virtustream

Whitepaper

Viewtrust™ for Enterprise Risk and Compliance Management

Threat to Cyber Security is 24/7. New attack vectors are being designed daily and the bad actors have to get it right only once. Enterprise has to defend itself continuously and has to get it right every time!

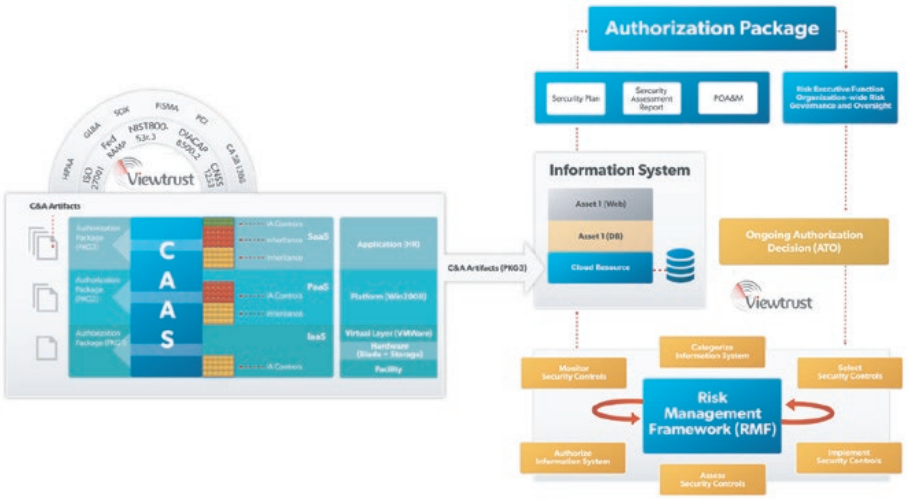
Virtustream's Viewtrust™ solution allows enterprises to build best proactive defenses against Cyber Threats and build an effective Cyber Security strategy with continuous monitoring of risk and compliance.

Regulatory requirements such as, GLBA, SOX, HIPAA, PCI or the Federal Information Security Management Act (FISMA) mandate 'continuous monitoring' of information systems for Private Personal Information (PPI) data as well as monitoring of unauthorized access to maintain integrity of data and systems.

The biggest challenge for enterprises today, is to truly understand what it means to conduct 'Continuous Risk and Compliance Monitoring', and what that fully entails. In this paper, we will review each one of these aspects of Continuous Monitoring and provide solutions to accomplish it using automation tools and techniques in context of the Risk Management Framework.

NIST SP 800-37 Rev1–Risk Management Framework (RMF)

NIST 800-37 Rev.1 (Chapter 3, P.36) says, "Organizations may choose to eliminate the authorization termination date, if the continuous monitoring program is sufficiently robust to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities with regard to the security state of the information system and the ongoing effectiveness of security controls employed within and inherited by the system" The organizations must still maintain formal authorizations and acceptance of risk but may leverage results of continuous monitoring assessments to support the ongoing authorization to operate (ATO).



The initial Authority to Operate (ATO) certification and ongoing Continuous Monitoring are required for newly procured systems as well as for continued operation of an existing system. Continuous Monitoring encompasses everything from monitoring changes to the System asset components, Situational Awareness data from assets, to conducting ports and protocol analysis using vulnerability analysis tools and keeping the system related Plan of Action and Milestones (POA&M) updated. It also includes policy monitoring and documentation updates for annual or significant change related re-certifications.

The Continuous Monitoring of a system requires compliance with three key requirements:

- Change and Configuration Management of Assets
- Monitoring of Security Controls using Automated Tools
- Documentation Updates and Reporting

Change and Configuration Management (CM) of Assets

The Configuration Management (CM) controls within NIST SP 800-53rev4address the needs of change and configuration management of a system with the goal of enabling and maintaining security while managing the risks on an on-going basis.

The NIST SP 800-128 draft specification provides a detailed guidebook for using configuration management to maintain integrity of IT resources. As per SP 800-128, the change and configuration management facilitates asset management, incident management; help desk, disaster recovery, and aids in software development, testing and release management. It also enables greater automation of processes, supports compliance with policies and preparation of audit. The Change and Configuration Management comprises a collection of activities that start with the establishment of the baseline configuration. Each item being tracked is known as a Configuration Item (CI). The baseline configuration provides information on the asset hardware, Operating System, applications installed, their versions and patches. Each baseline configuration needs to be formally reviewed and agreed upon and can only be changed through a change control process. The Configuration Management Plan (CM Plan) provides comprehensive details on description of roles, responsibilities, policies and procedures that govern the change in configuration of assets and systems.

The CM Plan includes:

- **Change Control Board** – Charter and organization structure.
- **Configuration Items (CI) Identification** – Process for selection and naming of items placed Viewtrust under CM.
- **Baseline Configuration Management** – process for establishing and managing the baseline for the CI.
- **Configuration Change Control** – Process for managing changes to the baseline
- **Configuration Monitoring** – Process for assessing compliance with baseline and reporting status (compliance or changes) to the CI

The Change and Configuration Management for security of Information Systems involves a set of activities that can be grouped into four phases:

- Planning
- Maintaining
- Implementing
- Monitoring

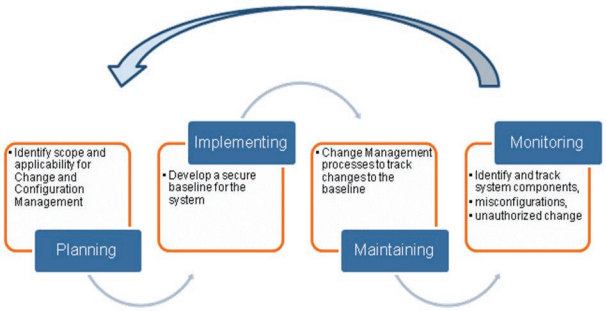
The other Information Assurance control families greatly affected by CM family include all the Technical Controls such as the Access Control (AC), Audit and Accounting (AU), Identification and Authentication (IA), System and Communication Protection (SC) and Operational Control such as the System and Information Integrity (SI) family of controls.

Monitoring of Security Controls Using Automated Tools

The objective of monitoring of security controls is to determine if the controls implemented or inherited by the system continue to be effective over time as the system undergoes changes. This encompasses ALL controls and not a subset. The Continuous Monitoring of controls requires monitoring of each control with varying frequencies based on:

- **Control volatility** – The more volatile controls need to be monitored more frequently
- Organization and system risk tolerance
- Current threat information that might affect the system

Change and configuration management phases



The Continuous Monitoring strategy needs to specify the monitoring frequencies along with the reporting frequency and the details required for reporting. As the size and complexity of today's system increases, it is hard to gather the required details and the frequency desired manually. The process of monitoring and reporting has to be automated using tools that provide situational awareness data in support of:

- Risk based decisions
- Evaluation of 'on-going' authorization
- Asset and configuration management to identify changes and their impact on security posture
- Reporting the system security status at any point in time

Some of the technical and operational controls lend themselves to automation much more easily than others. These controls can be evaluated and monitored using vulnerability assessment tools or event management and alerting systems that provide situational data based on logs and Simple Network Management Protocol (SNMP) alerts.

The supplemental guidance for the Continuous Monitoring control (CA-7) from NIST 800-53 Rev.3 states that, "A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational

The Configuration Management Phases address the CM family of controls within NIST800-53rev4. These are:

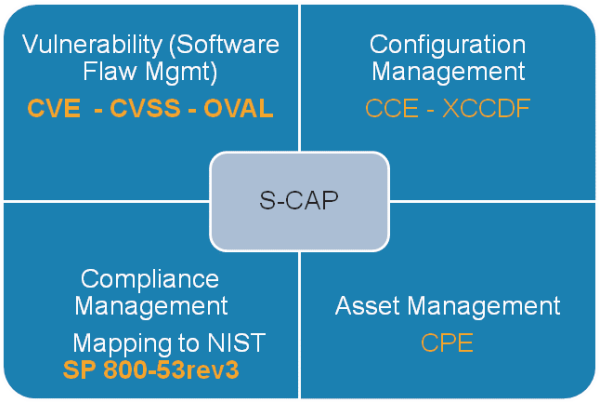
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CM-3	Configuration Change Controls
CM-4	Security Impact Analysis
CM-5	Access Restrictions For Change
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan

situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones - the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the impact level of the information system."

Vulnerability and Configuration Assessment Tools

The vulnerability and configuration assessment tools such as Tenable Security Center, Symantec CCS, McAfee ePolicy Orchestrator (ePO), Retina Scanner, and others, provide the ability to assess the impact of changes to the asset and the vulnerabilities introduced as a result of these changes. In addition, the tools provide an initial assessment of severity of the impact and possible solutions for mitigation.

The compliance with NIST Security Content Automation Protocol (SCAP) specifications, allows these tools to use a common identification of the vulnerability using the Common Vulnerabilities and Exposure (CVE) ID and a Common Vulnerability Scoring System (CVSS) for threat rating. The SCAP compliant tools also provide information on the controls being affected by these vulnerability and Configuration findings based on Open Vulnerability Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) benchmark tests as well as results being presented in Assessment Summary Results (ASR) standard format.



Situational Awareness with Event Management

Enterprise Event Management and a Compliance Reporting capability are imperative to successfully assess the security posture of a system and its assets on an ongoing basis. It is important to make sense out of vast amount of disparate data being collected from large number of systems to generate the Situational Awareness data. The ability to view the impact of the events on a system and their impact on Information Assurance (IA) controls is critical to providing a coordinated response and maintaining the confidentiality, integrity and availability of the information system.

Event Management Component of Virtustream Viewtrust™ solution, offers real-time situational awareness in a rapidly changing environment, with information security threats that may affect the IT controls and integrity of the resident information. The Viewtrust Event Management Component collects information such as security logs, application event logs, system logs and database audit table logs from multiple devices across multiple platforms and processes the information on a local or an enterprise level, as shown in the figure. The log and audit data are then normalized for automatic event correlation. The event correlation and analysis, results in significant data reduction and bubbling of critical events to the top, thus providing actionable situational awareness data.

The situational awareness data from an asset needs to be mapped to the System that includes this asset in its system definition and the IA control that may have been affected. This provides data to the system owner and the Designated Approving Authority (DAA) on evaluating the risk to the Information System. The remediation action may then be documented as a task or a Plan of Action and Milestones (POA&M) item.

Documentation Updates and Reporting

The critical documents such as the System Security Plan (SSP), Security Assessment Report (SAR) or the Security Test and Evaluation (ST&E) report and the POA&M, need to be updated and kept current as per the Continuous Monitoring process. These three key documents and the supporting artifacts are required for any authorizing official to conduct their evaluation of risk, and granting of continued authorization. The POA&M reports are especially critical, as they need to be made available to OMB upon request or at least quarterly.

There is a significant amount of effort involved in keeping these detailed information documents updated and reflect the current state accurately.

Just as the asset information becomes potentially stale within twenty-four hours of documentation, the SSP and SAR documents are equally prone to become stale in a short order. An automation tool is the only way to keep these extensive (sometime 200-300 pages) documents updated on an on-going basis.

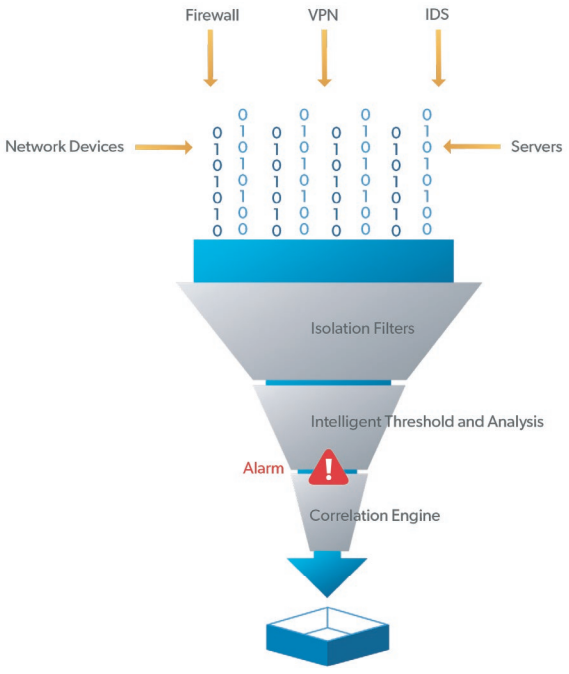
The SSPs need to reflect changes to the System and its assets based on Change and Configuration Management process as well as any updates to the control implementation, while the SAR/ST&E documents need to reflect the testing and validation of the controls to identify any risks introduced due to these changes. Any new risk identified or an impact on the existing POA&M item needs to be reflected and reported to the authorizing official and OMB.

Viewtrust Solution for Continuous Monitoring

The Viewtrust solution allows agencies to meet the key requirements of Continuous Monitoring discussed earlier and listed below:

- Change and Configuration Management of Assets
- Monitoring of Security Controls using Automated Tools
- Documentation Updates and Reporting

The Viewtrust solution provides a scalable data ingest, collection, storage, processing platform which is currently supporting critical Federal enterprise environments monitoring millions of devices and processing multitude of data input types from thousands of sensors. Through a common operational and situational awareness picture, Viewtrust delivers accurate and timely view of the operational risks by providing a 360-degree view of assets, their software and hardware inventory, vulnerabilities (VUL) and compliance with approved configuration baselines. The Viewtrust solution helps in the reduction of network vulnerabilities through the synchronization of processes and technologies that address not only compliance driven mandates such as the Federal Information Security Management Act (FISMA), but a holistic view of the enterprise Information Technology (IT) infrastructure for cyber and Continuous Risk management objectives across disparate organizational functional groups and across widely dispersed locations. The key attributes of the solution include:



Scalability: Viewtrust, can be configured to support ingest of organization's device related data. Scalability can be imposed across data storage per size, frequency, and retention metrics. Additionally, the platform demonstrates data collection flexibility and analysis scalability; the solution can be deployed stand-alone or can be setup in tiered architecture to accommodate distributed enterprise implementation.

Agnostic Sensor Coverage: The Viewtrust data ingestion is preconfigured to support SCAP input formats, VUL scanner output ingest, and can be adapted to non-standard or legacy data needs. Viewtrust supports network, asset, configuration and vulnerability scans to identify and account for rouge assets and network devices. The process supports ingest of gigabytes to petabytes of data across the enterprise. Sensor integration can consume both DOD and NIST versions of ARF and ASR formats; native integration is supported for scanners such as Tenable Nessus, eye Retina, Qualys, McAfee or host-based agents provided by McAfee ePolicy Orchestrator (ePO) and Host Based Security System (HBSS) amongst others. The platform can consistently maintain data collection and monitoring for all required conditions across all devices in each set of successive scans.

Monitoring Management/Work Flow Capabilities:
The solution controls all workflow requirements in terms of risk monitoring, compliance with baseline specifications as well as response metrics and related corrective actions. The built-in workflow manager can be customized to map business processes. For example, the task workflow for asset removal or waiver. Each deviation from a policy or the benchmark is marked with a risk value, which can then trigger the business logic to create alerts to systems administration or Information Assurance Officer (IAO) for action such as authorization or disallow connection. The platform accepts compliance 'benchmark test' results based on SCAP Asset Reporting Format (Inventory) or Assessment Summary Results (ASR); the ASR files contain results from SCAP XCCDF or OVAL tests for policies or baseline compliance. The Business Logic also provides risk analysis and scoring for non-compliance with Standard Operating Environment (SOE) or compliance with Anti-virus updates or host intrusion detection signatures.

Data Warehousing: The platform can utilize SQL-based RBDMS data storage (e.g. MS SQL, ORACLE, DB2), thus providing encrypted and scalable capability. Additionally, data warehousing can be configured based on a NoSQL Hadoop based solution offering linear scalability based on a multi-node cluster solution (i.e. "Big Data" data mining servicing). The Hadoop option utilizes the Apache HBase database, which is a distributed 'Columnar Family Database' and is layered upon the Hadoop Distributed File System (HDFS). HBase is a NoSQL database and provides a SQL like interface with Hadoop Hive.

In summary, Virtustream Viewtrust solution for Cyber Security provides a Continuous Risk and Compliance Monitoring (CRCM) capability that provides:

- Proactive Risk Management using Standards based Framework
- Continuous Monitoring of each asset for Compliance and Risk by building a 360 degree view of each asset within the enterprise
- Continuous monitoring requires ability to process massive volumes of variety of data quickly (Volume, Variety and Velocity). The data could be structured or unstructured.
- Perform deep automated and manual analysis based on threat and impact analysis
- Building and utilizing knowledgebase for continuous refinement of data analytics
- Enabling near automated mitigation by interfacing with other tools and technologies

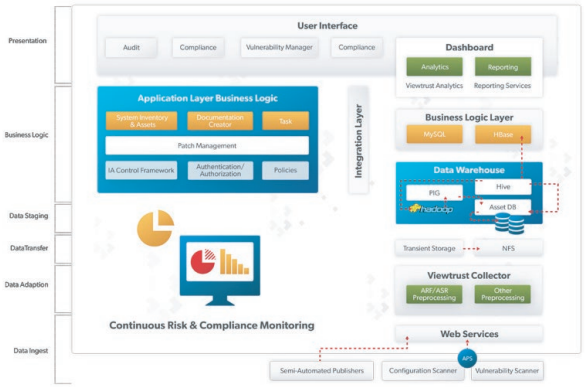
Viewtrust Reference Architecture

The Viewtrust solution is comprised of certified components and interchangeable plug-in modules with variety of storage options. The platform ingests data from a wide variety of sensor inputs that are proprietary to the vendor formats or SCAP standard compliant. The data ingested is stored in either a conventional Relational Database Management System (RDBMS) or NoSQL "big-data" Hadoop based repository. The solution offers mature business logic component, customizable workflow manager and related asset data management functionality as it gathers and analyses the Hardware/ Software Inventory, Configuration Settings, and Vulnerability Management across the enterprise.

As depicted in figure below the architecture of the Viewtrust as applied within the entirety of the solution can be broken into the following service layers: Data Ingest Layer, Data Adaptation Layer, Data Transfer Layer, Data Staging Layer, Business Logic Layer and Presentation Preparation Layer.

The Viewtrust monitoring data lifecycle operates as follows:

1. Data Ingest Layer: Data ingest supports pull and/or push interaction across the device spectrum; the product supports SCAP and a large collection of common non-SCAP compliant device requirements, as well as VUL Scanner intake for common applications such as Tenable and Symantec, McAfee, and Security Event Information Management (SEIM). The sensors against such elements as ePO servers, ACAS Security Center or other 'Semi-automated' publishers 'PUSH' information to the Continuous Monitoring and Risk Scoring (CMRS) Collector Web Service, namely, the Viewtrust Web-Service. The information can be in standardized ARF and ASR reporting Extensible Markup Language (XML) schema.



2. Data Adaptation/Transfer Layer: The Viewtrust processes the data received by the Viewtrust Web Service using pre-processors. The pre-processors parse incoming ARF/ASR files and upload the information to the relational database management system (RDBMS) or Hadoop Distributed Files System (HDFS) based repositories. The Viewtrust Collector converts the parsed ARF/ASR content and uploads the data to HDFS. Data is also forwarded to a long-term storage, such as Storage Area Network (SAN), facility.

3. Data Staging Layer: Data repositories, deployed as either traditional RDBMS or NoSQL Hadoop HBase data store, are used to accommodate diverse data size, frequency and retention specification. As an RDMBS solution the environment can be established based on any standard product suite. (e.g. SLQ/ORACLE/ DB2). Alternatively, as a Hadoop solution, HBase enables distributed store and parallel processing of large data volumes across inexpensive, industry-standard servers that both store and process the data, and can scale linearly.

4. Business Logic Layer: The business logic layer implements the computation of various compliance and risk scoring models and associated algorithms based on organizational business objectives.

5. Presentation and Analytics Layer: The presentation layer readies data for data analytics and presentation using a power Business Intelligence (BI) tool. The BI Engine supports multi-dimensional 'cube' based analysis capability. The Viewtrust reporting module outputs in a schema format consistent with the dashboard tool to be deployed. The reporting engine feeds the Risk Scoring charts and tables as rendered via respective dashboard tools and their configured levels of authority and functional capability.

Viewtrust Component for FISMA A&A Documentation

Virtustream's Viewtrust™ solution has been designed to guide agency assessment and authorization (A&A) teams through a structured methodology that strictly follows the NIST/DOD guidelines and helps meet the requirements of Continuous Monitoring. It also helps A&A team to prepare the initial and subsequent updates to A&A packages, complete with the necessary documentation for getting and maintaining the ATO.

The Viewtrust solution provides a full view of your current security posture through self-assessment while breaking down the improvement process into straightforward, manageable and repeatable steps. Using a methodical analysis, potential security gaps are identified and addressed with auditable steps. The comprehensive and intuitive step-by-step approach allows you to quickly assess your FISMA preparedness, as well as maintain authorization by meeting the requirements of Continuous Monitoring.

The Viewtrust solution delivers:

- Change and Configuration Management automation through built-in workflow manager with direct link to the Asset Management
- Asset Management module provides tracking of asset changes with built-in asset discovery capability and provides comparison with the baseline configuration
- Intuitive interfViewtrust for evaluating 800-53 controls and validating the control implementation via 800-53a
- Complete visibility of A&A efforts via dynamically updated Dashboard
- Document creation via templates and wizards
- Zero duplication and increased accuracy in documentation with automatic change propagation
- Complete task planning, scheduling and assignments via workflow manager
- Tracking of POA&Ms and automated alerts based on milestone dates
- Knowledgebase repository for continuity and sustainment of the work efforts in constantly changing environment

Summary

The Threat

Virtustream' Viewtrust™ provides a complete tool to meet the requirements of Enterprise Risk and Compliance management. It provides a comprehensive yet cost effective solution for Continuous Monitoring of risk and compliance. The Viewtrust solution:

- **Simplifies the Continuous Monitoring Process** – so the process is straightforward and covers all the requirements of NIST 800-37 Rev.1, Risk Management Framework.
- **Continuous Monitoring based on SCAP and non- SCAP data ingest** - Viewtrust solution ensures effective collection, assimilation and analysis of security content. Applying a standard/non-standard sensor ingest capability, sophisticated rules based risk analysis engine, and a readily adaptable standard/non-standard dashboard interfViewtrust, Continuous Risk and Compliance monitoring requirements are facilitated in a proven, cost effective turnkey solution.
- **Provides Change and Configuration Control Management** - using the built-in workflow manager and Asset Management

- **Achieves Process Automation** – so more work can be done with less people; through streamlined A&A processes, and the ability to engage team members of different background and skill sets at a high level of effectiveness for updating, testing and validating IA controls
- **Automates Documentation and Artifact Creation Process** – so as to focus more on the task of Information Assurance than cumbersome documentation. The automation process also streamlines the data gathering process and produces documents of consistent quality.
- **Provides Program Dashboard for A&A Effort** – so the leadership has the most up-to-date knowledge of the security risk, threat assessment and status of the A&A efforts to better manage the program and achieve 100% compliance required by the law.

Contact Info

Bethesda, Maryland (Headquarters)
4800 Montgomery Lane, Suite 1100
Bethesda, MD 20814
T +1.240.252.1007
F +1.301.718.7880
info@virtustream.com
www.virtustream.com

About Virtustream

Virtustream, a Dell Technologies Business, is the enterprise-class cloud service and software provider trusted by enterprises worldwide to migrate and run their mission-critical applications in the cloud. For enterprises, service providers and government agencies, Virtustream's xStream management platform and Infrastructure-as-a-Service (IaaS) meets the security, compliance, performance, efficiency and consumption-based billing requirements of complex production applications in the cloud – whether private, public or hybrid.

