Dimension Data Cloud Technical security overview

Dimension Data's **Managed Cloud** provides a **secure and scalable cloud platform** with a **network-centric design** and **multiple layers of security** for the delivery of **Infrastructure-as-a-Service** (IaaS).

We offer multiple cloud deployment models with different levels of resource segregation – from a shared-service cloud with virtual segregation of compute and storage, to a fully dedicated private cloud service that can be deployed on your premises or from your data centre.

Using our network-centric model and a defence-in-depth security architecture approach, Dimension Data's Managed Cloud Platform allow clients to create dedicated layer 2 networks, and control communication into and out of these networks. Virtual server resources can be quickly brought online and taken offline, allowing for elasticity in resources.

Our cloud network capabilities enable the deployment of network domains as well as layer 2 virtual local area networks (VLANs) across data centres in different geographies. Clients can seamlessly extend their data centres to the Dimension Data cloud using their existing network and infrastructure topologies, while maintaining isolation and segregation across departments and groups within the organisation to maintain security standards.

Dimension Data provides a service level agreement (SLA) of 99.999% availability for its public and private cloud environments across all geographic regions.

This technical white paper is intended to answer questions regarding how security is maintained in our private cloud and multi-tenanted cloud environments. It also includes guidance on good security practices for clients using our Managed Cloud Platform.

'Dimension Data's **Managed Cloud is built from the network up** using dedicated physical networks and enterprise-grade security controls on best-of-breed hardware and software with full N+1 resiliency across the entire stack.'

Contents

Security overview

The Dimension Data Managed Cloud Platform provides a secure environment for clients to operate their information systems. It's built from the network up using dedicated physical networks and enterprise-grade security controls on best-of-breed hardware and software, with full N+1 resiliency across the entire stack.

At the core of our Managed Cloud is the Dimension Data CloudControl™ management system which is used to support the management, governance, and automation of each client's Dimension Data cloud environment. Clients perform all cloud management activities via the web user interface or application programming interface (API). The CloudControl orchestration and management systems strictly control the actions that can be taken by clients, ensuring that all management requests only affect the cloud systems managed by each client.

Permanent protection

Dimension Data performs 24/7 security monitoring and management of all CloudControl systems, which ensures that the security of all clients is maintained. The CloudControl systems are protected by multiple layers of security including intrusion prevention. Penetration tests are also performed against the CloudControl systems by external testing firms to ensure that there are no remotely exploitable vulnerabilities in the management systems.

Multi-tenant protection

In our multi-tenant environments, each cloud client is allocated its own networks and virtual servers. Clients are segmented from other clients through the use of enterprise-grade network segmentation. The Dimension Data CloudControl management system ensures that clients can't access networks and systems owned by other clients, and CloudControl presents no ability to bypass the management interface.

By enforcing multi-tenanting separation in the orchestration layer, clients are prevented from exploiting the underlying control systems, or making any configuration changes that could negatively affect other clients.

Within our fully dedicated private cloud environments that provide dedicated compute and storage resources, these secure multi-tenant capabilities are also provided. This enables our private cloud clients to securely segregate groups, divisions, or functional areas from each other.

Client security tools

Each client has the ability to fully manage all access to its networks, restricting or allowing all communication at the IP and port level. In addition, Dimension Data CloudControl allows clients to create multiple administrative user accounts, with each account granted granular control over cloud networks and virtual server systems. Using this capability, clients can enact common criteria role separation to ensure that no single administrator can change the configuration of virtual servers and virtual networks.

In order to manage the operating systems and applications of virtual servers, each client is provided with a secure, Internet Protocol Security (IPSec)-based VPN. This allows the client secure IP access to its cloud networks so that it can access their virtual servers without exposure to the Internet.

Dimension Data's Managed Cloud deployment options

Dimension Data Managed Cloud provides clients with a choice as to the degree of segregation required for cloud deployment. Often, clients choose multiple cloud deployment options in order to implement the best-fit model for each of their applications, and to support the full application lifecycle from development through to production.

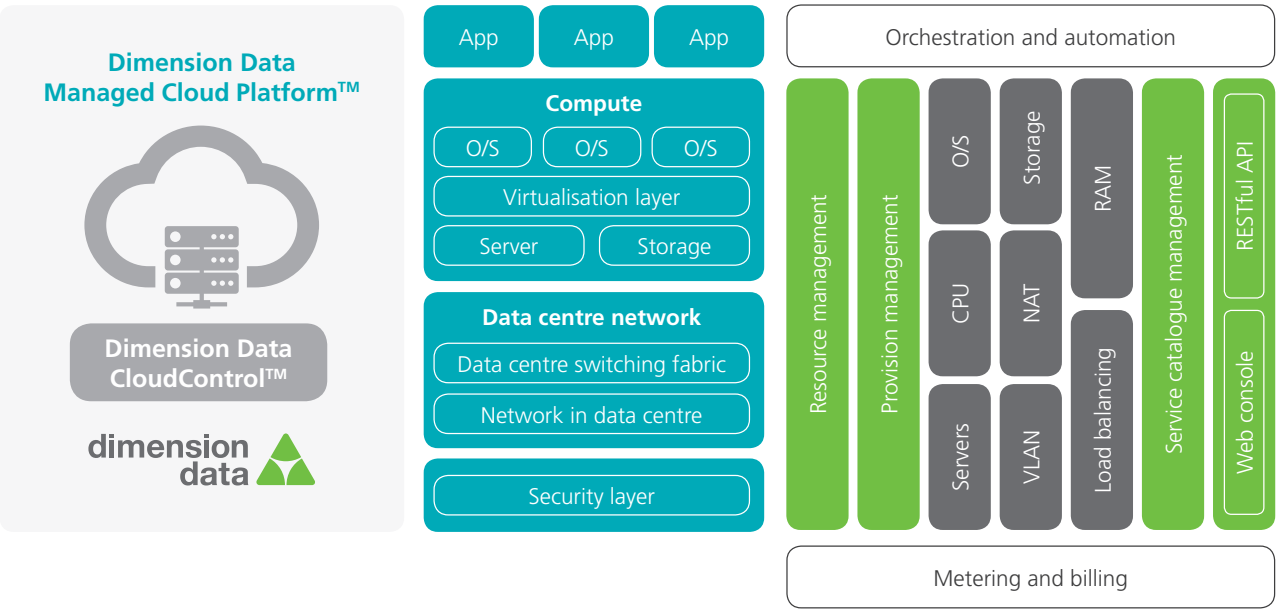
Dimension Data provides the following infrastructure-as-a-service offerings:

Private Cloud can be deployed at the client's premises or from one of Dimension Data's worldwide data centres. Our Private Cloud delivers hypervisor, storage, compute, and network physical isolation.

Hosted Private Cloud is deployed from one of Dimension Data's worldwide data centres. In these environments, the compute and storage infrastructure is dedicated to each client.

Dimension Data CloudControl™ – cloud management system

Orchestration, adminstration, billing, provisioning, management, support, federation



Public Cloud leverages a shared, multi-tenant compute, storage, and network infrastructure with separate, client-specific layer 2 networks and customisable firewalls.

Managed Hosting environments are physical and virtual infrastructures dedicated to each client, and hosted in a Dimension Data data centre.

All of Dimension Data's Managed Cloud offerings use the same underlying CloudControl management system.

With all of Dimension Data's cloud services, clients can create and deploy multiple, virtual data centres that are logically segregated. Each of these virtual data centres or network domains includes firewall and load balancing capabilities, and can be independently customised – based on specific needs.

When the private cloud solution is located on client premises, Dimension Data doesn't provide service level agreements for physical security, reliability of Internet services, power, or cooling.

Managed Cloud Platform security architecture

Resiliency

All systems within the Dimension Data Managed Cloud Platform are fully resilient, using an N+1 resiliency model. This resiliency is applied to the data centre physical power and cooling, all network equipment, all virtual server hosting systems, all storage systems, and all components of the CloudControl management environment.

Compliance and security standards

Dimension Data clouds hold certifications for:

- International Organization for Standardization (ISO) 27001 for information security management systems and processes
- ISO 27018 a global standard for privacy and data protection in the cloud
- Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) – an industry programme for security assurance in the cloud

Our cloud solutions are regularly audited for compliance with the Statement on Standards for Attestation Engagements (SSAE)-16 SOC 1. Within the North America geographical region, Dimension Data also maintains Payment Card Industry Data Security Standard (PCI DSS) Level 1 service provider compliance in its managed hosting environment for clients processing or handling payment card data.

For information regarding the status and our response to the European Union's decision on the US Safe Harbor Framework, please refer to the Cloud Security Brief: Data Protection and Privacy.

Each Dimension Data cloud data centre meets or exceeds the Uptime Institute's Tier-3 data centre standards.

Secure facilities

Physical security

All Dimension Data cloud data centre facilities are secure locations that are permanently manned by on-site guards, and have closed-circuit television (CCTV) cameras that cover the entire centre. Multifactor biometric authentication is required for access inside the data centre, and the Managed Cloud infrastructure is further segmented within a locked cage environment – also monitored by CCTV cameras.

Power and environment

Each data centre is protected against environmental failures via the use of redundant uninterruptible power supply (UPS) systems, backup power generation, and resilient cooling configured in an N+1 redundancy configuration.

Fire detection and suppression

All Dimension Data cloud data centres use multi-zoned, dry pipe, water-based fire suppression systems. The air is automatically sampled for evidence of fire to provide the time to generate fire and safety alarms before fire suppression pipes are pressurised with water. If a fire occurs, water discharge is restricted to the areas within the data centre where a fire alarm has been triggered.

Flood control and earthquake

All Dimension Data public cloud data centres are built above sea level with no basement areas, and there are dedicated pump rooms for drainage of any water ingress. Exterior walls include moisture barriers, and moisture detection systems are in place to detect slow water ingress. All facilities meet, or exceed, local requirements for seismic building codes.

Configuration management and software lifecycle management

All changes to Dimension Data Managed Cloud Platform are strictly controlled. Changes can't occur without them passing through a workflow change control process, which requires sign off by multiple authorised personnel.

Updates to our Managed Cloud Platform are applied regularly, and must pass through multiple testing phases. All changes to CloudControl systems include automatic deployment to dedicated test environments. This is to ensure the completion of functionality and performance testing before being accepted and committed for deployment.

In addition to the above, changes are pre-scheduled and follow an implementation and test plan that measures the success, or failure, of a new code or infrastructure deployment. Back-out procedures in the case of any failure are documented as part of the change plan.

'All Dimension Data **cloud data centre facilities are secure locations** that are permanently manned by on-site guards, and have closed-circuit television (CCTV) cameras that cover the entire centre.'

CloudControl

All Dimension Data Managed Cloud offerings are built around our CloudControl management technology. The CloudControl systems are the interface between the clients and the Managed Cloud network, server, and storage control systems, and provide the assurance of secure separation between clients hosted within the Managed Cloud Platform.

The full suite of CloudControl systems perform the orchestration of server, storage, and network resources, controlling the segmentation between servers and networks on the infrastructure used to create the multi-tenant environment. As such, the security of this environment is paramount to providing a secure environment for all Managed Cloud Platform clients.

CloudControl security

Dimension Data's CloudControl resides on a dedicated network and server infrastructure, separate to the infrastructure used to host client networks and servers. All CloudControl systems are penetration-tested by external security assessment firms; testing occurs regularly and after every major functionality change. The CloudControl systems are also subject to rigorous software patching cycles.

Network traffic within the CloudControl environment (Dimension Data cloud-hosted environments only) is also monitored by both network intrusion detection systems and host-based intrusion detection systems, which provides round-the-clock monitoring of each Managed Cloud Platform. The Dimension Data Security Operations Centre performs 24/7 management and monitoring of all Managed Clouds around the world, and reacts to any abnormal events in real time.

CloudControl resiliency

All CloudControl management systems are hosted on separate network and server hardware to client systems. N+1 resiliency is applied to all CloudControl devices, which allows for multiple device failures with no impact to the accessibility of CloudControl, or the performance of the management interfaces.

CloudControl management interface

All client access to cloud management settings is performed via CloudControl using either the web management interface or the CloudControl API. Both methods use Secure Sockets Layer (SSL) encryption with 128-bit keys for security. All requests made to the CloudControl interfaces are assessed and enacted only if the requested changes are for resources owned by the client.

The CloudControl interfaces also restrict clients to actions which are necessary for the management of their cloud networks and virtual servers. No direct access is provided to the underlying systems. This provides all Managed Cloud Platform clients with the assurance that their cloud networks and systems are protected against configuration settings which could affect their performance, security, and availability.

No other access method is provided to clients. This ensures that it isn't possible to directly attack or affect the cloud network and virtual server hosting technology.

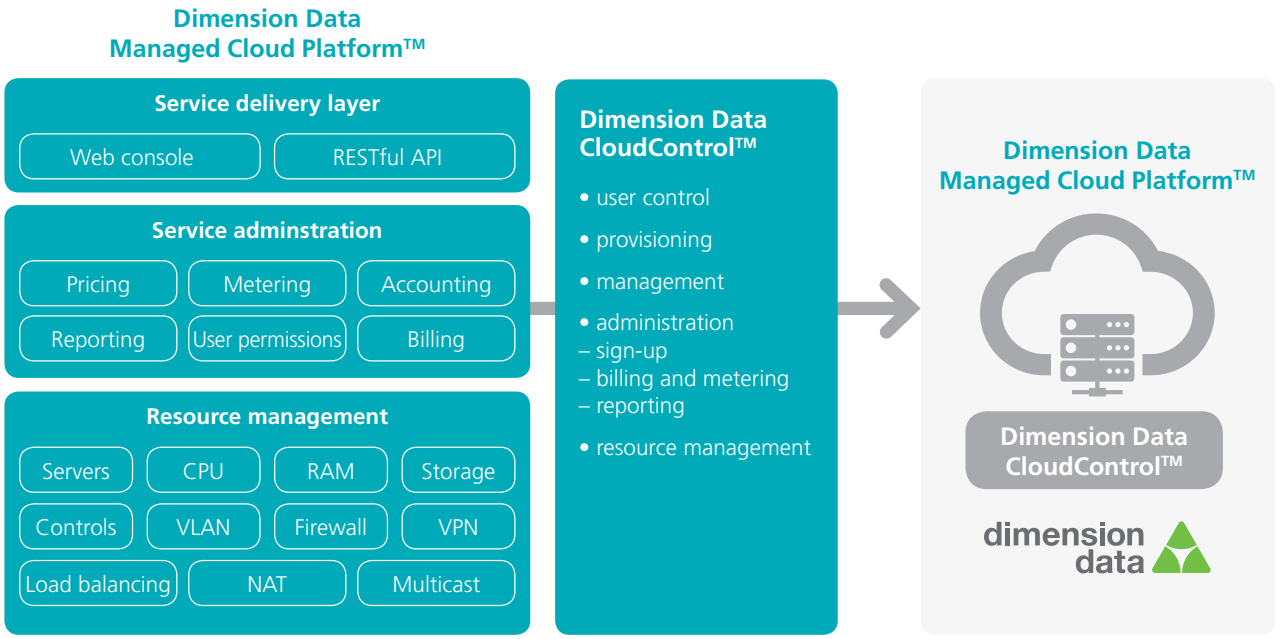
CloudControl network traffic encryption

All CloudControl operations are encrypted using Secure Hypertext Transfor Protocol (HTTPS) between the clients and the CloudControl web servers. Transmission encryption is performed using the Rivest Cipher 4 (RC4) encryption algorithm over the Transport Layer Security (TLS) protocol with 128-bit keys. The CloudControl web infrastructure uses a 2048-bit digital certificate for authentication of the web server and encryption of the RC4 initialisation vector keys.

Remote access

Clients can also access their Managed Cloud networks using the CloudControl remote access virtual private network (VPN). This service allows administrators to authenticate using their Managed Cloud account, and connect either using a web-based SSL VPN portal or a locally installed Cisco VPN client. Both clients use RC4 128-bit encryption over HTTPS and can be used to communicate with servers inside the client's cloud networks via the IP protocol.

Each VPN client is allocated an Internet Protocol (IP) address which is granted explicit rights to connect to its Managed Cloud networks, and logically appears to be one IP hop away from their servers.

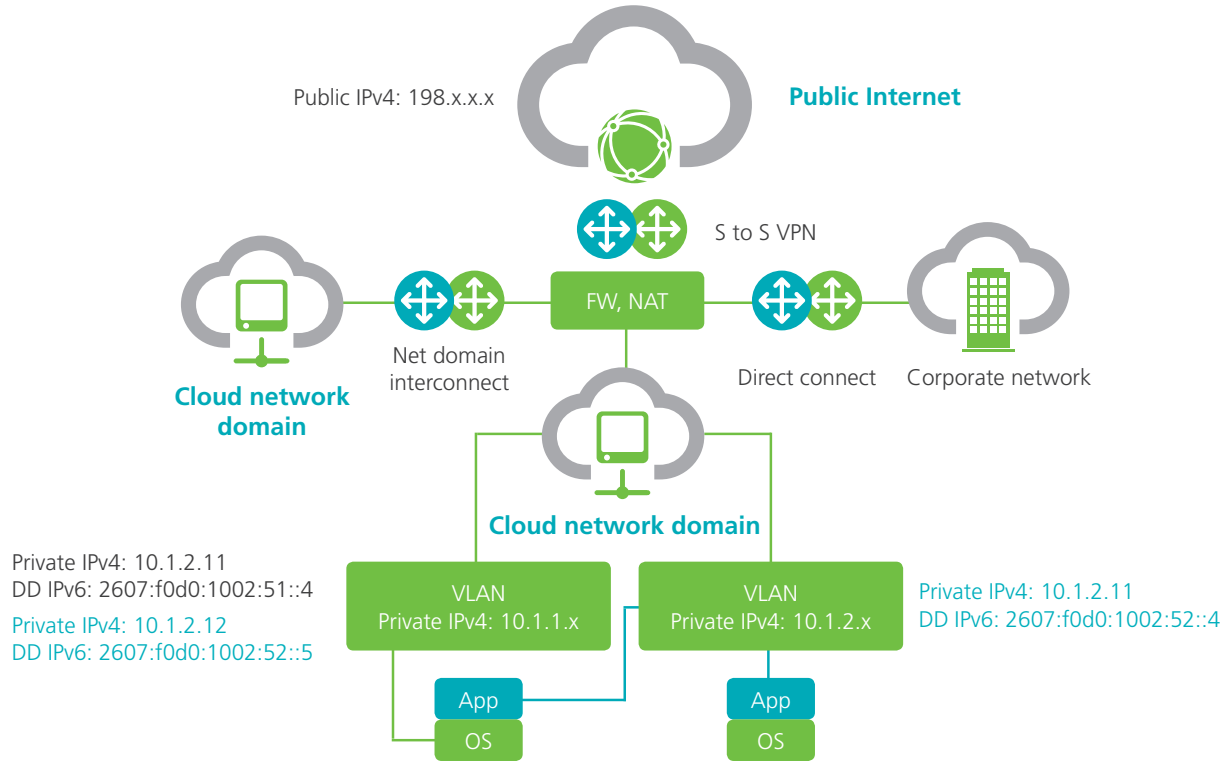


Cloud connectivity

Dimension Data cloud connectivity provides the ability to interconnect any of Dimension Data's Managed Clouds – our public, shared resource cloud, hosted private cloud, or our dedicated private clouds to the client's enterprise networks – in a secure manner. Network Domain Connect choices of Direct, Private, Interconnect, and Site-to-Site (S2S) are each described in the table below.

These cloud connectivity choices allow multiple, disparate environments to communicate with each other outside of both the public IP connectivity and the optimised VPN network that's provided by Dimension Data between different cloud data centre locations. This allows clients to extend their corporate networks seamlessly into the Dimension Data cloud environment.

Network Domain Connect	Description
1. Direct	• connect via a physical port (i.e. leased line, MPLS) • includes cross connect within Dimension Data data centre to third-party WAN provider • 1 GB and 10 GB port options
2. Private	• connect using pre-existing connectivity at a Dimension Data data centre from managed MPLS vendors • 100 Mbps service • available in select geographies
3. S2S VPN	• site-to-site virtual private network (VPN) connections via the Internet using Internet Protocol Security (IPSec) or IPSec Virtual Tunnel Interface (VTI) options • VTI routing via Border Gateway Protocol (BGP) • Advanced Encryption Standard (AES) 256-bit encryption
4. Interconnect	• direct, private connectivity between multiple client environments within a Dimension Data cloud data centre



Client cloud networks

The first building block for Managed Cloud Platform clients is one or more cloud networks. Each cloud network created by clients is a dedicated layer 2 VLAN created and controlled on a Cisco SDN infrastructure. Virtual machines can be deployed with multiple virtual NICs (VNIC), with each VNIC being assigned an RFC 1918 IPv4 address and a unique IPv6 address. No software emulation of VLANs is performed in the Managed Cloud environment.

With Dimension Data's Managed Cloud offerings, clients can create and deploy multiple, virtual data centres that are logically segregated with their own dedicated cloud network domain and layer 2 VLANs within that domain. Virtual data centres, each with its own network domain, can be used to segregate application sets, functional areas, or groups. With network domains, clients can build multi-tier network architectures to separate data tiers from front-end web tiers, which provides an additional layer of firewall rules to protect sensitive data. With each virtual data centre and network domain, clients can:

- choose a private IPv4 address space to be used for each VLAN
- assign tiered storage to virtual servers to meet application data performance levels
- allow VLANS with the same private IP address assignments to remain isolated from each other
- support both IPv4 and IPv6
- control the IPv4 and IPv6 traffic
  - between different VLANs in the same network domain
  - between the public Internet and VLANs in the network domain
  - between any of the Network Domain Connect interconnections
- customise the firewall and load balancing
- determine public Internet connectivity and optional connectivity to non-public networks via Network Domain Connect

Each network domain has its own private IP address space that isolates each client's cloud servers from the public Internet. Cloud servers are assigned private IPs when they are deployed and only become accessible to the public Internet when administrators specifically enable such access through a network address translation (NAT) or virtual IP (VIP). With this approach, cloud servers are completely isolated from the public Internet unless the network administrator establishes connectivity to them.

Network access controls

Every cloud network is protected by access control lists (ACLs) that define what IP traffic may enter and leave the network. Inbound access to cloud networks from the Internet is disabled by default, ensuring a default security posture. Outbound access from cloud networks to the Internet is enabled by default. All ACLs are fully stateful and include Deep Packet Inspection for support of complex protocols.

The ACLs for each cloud network are completely under the client's control and can be used to provide strict or open access, to and from each cloud network. ACLs can be applied to allow/deny access on both inbound as well as outbound traffic.

Cloud network IP addressing

Every cloud network created by clients is allocated a small block of publically reachable IPv4 addresses used for NAT. IPv6 addresses are unique and don't leverage NAT.

Cloud network resiliency

The Dimension Data Managed Cloud Platform uses N+1 resilient, Cisco enterprise-grade switching and routing infrastructures with multiple hardware modules in each switch for resiliency of IP routing, access controls, and server load balancing. Failures of any management, network, or security modules within a switch, or failure of an entire switch, don't affect the accessibility or performance of client cloud networks.

All network equipment is connected using multiple physical network paths with each path providing enough bandwidth to service Managed Cloud Platform operations in the event of a failure. All physical server hardware is connected to redundant core switches with redundant security blades providing layer 2 isolation and network functions.

Client virtual servers

Virtual server hosts

The Dimension Data Managed Cloud uses VMware ESX hosts to host client virtual servers. All management of VMware ESX functionality is performed by the CloudControl management systems or Dimension Data personnel, with no VMware management interfaces exposed.

Virtual server images

Virtual servers created by clients are based on either operating system (OS) virtual images created by Dimension Data, or Open Virtualisation Format (OVF) images imported by the client. These images include the necessary tools to allow for pre-build configuration settings to be applied to them as part of the initial server creation process. Only the necessary software or OS components are included in the OS images, and clients are free to remove any components they deem aren't required for each server once a VM has been built.

Virtual server (ESX) host resiliency

All ESX servers use multiple physical network cards, and connect to the redundant core switches. Link bonding and Link Aggregation Control Protocol (LACP) is used to provide zero downtime in the event of a network failure. All storage used by the ESX hosts is provided by EMC SAN storage systems, with multiple host bus adapters installed in each ESX host, and multiple connections to the SAN array.

All ESX hosts are clustered in an N+1 resiliency model, which provides protection against hardware failure due to CPU, memory, or motherboard faults. Failover to another ESX host for client virtual servers is automatic, with the servers being automatically restarted. Any affected virtual servers are only offline for the time it takes for them to be restarted.

Virtual server resource dedication

Clients with either the Private or Hosted Private Managed Cloud are provided with dedicated resilient ESX server clusters for their own use. Public Managed Cloud Platform clients share ESX server resources with other clients within the same Managed Cloud data centre.

Server administrator passwords

Clients are asked to provide a root/administrator password for their servers just before they're created. This password is briefly stored on the virtual server operating system disk for the purposes of automated build and start-up, after which it's erased with no record of the password kept by Dimension Data.

Operating system vulnerability management

All operating system images created by Dimension Data are periodically patched with the operating system security patches installed. When clients bring up a new server, that server will start operating with those patches installed. After this point, it becomes the client's responsibility to maintain patching of the operating systems and any applications installed on their virtual servers.

For clients without the desire or skills to manage their virtual server operating systems, Dimension Data offers Managed Services for Cloud Operating Systems, a suite of server management offerings that provides system monitoring (CPU, disk, etc.), server administration, and operating system (OS) and patch management, including security patching.

Operating system security settings

All operating system images created by Dimension Data are configured with the basic required components to perform common Internet service roles (such as web servers). It also allows clients to add their own desired functionality using the relevant package management tools for the operating system used.

Once an image is customised, clients can clone the image and use it as their new, base operating system image for new virtual machines. This allows clients to create their own secure Standard Operating Environment (SOE) within their Managed Cloud environment.

Local storage

All client virtual servers are provisioned with an initial 'operating system' disk, which is a Virtual Machine Disk (VMDK) file hosted on the Managed Cloud SAN storage systems. Clients can deploy an additional 14 disks (maximum 1000GB per disk) to each virtual server, with a maximum locally attached storage size of 14 terabytes across all disks.

Storage resiliency

All locally attached disks for virtual servers are located on highly resilient EMC storage area network (SAN) storage that use multiple physical disks arranged in a redundant array of independent disk (RAID) arrays. These are presented to virtual servers as locally attached Small Computer System Interface (SCSI) disks. Dimension Data manages all physical disk maintenance for clients, ensuring that any physical disk failures are invisible to clients and don't create service outages.

Storage encryption

Dimension Data doesn't encrypt client storage; such an offering would mean that Dimension Data would need knowledge of the encryption keys for the deployment of the service on our storage infrastructure.

When encryption at rest is desired for specific risk mitigation or compliance circumstances, Dimension Data recommends that clients enable encryption of data using tools within their virtual servers or within the applications themselves.

Storage resource dedication

For clients using our Private Cloud and Hosted Private Cloud storage, resources are dedicated to each client.

Systems with the most highly sensitive information can be located outside of the Dimension Data Managed Cloud Platform environment and linked via a secure tunnel.

'All client virtual servers are **provisioned with an initial 'operating system' disk**, which is a Virtual Machine Disk (VMDK) file hosted on the Managed Cloud SAN storage systems.'

Hybrid network-attached storage (NAS)

Dimension Data's Managed Cloud clients that require shared storage across multiple virtual servers can use the Dimension Data Hybrid NAS solution. The Hybrid NAS solution is located within the same Dimension Data cloud data centre, but outside the control of the CloudControl management systems.

Hybrid NAS resiliency

The Hybrid NAS solution is hosted on N+1 resilient storage appliances with multiple controllers and disk trays configured in resilient RAID arrays. Failure of NAS controllers or disks is invisible to clients, with no downtime or performance degradation.

Hybrid NAS security

Each NAS client is allocated their own dedicated vFiler instance with access restricted to their cloud networks. Access to the NAS is restricted at deployment time to the cloud networks the client requests; this can be all, or some of the client's cloud networks. Any client who grants access to the NAS from all of their client networks can further restrict this access using custom access control lists (ACLs).

The hybrid NAS deployment doesn't implement user-based security, and it's designed to serve as shared storage for server workloads rather than user-based file and print services.

Auditing and monitoring

Dimension Data's CloudControl software audits all administrator activities performed by clients and allows each client to download copies of these logs in comma-separated value (CSV) format. Any action taken by a client through the CloudControl web interface or API is fully monitored and the results of those actions are captured within the audit trail. The audit trail captures the full content of each command entered and the details of any changes made as part of the change.

The audit trail itself can be accessed via the API, which allows clients to automatically monitor all administrator activity on their Managed Cloud accounts, and import these into log management systems or incident management systems.

Activities logged

The Managed Cloud administrator logs include details of any commands issued from the CloudControl web interface or the API. Most functions also log both the command request and the actual implementation of that request by the CloudControl software. Activity logs are retained for one year, and are available for download from the web-based user interface or API.

Access to administrator logs

To maintain security against tampering of the administrator logs, once a log entry has been created, clients can't remove the log entries. Copies of the administrator logs can be downloaded by any sub-admin accounts that have the 'report' access role.

User management

Primary administrator

All Managed Cloud Platform clients start with a primary administrator account. This account maintains full access to all cloud networks and servers for the client, and can create sub-administrator roles with more granular permissions to create and edit network, server, or storage resources.

Sub-administrators

The primary administrator can create sub-administrators and grant them specific permissions only to create and edit the cloud network, server, and storage resources. This reduces the likelihood of accidental or malicious removal of resources, and allows for accurate auditing of administrator activities.

Access roles

Sub-administrator accounts can be granted one or more security roles, those being 'network', 'server', 'create image', and 'reports'. If no role is chosen, the user will only have 'read-only' access. They can view networks, servers, and images, but can't deploy, modify, or delete them.

The network role allows the user to utilise any of the network functions, allowing them to create new networks, delete networks, or modify existing ones (such as adding/removing firewall rules).

The server role allows the user to deploy servers, modify the characteristics of servers, or delete servers. They can take any action on the server function – except the creation of a customer image.

The create image role allows the user to create customer images from any deployed server.

The reports role allows the user to view the report functions available on the 'reports' tab.

Clients that require more granular access control can leverage their own identity management infrastructure and web portals with controlled access to pre-configured API scripting, to control what actions a user can perform.

Data sovereignty

Dimension Data's Hosted Private and Public Managed Cloud Platform clients have a choice of region in which their accounts are created. As such, all clients have full control over the region where their servers and storage resides, and can explicitly choose to use multiple regions or a single region.

Geographical failover

To enable clients to implement resiliency against failure of access to an entire Dimension Data Managed Cloud region, clients can choose to have cloud networks and servers located in multiple geographical locations, and can create ACL rules to allow direct IP communication between their geographically separated cloud networks.

Clients are responsible for implementing the failover solution; Dimension Data recommends the use of global load balancer technology to perform the monitoring. As part of Dimension Data's Managed Services for Operating Systems we're able to help clients configure, deploy, and monitor failover solutions.

Locations of Dimension Data's cloud data centres – across six continents

Additional Dimension Data security services

A complete approach to security is required to address today's security challenges. It must include the people, processes, technology, and threat insights to proactively protect and defend your organisation against an increasingly complex and challenging threat landscape. Complete security must include your entire IT landscape, including the cloud infrastructure and applications, end-point devices, networks, and your data centre.

Dimension Data's Managed Security Services are designed to manage and operate your infrastructure in a way that ensures that all your policy, compliance, performance, availability, and capacity needs are met.

Security Architecture Assessment

The Security Architecture Assessment is a flexible engagement that provides a detailed assessment of your security architecture – from policies to technical controls. Security architecture includes the unified and integrated design, implementation, and operation of security practices across your organisation. Our assessment helps formulate a plan to manage risks, and maintain compliance with external regulations and contractual mandates.

Threat management services

Real-time Threat Management-as-a-Service safeguards your organisation by delivering complete visibility of the security activity on your network, proactively assessing threats and security risks, and implementing threat analysis and incident response. We provide support during the process of identification, investigation, response and containment, and rectification. The service combines collection, correlation, management, early-warning, and detection with 24/7 expert security analysis and incident response to keep your network ahead of today's evolving risks. Options include network behavioural anomaly detection, compliance-aware monitoring, identity and role correlation, and insider-threat monitoring.

Managed Security Information and Event Management (SIEM) detects and responds to IT security threats and breaches, mitigates risk, and ensures compliance through the monitoring and management of SIEM systems. The service includes round-the-clock monitoring, daily management, software upgrades, patches, system configuration, and rapid intrusion detection, escalation, and response.

Managed Network Security Services

Managed Intrusion Detection and Prevention provides a fully managed, 24/7 service that uses network-based intrusion detection and prevention systems to protect networks from attack and misuse. The service includes round-the-clock monitoring; daily management including the fine-tuning of filters, software upgrades and patches, and system configuration; and rapid intrusion detection, escalation, and response.

Managed Firewall protects your key information assets across networks, hosts, applications, and databases with firewall management, monitoring, and maintenance by our experienced security analysts. We offer custom firewall configurations to deliver cost-effective security. The service includes daily management with complete firewall system maintenance that incorporates rule-based backup and restoration, software upgrades, patches, and system configuration.

Managed Web Gateway ensures that your web gateway technologies are monitored and managed effectively to provide continued protection from information leakage.

Web Security Services

Web Security-as-a-Service ensures that your organisation can embrace cloud and social media technologies to deliver and exchange information while protecting it from accidental data loss, malicious attacks, and emerging threats.

Cloud Security Appliance Services

Dimension Data, in conjunction with leading security vendors, is developing the next-generation firewall, optimised to run on our Managed Cloud Platform as a consumption-based service. The Cloud Security Appliance Service enables the organisation to configure security zones for workloads based on its existing security design standards. This may be a simple, single firewall to create a demilitarised zone (DMZ) between the external network and a web server or a complex, multi-zone design to protect network flows between IT solution components. The Cloud Security Appliance Service allows the organisation to reproduce the security perimeter environment that it has in place for its data centre, in the cloud.

Email Security Services

Email Security-as-a-Service delivers a turnkey email protection and availability solution that ensures a consistent, 'always-on' email experience for your users while guarding against email threats including viruses, phishing, spam, spyware, data theft, and blended threats. The service:

- blocks threats before they reach your network
- eliminates losses associated with system outages, message interception, or corruption from an infected email base
- prevents users from clicking on malicious links within emails
- encrypts sensitive company data to maintain compliance with privacy and security regulations
- guarantees business continuity with access to a secure web interface for users and administrators to compose, send, receive, and manage email during a mail service outage or disaster

Managed Email Gateway ensures that your email gateway technologies are monitored and managed effectively to provide continued protection from information leakage and from viruses, trojans, spyware, and malicious code distributed via email. Our service provides a customised, email gateway configuration for your organisation with guaranteed responsiveness to availability events, issues, or system performance. The service includes daily management and email gateway system support including policy backup and restoration, software patches, and system configuration.

'Dimension Data's Managed Security Services are designed to **manage and operate your infrastructure** in a way that ensures that all your policy, compliance, performance, availability, and capacity needs are met.'

Frequently asked questions

Can I install my own network security device?

The Dimension Data Managed Cloud solution doesn't support the installation of layer 2 transparent devices. Clients can't bring their own hardware devices to either the public or hosted private cloud solutions. However, clients with our Private Cloud deployed on their site can install network security devices inside their data centre – 'upstream' of the managed cloud infrastructure. In supported geographies, clients may connect via a private, layer 2 connection using our Network Domain Connect service.

All clients are free to install any software agent on their servers. Therefore, the functionality offered by traditional layer 2 transparent devices can be performed using tools such as host-based IPS and firewall protection.

Are virtual appliances supported?

Dimension Data's Managed Cloud Platform supports the importation of open virtual format (OVF) images. However, we don't support the importation of open virtual appliance (OVA) format images. Each virtual image requires some amount of automated system preparation by the CloudControl infrastructure, which may not be possible on many appliance virtual machines. Dimension Data has a validated workload process that allows vendors to validate their workloads on the Dimension Data Managed Cloud Platform with the help of our Solution Architects.

Can I install my own hypervisor security controls?

To ensure that no client can negatively affect the performance or security of any other client, there is no access to any hypervisor functionality, and clients can't install or use hypervisor security controls such as VMware vCloud Networking and Security. Dimension Data maintains strict control over the hypervisor to ensure the highest security is provided to all clients.

Does Dimension Data utilise any VMware hypervisor security controls?

The Dimension Data Managed Cloud Platform uses dedicated, network security devices from Cisco systems for all network security. Dimension Data also provides integrated, 'east-west' security controls using VMWare NSX Firewall as an option for dedicated VMWare environments (Private and Hosted Private cloud).

Does Dimension Data monitor my audit logs for suspicious activity?

No, due to the wide variety of client needs, Dimension Data doesn't assume what administrative tasks for each client are normal or abnormal. However, Dimension Data monitors the CloudControl portal to detect attacks made against it, which may result in clients being alerted to the fact that their accounts are being targeted.

Can Dimension Data monitor my systems for accessibility?

Server start and stop events are included in administrator logs and can be used to detect a manually initiated server shutdown from within the administrator user interface.

Dimension Data also provides an integrated capability for cloud monitoring. Cloud monitoring provides customers with the ability to view a series of dynamic graphs illustrating the performance of their cloud servers, create alert-driven notifications using thresholds based on this information, and manage their cloud environments by configuring powerful auto-scaling capabilities. Both cloud server performance data and the customer notification/auto-scaling managers are accessible via the cloud monitoring portal.

For clients without the desire or skills to monitor their virtual server operating systems, Dimension Data offers a suite of server management offerings under the Managed Services for Cloud Operating Systems, which provides system monitoring (CPU, disk, etc.), server administration, and OS support and patch management, including security patch management.

Can I increase the network security between my cloud networks?

Clients are able to fully control the ACLs that define what IP traffic can enter and exit each of their networks. Each client cloud network is a dedicated VLAN which reaches all other networks (including the CloudControl remote access VPN) by passing through a Cisco security module.

By default, all IP traffic is permitted between a client's remote access VPN and all of its cloud networks. The inbound ACL for each cloud network can be configured to restrict this traffic.

Can I restrict communication between my servers within a network?

The Dimension Data Managed Cloud Platform doesn't provide the capability to perform within-VLAN filtering. Clients can configure and install any IP filtering solution on their virtual servers, which provides the same functionality. Any communication between servers on other client cloud networks can be controlled using ACLs.

Can I monitor all VLAN traffic on my networks?

The Dimension Data Managed Cloud Platform Services don't allow the monitoring of traffic on client networks using packet sniffers. All servers located in client cloud networks can only see IP traffic destined to them and IP broadcast traffic for their VLAN. To ensure that clients can't attempt to 'break out' of the hypervisor and view traffic destined for other client networks, promiscuous mode has been disabled in the hypervisor and can't be used by any client.

Are my servers backed up?

All virtual server storage (including operating system drives) are stored on resilient EMC SAN storage arrays. Clients are free to manually or programmatically (via the API) clone their virtual servers. These clones are labelled as 'client images' and can be used to redeploy a server in the event of failure or server corruption.

Dimension Data also offers an integrated cloud backup and recovery solution for all cloud virtual machines, managed hosting, and on-premise servers. The Cloud Backup and Recovery service is provisioned using the cloud API, the cloud admin user interface, or the cloud backup service portal. Cloud Backup and Recovery includes the backup of files, system states, as well as agents for popular applications such as Active Directory and databases.

What happens if an ESX server fails?

The Dimension Data Managed Cloud Platform has been built for resiliency. VM hosting ESX servers are configured in clusters with the cluster consisting of actively used ESX hosts and standby servers. Every ESX server uses a combination of bonded NICs, resilient SAN arrays, multiple paths to the SAN, and redundant power supplies.

Client virtual machines are only active on one ESX chassis at any given time. If an ESX server fails, all virtual machines on that chassis will fail. Each virtual machine will then be automatically re-started on another ESX server in the cluster, resulting in a few minutes of downtime while the virtual servers are moved and restarted. For added resiliency, clients can use Dimension Data's server anti-affinity rules to deploy virtual servers on different physical servers.

Can I customise my server operating system settings before creating new virtual servers?

Clients can create their own custom operating system images of server operating systems. To do so, the client must start up a fresh virtual machine from one of the supplied images from Dimension Data or import their own image. Custom settings can be applied to this image, and it can then be configured as a custom image which can be used to create new virtual servers.

Custom images are not maintained by Dimension Data; if a client doesn't maintain patching of the operating system for custom images, new virtual machines based on the image may be insecure.

How can I defend against downtime caused by a virtual server failure?

If an application hosted on a virtual server fails due to software-based issues outside of Dimension Data's control, resiliency can be created by deploying multiple servers within the application and use load balancing configured within the client's cloud network. For added resiliency, clients can use Dimension Data's server anti-affinity rules to deploy virtual servers on different physical servers.

Are complex protocols such as File Transfer Protocol (FTP) supported, given that NAT is a requirement for external access?

All ACLs are fully stateful and include Deep Packet Inspection which supports the following complex protocols:

• FTP • DNS • CMP • SCCP • RTSP • ILS • SIP

Can I get log entries for ACL rule hits?

The Dimension Data Managed Cloud Platform doesn't currently allow for the monitoring of ACL rule hits. If connection logs to servers are desired, this functionality can be deployed by using software tools on a client's virtual server operating systems, such as host-based firewalls and web server logs.

How do I create Tier-2/Tier-3/ intranet networks?

By default, all Dimension Data Managed Cloud networks are configured the same. To make a network unreachable from the Internet permanently so that any accidental NAT changes don't expose systems, clients can delete the default inbound ACL and replace these with new ACLs which are more restrictive, allowing access only from their other cloud networks.

Access from these networks to the Internet can also be controlled by editing the outbound ACL, which allows clients to block or restrict all outbound Internet connectivity, and connectivity to all other cloud networks.

Can I communicate with other Dimension Data Managed Cloud clients from my cloud networks?

If both parties involved in the connection use ACL entries that permit traffic between the private IP addresses of their own cloud networks, the communication is permitted. This is possible between any Dimension Data Public and Hosted Private Cloud, regardless of the source and destination Managed Cloud data centre, which allows true private and secure global communication.

All communication between Dimension Data's Managed Cloud data centres is encrypted using IPsec tunnels using Triple Data Encryption Standard (DES) 168-bit three-key encryption. Authentication of the encrypted tunnels is made using multiple, site-specific pre-shared keys, which are managed out-of-band by Dimension Data. Public key infrastructure (PKI) authentication isn't used for the encrypted tunnels to reduce the attack surface of the authentication method.

Can I communicate with my own data centre using a site-to-site VPN?

Dimension Data offers a managed, site-to-site VPN service for clients as one of our four Network Domain Connect options.

Can I change the IP addresses of my virtual servers?

The entire IPv4 RFC 1918 range is routable within a given cloud network domain. Users can deploy VLANs onto the cloud network domain and choose between their own /24-/16 private IPv4 blocks for use by any NIC connected to that VLAN. However, although a /24 block provides a contiguous block of 255 private IP addresses, only 248 private IP addresses are available for use by cloud server NICs as the system reserves x.x.x.0 through x.x.x.5, x.x.x.7, and the broadcast address {x.x.x.255} for its own use (meaning x.x.x.6 and x.x.x.8 - x.x.x.254 are available for use on a /24 block).

Is IPv6 supported?

Native IPv6 is supported by Dimension Data for cloud networks.

Can I remove the outbound source NAT from my cloud networks?

No, the outbound source NAT rules aren't alterable by clients. To block outbound access, clients can edit the default outbound ACL for their cloud networks to stop connections to external networks.

Can I remove the public IP addresses from my cloud networks?

The first two public IP addresses allocated to each cloud network can't be removed. Any additional public IP address blocks requested by clients can be removed.

Security best practices

Administrator account management

Restrict knowledge of the primary administrator account

The most powerful user account for any Managed Cloud Platform client is the primary administrator account. Access to this account should be restricted, and it shouldn't be used for daily management operations. Dimension Data recommends the use of a long passphrase and that the password used for this account isn't used for any other system or service. As a best practice, it's recommended that the primary administrator account should not be used for any routine Managed Cloud Platform operations, as it can't be traced back to an individual administrator.

Network security controls

Default network security posture

When a network is created, it's automatically allocated a private IP address range and a small block of public IP addresses. Outbound access to the Internet is immediately possible due to source NAT being configured automatically. Inbound ACL rules exist by default to allow access to ports 80 and 443 on any IP address within the cloud network. Inbound access from the public Internet isn't enabled until a static NAT rule is created to map one of the public IP addresses to the private IP address of a server. If multiple, cloud network layer 2 VLANs are set-up, care should be taken to modify ACL rules accordingly to explicitly restrict access to IP addresses or ports that shouldn't be accessed (e.g. application and data tier servers not in a dimilitarised zone (DMZ).

ACLs

All communication into and out of every cloud network is governed by the ACLs applied to that network. Each network has an inbound and outbound ACL, which controls the ability of other networks to initiate connectivity to the network, or allow hosts within the network to reach other networks or the Internet.

For each cloud network, there are invisible ACLs in place which allow the client's remote access VPN to reach all cloud networks created under the primary account.

For all normal CloudControl operations, sub-administrator accounts should be used – with their access rights restricted to the networks and servers within their account. As with the primary administrator, each sub-administrator account shouldn't use a password which is used anywhere else.

For the greatest network security, sub-administrators shouldn't be granted the 'network' role unless they require the ability to create and modify networks (including ACL rules).

Audit log management

Dimension Data recommends that administrator audit logs are reconciled with expected activities on a regular basis. The CloudControl API interface allows for the collection of administrator audit logs, which allows logs to be automatically downloaded and imported into a log analysis tool. Dimension Data recommends the use of security event and incident management technology, which has behavioural learning capabilities for intelligent log analysis, and the generation of alerts when high-risk or unexpected actions are undertaken.

Virtual server security

Whilst Dimension Data provides server images in a secure format, some settings should be further hardened to match client security requirements. For example, direct root access is enabled (and required during server builds) for SSH access on Linux servers. Post deployment of servers, clients should apply additional security settings relevant to their information security management framework and related standards.

To learn more about our cloud services, visit: **dimensiondata.com/cloud**

dimension data

Middle East & Africa

Algeria • Angola
Botswana • Congo • Burundi
Democratic Republic of the Congo
Gabon • Ghana • Kenya
Malawi • Mauritius • Morocco
Mozambique • Namibia • Nigeria
Oman • Rwanda • Saudi Arabia
South Africa
Tanzania • Uganda
United Arab Emirates • Zambia

Asia

China • Hong Kong
India • Indonesia • Japan
Korea • Malaysia
New Zealand • Philippines
Singapore • Taiwan
Thailand • Vietnam

Australia

Australian Capital Territory
New South Wales • Queensland
South Australia • Victoria
Western Australia

Europe

Austria • Belgium
Czech Republic • France
Germany • Hungary
Ireland • Italy
Luxembourg • Netherlands
Poland • Portugal
Slovakia • Spain • Switzerland
United Kingdom

Americas

Brazil • Canada • Chile
Mexico • United States

For contact details in your region please visit **dimensiondata.com/globalpresence**

dimensiondata.com