Operating
Highly Secure
Enterprise
Hybrid Cloud

Safely operating Systems of Record
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
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

Key Priorities

Global Product Data Interoperability Summit | 2016

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
A changing conversation

Global Product Data Interoperability Summit | 2016

Supply Utility: Deliver Business Value

- Public vs. Private
- Infrastructure
- Server Deployment
- Self-Service
- Hybrid
- Applications
- Service Delivery
- Managed Services
Built for the Enterprise

Global Product Data Interoperability Summit | 2016
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
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

<table>
<thead>
<tr>
<th>Automation</th>
<th>Description</th>
<th>Illustrative Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kernel patch automation</td>
<td>Orchestration of the entire kernel change process</td>
<td><strong>85%</strong> reduction in time and labor <strong>95%</strong> reduction in human error</td>
</tr>
<tr>
<td>SAP patching and pre- and post-upgrade automation</td>
<td>Simplifies system prep process for patching and upgrade, along with post-system technical processing (SGEN) and system notifications</td>
<td><strong>85%</strong> acceleration in pre- and post-processing</td>
</tr>
<tr>
<td>On-demand and custom health check and validation checklist automation</td>
<td>Complete customizable health checks for your system landscapes</td>
<td><strong>&gt;70%</strong> reduction in manual labor</td>
</tr>
<tr>
<td>Security automation for frequent tasks</td>
<td>User locks, system log and audit details, risk assessment information, SAP Portal Hotfix summary, license details</td>
<td>Time savings varies by user</td>
</tr>
<tr>
<td>Complete root cause analysis and dashboard overview automation</td>
<td>Quickly view where systems exceed best practice thresholds</td>
<td>Time savings varies by user</td>
</tr>
</tbody>
</table>
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
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
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 stakeholders 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 ongoing compliance across the Enterprise Information Systems on-demand?
Challenge 3: Automated Continuous Monitoring

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 in a nutshell

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?
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

Global Product Data Interoperability Summit | 2016

- 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

Continuous Monitoring with Automated Tools and Human Inputs

Authorization Package

- Security Plan
- Security Assessment Report
- Plan of Action and Milestones

RISK EXECUTIVE FUNCTION
Organization-wide Risk Governance and Oversight

Ongoing Authorization Decision (ATO)

INFORMATION SYSTEM

- Monitor Security Controls
- Authorize Information System
- Assess Security Controls
- Select Security Controls
- Implement Security Controls
- Category Information System
- Risk Management Framework (RMF)

Continuous Monitoring with Automated Tools and Human Inputs
## Addressing regulated and non-regulated markets

### Cyber Risk | Compliance Risk | IT & Operational Risk

<table>
<thead>
<tr>
<th></th>
<th>Federal</th>
<th>Financial</th>
<th>Healthcare</th>
<th>Energy</th>
<th>Retail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Risk</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Situational Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>FISMA/</td>
<td>GLBA</td>
<td>HIPAA</td>
<td>NERC</td>
<td>ISO27001</td>
</tr>
<tr>
<td></td>
<td>FedRAMP</td>
<td>SOX</td>
<td>HITECH</td>
<td>CIP</td>
<td>PCI</td>
</tr>
</tbody>
</table>
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

- Tiered deployment of collectors in Hybrid environments
- Centralized or distributed analysis
- Cube-based analytics with SQL or NoSQL data warehouse.
### Content sources, formats and ingest options

#### Native Support for NIST Secure Content Automation Protocol (SCAP)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Big Data</th>
<th>NIST SCAP</th>
<th>DoD SCAP</th>
<th>Proprietary</th>
<th>Ingestion</th>
<th>CMaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACAS</td>
<td></td>
<td>ARF</td>
<td></td>
<td>ARF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArcSight</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BDNA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Associates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DbProtect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eEye Retina</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FireEye</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ForeScout</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infoblox</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lumension</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee ePo Commercial</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee ePo DoD</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee MVM</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft System Center</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>nCircle</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Palo Alto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QRadar</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rapid7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RedSeal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Splunk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable Nessus</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable Security Center</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>uCMBD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VT ComplyVision WMI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Webinspect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Building Inventory & Policy-Based Analysis

Global Product Data Interoperability Summit | 2016

ACE Collector

Actual State Database

Compare

Delta Analysis & Common Operational View

Desired State Specifications

Policy Repository per D/A

Sensor 1

Sensor 2

Sensor 3

Sensor n
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
### Audit Scripts and Task Creation

- Creating audit documents and artifacts

#### Security Assessment and Audit

The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

<table>
<thead>
<tr>
<th>SrNo</th>
<th>Posted By</th>
<th>Comments</th>
<th>Date Posted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Administrator Virtustream</td>
<td>New Task Created for,CIP-014-2.R1R1.2, Task No. CEF6-2</td>
<td>3/20/2016 9:18:34 AM</td>
</tr>
</tbody>
</table>
### Compliance View dashboard

**Global Product Data Interoperability Summit | 2016**

#### Details for CIP-004-5.3 [Total Count: 77]

<table>
<thead>
<tr>
<th>#</th>
<th>Case Name</th>
<th>Asset Name</th>
<th>Description</th>
<th>ID</th>
<th>Score</th>
<th>Sensor Type</th>
<th>Severity</th>
<th>Last Process Date</th>
<th>View Details</th>
<th>Related Task(s)</th>
<th>Remediation Status</th>
<th>Vulnerability Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sample NERC CIP Case</td>
<td>172.16.42.14</td>
<td>Buffer overflow in the convert function in Microsoft SQL Server 2000 SP4, 2000 Desktop Engine (MSDE 2000) SP4, and 2000 Desktop Engine (WMSDE) allows remote authenticated users to execute arbitrary code via a crafted SQL expression.</td>
<td>CVE-2008-0086</td>
<td>9.0</td>
<td>ACAS-CVE</td>
<td>High</td>
<td>09/21/2015 00:15:35</td>
<td></td>
<td></td>
<td></td>
<td>Fail</td>
</tr>
</tbody>
</table>
Built-in quantitative risk analysis

Algorithmic Approach

Sensor Data Sources
- Nessus, AppScan, Onapsis
- Vormetric/ProtectV
- Nessus, Patch Mgmt.
- vGW, McAfee (EPO), FortiNet
- vGW, McAfee (EPO)
- vGW
- CISCAT/Nessus/xCDF
- xStream/Mt. Wilson
- xStream
- Firewall/IDS/IPS/AlgoSec
- Firewall/Fortinet/Juniper
- IDS/IPS/AlgoSec
- ViewTrust-ERM
- ViewTrust-ERM
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

Global Product Data Interoperability Summit | 2016

Application Managed Services

Infrastructure Managed Services

Virtustream Software Suite

ViewTrust

Private Cloud

Infrastructure as a Service

Object Storage Service

ON PREMISES

OFF PREMISES
Continuous Compliance for Hybrid Cloud

Enterprise Risk Management

Virtual Datacenter 1/SDDC

Unified View

Automated Continuous Assessment for Risk and Compliance

Public/Managed + Private
IntelTxT for trusted boot and geo-fencing
Compliance as a Service with Power of Inheritance

IaaS

PaaS

SaaS

Inheritance of controls by CSC

Cloud Service Provider (CSP)

Cloud Service Customer (CSC)

Application (HR)

Platform (Win2008)

Virtual Layer (VMware/Xen)

Hardware (Blade + Storage)

Facility
Cloud Audit and Compliance

Global Product Data Interoperability Summit | 2016

Audit Artifacts

Authorization Packages (PKG1)
Authorization Packages (PKG2)
Authorization Packages (PKG3)

Security Assessment Review (SAR)
System Security Plan (SSP)
SY51
CCP4
CCP2

Authorization Package (PKG3)

Cloud Audit and Compliance

Audit Artifacts

Authorization Packages (PKG3)

IA Controls
Inheritance

SaaS
Inheritance

PaaS
Inheritance

IaaS
IA Controls

Application

App1
App2
App3
App4
App5

Platform

OS1
OS2
OS3

Hypervisor
Virtual Layer

Hardware

Facility

CCP1
CCP2
CCP3
CCP4

JVM
DB
Python
IDM
PHP

Copyright © 2016 Boeing. All rights reserved.

Copyright © 2014 Northrop Grumman Corporation. All rights reserved.

GPDIS_2016.ppt | 45
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
Kaus Phaltankar
kaus@Virtustream.com
Kaus.Phaltankar@dell.com
+1 (703) 627-7539