

NaviSite®

DATA SHEET

NAVISITE MANAGED CLOUD SERVICES: Multi-Prong Cloud Security



Benefits

- Network Intrusion Detection & Prevention
- SAS 70 Type II Data Centers for Physical and Logical Controls
- Third-Party Penetration Testing
- Log Aggregation and Correlation
- Tripwire for File Integrity Services
- Automated Vulnerability Scans
- Anti-Virus Systems

NaviCloud is a highly secure enterprise-class cloud platform for NaviSite's portfolio of cloud services including Managed Cloud Services (MCS), Managed Application Services (MAS) and Managed Messaging Services (MMS). The Platform provides a robust, virtualized infrastructure deployed as multiple, secure infrastructure clouds hosted in NaviSite's SAS 70 Type II compliant data centers.

The NaviCloud Platform includes the basic building blocks of a system infrastructure service – virtualized servers; Windows and Linux operating systems; robust storage; state-of-the-art networking; best-of-breed firewalls; and content-aware load balancers. Load balancing options include low-cost shared solutions to support smaller environments, and multiple virtual load balancers – deployed and managed from within the cloud portal – to support more complex environments.

NaviCloud is built on state-of-the-art enterprise-class infrastructure. Cisco's Unified Computing System (UCS), a next-generation server platform, is configured with dual-fabric interconnects for high-availability, while VMware's vSphere 4 provides a flexible cloud operating system. NaviCloud-enabled data centers are interconnected by dedicated 1 Gbps Ethernet links, minimizing network-oriented bottlenecks. High-speed connections to physical servers hosted in NaviSite data centers, coupled with load balancing technology, ensure that complex applications scale to meet business demands. High availability components are used for all hosted workloads and disaster recovery can be provided for mission-critical services

A HIGHLY SECURE CLOUD PLATFORM

The NaviCloud Platform features a comprehensive approach to security that addresses physical, infrastructure, network, identity, data, and compliance requirements (Figure 1).

Compliance

Compliance is at the heart of the NaviCloud Platform. All NaviSite cloud-enabled data centers are SAS 70 Type II compliant, and undergo rigorous voluntary reviews of policies, practices and security measures.

SAS 70 Type II Certification is an internationally recognized auditing standard of the American Institute of Certified Public Accountants and is further assurance that NaviSite follows stringent controls and safeguards.



Physical Security and Environmental Safeguards

NaviSite monitors its data centers from two global network operations centers. Physical access to data center facilities is restricted. Entering the the data center requires mandatory visitor registration, visitor escorts, employee badge access, and biometric palm scanner authentication.

NaviSite has also installed sophisticated monitoring devices in each facility: early-warning fire detection systems; smoke and high temperature detectors; and 24 x 7 digital video surveillance cameras. Full data-grade HVAC systems are set up to regulate air temperature and humidity – maximizing the performance of your equipment. In addition, state-of-the-art fire suppression systems are installed for additional protection. In addition, multiple points of entry, control systems, backup generators, diverse power routes and n+1 redundancy serve as support measures for optimizing performance and ensuring business continuity. Maintenance is performed by authorized vendors on a pre-defined schedule – at least once a year – for wide range of environmental safeguards.

ENVIRONMENTAL SAFEGUARDS	NAVISITE DATA CENTERS
Fire Dection and Prevention System	Yes
Sprinkler System	Yes
UPS Units	Yes
Backup Generator	Yes
Fire Extinguishers	Yes
Temperature Monitoring Devices	Yes
Dedicated Air Conditioning	Yes
Raised Floor	Yes

Network and Infrastructure Security

In addition to the physical security measures outlined above, NaviSite's logical security measures extend through network, operating system (OS), and database access layers of technology. Customers and NaviSite employees must log into systems through approved secure connectivity options. NaviSite's logical security measures include the following:

- **Internal and Customer Systems:** Authentication and password technology implemented on the network to prevent unauthorized access
- **Remote Access Tools:** NaviSite hosted systems use encryption when transiting shared network segments
- **VPN Access:** Customer systems configured to limit customer access to their own systems based on network and authentication parameters
- **Inspection Firewall:** Defaults to blocking all packets in order to filter unauthorized inbound network traffic from the Internet
- **Distinct Networks and Firewall Configurations:** To separate customer network traffic from NaviSite employee network traffic
- **Database Configurations:** To prevent unauthorized viewing or modification of customer data by other customers in shared environments
- **Operating System Controls:** Database and network security configuration must adhere to the defined change management process
- **Key Documents:** Security policies, change management policies, and configuration standards are secured to prevent unauthorized changes to these documents

All customer traffic is carried on secure VLANs, and must pass through a firewall to access other cloud VLANs or physical networks. NaviSite's advanced firewall technology also provides intelligent threat defense with advanced capabilities, including identity-based access control.

Customers can choose from several firewall implementation models:

- **Shared Firewall:** A shared firewall ensures segregation of VLAN traffic terminating on the same physical segment
- **Virtualized Firewall:** Customers have their own individual security contexts (virtual firewalls) on an enterprise firewall appliance. Security contexts are isolated from each other, ensuring that customers see only their own, secure firewall instance
- **Dedicated Firewall:** Customers have a pair of dedicated firewall appliances

Network Intrusion Detection Systems (IDS) are also in place to detect malicious activity. NaviSite's IDS detects malicious activity, such as:

- Denial of service attacks
- Unauthorized access attempts
- Pre-attack reconnaissance

The IDS system consists of sensors or modules that provide automated detection and response to threats. These modules are installed at strategic locations throughout the network and include:

- **Network Sensor:** Monitors network traffic in real time for signs of malicious intent and responds automatically

Data Security

- **File Integrity:** NaviSite uses TripWire's file integrity services to assess integrity throughout the entire NaviSite Cloud Platform. File integrity services monitor both file and configuration integrity – looking at raw file contents, permissions, registry settings, and security settings. Using a baseline for comparison, the file integrity service detect changes that could potentially introduce vulnerabilities.
- **Threat Assessment:** NaviSite employs short- and broad-range automated vulnerability assessments. Short-range assessments are deployed on a monthly basis and include a minimum of five hosts. These vulnerability assessments also include port scans. IP addresses are scanned for all ports that are open to that system. All of the identified ports are then checked for known vulnerabilities. Broad range assessments are deployed on a quarterly basis for a minimum of 20 hosts. NaviSite also offers third-party penetration testing for customers who request the service. Third-party penetration testing involves simulating an attack to identify security – technology, process, and procedural – weaknesses.
- **Data Backup and Protection:** NaviSite employs secure data backup and protection procedures, policies, and technologies. NaviSite can store client data in an encrypted format either onsite or in a remote data center. For those requiring longer retention periods, data can be written to tape and stored in a secure offsite location.

Identity and Access

Security also extends to management. Role-based access control ensures that users have only the permissions required for their business or support roles. Permissions can also be set on objects or groups managed by NaviSite. All activity is logged for auditing purposes. NaviSite's real-time security management employs sophisticated log aggregation and event correlation, which facilitates quick and efficient identification – and resolution – of potential security threats.

PCI DSS Compliance

NaviSite data centers adhere to the Payment Card Industry Data Security Standard (PCI DSS) objectives established by the PCI Security Standards Council. PCI DSS compliance ensures that the requisite security controls are in place to protect credit card information and prevent fraud and abuse.

In March 2010, the Cloud Security Alliance published its “Top Threats to Cloud Computing V1.0,” which identified seven types of threats:

TOP THREATS	REMEDATION
Abuse and Nefarious Use of Cloud Computing	All customers are subject to a formal sales process prior to provisioning on the cloud allowing for greater control over the identities of users
Insecure Interface and API	Access to the management console can be protected with strong authentication (Two Factor). No customer API access is currently allowed.
Malicious Insiders	All NaviSite employees are subject to background checks prior to employment. All activities executed through the management interface are recorded.
Shared Technology Issues	The hypervisor is configured in accordance with VMware and industry best practices for hardening.
Data Loss or Leakage	VMs are securely deleted from the underlying disk when removed via the web interface. Additional technologies such as SSL, PKI, can be added to individual VMs.
Account or Service Hijacking	Strong authentication is available for the cloud management interface and recommendations are made for customers to use dedicated accounts for each end-user.
Unknown Risk Profile	NaviSite will provide customers with access to third-party audit reports attesting to adherence to security controls for the cloud and physical hosting platforms.

Source: PCI Security Standards Council

ABOUT NAVISITE MANAGED CLOUD SERVICES (MCS)

NaviSite’s Managed Cloud Services enable on-demand scalable provisioning of IT services including applications, servers, storage, and networks. The NaviCloud Platform offers unique enterprise IT advantages that tap into the core of NaviSite’s application and enterprise infrastructure management expertise.

Designed specifically to meet enterprise IT demands, the NaviCloud Platform delivers services on best-of-breed technology infrastructure from leading vendors including Cisco Systems™ and VMware™ - all provided under one of the industry’s strongest SLAs.

Whether supporting seasonal computing demand spikes, creating robust and cost-effective software testing and development environments, or building full application lifecycle management for mission critical enterprise applications, the NaviCloud Platform offers today’s premiere cost-effective enterprise-class infrastructure option.

To contact a NaviSite MCS security expert, please visit us at <http://www.navisitemcs.com> or call 877-485-9251.

NaviSite®

400 Minuteman Rd
Andover, MA 01810

www.navisite.com
877-485-9251

Copyright 2010 NaviSite
Part #MCS-DS-10-002