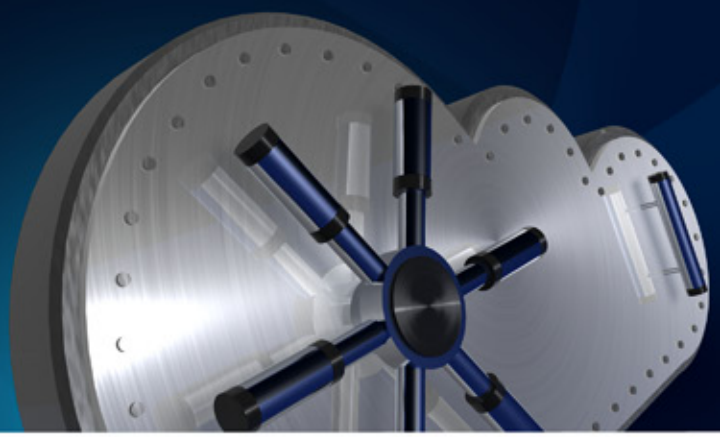
OPTiMO CLOUD SOLUTIONS

ENTERPRISE CLOUD AND MANAGED HOSTING

Enterprise-Class Security



OPTiMO Cloud Security

With the constant threat of security breaches, having a clear and robust security implementation is a necessity, not an option. With OPTiMO Cloud Managed Hosting, the solutions necessary to protect our customers' application and data assets are included with the service. OPTiMO Cloud is guided by a "defense-in-depth" security strategy, in which a series of security layers are implemented so that no single solution is relied upon to provide security.

SECURE DATACENTERS

OPTiMO Cloud delivers its Cloud and Managed Hosting Solutions from top-tier colocation facilities in the Sunnyvale, CA; Ashburn, VA; London, UK; and Paris, France. Our facilities meet or exceed Tier III standards, the highest commercially available datacenter rating as measured by the Uptime Institute (http://uptimeinstitute.org/). Network connectivity is provided Global Tier-1 IP Networks.

- All areas within the facility are monitored 24x7x365 by closed-circuit cameras and onsite guards
- OPTiMO Cloud data center space is physically isolated and accessible only by OPTiMO Cloud administrators
- Access is restricted by authorized personnel through biometric two-factor authentication
- CCTV digital cameras cover the entire center, including cages, with detailed 24x7 surveillance and audit logs

OPTIMO CLOUD HOSTING SECURITY

OPTiMO Cloud Hosting provides the security and control enterprises demand. Unlike other commodity cloud services, OPTiMO Cloud provides an environment to configure and lock-down your compute and storage environments. With OPTiMO Cloud Networks, customers are able to configure VLANs between servers, configure ACL-based firewalls, and control and track administrative usage. Data is encrypted while being transferred as well as at rest.

OPTiMO Cloud Servers and OPTiMO Cloud Files, our Cloud-based computer and storage services, can be linked by OPTiMO Cloud Networks, our Customer-controlled network configuration services. Rather than implementing our network security on top of our virtualized servers, OPTiMO Cloud Networks is a truly network-based implementation running within our Cisco switching fabric. Customers manage and configure OPTiMO Cloud Networks via the web-based OPTiMO Cloud .net user interface or Open API.

CUSTOMER-CONTROLLED NETWORK CONFIGURATION

- Configurable Layer-2 VLANs based on Cisco-based switching fabric
- Customizable ACL-based firewall rules allow you to control access into each network VLAN
- NAT and VIP functions to expose your private IP
- Addresses to the public Internet
- Load-balancing and port translation across multiple virtual servers, with the ability to take servers in and out of service manually, programmatically, or based on monitoring probes
- Layer 2 Multicast support for clustering implementations

ENCRYPTION

Data stored with 256-bit encryption at rest and 128-bit SSL encryption while in transit.

SECURE ACCESS

Access to OPTiMO Cloud via the Public Internet, MPLS, VPN, Carrier Ethernet or Private Networks.

OPTiMO CLOUD SOLUTIONS

OPTIMO CLOUD HOSTING SECURITY

ROLE-BASED ADMINISTRATIVE CONTROL

- VPN administration of all servers
- Unique username and password for multiple administrators
- Role-based permissions allow administrator to limit to manage only certain resources, such as servers, storage or networks

REPORTING

Audit logs of all environmental changes.

COMPLIANCE

OPTiMO Cloud maintains SAS-70 attestation in conjunction with our auditor SAS 70 Solutions. Our SAS-70 attestation is based on an in-depth series of documented controls covering the operational management of the OPTiMO Cloud Hosting infrastructure.

24X7 INCIDENT RESPONSE

OPTiMO Cloud Security Incident Response Team (OSIRT) to handle reports of security incidents. The OSIRT will escalate the incident to law enforcement and/or executive management as prescribed in security policies.

OPTIMO CLOUD MANAGED HOSTING SECURITY

With the constant threat of security breaches, having a clear and robust security implementation is a necessity, not an option. OPTiMO Cloud is guided by a "defense-in-depth" security strategy, in which a series of security layers are implemented so that no single solution is relied upon to provide security.

FIREWALL

Fully-managed, hardened, stateful inspection firewall technology with customized customer-specific firewall rules.

INTRUSION DETECTION

Fully-managed Intrusion Detection System (IDS) utilizing signature, protocol and anomaly based inspection methods.

EDGE-TO-EDGE SECURITY VISIBILITY

Edge-to-edge security, visibility and carrier-class threat management and remediation utilizing industry leading Arbor Networks Peakflow to compare real-time network traffic against baseline definitions of normal network behavior, immediately flagging all anomalies due to security hazards such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, worms or botnets.

SECURE ACCESS

Access to OPTiMO Cloud via the Public Internet, MPLS, VPN, Carrier Ethernet or Private Networks.

SAS 70 AND PCI COMPLIANCE

- OPTiMO Cloud maintains SAS-70 attestation in conjunction with our auditor SAS 70 Solutions. Our SAS-70 attestation is based on an in-depth series of documented controls covering the operational management of the OPTiMO Cloud Hosting infrastructure
- OPTiMO Cloud offers a PCI-compliant environment that implements a number of security measures required for applications storing, transmitting, or processing credit or debit card information

24X7 INCIDENT RESPONSE

OPTiMO Cloud Security Incident Response Team (OSIRT) to handle reports of security incidents. The OSIRT will escalate the incident to law enforcement and/or executive management as prescribed in security policies.

CONTACT US TODAY

Discover the benefits of the Cloud. Contact our experts at ***contactus@OPTiMO-IT.com*** *or call* ***877-564-8552*** *today!*

Visit OPTiMO-CLOUD.COM for more information.