HYTRUST

Winning the war on mission-critical security challenges

From the front lines to the bottom line

White Paper

Table of Contents

3 The challenges of adopting virtualization

3 'Air-gap' security risks

4 Compliance security risks

5 Log gap security risks

5 Overcoming these challenges with – Intelligent Workload Security framework

6 Intelligent Workload Security framework

7 The HyTrust Solution based on Intelligent Workload Security framework

7 Deploy military-grade security

7 Deploy automated continuous compliance

8 Reduced cost and complexity

8 To summarize

9 About HyTrust

10 Appendix A

HYTRUST

White Paper

Winning the war on mission-critical security challenges

From the front lines to the bottom line

The challenges of adopting virtualization

Government, military, and major national civilian agencies make enticing targets for cyber crime and cyber espionage. To combat this reality, significant measures have been implemented or are underway to make networks and data safe in the federal government, the military, state and local governments, and large national organizations such as airports. Yet, there are still numerous challenges blocking an ultimate victory over cyber crime at every level.

In addition, president Barack Obama's government budget for fiscal year 2015 cut the government's IT spending by about 3%, including a 6% cut from the IT budget of the Department of Defense and a 0.2% cut from the total IT budget of major civilian agencies.

To overcome the ongoing cybersecurity battles, while simultaneously faced with the need to reduce its expenditures on information technology, federal, state and local government have widely adopted virtualization to take advantage of not only the increased agility, but also the greater efficiency and cost savings. While virtualization does enhance the agility and cost effectiveness of IT, it also creates its own, unique set of cybersecurity challenges. Among them:

- Decreased agility and increased costs created by air-gapping practices, designed to keep data of different risk classifications isolated and physically separate for different tenants and different missions.
- A lack of automated continuous compliance capabilities with various regulations.
- Security log gaps created by data that is too high level and supplies no critical details.

This white paper overviews the unique challenges faced by government and military organizations and introduces a solution that enables secure and logical boundaries for mixed workloads on the same platform, automated continuous compliance, and detailed, real-time, and auditable log data in granular detail.

'Air-gap' security risks

Air-gapped systems are isolated from the Internet and are not connected to other systems that are connected to the Internet. They have been used in situations that demand high security because they make siphoning data from them difficult. For many years, it was believed that air-gapped systems provided the most secure

Researchers expose air-gap weaknesses

Two separate groups of researchers have exposed the weaknesses of the common practice of separating data in data centers through "air-gapping":

- One set of researchers demonstrated a method for leaking data from air-gapped systems using radio frequencies to transcribe keystroke data from an isolated computer to a mobile phone's FM radio receiver without using Wi-Fi or Bluetooth.
- A second set of researchers showed how air-gapped systems can be compromised using keystrokes that capture side-channel signals from computers connected to secure isolated networks.

Data center consolidation creates new risks

The U.S. government has been tasked with consolidating its 9,658 data centers, thereby, reducing both the total number and budget to run them by the Federal Data Center Consolidation Initiative (FDCCI). The government's definition of a data center is broad and includes small operations tucked into oversized closets. The government planned to shut 44 percent of its data centers by the end of 2015 and expected to save $3.3 billion by the end of 2015. However, some experts warn that the data center consolidation initiative could create new security risk, including an increased risk of data breaches and a reduced ability to keep multi-tenancy data separated.

platform in classified government and financial systems, because they are physically isolated from other machines, networks, and the Internet. In fact, to keep data with different risk classifications isolated and physically separate for different tenants and different missions, most government data centers are physically air-gapping data.

What's more, in practical experience, air-gapping has created an unforeseen problem in combat. While many combat missions are executed with precision timing—in minutes, not hours—waiting for mission-critical data can undermine the impact—and put missions and lives at risk. In short: soldiers in the field cannot wait for IT teams back home to gather the intelligence data they need—or worry about the costs of gathering the required data from multiple air-gapped sources. The cost of time, dollars, and lives is too high to put at risk.

While air-gapping was once viewed as an ideal solution for keeping groups of data separate from other groups of data, practical experience and several recent studies have exposed significant weaknesses in the common data-separation practice. (See sidebar.) Among the limitations of physical separation as a security technique are decreased agility and increased costs. With data secured in multiple environments, accessing that data becomes a cumbersome, time-consuming, and multi-step process. While creating often-critical access delays, it also opens the door for the risk of errors and the likelihood that some unknown or unauthorized external connection to arise. Further, a delayed response to time-sensitive created by accessed air-gapped data could impact military response, national security, and soldiers' and citizens' lives.

Compounding the problem is the Federal Data Center Consolidation Initiative's (FDCCI) mandate for the consolidation of government data centers. (See sidebar.) As federal CIOs have worked to consolidate and overhaul their agencies' data centers, a new report found that the initiative is creating new security concerns despite common air-gapping measures. In the survey of 300 federal IT managers, over two-thirds (67 percent) of respondents indicate that they have security concerns about their data-center modernization efforts—which include reducing the total number of facilities, virtualizing machines, and moving systems to the cloud. Chief concerns include advanced targeted attacks (ATAs) and advanced persistent threats (APTs), along with zero-day attacks. Another significant concern is increasing the risk of data security breaches within the data centers.

The security challenges and risks associated with air-gapping data can be mitigated by a technology that can guarantee multi-tenancy data separation, and allow mixed workloads on the same platform without any data contamination.

Compliance security risks

Not only do U.S. Government CIOs and CISOs have to keep public information and critical infrastructures secure, but also they must comply with an ever-increasing number of government security regulations—a task that can be extremely challenging. "In today's threat-driven environment the bitter truth is that one can schedule an audit, but one cannot schedule a cyber-attack. This has led many industry standard bodies ... to change their approach and incorporate the concept of continuous compliance into their regulations. These renewed guidelines encourage organizations to find ways to streamline governance processes, continuously monitor compliance and their security posture, and correlate it to business criticality." However, few government agencies and organizations have the technology to execute continuous compliance.

The security departments of government agencies face three overarching challenges in meeting security compliance requirements in a virtualized environment:

"Federal cybersecurity policy is a confusing maze of overlapping and sometimes inconsistent rules that are applied and enforced differently across various federal agencies. Congress and the White House have deputized various agencies to spearhead the federal government's cybersecurity efforts. Yet, truly coordinated policy and regulation have remained elusive. Based on our analysis, a primary reason for this is that most every agency and even many sub-agencies want a role in cybersecurity policy and data security as relates to their areas of responsibility."

— Morrison & Foerster's Government Contract Insights

SIEM Tools Providers
Forensic quality logs are important for security audits, and getting maximum returns on investment in various SIEM tools, like HP ArcSight, Splunk applications, McAfee NitroSecurity, IBM QRadar, and LogRythm.

1. Compliance is not automated in virtualized environments. It's a static and a manual process with a potential to introduce security threats and increases risk.

2. Compliance reports do not contain enough granular detail to clarify what incidents occurred, when exactly they happened, and who was responsible.

3. Many mission-critical systems within a government are required to conduct certification and accreditation (C&A) every six months, for example, for the U.S. Intelligence Community Directive 503 (ICD-503). This is challenging with a manual process (in virtualized systems). What's more, it's risky. Among the risks, a virtual admin could open a port in violation of standards and five months could pass before logs would report the open port. The security consequences could be potentially disastrous.

The security challenges and risks associated with compliance requirements can be mitigated by a technology that automates continuous compliance, produces forensic analysis, supplies clear audit trails, and enhances role-based controls.

Log gap security risks

Regular log collection is critical to understanding the nature of security incidents during an active investigation and post-mortem analysis. Logs are also useful for establishing baselines, identifying operational trends, and supporting the organization's internal investigations, including audit and forensic analysis. In some cases, an effective audit-logging program can make the difference between a low-impact security incident, which is detected before covered data is stolen, and a severe data breach where attackers download large volumes of data over a prolonged period of time.

Yet, the federal government's cybersecurity initiatives are marked by significant log gaps, especially of real-time and auditable tracking of important details. While some platforms provide some of the log data required to show compliance, there are often large log gaps, such as no unique user ID for every administrative operation and no record of denied operations. Without appropriate audit logging, an attacker's activities can go unnoticed and evidence of whether or not the attack led to a breach can be inconclusive. As a result, the risks of insider threats or fraudulent activity are greater.

The security challenges and risks associated with log gaps can be mitigated by a technology that ensures workloads stay within logical and physical boundaries, roles are monitored, downtime is eliminated, and they are deployed quickly.

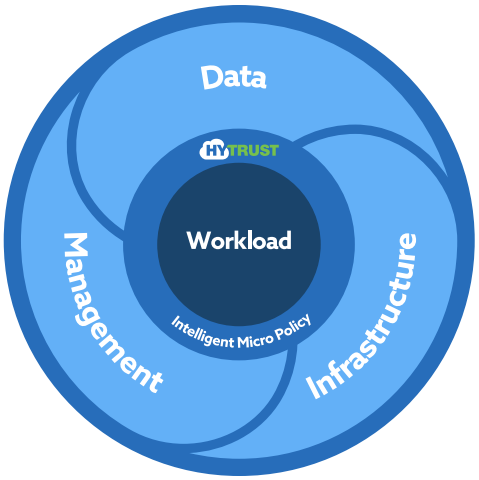
Overcoming these challenges with — Intelligent Workload Security framework

As the widespread adoption of virtualization has infiltrated every major government agency and business organization, its created a new set of challenges attacking cybersecurity missions, including air-gapped, compliance, log gap risks. What's needed to overcome these challenges is a framework that addresses them all head on with military-grade security, automated continuous compliance, and reduced complexity and costs. There is a framework now that conquers all three—the Intelligent Workload Security framework. Here's how the three-pronged solution combats mission-critical risk:

- **Military-grade Security** - Secure multi-tenancy without inefficient air-gapping
- **Continuous Compliance** - Automated with reinforcement, analysis, and audit files
- **Complexity and Cost Reduction** - Flexible policy changes through a layer of abstraction from underlying hardware

Intelligent Workload Security framework

Automated Continuous Compliance
- Clear audit trails
- Automated compliance
- Role-based controls



Military-grade Security
- Encryption and key management
- Secure multi-tenancy

Reduced Cost and Complexity
- No touch maintenance
- Zero downtime
- Cross-platform policy

Military-grade Security. Intelligent Workload Security executes workloads and protects and encrypts data on any private, public, or hybrid cloud deployment. It deploys strong, but easy-to-use, key management, which is critical for ensuring workloads migrate without risking data loss.

Automated Continuous Compliance. Intelligent Workload Security provides continuous monitoring and enforcement of virtual workloads that contain sensitive data, which is subject to numerous regulations. It executes these tasks without false positives or the need for manual intervention. Furthermore, the solution also provides automated continuous compliance to various regulations such as shown in Table 1. While legacy security controls may meet these stipulations when virtual workloads are first deployed, security oversight quickly dissipates as workloads migrate across servers, data centers, and from private to public clouds.

Leading government security compliance regulations (Table 1)

Acronym	Name	Acronym	Name
FISMA	Federal Information Security Management Act	CNSSI 1253	Committee on National Security Systems (CNSS) Instruction
FIPS	Federal Information Processing Standards	FedRAMP	Federal Risk and Authorization Management Program
NIST 800-53	National Institute of Standards and Technology	CJIS	National Institute of Standards and Technology
ICD-503	U.S. Intelligence Community Directive 503		

Reduced Cost and Complexity. Intelligent Workload Security provides a layer of abstraction from the underlying physical hardware, so that government agencies and other organizations can incorporate all required policy changes, without worrying about the vendor or technology stack. The solution also provides logical and auditable separation of different classifications of workloads without requiring additional costs from air-gapped infrastructure to meet security and compliance needs. This reduces complexity as well as costs.

"Every agency within the U.S. Government fully understands the need to rapidly deploy virtualization technologies and strategies to enhance the ability to respond to market forces while continuing to reduce costs. I look forward to working with HyTrust to address the demanding security needs of this vital sector while enabling full innovation."

—Ambassador Robert Gelbard
former U.S. state department career diplomat

The HyTrust Solution based on Intelligent Workload Security framework

Whether executing detail missions on workloads or supporting soldiers' missions in the field, no CIO or CISO wants to be undermined by security challenges—especially when they are preventable. Overcoming critical challenges, like decreased agility, compromised compliance, and chronic log gaps, is now possible—by deploying the HyTrust solution based on Intelligent Workload Security framework. With this solution, government agencies, the military, and national organizations will gain these mission-critical capabilities.

Deploy military-grade security

- **Secure Multi-Tenancy.** Enables secure, logical data and workload boundaries, which allow mixed workloads on the same platform without any data contamination. This makes secure multi-tenancy possible by closing gaps in virtual infrastructure access control, network segmentation, and logging, as well as by adding critical data security through encryption. By doing so, the solution fulfills the requirement for effective workload isolation—preventing unauthorized communications and access, and by logging all administrative activities. Government agencies can move forward with private and hybrid cloud adoption plans knowing their mission-critical applications and data are truly isolated from other tenants' users and virtual environments.

- **Mission-Critical Data Protection.** Enforces two-factor authentication on all critical or destructive actions, thereby, preventing accidental or malicious actions from breaching the network—either internally or externally.

- **Encrypt Data at Rest.** Sensitive workloads remain encrypted whenever they are not used for application processing on any cloud platform or location. When in use, the decryption is controlled so that sensitive workloads can only execute on authenticated servers when allowed by IT, security, compliance, and risk teams. This eliminates the risk of lost or stolen workloads falling into the hands of cyber adversaries.

- **Guaranteed Data Separation.** Ensures that admins can only access their own missions and agency data and applications as can be seen in the log files and audit logs. Two models of automatic data separation are supported:

  - **Software-based Approach -** leverages sophisticated workload tagging classifications. The advantages include fast setup and deployment independent of hardware platforms. Also, admins can set logical boundaries to ensure workloads remain within the set boundaries, regardless of the operator's request.
  - **Hardware-based Approach -** employs Intel TXT platform, which enhances security in this environment. Missions are locked down from the VM to the processor BiOS using Intel TXT. See Appendix A for more details.

Deploy automated continuous compliance

- **Automated Continuous Compliance.** Automates uninterrupted compliance with FISMA, NIST 800-53, NCSSI 1253, CJIS, and ICD-503 with no visibility gaps. What's more, it delivers continuous enforcement, without false positives or manual intervention security. Compliance functionality includes:

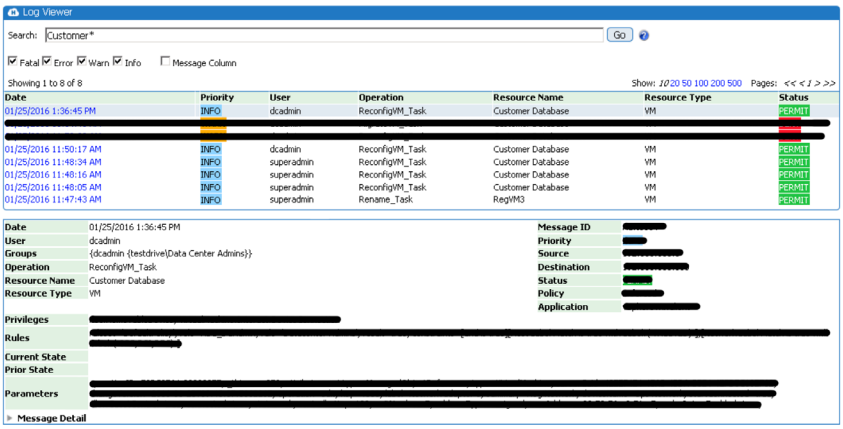
  - Applies an automated ICD-503 compliance template.
  - Virtual systems are compliant in less than one minute from hardware to the hypervisor, versus one week, such as in outdated manual static mode.
  - ICD-503 compliance is continuously monitored and alerted in real-time. For example, if a virtual admin opens a port in violation of standards, they receive an alert in five minutes, so every threat can be averted.

"Customers need an assured root-of-trust and attested parameters like location information that can be relied upon to allow seamless movement of VMs in various cloud deployments. As enterprises become increasingly reliant on software-defined networks within virtualized and cloud infrastructures, this is exactly the kind of policy-driven control with an assured source of such policy information needed to enhance security and ensure compliance."

— Ravi Varanasi
General Manager
Cloud Security, Intel

- **Forensic Analysis.** With continuous protection and monitoring, fast and real-time analysis becomes easy. Hytrust delivers easy and fast analysis, so that admins can find which actions led to what violations and take rapid action.

- **Clear Audit Trails.** Displays in granular detail what happened and when (far beyond what virtualization management software provides). Provides CISOs and compliance officers an audit trail to ensure they remain in compliance as VMs move and execute workloads. Additionally, the solution reports any VMs that violate policies, so that security controls and investigate policy violations can be fine-tuned.



This is the data in the native virtualization logs

- **Enhanced Role-Based Controls.** Admins can deploy their own missions without fear of overlapping, security and compliance violations, or data contamination.

Reduced cost and complexity

- **Eliminate Air-Gaps.** Eliminates air gaps, while still ensuring workloads stay within logical or physical boundaries on specific hosts, data centers, or geographical regions—automatically without additional monitoring.

- **No-Touch Maintenance.** Intelligent micro policy controls and multi-admin capabilities keep everyone in their designated roles automatically.

- **Zero Encryption Downtime.** Intelligent workloads take action automatically without requiring downtime and key encryption functions.

- **Fast Deployment.** The solution is pre-integrated with VMware SDDC/NSX, and works across any VCA, AWS, or other public platform.

To summarize

Combating an ever-increasing number of cyber threats is mission one in today's organization, including governments, the military, and large civilian entities, such as airports. Leading-edge technologies can help achieve cybersecurity goals. But, often, they can also create new challenges that expose networks to both internal and external invasion. Virtualization is a good example. While it has brought increased agility and cost savings to the cybersecuity battleground, it has also exposed organizations to three key threats: air-gapping issues, a lack of continuous compliance, and security log gaps.

Government ready and tested

- Automated compliance enforcement for 800-53 (ICD-503, CNSSI 1253, FedRAMP), NIST SP800-125a – reducing time for audits down from months to minutes.
- Enforce mission separation with logical (hardware based) attestation – minimize data center footprint without compromising security
- Military ready encryption to ensure workloads cannot be moved or stolen – protect from insider or external threats
- Forensic grade logs for accountability and insider oversight – prove what actions occurred
- Funded by In-Q-Tel with a number of government customers

What's needed to overcome these new potentially devastating security exposures is a framework that delivers three essential capabilities: military-grade security, continuous compliance, and complexity and cost reduction. A new technology solution gives security organizations a framework that provides these advantages: the Intelligent Workload Security framework. HyTrust is among the first companies to deliver this solution to today's organizations—so they can reinforce their security walls and thwart preventable breaches. In this way, governments, the military, and other organizations can safeguard their systems on the front lines, while gaining significant cost savings for their bottom line.

About HyTrust

HyTrust is the Cloud Security Automation company. Its virtual appliances provide the essential foundation for cloud control, visibility, data security, management and compliance. HyTrust mitigates the risk of catastrophic failure— especially in light of the concentration of risk that occurs within virtualization and cloud environments. Organizations can now confidently take full advantage of the cloud, and even broaden deployment to mission-critical applications. The company is backed by top tier investors VMware, Cisco, Intel, In-Q-Tel, Fortinet, AITV, Granite Ventures, Trident Capital, Epic Ventures and Vanedge Capital. Visit us at **www.hytrust.com**

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100

Appendix A

HyTrust, through its technology collaboration with Intel, has introduced new capabilities to secure the most important elements in virtualized datacenters and the cloud- applications and data—against the loss of control in cloud environments. This solution mitigates the risks that virtualization and the cloud create, simplifying regulatory compliance, preventing data theft or misuse, and ensuring availability of enterprise applications and data.

Built upon Intel®'s asset tagging and attestation services with root-of-trust supported by Intel Trusted Execution Technology, or Intel TXT, this solution leverages Intel's TXT to provide processor-level attestation of the hardware, BIOS and hypervisor. The combination of HyTrust's policy engine and Intel TXT can enable the government to set policies ensuring that sensitive applications and data workloads can only run on authenticated trusted hosts, physically located in specific trust zones, data centers, or geographic locations.

This solution can add three additional layers of protection:

1. Platform hardening: Intel TXT provides the capability for server attestation, allowing security teams to validate server configuration integrity and identify any unauthorized changes to the system.

2. Geo-fencing and location-based controls. Users can put policies in place to ensure that virtual workloads only run in specific geographies or locations. This is essential for compliance with existing and burgeoning privacy regulations.

3. Encryption/decryption. Virtual workloads remain encrypted and can only be decrypted when executed on a TXT-validated server.