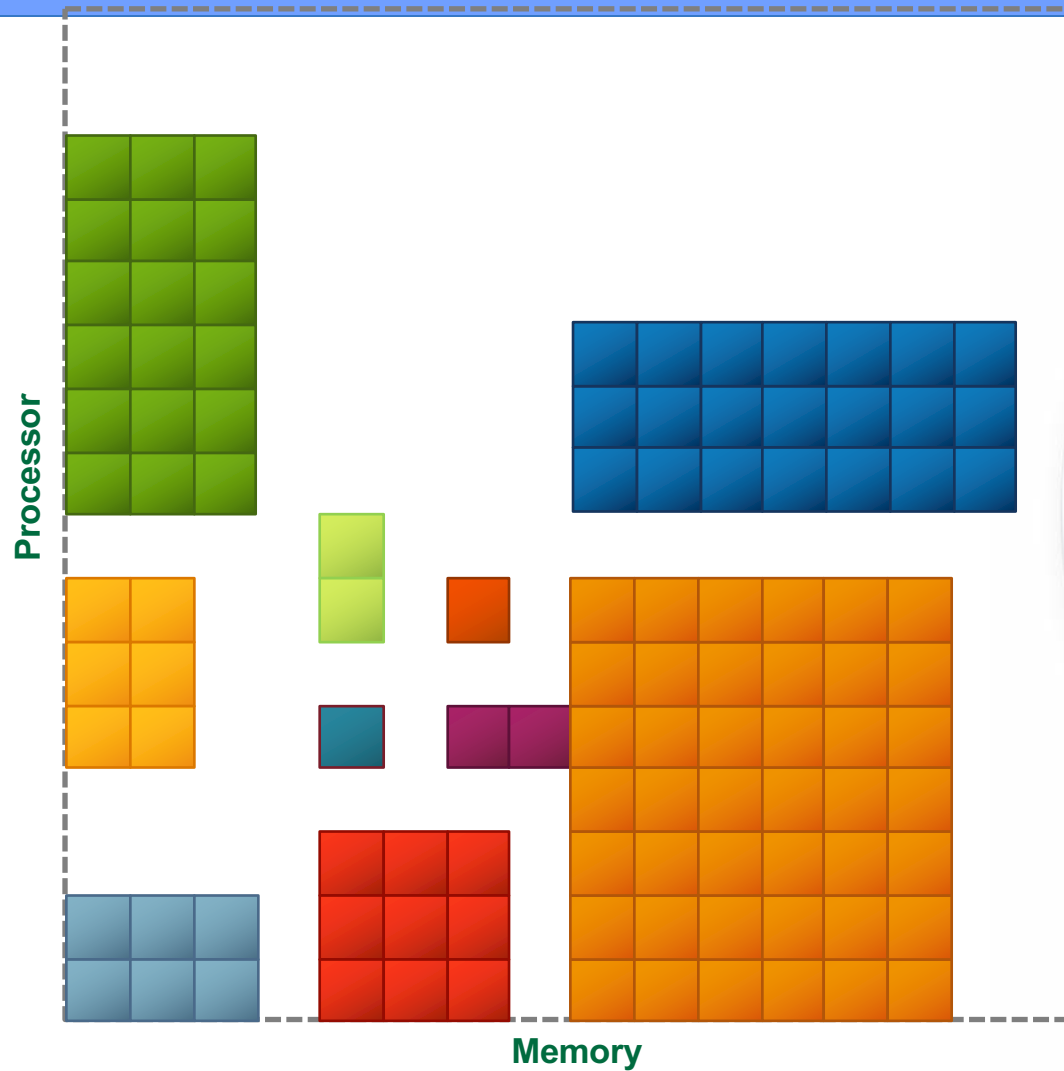- SLAs for application performance
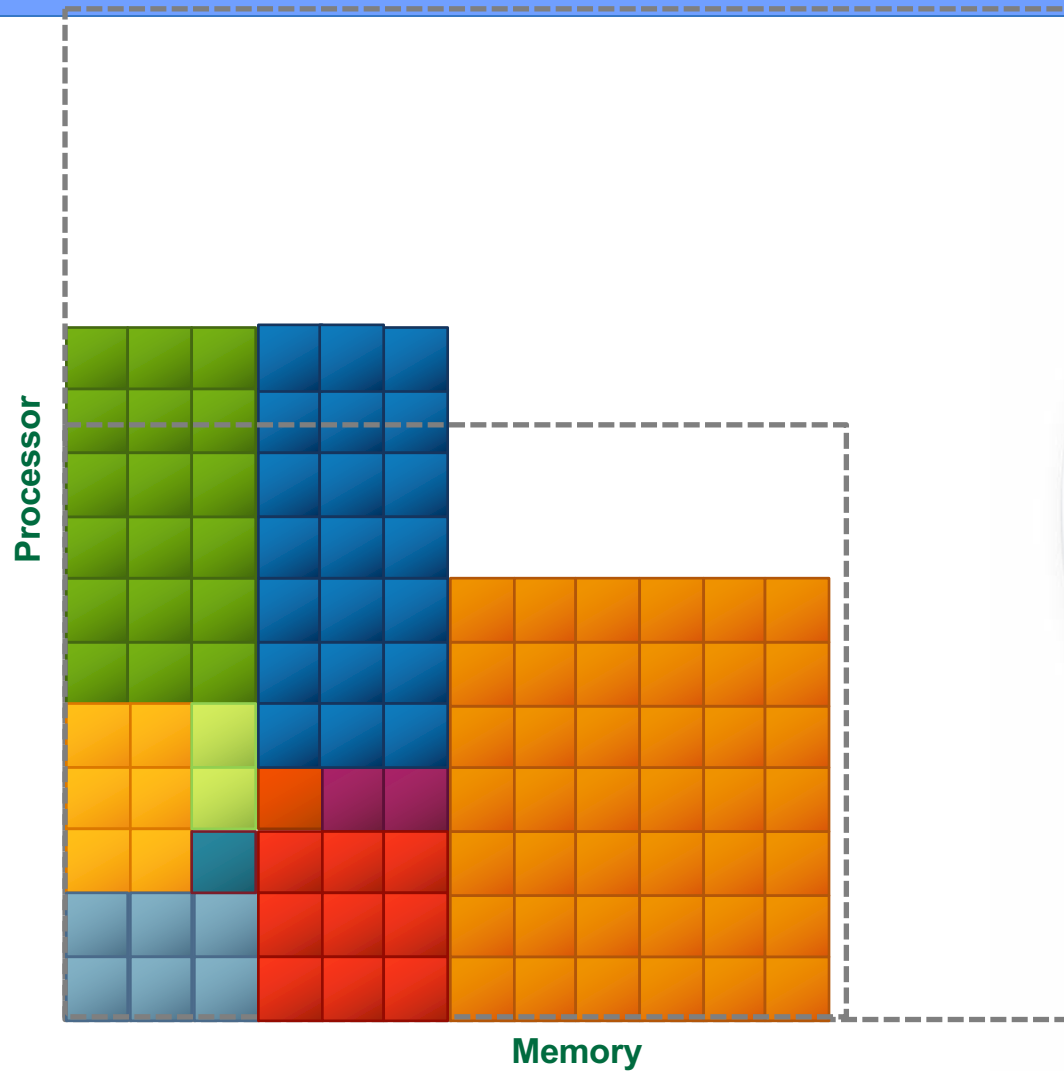
- Fewer hosts, better utilization

1 µVM:
200MHz CPU, 768Mb RAM, 40 IOPs, 2Mb/s Bandwidth

Processor

Memory

Processor

Memory

μVM

CPU   RAM   Gbps   IOPs

XStream
POWERED CLOUD

ELYSIUM   Parker   NORTHROP GRUMMAN   BOEING   GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

xStream App Director module

**Cloud Agility, Automation & Optimization for Enterprise Applications**

xStream μVM engine provides workload optimization, application performance assurance and utilization analytics

Automated operations simplify application deployment in less time, with less cost

In-life application automation for continual maintenance and management of complex applications, including in-depth reporting & monitoring

Customizable alerting and self-healing for more effective management of mission-critical systems

SAP automation module available Q2; Oracle & Epic to follow in H2
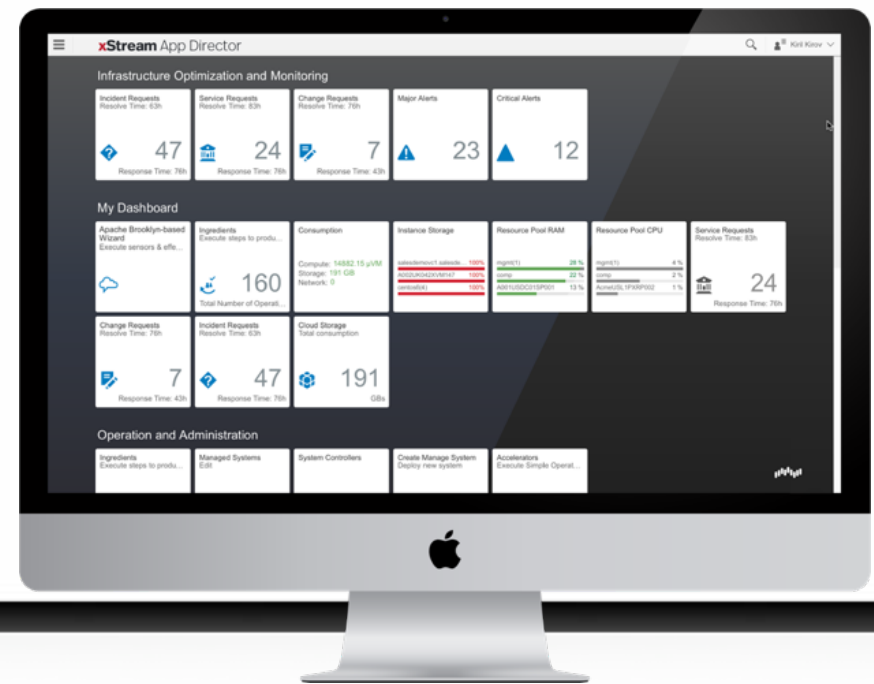
Sample App Director automation benefits: SAP

Global Product Data Interoperability Summit | **2016**

Automation	Description	Illustrative Benefits
Kernel patch automation	Orchestration of the entire kernel change process	**85%** reduction in time and labor **95%** reduction in human error
SAP patching and pre- and post-upgrade automation	Simplifies system prep process for patching and upgrade, along with post-system technical processing (SGEN) and system notifications	**85%** acceleration in pre- and post-processing
On-demand and custom health check and validation checklist automation	Complete customizable health checks for your system landscapes	**>70%** reduction in manual labor
Security automation for frequent tasks	User locks, system log and audit details, risk assessment information, SAP Portal Hotfix summary, license details	Time savings varies by user
Complete root cause analysis and dashboard overview automation	Quickly view where systems exceed best practice thresholds	Time savings varies by user

ELYSIUM   Parker   NORTHROP GRUMMAN   BOEING   GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT **2016**

Managed Services

Maximize Performance, Reduce Complexity & Leverage Best-In-Class Expertise

Complete On-Premises Managed Services

- Storage as a Service
- Backup & Recovery Services
- Private and Hybrid Clouds

Comprehensive Solutions

- ITIL-based operational standards
- Performance underpinned by service-level guarantees
- Alert management with performance & capacity reporting
- Flexible consumption-based models
- Seamless coverage through global delivery network
- Collaborative governance model

ELYSIUM Parker NORTHROP GRUMMAN BOEING GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

Virtustream & SAP

Unparalleled Expertise & Assurance

Deep SAP Expertise

- ~200 SAP clients running **production** SAP
- First Production SAP Customer in a Multi-tenant Cloud
- First Production SAP ECC Running on HANA in the Cloud
- ~500 SAP HANA Instance Migrations to date
- Complete SAP Portfolio Coverage, Including ERP, CRM, Analytics, Landscape Virtualization Manager (LVM), Virtual Appliance Factory, HANA & Business One in the Cloud

Comprehensive Certifications

- One of only five global HEC premium suppliers
- SAP Certified for Hosting Services
- SAP Certified for HANA Operations
- SAP Certified for Cloud Services
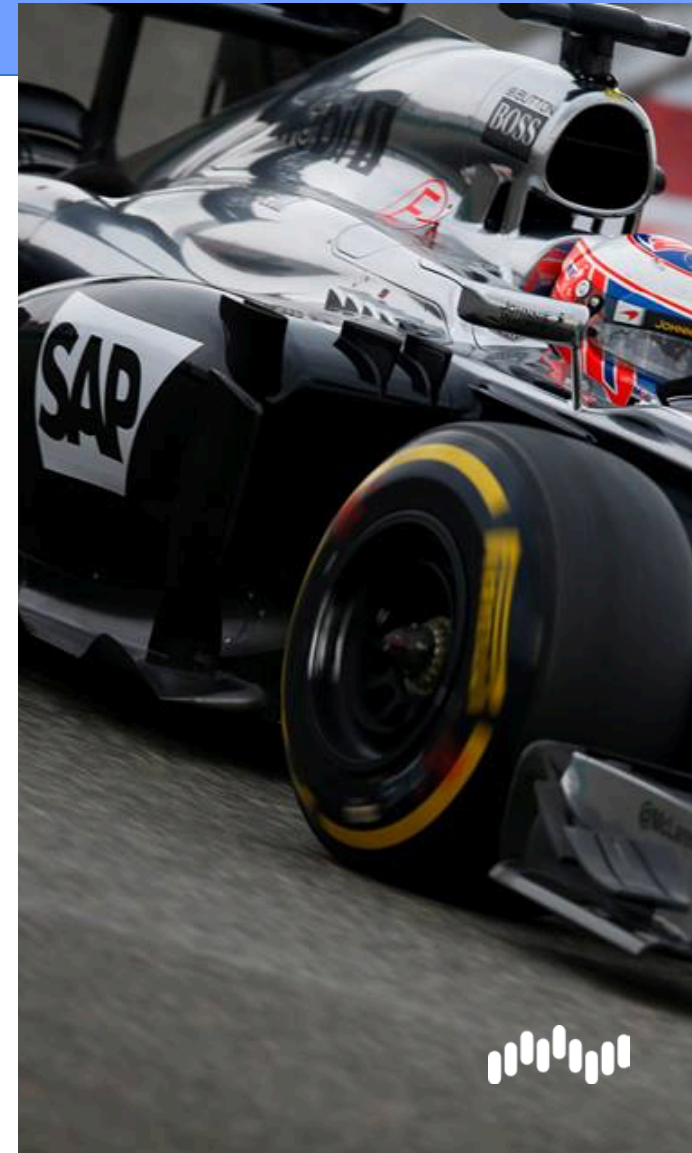
Summary: Enterprise-class cloud

Global Product Data Interoperability Summit | **2016**

Better App Performance

Tuned for mission-critical apps

Run enterprise apps up to 2x faster

SLAs for application performance

Greater Agility & Efficiency

Blueprint-based app deployment

Lifecycle Application Automation

Deeper insight into utilization

Higher Security

Comprehensive platform security

360-degree risk view

Continuous compliance monitoring

Superior Economics

Pay for what you use

Lower your infrastructure costs by 30% or more

Application automation drives substantial labor efficiencies

Cloud security: defense in depth

Chip-to-Compliance IaaS Security Architecture

- RBAC & multi-factor authentication

- Dedicated VLANs and security zones

- Encryption at rest, in use and in motion

- Secure, dedicated connectivity options

- Silicon-level system integrity attestation

- Geo-fencing & geo-tagging

- Continuous logging & compliance

Compliance

- ISO 27000:2013 & Shared Assessments
- SSAE16, ISAE3402, SOC2
- FISMA
- FedRAMP
- PCI 3.0
- HIPAA/HiTECH
- Cloud Security Alliance STAR
- ITAR/EAR
- NIST 800-53 (US Government)

Challenge 1: Risk Management

Your CEO asks you…"What is my risk posture today and are we managing risk properly?"

- What is the impact of latest threats on our overall risk posture?
- What is the impact on the enterprise mission risk?
- Which enterprise divisions and systems will be affected?
- Where are those systems and associated assets located?
- Can we build a prioritized list of assets for mitigation actions?

Can you quickly answer this question today without a major staff effort?

Challenge 2: Compliance

Achieving and maintaining regulatory and industry compliance

- How can I prepare my audit package with minimal resources?
- How can all stake holders collaborate to achieve compliance?
- Can I reduce the cost of annual audits?
- Can I reduce the cost of maintaining compliance across multiple regulations?
- Can you get the status of on-going compliance across the Enterprise Information Systems on-demand?

The only constant is change!!

- Enterprise environment is constantly changing
- Threats to the environment are constantly evolving
- Enterprise is subject to new industry or government regulations
- Information sources are constantly being added and data challenges are ever expanding
  - Data types could be structured or unstructured
  - Data ingest could be centralized or distributed due to distributed data sources
  - Frequency of data capture, size of each data stream and data persistency accumulates multi-GB, TB or even PB data sets
  - Data processing on large data set requires horizontal scalability

Can you continuously monitor and trend the risk posture management over time?

The challenge for CEO/CIO/CISO/CRO/CTO/Ops:

Need a proactive view of risks across my cloud and non-cloud assets due to Cyber, Compliance and IT Operations on a continuous and automated basis.

- How do I view security and compliance risk across all my IT assets within an enterprise, cloud or across a hybrid environment on a single pane of glass?
- How do I reduce the cost and complexity of managing a variety of Compliance Regulations with shrinking budgets?
- How do I become proactive rather than reactive in dealing with enterprise and mission risks?
- How do I perform continuous monitoring of risk with an ever-increasing volume of data?
- How do I create a singular 360°operational view of enterprise risk and prioritize my mitigations?

Continuous Enterprise Risk & Compliance Monitoring

Viewtrust provides **continuous monitoring of risks** across enterprise cloud and non-cloud environments to **proactively address risks** due to Cyber, Compliance, and IT Operations.

All Federal Systems have to have FISMA/FedRAMP compliance with implementation of NIST Risk Management Framework (RMF)

Enterprise Priorities

Based on our customer feedback in 2015-2017, cloud security, mobile, data protection, privacy and regulatory compliance will be top priorities across every industry as businesses look to:

- Manage IT and operational risks proactively rather than reactively
- Manage enterprise and cyber risk with a central authoritative system that integrates with their existing point security solution
- Perform continuous monitoring of risk with ever demanding system volumes, data and mobile/portable technology (BYOD) and applications
- Reduce the cost and complexity of managing and reporting variety of compliance regulations with shrinking budgets
- Eliminate costly non-compliance costs and audit disruptions

Why proactive risk based approach?

- Prevention is better than cure

- 89% of the security compromises can be avoided - Online Trust Alliance (OTA) analysis of international incidents

- 97% of data breaches are preventable – Verizon Risk Survey

- Focus on what is important to business - Symantec/NCSA Study

  - Nearly two-thirds of the businesses affected are out of business within 6 months and Cyber-attacks cost companies an average of $188,242 each incident.

- Quantitative risk analysis is better for data analysis and trending

- The risk analysis has to be holistic and continuous Vs. Snap-shot in time

Evolution of Security and Compliance Solutions
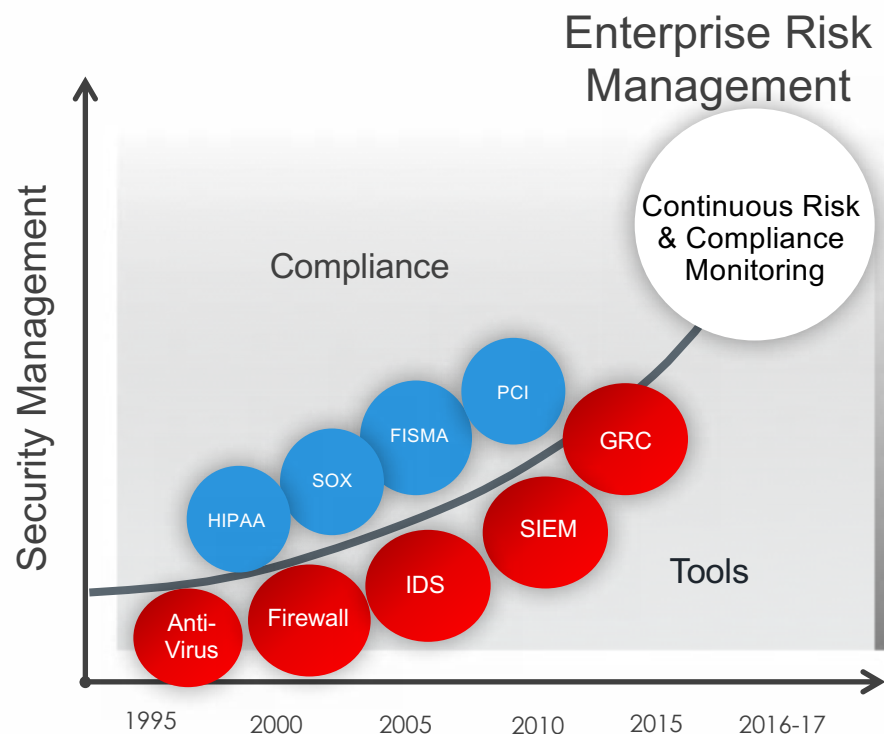
- Managing security against threats started with tools – Anti-Virus, Firewalls, IDS's, SIEMs, etc..
- Industry regulations (FISMA, SOX, etc.) implemented to start managing security by compliance

Today, with constant attacks on networks and data enterprises must evolve to manage security by Risk and do it continuously!

Using NIST Risk Management Framework
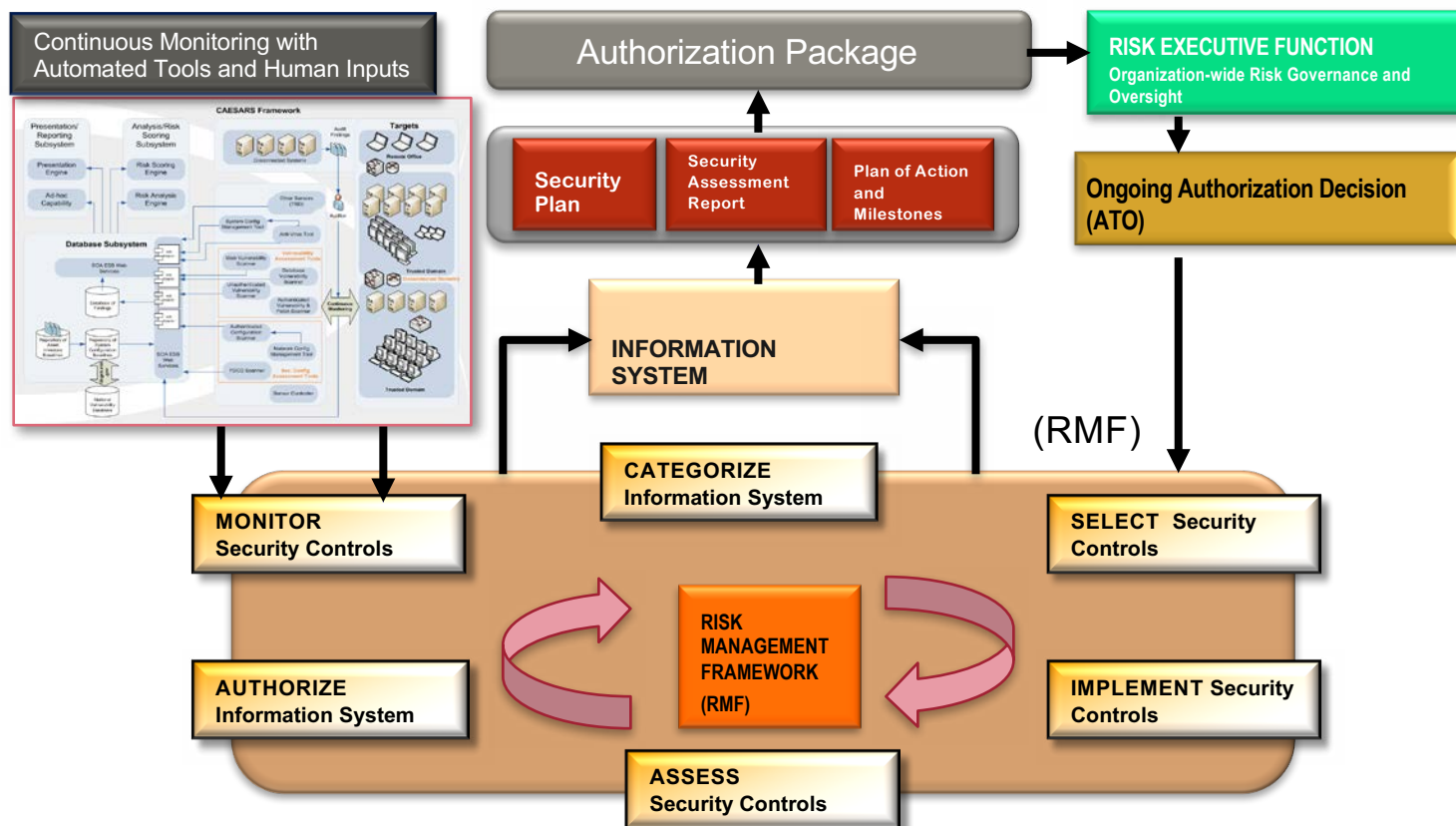
Addressing regulated and non-regulated markets

Cyber Risk | Compliance Risk | IT & Operational Risk

Presentation and Data Analytics Dashboard

	Federal	**Financial**	**Healthcare**	**Energy**	**Retail**
Enterprise Risk Management	✔	✔	✔	✔	✔
Cyber Situational Awareness	✔	✔	✔	✔	✔
Regulatory Compliance	FISMA/ FedRAMP	GLBA SOX	HIPAA HITECH	NERC CIP	ISO27001 PCI

Automated risk and compliance management

- Provides a unified view of enterprise risk on a single dashboard

- Automates Compliance and Risk management for private or hybrid clouds

- Provides continuous analysis of risk with heat maps for proactive view

- Collaborative and workflow driven platform for compliance automation and documentation

- Scales with Big Data analysis and analytics engine

- Provides mission risk view to address what is critical to the business

Operational deployment model

Quantitative Risk & Compliance Analysis

Reference IA Controls Framework

SAP GRC

Configuration Manager

Vulnerability Scanner

IT System Assets

Asset Manager

Log Manager

Patch Manager

Sensors

Collector(s)

SQL or NoSQL

Enterprise Risk and Compliance Reporting

Unified Dashboard
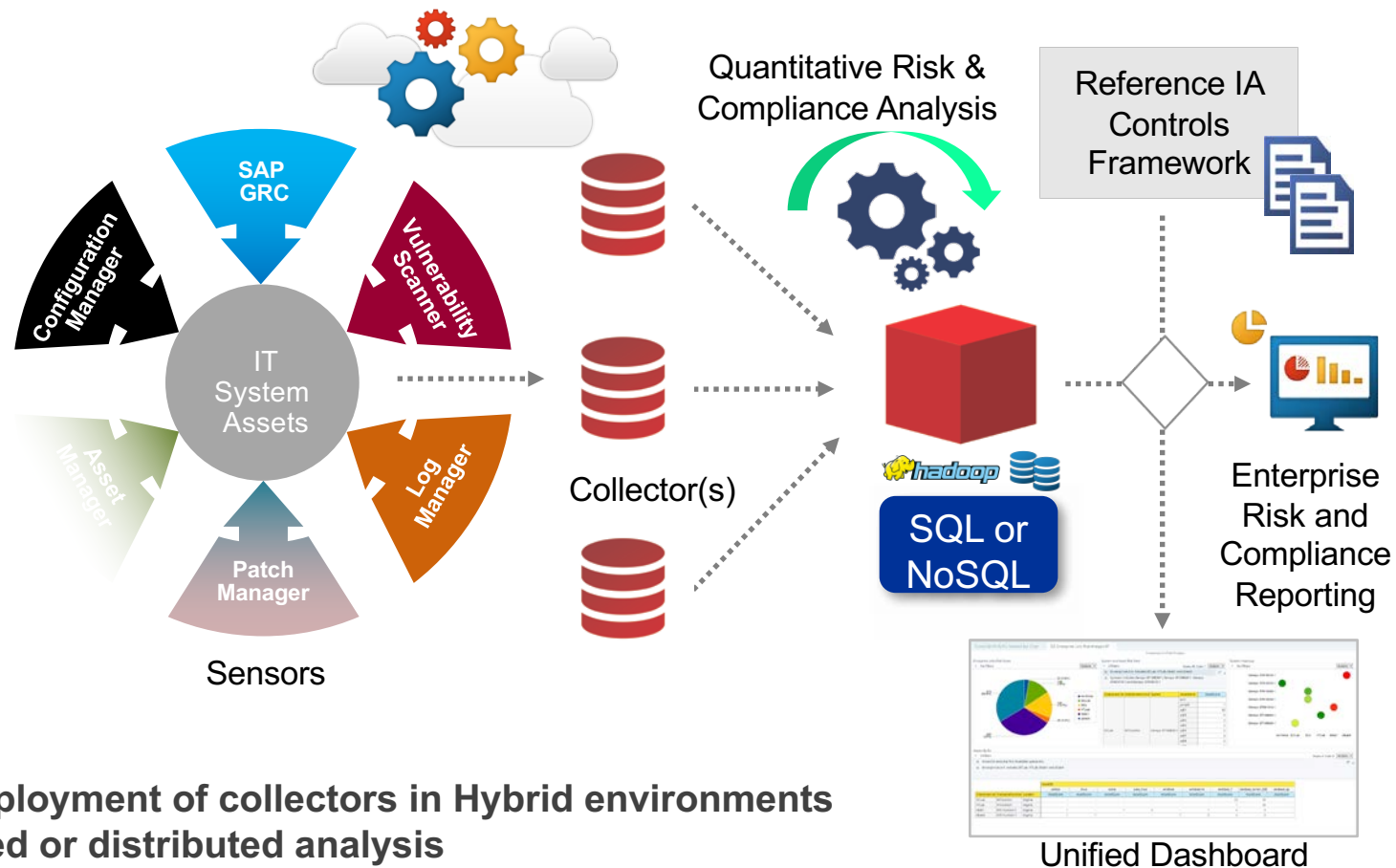
- **Tiered deployment of collectors in Hybrid environments**
- **Centralized or distributed analysis**
- **Cube-based analytics with SQL or NoSQL data warehouse.**

ELYSIUM Parker NORTHROP GRUMMAN BOEING GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

Vendor	Big Data	NIST SCAP (CVE) ARF	NIST SCAP (CCE) ASR	DoD SCAP (STIG) ARF	DoD SCAP (IAVM) ASR	Proprietary XML	CSV	Syslog	Other	Ingestion Automatic	Manual	CMaaS Hardware	Software	Config Mgmt	Vulnerability	SIEM
ACAS				✔											✔	
ArcSight																✔
BDNA							✔							✔		
Computer Associates														✔		
DbProtect															✔	
eEye Retina						✔									✔	
FireEye															✔	
ForeScout	Yes						✔					✔	✔			
Infoblox												✔				
Lumension															✔	
McAfee ePo Commercial	Yes	✔								✔	✔			✔		
McAfee ePo DoD	Yes			✔	✔					✔	✔	✔	✔	✔		
McAfee MVM	Yes					✔				✔	✔				✔	
Microsoft System Center														✔		
nCircle													✔	✔		
Palo Alto																
QRadar							✔									✔
Rapid7															✔	
RedSeal														✔	✔	
Splunk																✔
Symantec	Yes	✔								✔	✔			✔	✔	
Syslog								✔								
Tenable Nessus	Yes					✔				✔	✔				✔	
Tenable Security Center	Yes			✔	✔					✔		✔	✔		✔	
uCMBD														✔		
VT ComplyVision WMI												✔	✔			
WebInspect															✔	

Native Support for NIST Secure Content Automation Protocol (SCAP)

ELYSIUM Parker NORTHROP GRUMMAN BOEING GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016

Building Inventory & Policy-Based Analysis
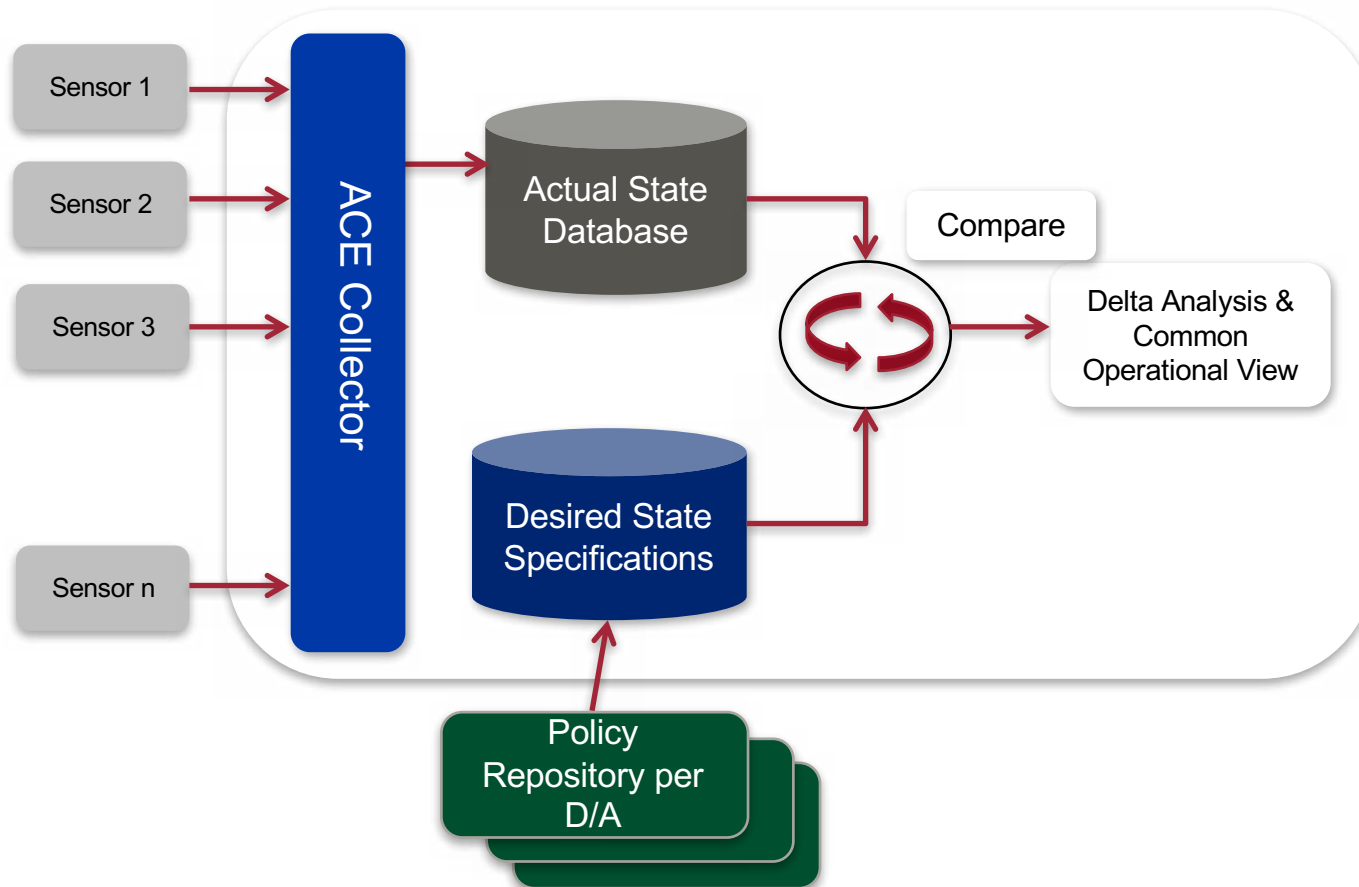
30

Unified View of Risk and Compliance

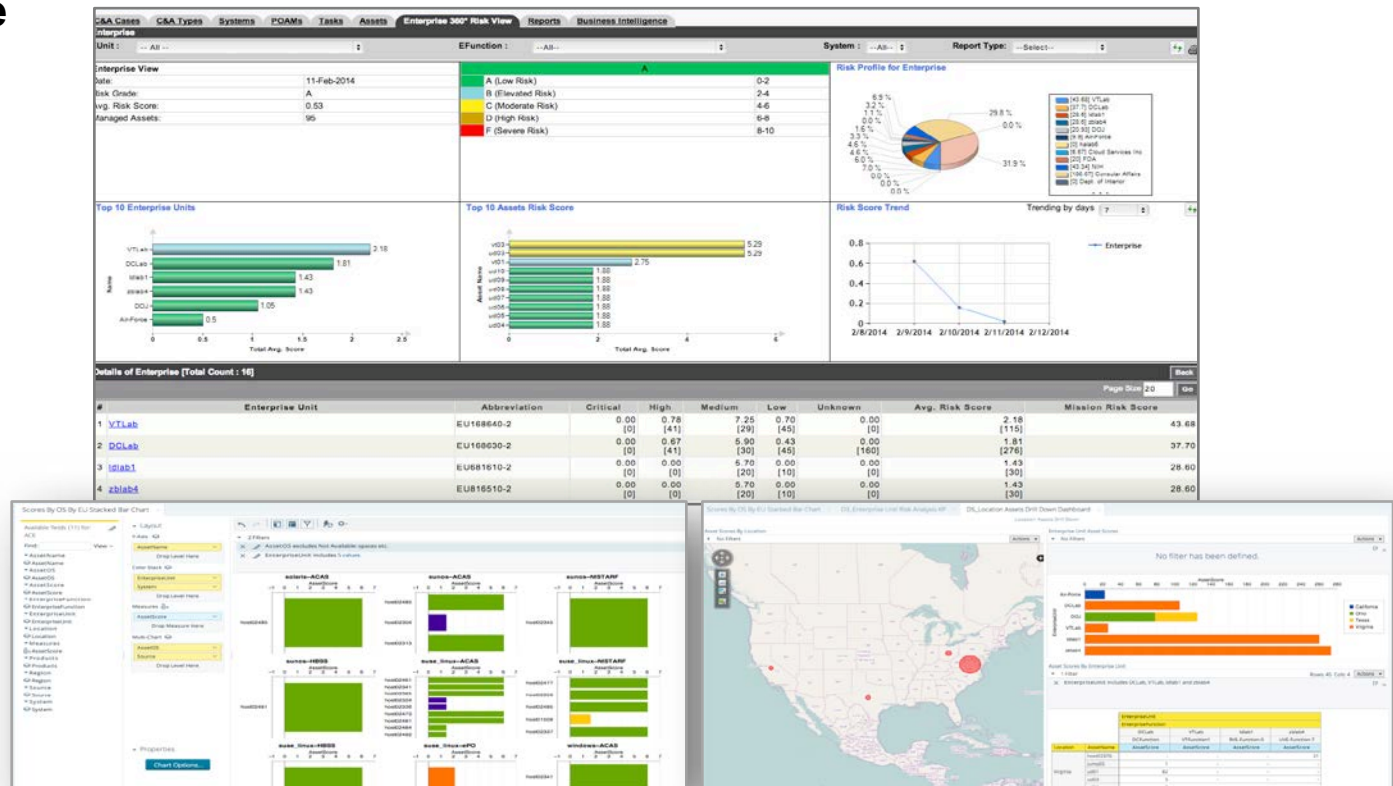**Enterprise dashboard
for Risk and Compliance**

- Quantitative Risk Analysis
- Risk trending
- Complete drill-down capability

**Continuous Risk
Monitoring**

- System and Asset Risk Scoring
- Risk Reporting and Analytics

Continuous Compliance

- Asset Tracking
- System Certification
- Compliance Reporting

31

Security Assessment and Audit

- **Audit Scripts and Task Creation**
- **Creating audit documents and artifacts**

Compliance View dashboard

Built-in quantitative risk analysis

Algorithmic Approach

$$\min_{x\in X}\left\{g(x) \equiv c^T x + E\left[Q(x,\xi)\right]\right\}$$

$$\min_{y} q^T y \; subject \; to \; Tx + Wy \leq h$$

Sensor Data Sources

Security Layer	Score	Sensor Data Source
Application & Data — **Data Security**	App: 4	Nessus, AppScan, Onapsis
	Data: 4	Vormetric/ProtectV
Patch Management	Patch: 4	Nessus, Patch Mgmt.
Intrusion Prevention	Intru: 4	vGW, McAfee (EPO), FortiNet
Virus Protection	Virus: 4	vGW, McAfee (EPO)
Host-Based Firewall	FW: 4	vGW
Server Hardening — **Operating System**	OS: 4	CISCAT/Nessus/xCCDF
Host TPM (TXT) — **Host Security**	TXT: 4	xStream/Mt. Wilson
Geo Tags (geo location)	Net: 4	xStream
Internal Network	DC: 4	Firewall/IDS/IPS/AlgoSec
Perimeter Security — **Physical Security**		Firewall/Fortinet/Juniper IDS/IPS/AlgoSec
Policies, Procedures and Awareness	Total: 4	ViewTrust-ERM
	Trust Rating	ViewTrust-ERM

ELYSIUM   Parker   NORTHROP GRUMMAN   BOEING   GLOBAL PRODUCT DATA INTEROPERABILITY SUMMIT 2016
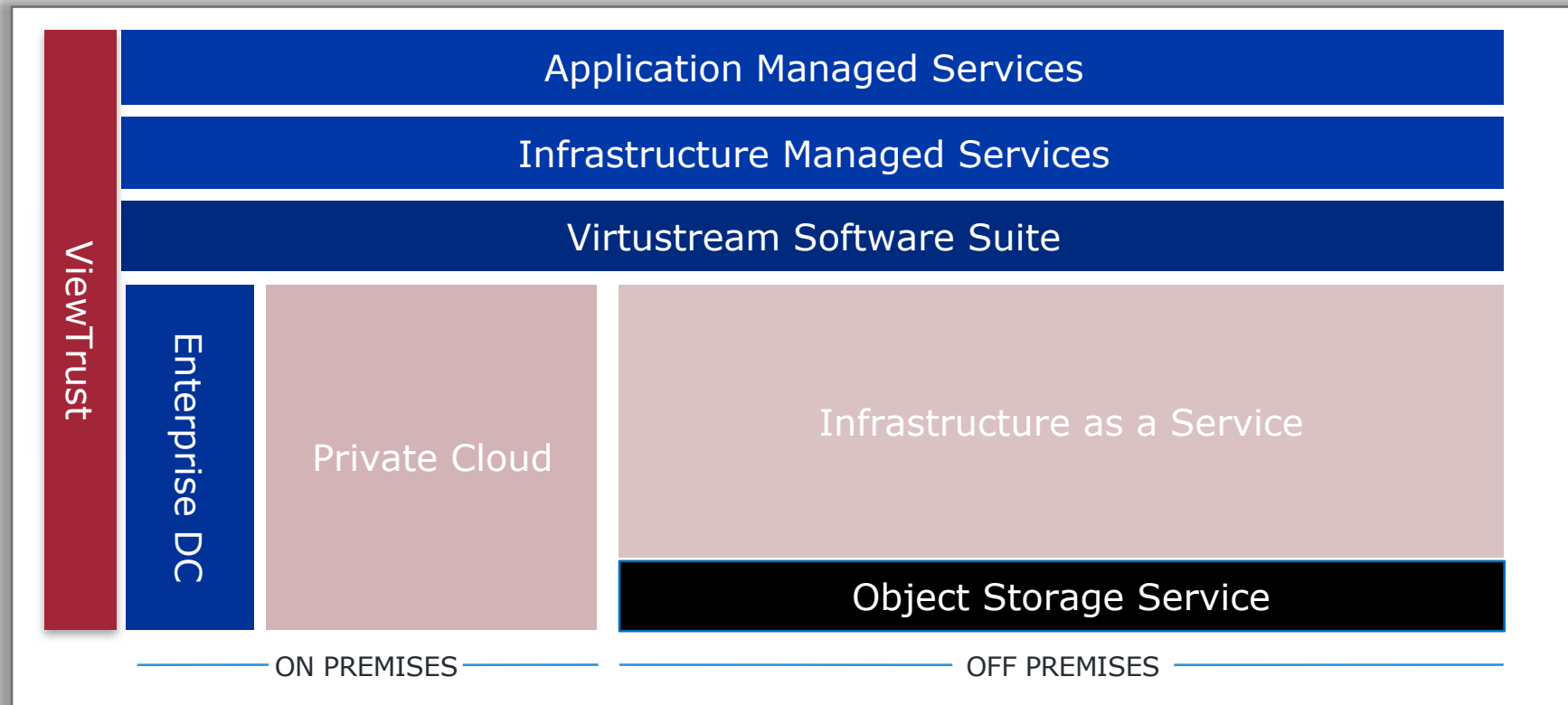
Cloud Security Challenges

Who owns the Security and Compliance responsibility?

– Line-of-demarcation

- Multi-tenancy challenges
- Data ownership issues
- Quality of service guarantees – SLAs
- Data dispersal and international privacy laws
- Regulatory Compliance is for all assets – Cloud, Non-Cloud, Hybrid or Federated deployments
- Needs to support multiple regulatory and industry compliance requirements – PCI, HIPAA, NERC CIP, GLBA, SOX, FISMA, FedRAMP
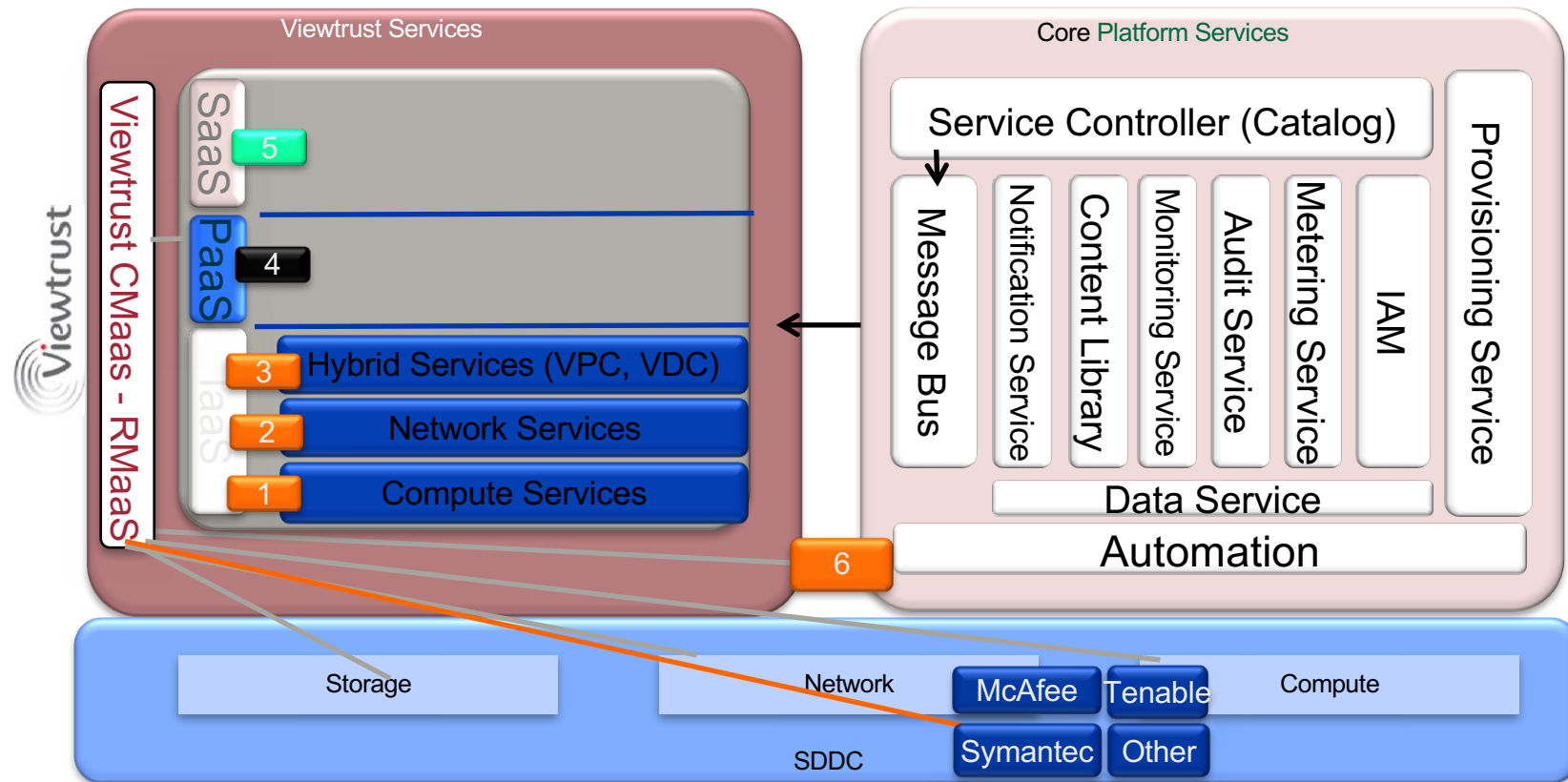
Enabling risk and compliance for hybrid cloud

Viewtrust Continuous Compliance for Cloud

Global Product Data Interoperability Summit | **2016**

Continuous Compliance for Hybrid Cloud
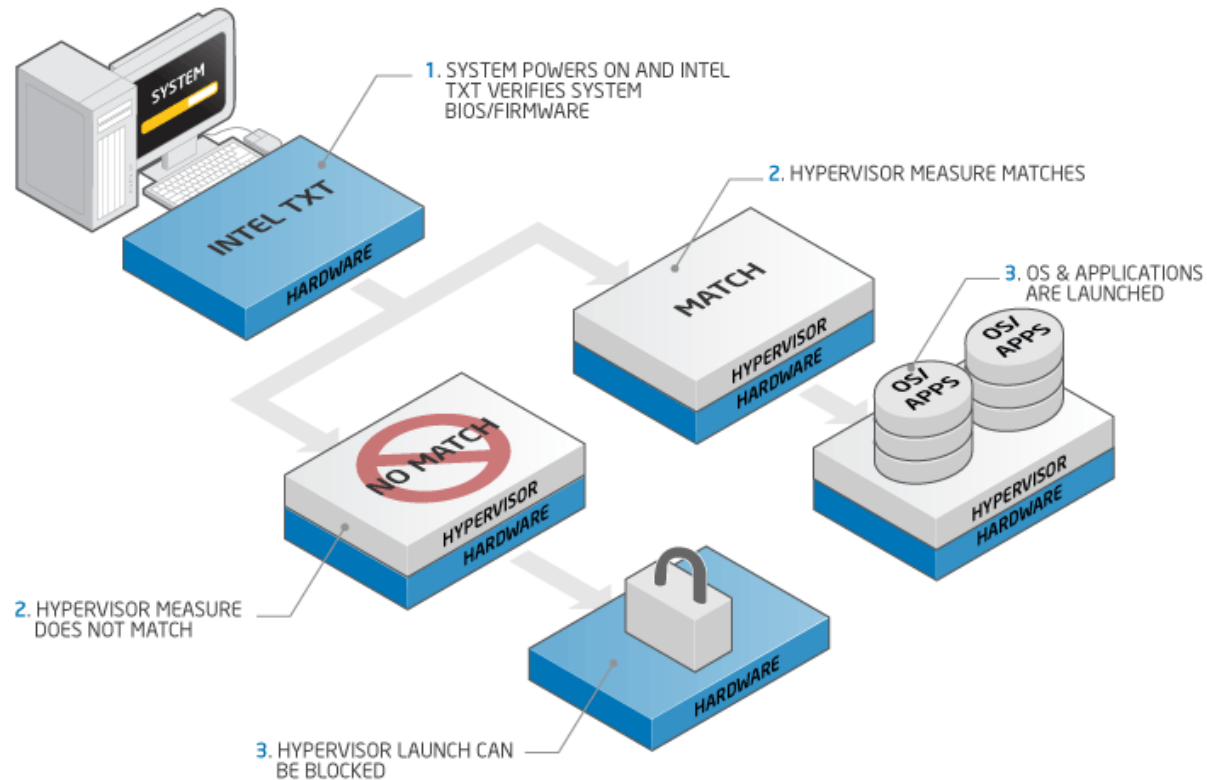
Global Product Data Interoperability Summit | **2016**
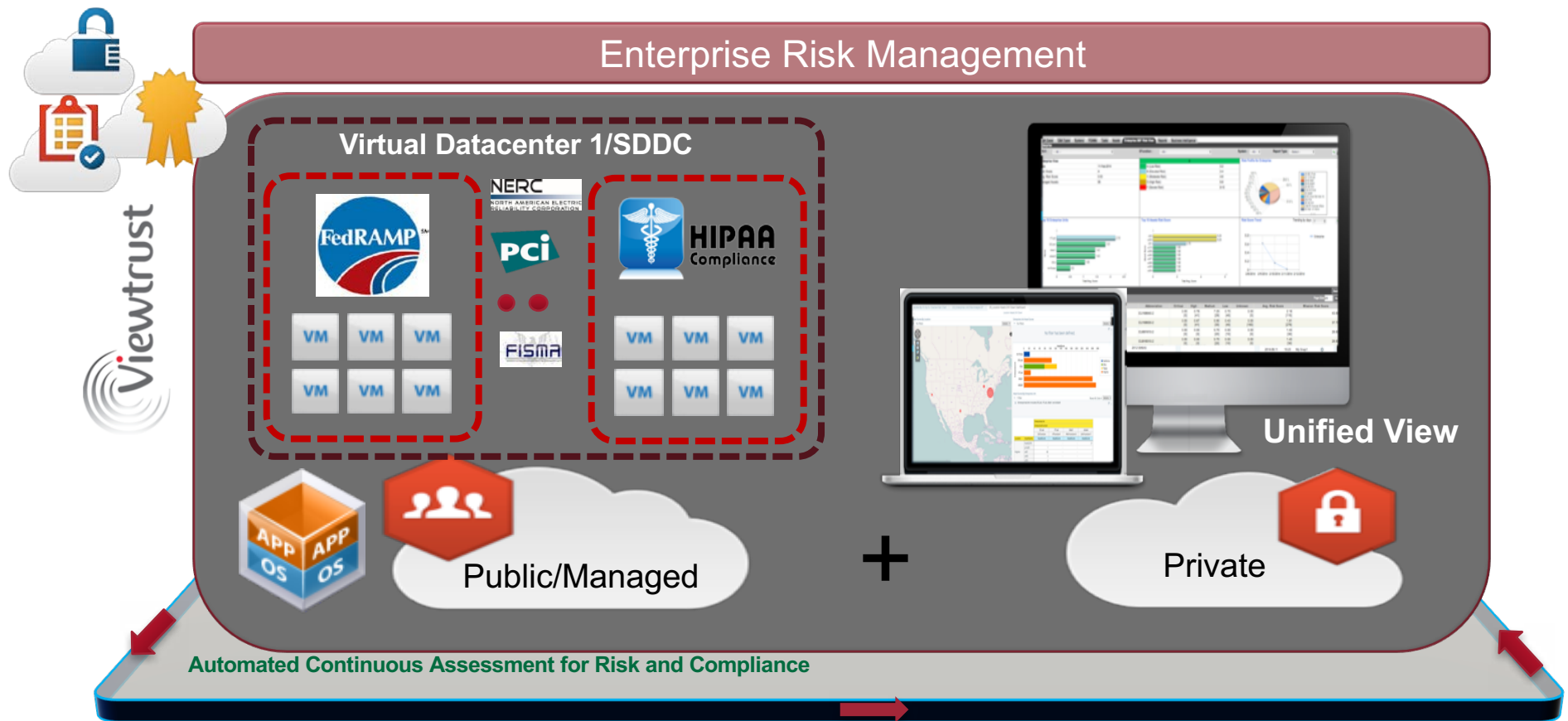
27

Intel TxT for trusted boot and geo-fencing

Compliance as a Service with Power of Inheritance
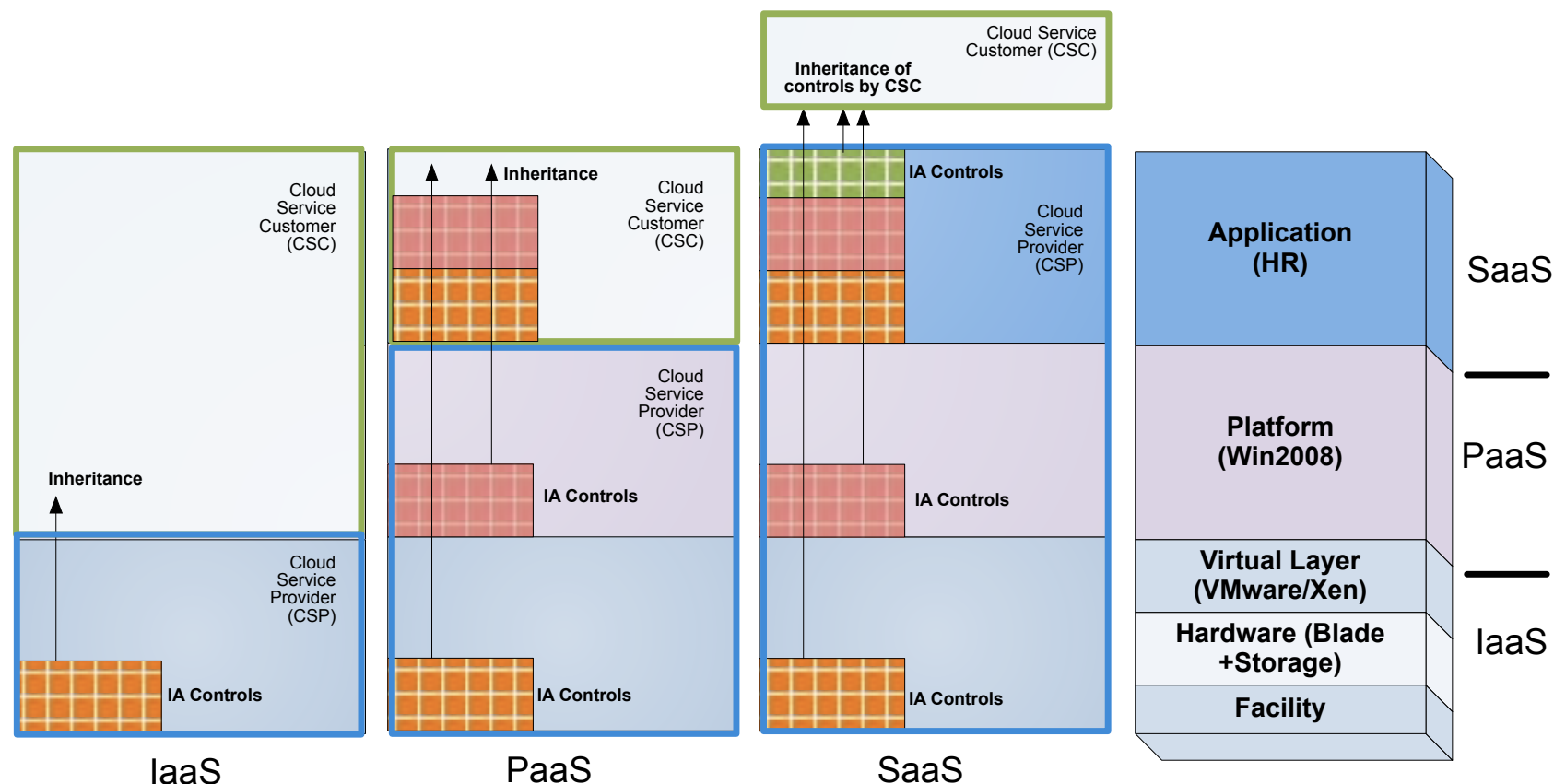
28

Cloud Audit and Compliance
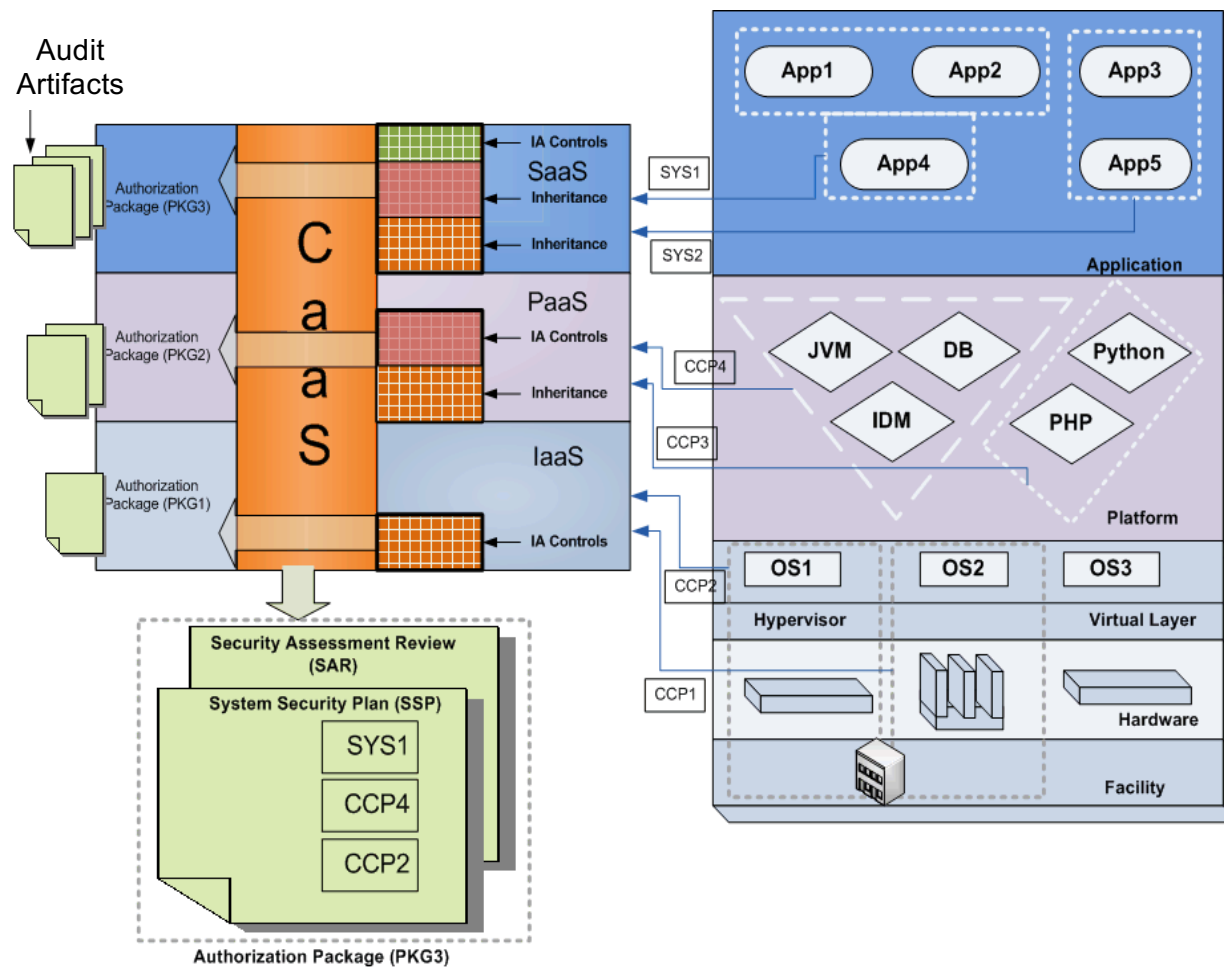
Rapid ROI with Viewtrust

Reduced Compliance Costs via efficiency through automation:

- Entire Compliance lifecycle automation

- Efficient, Collaborative, and Consistent audit practice

- Support multiple compliance frameworks unified in one tool

Reduce Enterprise security tool – TCO:

- Automation of existing security tools and breaking data silos

- Automated risk analysis based on threat and impact analysis

- Automated identification and remediation of risk through workflow management

34

Kaus Phaltankar
kaus@Virtustream.com
Kaus.Phaltankar@dell.com
+1 (703) 627-7539