Overview of Knight Point Cloud Security: CloudSeed® and Zeus

TABLE OF CONTENTS

INTRODUCTION TO HORIZON®

Since its founding in 2006, KPS has built a large set of performance capabilities with the general purpose of providing innovative information technology (IT) solutions in both public and private sectors. Based on the experiences gleaned in providing these services, KPS realized the potential benefits to our customers of offering any combination of services and products in any business model, giving the ability to truly have the technology they needed, when, where, and how they needed it. As such, KPS invested in the development and perfection of unifying the delivery of services and products through any combination of traditional, on-premises as-a-Service (aaS), off-premises aaS, and third-party aaS business models. This capability takes the respective services that KPS previously established as individual offerings and assembled them under a single service delivery "umbrella" called Horizon®.

Horizon® is a service delivery methodology and portfolio of service and product offerings that can be combined into single, unified solutions that make use of common tools, processes, methods, and support. The Horizon® methodology presents customers the ability to "check off" each of the individual capabilities necessary for a given solution and have them delivered consistently and successfully. This consistency and success is based on KPS' ability to leverage several key tenants of best-practice service delivery as well as two enabling technologies: CloudSeed® and Zeus.

THE CLOUDSEED® TECHNOLOGY

CloudSeed® is an open-source engineered solution for automated and scalable cloud infrastructure deployments – a "Cloud Creation Intelligence". CloudSeed® was created with the intent of eliminating the need for complex implementations of physical and virtual server and storage environments. Our patent pending design and technology simplifies all aspects of creating and managing a Cloud by abstracting the complex stacks that traditionally make up a cloud into the most basic components. By recognizing any underlying hardware to be used for a single purpose – network, compute, or storage – CloudSeed®-based clouds are able to make use of any hardware, from any vendor, at any time. Through this technology, customers are able to instantiate an entire cloud from scratch in under 20 minutes. All KPS clouds – private, community, public, or hybrid – make use of the CloudSeed®

technology and standard architecture (a sample private cloud architecture is shown in *Figure 1 - KPS Standard Architecture* below), which allows them all to re-use many of the same technical controls implemented in Knight Point's "CloudSeed" Federal Cloud. Through this standardization, KPS' cloud solutions give previously unparalleled flexibility, compatibility, and security in their cloud deployments.

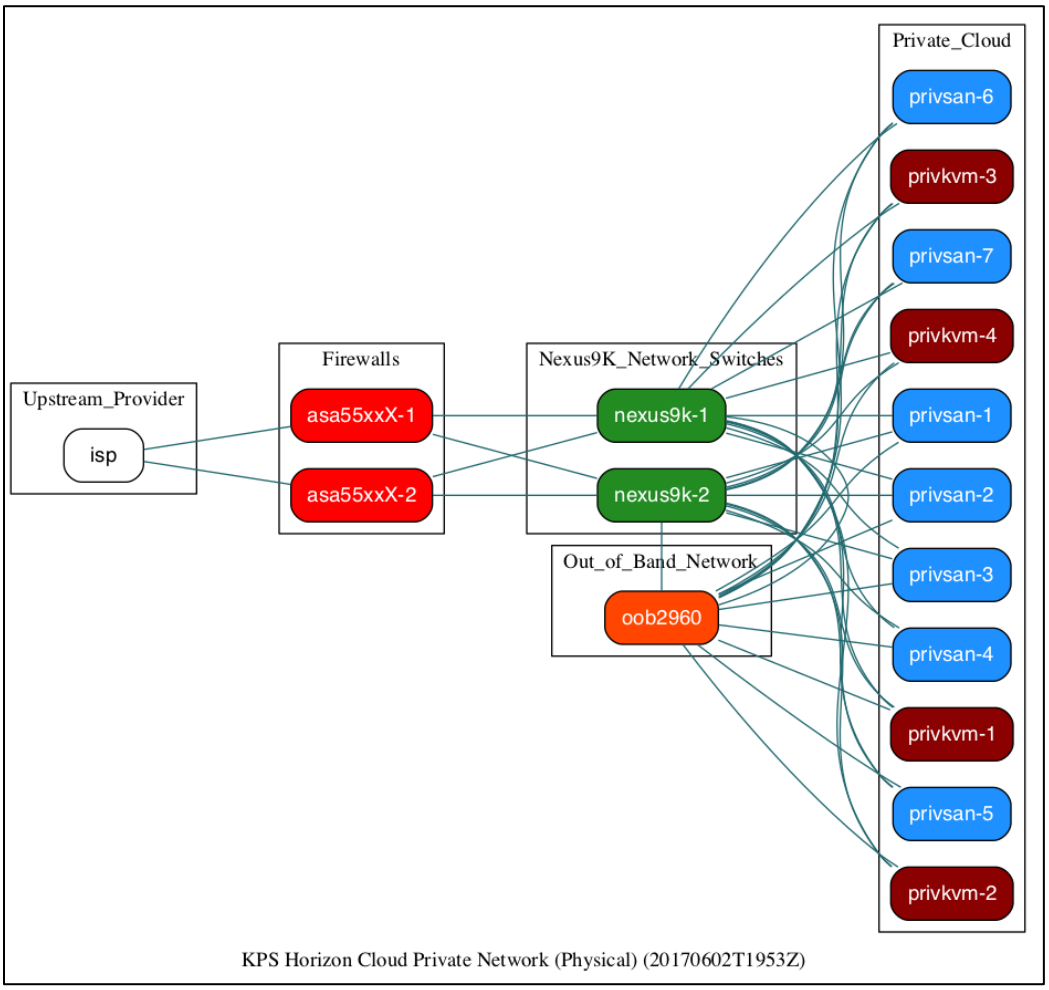


FIGURE 1 - KPS STANDARD ARCHITECTURE

THE ZEUS TECHNOLOGY

All infrastructure resources in KPS' cloud solutions are managed and monitored through the KPS tool, "Zeus", which gives customers the ability to view and manage cloud resources across the full range of possible KPS cloud deployments – Public, Federal Community, and Private - as well as across multiple CSPs (AWS, Azure, etc.) and on-premises virtualization technologies (ESXi, KVM, etc.). By providing customers a single pane of glass to both view and manage all of their infrastructure solutions, Zeus allows for true "hybrid" cloud solutions that can combine pre-existing customer solutions with new cloud-based solutions. Zeus gives customers a truly "holistic" view into their infrastructure, and allows them to move workloads across solutions as-needed to address specific business requirements.

THE SHARED RESPONSIBILITY SECURITY MODEL

Customers looking to secure an application in any cloud environment should always consider the boundaries of their system, and who has responsibility for securing those boundaries. As part of the Horizon® service methodology, KPS implements a shared responsibility model. This model enables the customer to leverage KPS' security operations and expertise for as much of the system's architecture as they would like, while retaining the responsibilities they need based on the sensitivity of the system and its data.

Securing a traditional application stack requires an application owner to review the people, processes, and tools that comprise the three "layers" of the application stack: the infrastructure the application resides on (both physically and virtually), the platform tools that enable the application to run properly, and the software or application itself. Securing an application stack in the cloud follows this same principle, however adds the additional need to consider the people, processes, and tools used by the Cloud Service Provider (CSP) to manage the cloud system. This is an extremely important aspect of securing an application in the cloud because the people, processes, and tools used to manage a cloud system are what ensure tenant environments remain isolated, cloud applications remain separated, and customer data remains private.

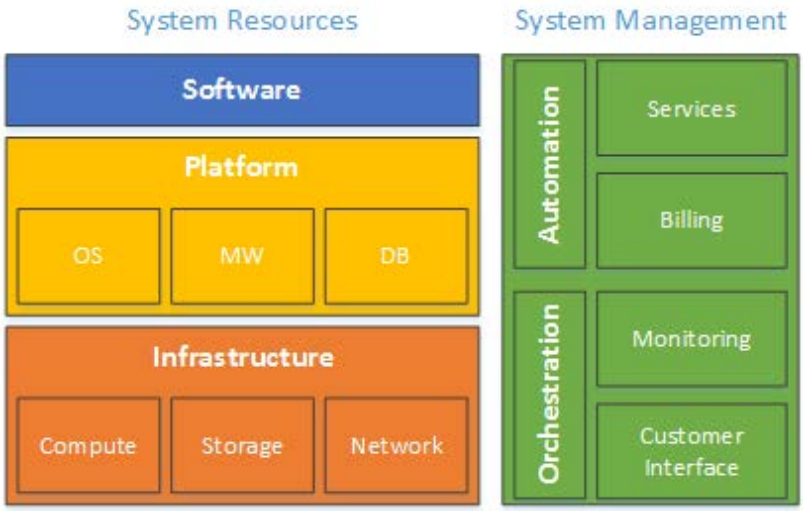


FIGURE 2 - KEY SECURITY CONSIDERATIONS IN THE CLOUD

To secure a system in the cloud, customers should ensure all of the components in *Figure 2 - Key Security Considerations in the Cloud* are secure. In accomplishing this, certain aspects are secured by the CSP per their policies and procedures, and certain aspects are secured by the customer per the customer's policies and procedures – hence the "Shared Responsibility" model. In the end, however, it is important to not confuse responsibility with accountability. Despite their being shared responsibility, at the end of the day, the system owner on the customer side is ultimately accountable for the business success of their application, and therefore the security of their application. Accordingly, the customer should very carefully review two items governing the security of their system. First, customers should review the people, processes, and tools used by the CSP to secure their portion of the stack. CSPs standardize their delivery across all customers and as a result, sometimes unique aspects of a customer's system that demand uncommon security elements can go unaddressed. Second, customers should take note of the SLAs and processes that govern the integration points between the area of customer responsibility and the area of CSP responsibility. These integration

points are critical to the long-term security of a system, and ensure that no aspects of the system "fall through the cracks".

KPS SECURITY RESPONSIBILITIES FOR OUT-OF-THE-BOX OFFERINGS

KPS' out-of-the-box offerings are designed to take advantage of the two KPS technologies (CloudSeed® and Zeus) while acting as stepping stones to more complex, holistic Horizon® solutions. These solutions offer a standard set of security controls that serve as a baseline to meet common security risk management frameworks and standards (such as FISMA, FedRAMP, ISO 27000, DoD SRG, etc…).

THE KPS INFRASTRUCTURE-AS-A-SERVICE (IAAS) CLOUDS

The first set of out-of-the-box offerings available to KPS customers focuses on taking advantage of the CloudSeed® technology to provide IaaS clouds in public, community, private, and hybrid deployment models across both on-premise and off-premise delivery methods. In the standard deployment of each of these services, the boundary of KPS responsibility is well defined as the infrastructure layer of the system and the associated system management capabilities. In addition to a well-defined boundary, KPS also offers standard performance and notification expectations (in the form of Service Level Agreements and Objectives) to help guide the integration of customer and KPS responsibilities.

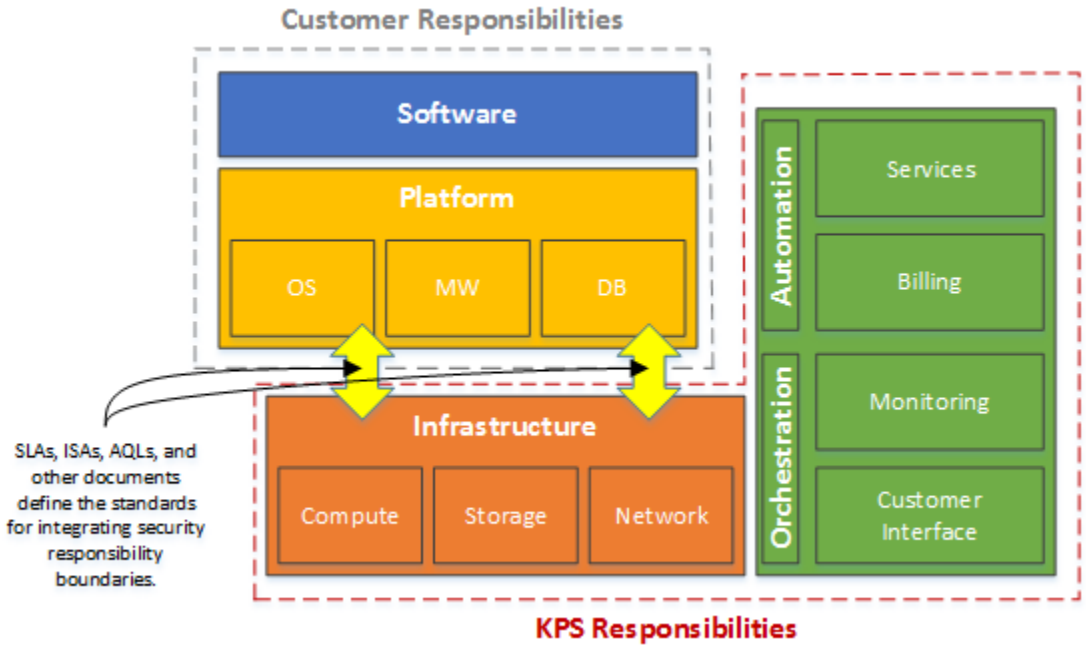


FIGURE 3 - KPS SECURITY RESPONSIBILITIES FOR THE KPS IAAS CLOUD SOLUTIONS

The security responsibility boundaries identified in *Figure 3 - KPS Security Responsibilities for the KPS IaaS Cloud Solutions* apply to each of the following standard offerings:

THE KPS "CLOUDSEED" FEDERAL CLOUD

The KPS Federal Community Cloud, titled after its namesake cloud intelligence technology CloudSeed®, is an off-premises IaaS solution that is FedRAMP Moderate Authorized and meets DoD PA SRG Level 5 controls while leveraging Cisco hardware, world-class Equinix facilities, and open-source technology to provide compute, storage, and network resources to Federal customers in a secure manner. Customers

can engage resources in an a la carte, and "pay for performance" model that enables them to understand the exact cost, system performance, and system capacity that defines their application environment.

THE KPS PUBLIC CLOUD

The KPS Public Cloud is an off-premises IaaS solution that is managed through the same technical and management security controls as the KPS "CloudSeed" Federal Cloud. As a result, the same benefits of the KPS "CloudSeed" Federal Cloud can be realized through the KPS Public Cloud. In fact, the only tangible difference between the KPS Public Cloud and the KPS "CloudSeed" Federal Cloud is compliance with the DoD SRG IL 5 security requirement for an exclusively Federal customer base. Unlike the KPS "CloudSeed" Federal Cloud, which is available only to Federal customers, the KPS Public Cloud is made available to any customer – Commercial or Federal.

KPS PRIVATE CLOUDS

While KPS Private Clouds can be on-premises or off-premises solutions that leverage varying levels of the technical and management security controls implemented in other IaaS solutions (See the *Customizing Security Boundaries and Responsibilities* section), the standard KPS private cloud is offered as a fully managed, off-premise (in KPS facilities) solution that leverages all the same technical and management controls as other KPS IaaS deployments.

ZEUS

Zeus is hosted within the KPS Public and Federal clouds and is provided in a software-as-a-service (SaaS) delivery model for use in private clouds. As a result of managing and being hosted within each of these cloud systems, Zeus is included within the security boundaries of those systems' audits and certifications. Through Zeus, customers are able to access, monitor, and manage cloud resources in on-premise and off-premise 3rd party clouds, traditional virtualized environments, and KPS clouds all through one central pane of glass. This capability is enabled through the use of secure API calls made to each respective environment and as a result, part of the instantiation of any KPS cloud solution includes the setup of accounts for Zeus to access whatever other environments a customer requires.

CUSTOMIZING SECURITY BOUNDARIES AND RESPONSIBILITIES

KPS security responsibilities can differ from solution to solution depending on the needs of the customer and their system. Despite the out-of-the-box solutions KPS provides having standardized security boundaries, our commitment to providing customers the Technology You Need, When You Need It® has led to an unparalleled flexibility in a customer's options for securing their systems. KPS' security responsibilities can be lessened, and taken on by the customer through additional service level documents, such as a Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA), or contractual assumptions that document which part of the service KPS is no longer responsible for providing. Additionally, a customer's responsibilities can be augmented or covered by KPS through an engagement of KPS as-a-Service managed services or T&M-based professional services (which also requires edited service level documents). As an example, *Figure 4 - KPS OS Managed Services* depicts the changes if a customer were to engage KPS for management of the Operating System (OS) their

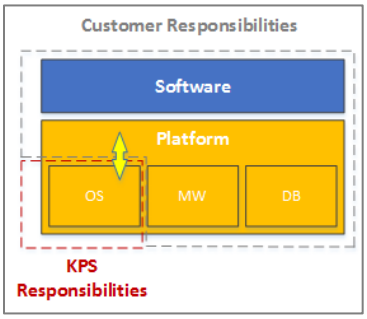
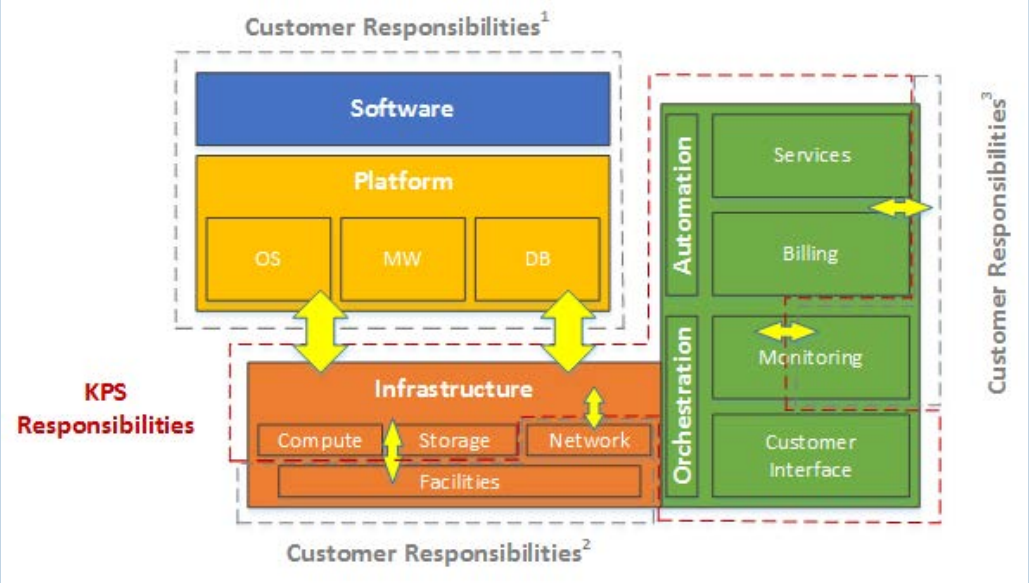


FIGURE 4 - KPS OS MANAGED SERVICES

application resides on. KPS would manage, patch, and maintain the OS per the change, patch, and configuration management policies and procedures used to perform those activities on the rest of the systems within the KPS security boundary.

Establishing an On-Premise Private Cloud

The most common customization of KPS' out-of-the-box offerings is for the creation of on-premise private clouds that customer administrators manage and operate. This common customization enables customers to take advantage of KPS' technology while utilizing their own facilities and management processes (e.g. Change Management) in operating the system. In this customization the boundaries of KPS and customer responsibilities change significantly.



Most notably, the customer takes on four distinct net-new responsibilities for this custom solution:

- The responsibility of providing secure facilities and conditioned power to the cloud system (2)
- The responsibility for ensuring network connectivity from an upstream ISP (2)
- The responsibility to utilize the standard set of KPS back-end network, security, and virtualization tools, called the Horizon® Cloud Management Suite (HCMS), to monitor the system's security (3)
- The responsibility to accept patches from KPS for all backend cloud management systems (3)

Since each of these responsibilities has the potential to affect the ultimate SLAs provided to the customer (1), several contractual assumptions are added to ensure clear customer expectations:

- System availability is dependent on the availability of power provided by the customer
- Network availability and performance is dependent on the network provided by the customer and their upstream ISP
- System security and uptime SLAs are dependent on the customer meeting the same 24/7 monitoring standards as the standard KPS offering
- System uptime and security is dependent on the customer's acceptance of hot patches and system upgrades pushed by KPS

This solution is in use by both Federal and Commercial customers to provide IaaS cloud services to both internal and external customers. Most commonly, this model is leveraged by customers who have cyclical system performance requirements, or who want to avoid capital IT expenses and leverage existing IT staff when going through equipment refreshes or standing up new and/or temporary sites/locations.

SECURITY COMPLIANCE, ACCREDITATIONS, AND CERTIFICATIONS

KPS operates all solutions per industry best practices and the most stringent Federal and Commercial security standards. As evidence of these best practices, KPS cloud solutions hold accreditation and are compliant with several well-known standards.

KPS leverages Equinix facilities for off-premise solutions. These facilities meet the following compliance standards:

- SOC 1 Type 2
- SOC 2 Type 2

KPS IaaS cloud offerings are available at varying compliance levels with prominent Federal Risk Management Framework (RMF) standards:

Federal Security Standard	**KPS "CloudSeed" Federal Cloud** (Including Zeus)	**KPS Public Cloud** (Including Zeus)	**KPS Private Clouds**
FISMA	Compliant	Compliant	Customer Dependency*
FedRAMP Moderate	Compliant and Authorized	Compliant	Customer Dependency*
FedRAMP High	Non-Compliant	Non-Compliant	Customer Dependency*
DOD SRG IL 2	Compliant (Undergoing Authorization)	Compliant	Customer Dependency*
DOD SRG IL 4	Compliant (Undergoing Authorization)	Non-Compliant	Customer Dependency*
DOD SRG IL 5	Compliant (Undergoing Authorization)	Non-Compliant	Customer Dependency*
DOD SRG IL 6	Non-Compliant	Non-Compliant	Customer Dependency*
CJIS	Customer Dependency*	Non-Compliant	Customer Dependency*

**While technically able to be compliant with the highest levels of security, the customer's use of these solutions depend heavily on their respective management practices, resulting in significant customer dependence for compliance with Federal standards.*

TABLE 1 - KPS IAAS CLOUD COMPLIANCE MATRIX

Additionally, the policies and procedures that govern the management and operations of KPS cloud solutions are compliant (and accredited where possible) with several Industry best-practice standards:

- ISO 27000
- ISO 20000
- ITIL v3
- CMMI Level 3

STANDARD KPS SECURITY CONTROLS

The following sections provide additional information on the standard security controls in place to secure KPS' out-of-the-box offerings. In many cases these controls can be leveraged by customers in creating custom solutions that meet the exact needs of (e.g. leveraging colocation and managed services to take advantage of KPS' secure facilities and operational management best practices for a traditional, customer-owned environment).

PHYSICAL AND ENVIRONMENTAL SECURITY

All of the KPS off-premise cloud solutions reside in world-class, state-of-the-art, and highly secure data centers. These facilities are divided in to five concentric layers or levels of security: Exterior Access, Mantrap, Common Areas, Colo Access, and Customer Cages. Biometric scanners and proximity card scanners are utilized throughout the facility for access between each level and KPS is solely responsible for updating and maintaining the list of personnel with authorized access.

FIRE DETECTION AND SUPPRESSION

KPS' facilities utilize both fire detection and suppression systems. The facilities employs a multi-zone dry-pipe sprinkler with nitrogen purge system and Very Early Smoke Detection Apparatus (VESDA), system that conduct air sampling to provide the earliest possible warning and mitigation of impending fire hazards. Sprinkler systems are implemented with double interlock pre-action and detection systems. Water is not in the system during normal operations. Pre-action detection with intelligent heat detectors will cause audio/visual alarms to be activated and signals are sent to the valves in the affected zones. Water is then triggered to enter that zone. Fire extinguishers are provided throughout the system. The extinguishers are dry chemical or clean agent extinguishers. The suppression systems are monitored 24x7 by an external alarm monitoring company that automatically dispatches fire and rescue personnel to the facility.

POWER

All network and power transmission lines and communication lines for the data centers that directly enter the facility run through wire management structures and conduits to prevent accidental damage, eavesdropping and disruption. The data center facilities employ N+1 Block Redundant power configuration. There are multiple diesel fuel generators used to power the facility in the event of an outage. Standby power is also in an N+1 configuration, and UPS systems (which automatically engage and transfer facility load in the event of primary power source loss) are in double N+1 configuration.

CLIMATE AND TEMPERATURE

The Building Management System (BMS) is in place at all facilities. The BMS is a control, monitoring and reporting system used to monitor and control environmental systems and alert staff to any potential issues. The facility environmental systems are monitored and managed by these facility engineers who can be reached on a 24 hour basis. The BMS system monitors and controls the heating, ventilation and air-conditioning (HVAC) system. It controls and monitors space temperature and humidity within the facilities, space pressurization, HVAC equipment status and performance, and outside air conditions. The system is also used to monitor ambient temperature of the power rooms and cabinets in order to verify proper environmental conditions.

CLOUD ARCHITECTURE AND OPERATIONS

KPS employs a highly redundant architecture that leverages Cisco's ACI Fabric, Firewall clustering technologies, and security contexts to ensure complete network separation between tenants of the cloud systems. Additionally, KPS ensures each virtual interface representing each customer's VLAN has both ingress and egress access-lists assigned to the interface. If traffic is not explicitly allowed by the access list, it is dropped by default.

NETWORK SECURITY

Making use of high-end Cisco networking equipment and technologies, KPS has ensured the network infrastructure supporting each cloud systems is logically and physically separated into differing segments, dependent upon purpose and function.

FIREWALLS AND THE ACI FABRIC

Cluster communication between the ASA Firewalls traverses the Cisco Nexus 9K "ACI" Fabric. All customer production layer 3 interfaces exist on the Cisco ASA Firewalls. By default all routing is done on the firewalls in order to provide a stateful firewall between the tenants as well as between the tenants and the internet. If two customers wish to have a line-rate, unfiltered link between them, a memorandum of understanding must be signed and router interfaces can be created on the Nexus 9K "ACI" fabric.

SECURITY CONTEXTS AND INFORMATION FLOW

KPS IaaS Cloud offerings have information flow control policies that require the segregation of information flows within the system and between external interconnected systems. Each segment is segregated within its own context. There are two "levels" of separation; the separation that occurs from the inside network to the outside networks (on the firewalls) as well as the separation that occurs inside each firewall security context.

On the firewall itself, all "outside" traffic to the internet is processed by a dedicated security context, which handles all routing protocols and acts as the first layer of defense for the outside network. For the cloud tenant environments themselves, dedicated security contexts are used. IDS/IPS (Sourcefire) monitors all traffic and ASA access lists are applied to ALL interfaces on ALL contexts for both inbound and outbound traffic.

SECURE CONNECTIONS

KPS is able to support a number of connection-types to VMs within customer tenants. Knight Point acts as the ISP for any tenants of the Federal and Public cloud systems, providing the full range of typical ISP services including Public IP allocation for both IPv4 and IPv6 addresses. KPS cloud systems also enable LAN to LAN IPSEC tunnels, as well as physical direct connections

EVENT AND INCIDENT MANAGEMENT

KPS monitors events and protects systems against incidents across customer cloud solutions. An event becomes an incident when there is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents KPS protects against include:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

- Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

In protecting customer cloud environments, KPS carefully reviews and audits the following service elements:

- Threat Management & Event Correlation
- Centralized Log Management
- Compliance Reporting
- Network Behavior and Anomaly Detection
- Removable Media Device Detection
- User Tracking
- File Integrity Monitoring
- Quarterly Security Review

If an incident is detected that has the potential to affect a customer, KPS security personnel will first notify the designated POC for each customer. The customer POC then has the responsibility to disseminate information throughout the appropriate internal notification and escalation chains. If incidents occur at significant scale, KPS will notify the appropriate industry and/or Federal governing security bodies.

Standard reporting targets follow USCERT guidance where possible, but in all other cases (or where defined by a customer) KPS can customize notification timelines – particularly for private cloud and hybrid cloud solutions. *Table 2 - Sample Incident Category Notification Timelines* below shows a sample "custom" incident category notification timeline:

Incident Category	Description	Potential Impact	Notification Time Requirement
1	Root Level Intrusion	Moderate	2 Hours
2	User Level Intrusion	Moderate	2 Hours
3	Unsuccessful Activity Attempt	N/A	4 Hours
4	Denial of Service	Mod/High	15 Minutes
5	Non-Compliance Activity	N/A	4 Hours
6	Reconnaissance	N/A	4 Hours
7	Malicious Logic	Moderate	2 Hours

TABLE 2 - SAMPLE INCIDENT CATEGORY NOTIFICATION TIMELINES

REDUNDANCY

KPS Cloud solutions leverage significant redundancy for maximum availability of customer systems and data. In addition to inherent redundancy built into each cloud system, KPS public and Federal clouds leverage sites on both the U.S. East Coast and U.S. West Coast that allow customers to design their

cloud systems with geographic redundancy. These systems can be setup in hot-cold, hot-warm, and hot-hot configurations, giving customers DR flexibility without paying for the maintenance of a fully-redundant data center.

NETWORK REDUNDANCY

The physical layout of KPS Cloud solutions is fully double-redundant by design and is comprised of a spine and leaf topology. In this topology, the spine, or core switches have redundant connectivity: outwards connecting to both firewalls as well as inward connecting each of the individual rack specific leaf switches. Within each rack, the leaf or access switches have redundant connectivity: upward connecting each spine switch as well as inbound network connections from each server within the environment.

STORAGE REDUNDANCY

All KPS IaaS Cloud offerings utilize the Ceph storage solution, specifically Ceph clusters, which provide Copy-on-Write "crash-consistent" copies of data on the disk and replicate data across all nodes within the cluster, resulting in minimally triple-redundant storage. The minimal redundancy is customizable only in private cloud environments.

COMPUTE REDUNDANCY

KPS IaaS Cloud offerings redundancy for all compute resources by ensuring N+1 redundancy for all compute nodes within each cloud system. Additionally KPS cloud solutions utilize virtual CPUs through the hypervisor. Through virtualization of the CPU, KPS cloud solutions implement inherent redundancy of vCPU resources that can be modified per customer requirements for private cloud solutions.

OPERATING SYSTEMS

KPS makes available a standardized set of Operating System images for all Federal, Public, and Private cloud offerings via the KPS CloudSeed® Marketplace. Images are periodically updated and posted to the marketplace and are available for import, including highly secured images. Additionally, KPS offers licensing for the various Operating Systems offered through the marketplace.

GUEST OPERATING SYSTEMS

KPS security responsibilities exclude all customer hosted VMs. Customers are able to create VMs running their choice of x86-based operating system. Several standard OS images and licenses are provided as standard options within the KPS marketplace, including STIGed and vanilla versions of:

- Windows Server 2008 R2, 2012 R2, and 2016
- Red Hat Enterprise Linux 6 and 7
- CentOS 6 and 7

With regards to the Windows 2016 image, DISA has not released a Secure Hardened Baseline (SHB) for Windows Server 2016, and therefore no STIGed image is available for this yet. Additionally applications such as MS SQL Server (various versions including Standard and Web) are available inside any Windows image that is selected.

HOST OPERATING SYSTEMS

All utility servers used to manage the cloud infrastructure itself are hosted on individual VMs based upon a KVM Linux hypervisor hosting either a CentOS or RHEL VM. CentOS is a Linux distribution that provides a free enterprise class community supported operating platform compatible with Red Hat

Enterprise Linux while remaining completely autonomous. CentOS is the default host operating system used in all utility VMs, with RHEL being used for all utility VMs that require FIPS validated encryption, such as the Federal Zeus Portal and Federal SAML server. The hypervisor hosts themselves which are used to run the KVM Virtual Machines run the KPS CloudSeed® Operating System – a highly customized Linux distribution developed specifically to support the CloudSeed® technology by KPS cloud engineers.

SYSTEM ACCESS SECURITY

KPS Clouds are designed to enforce individual accountability for all users in the environment. Strong authentication is managed through the use of 2-factor authentication. All access is logged and audited, and all logs are reviewed on an ongoing basis.

INTERNAL ACCESS TO MANAGEMENT SYSTEMS

For any cloud operating under a fully-managed model, KPS cloud administrators have direct access to manage all infrastructure components, while customers have a user-friendly interface via the Zeus Portal to allow for optimized segregation of roles and responsibilities.

CREDENTIALS

KPS IaaS Cloud Offerings employ 2-factor authentication in all possible locations, leveraging the KPS Certificate Authority. KPS complies with the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (v1.2.3). All issued certificates (by either the Root CA or the Intermediate CA) are logged to a Fossil repository. Fossil repositories are cryptographic hash-based storage of data. A CRL is issued every 7 days (with a 2 week validity window) by the Root CA's designated CRL issuer and a CRL is issued every 1 day (with a 36 hour validity window) by the Intermediate CA.

PERSONNEL

KPS performs security and suitability investigations on personnel prior to hire. This includes defining the sensitivity and risk level designation of personnel as needed and providing mechanisms to hold internal users of cloud systems responsible for their actions. Specifically, KPS performs criminal background and credit checks prior to hiring any candidate. Candidates must attend security orientation, sign appropriate Rules of Behavior documentation, and meet with the Facility Security Officer prior to starting work. No access is granted to KPS systems until candidates have met all security requirements, attended all security trainings, and signed and acknowledged all necessary agreements.

ZEUS

Zeus is a role and permission web based application that serves as both the dashboard for administering KPS cloud solutions, as well as the management portal for engaging the full spectrum of Horizon® services. A user's role and privileges are determined by the responsibilities for the position to which they've been assigned. Zeus users are divided into three (3) different group types; Customer, (parent to customer dept); Customer Department, (parent to tenant) and Tenants. A Customer can have multiple Customer Departments and a Customer Department can have multiple Tenants. If a user has a role in Customer, it applies to the Customer Departments and Tenants that are children to the Customer. This also applies to Customer Departments for their children Tenants.

CUSTOMER CREDENTIALS

KPS employs two means for customer access to Zeus depending on whether customers are access the Federal or Public clouds. With regards to private clouds, Federal customers will utilize the Federal Zeus method, and Commercial customers utilize the Public cloud method.

Access to Zeus in the KPS Public Cloud utilizes standard username/password authentication, with the potential to add more controls as needed by each customer. Conversely, access to Zeus in the KPS "CloudSeed" Federal Cloud is standardized and utilizes two-factor authentication. Specifically, it leverages FIPS 201-approved products for Personal Identity Verification (PIV) capabilities. Zeus uses TLS Client Certificates to require all incoming connections into the Federal cloud to present a certificate issued by one of the trusted certificate authorities. Users who do not provide a certificate are not be able to login. Additionally, once a certificate is provided, users need to provide a corresponding username / CAC / PIV / Smart-card. If a username is then chosen, standard password authentication is used. KPS implements the following restrictions for password-based authentication in the Federal Cloud:

- A minimum password complexity of:
  - Case sensitive
  - Minimum of fifteen (15) characters
  - At least one each of upper-case letters, lower-case letters, numbers, and special characters
- Minimum number of changed characters when new passwords are created of: one (1)
- Storing and transmitting only cryptographically-protected passwords by following strict access control guidelines
- Password minimum and maximum lifetime restrictions of:
  - One (1) day minimum
  - Sixty (60) day maximum
- Prohibiting password reuse for multiple generations
- Allowing the use of a temporary password for system logons with an immediate change to a permanent password

3RD PARTY ZEUS ACCOUNTS

Zeus leverages API access to manage and monitor 3rd party clouds such as AWS, Azure, etc. As such, Zeus requires account access to these 3rd party accounts. Customers have two methods to accomplish this. First, if a customer creates an account through the Zeus interface, Zeus will leverage that account information transparently to perform all 3rd party cloud tasks. This method enables customers to leverage the full functionality of Zeus. If, however, an account is created through the 3rd party cloud interface (as opposed to the Zeus interface), your account info will need to be manually entered into the Zeus back end. In this case, customers are able to provide Zeus with its own account, a root account, or any other account so long as it has a level of access commensurate with the level of functionality Zeus is intended to be leveraged for.

CHANGE AND RELEASE MANAGEMENT

KPS leverages a robust Change Management (CM) policy that focuses on improving all aspects of service delivery by reducing the potential for service-impacting issues caused by changes made to the systems that support a customer's service. KPS CM policies apply to all aspects of the cloud system, including: the infrastructure, the platform (Operating Systems, Middleware, Database software), the application, and any other processes or procedures surrounding the system's support and operation.

For the KPS Federal, Public, and any fully-managed private IaaS cloud, *Figure 5 - IaaS CM Responsibilities* below shows the division of CM responsibilities between KPS and its customer.

Customer CM Responsibility: the customer retains CM responsibility for all platform and software layer Configuration Items.

CSP CM Responsibility: The CSP retains CM responsibility for the physical equipment the system resides on, the hypervisor that support the virtual environments, and any orchestration and automation tools used to support the environment.

CSP CM Automation: monitoring and notification of resource levels as well as automated ordering of additional physical capacity per the guidelines (typically in a capacity management plan) set by the CSP.

Integration Point Challenges: IaaS deployments are faced with the challenge of overcoming confusion on who has CM responsibility for "virtual infrastructure" aspects of the environment, for example:

- Virtual resource assignment
- System-specific network configurations
- Virtual firewall settings

The goal of IaaS offerings is to enable the customer to have responsibility for all of these, but for complex systems, support from the CSP is often needed.

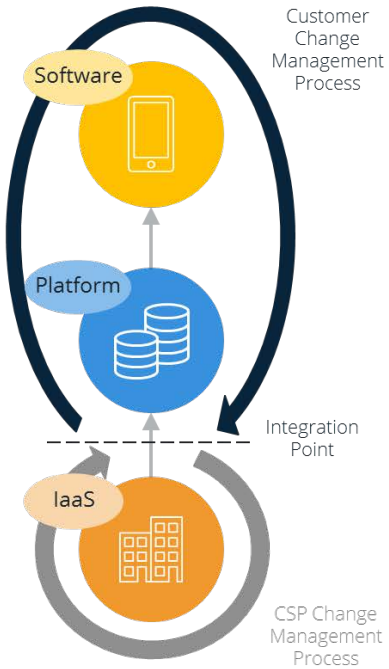


FIGURE 5 - IAAS CM RESPONSIBILITIES

KPS PRODUCTS AND SOFTWARE

KPS cloud systems use a combination of COTS, FOSS, and internally developed software. All COTS and FOSS applications have development integrity checks in place as part of the COTS application development. Functional and security testing is performed to ensure that any modification does not adversely impact the security controls and mechanisms. For software developed internally for use within KPS cloud solutions (including Zeus). All security requirements for integrity checks, input validation, etc. are followed by the respective development team. These security requirements are documented and tested as part of each release cycle.

KPS CLOUD INFRASTRUCTURE

KPS maintains a standard configuration baseline image for its cloud systems. The baseline image is stored and maintained on the PXE environment. Only the Cloud Administrator has access to the baseline configuration. The current baseline is tracked through the use of KPS' Service Desk tool and updated as needed. The baseline configuration is reviewed at least annually or in the event of a significant change. All changes to the baseline configuration are requested and approved in accordance with KPS' ISO 20000 / ITSM best practice procedures.

THE HORIZON CLOUD MANAGEMENT SUITE (HCMS)

In addition to the CloudSeed® cloud-creation intelligence, KPS clouds make use of the same cloud management technologies, collectively called the Horizon Cloud Management Suite (HCMS). This suite

of tools includes open-source and best-of-breed monitoring, scanning, management, and administrative tools that (in tandem with CloudSeed®) ease the management burden of a customer's cloud solution. In any KPS-managed deployments, our team accesses and utilizes these tools (leveraging the same access controls and "administrative security context" setup as our Federal cloud) to operate customer cloud solutions. In non-managed deployments, KPS aids in configuring and standing up all tools, then provides access to these tools to the customer administrators for continued operations.

HYPERVISOR

In order to abstract guest operating systems from the physical hardware each KPS cloud offering uses a blend of virtualization technology consisting of Kernel Virtual Machines (KVM) and VMWare's ESXi. KPS utilizes the KPS CloudSeed® Operating System for KVM compute hosts.

SECURITY MONITORING AND SCANNING

KPS IaaS cloud offerings utilize a selection of well-known security scanning tools to meet a full array of security compliance standards and requirements for scanning and continuous monitoring.

- Nessus is used for system-wide discovery scans, vulnerability scans, and data base scans
- Burp Suite Pro is used for web application scans
- OpenSCAP is used to configuration scanning and validation of STIG implementations

NETWORK MONITORING

KPS IaaS cloud offerings utilize Nagios to manage infrastructure, proactively monitoring all utility servers and hosts required to provide the IaaS service to our clients. Nagios keeps watch on all critical components of the IaaS offering and acts as an early warning system, notifying KPS in the event of a systemic failure. In addition, logs from firewalls, IDP, IPS and OpenNebula Server feed into a syslog server for centralized logging. Alerts and log data feed into an OSSIM that is monitored 24/7 for correlation and analysis.