TeraGo

Agility . Reliability . Creativity

Services Description

LAST UPDATED SEPTEMBER 2017

Table of Contents

Enterprise Cloud Services 1

- VMware Cloud services 1
- Enterprise Cloud Storage 2
  - Provisioned IOPS 2
  - Block Storage 2
  - Object Storage 2
- Managed Continuity & Resiliency services 3
  - Managed Disaster Recovery as a Service 3
- Self-service Backup & Restoration 5
  - Hosted Virtual Machine Backup 5
  - On-Premise Backup using Veeam Cloud Connect 6
- Self-service Disaster Recovery 7
- CLOUD Network Services 8
  - Connectivity 8
  - Private Interconnections 9
  - IP Addresses 9
  - DNS Service 9
  - Load Balancers 10
- Software 11
- Cloud Drive 11

VMware Cloud Managed Cloud Services 13

- Overview 13
- Managed Threshold Monitoring 13
- Managed OS patching 14
- Managed Firewall 15
- Customer managed Firewall 16
- Managed Trend Micro Security 17
- Managed SQL patching 18

Data Centre Colocation Services 19

- Mississauga, ON 19
- Kelowna, BC 20
- Vancouver Vault 21
- Vaughan, ON (Toronto north) 22
- COLOCATION SERVICES 23
- Data Center Security and Access Policy 25
- Network Services 28
  - Wide Area Network 28
  - Local Area Network 28
  - IP Addresses 28
  - DNS Service 29

Voice Services 30

Overview 30
LAN / WAN Requirements 30
Service Limitations 30
The Equipment and the Service 30
Available Special Needs Services 31
9-1-1 VoIP Service Conditions and Limitations 31
Connectivity Services 32
Wireless and fibre access 32
Private Line Data Services (formerly known as VLAN) 32
Internet Services 32
Technical Infrastructure 32
Symmetrical Speeds 32
Full Duplex Service 32
Distributed Denial of Services (DDoS) 32
REDUNDANCY 35

SERVICES DESCRIPTION

Enterprise Cloud Services

VMWARE CLOUD SERVICES

The Enterprise Hybrid Cloud for vCloud Air is powered by VMware technology. The service deploys VMWare vCloud Director, vSphere, vCenter Server, Operations Manager Enterprise, Hyperic, and a myriad of Enterprise Plus licensed features. All cloud services are offered out of TeraGo's western and eastern data centers, with the exception of Object Storage which is available only in the western data center.

Each Virtual Machine is pre-configured by TeraGo by default to be backed up on a daily basis with the last 6 restore points available for restoration. The licenses and storage space required for daily backups is included at no additional charge. Customer is responsible for capacity planning and purchase of additional backup storage space should more frequent backups be required.

This service includes:

- Preconfigured virtual machines with vCPU, RAM and base storage
- Daily backups of Virtual Machines with the previous 6 restore points retained
- 24x7x365 hardware and hypervisor monitoring and management.
- Hardware resource component maintenance and repair.
- Updates to BIOS/Firmware for hardware components that are provided where deemed necessary at the sole discretion of the service provider.
- VMware Enterprise Plus Edition.
- Management of Hypervisor and Hypervisor management systems.
- Virtual Machine High-Availability utilizing VMware HA, vMotion and Distributed Resource Scheduler.
- Installation, troubleshooting and reinstall of the Operating System selected:
    - Customers may provide a custom OVF image.
    - Optional Windows or RedHat Operating System license is available for an additional charge; limited to supported Operating Systems
    - Customer may supply, install and support their own Operating System upon approval
- Provide necessary operational support for Virtual Machines (VMs).
- Configure parameters for VMs or logical partitions with assistance from the Customer where applicable (such as application parameters).
- Off-server storage connectivity (storage tiers and capacity are available for additional cost).
- Multi-Path 10Gbps network connectivity between server hardware components and storage.
- Three (3) registered Internet Protocol ("IP") addresses; see section IP Address Services'.

The customer is responsible for configuring and managing Guest VM, operating system image and licenses, and installed software applications.

SERVICES DESCRIPTION

ENTERPRISE CLOUD STORAGE

Enterprise Cloud Services are delivered using highly reliable and performing persistent data stores. In order to keep your data secure and private, our storage services do not have a data collection and or data processing components. Data is encrypted at rest for all storage tiers. We offer three tiers of storage for development, production, and disaster recovery workloads that vary in terms of performance:

1. Provisioned IOPS storage
2. Block Storage
3. Object Storage

Provisioned IOPS

Provisioned IOPS storage is delivered as an all-flash block storage offering, which can provide guaranteed input/output per second (IOPS) for block-level storage to customers in a multi-tenant, highly-available configuration. A base level of 1 IOPS/GB is guaranteed with this storage tier and additional IOPS is available as an optional add-on (maximum up to 10 IOPS/GB)

Provisioned IOPS storage is powered by SolidFire technology, the only appliance in the industry able to deliver guaranteed IOPS. In addition, connectivity between storage and compute is provided over Ethernet utilizing iSCSI in a dual-path configuration. The storage cluster is configured in a fully N+1 design (considering drives, nodes, and network paths) which allows for in-service software upgrades and hardware failure without interrupting services. Last, this tier is securely presented to private cloud environments and suitable for customers requiring guaranteed IOPS for their application requirements.

Block Storage

Block storage service utilizes SAS disk with a read and write caching layer for improved performance. This storage service is suitable for mid-level I/O workloads. Most operating systems and applications are recommended for this storage service.

Block Storage can also be provisioned as utilizing a file gateway to provide a NFS mount, which operates on a private VLAN with a restricted subnet. NFS traffic is not visible to other customers using any related or separate systems or networks. Connectivity between storage and compute is provided over Ethernet utilizing NFS in a dual-path, fully redundant setup.

Both, Provisioned IOPS and Block storage include TeraGo managed daily backups with the last 6 restore points available for restoration. The licenses and storage space required for daily backups is included at no additional charge. Customer is responsible for capacity planning and purchase of additional backup storage space should more frequent backups be required.

Object Storage

Object storage service utilizes SATA disks, which allows data to be stored as complete objects with user-defined metadata and global identifiers. This metadata makes large and unstructured data sets searchable and index-able for more efficient processing for applications and archival retrieval. It is ideal for low I/O web and mobile applications as well as backup and archival storage. TeraGo Object Storage supports both S3 and OpenStack Swift formats, which makes it compatible with thousands of object storage-based applications available in the market

today. Object storage does not require subscription of any other TeraGo infrastructure or software tools, and is accessible from anywhere with an internet connection. Users may manage and organize their data through a self-managed user portal. Data integrity is ensured with N+2 object-level resiliency.

Included with all tiers of storage are:

- 24x7x365 hardware monitoring and management.
- Hardware resource component maintenance and repair.
- Updates to underlying hardware components.
- Datacenter network connectivity.
- Virtual fabric isolation.
- Initial volume creation.
- Initial storage connection and configuration technical support assistance.
- Direct access to storage configuration interfaces are not provided.

The customer is responsible for the following activities:

- Management of customer data.
- Request configuration changes through our ticketing system.

MANAGED CONTINUITY & RESILIENCY SERVICES

Managed Disaster Recovery as a Service

Disaster Recovery as a Service (DRaaS) is designed to provide resilience and recoverability to on-premise or hosted customer workloads in the case of an outage. Fully managed services as part of DRaaS enable failover as well as failback of applications and data within pre-set recovery time objectives (RTO) and recovery point objectives (RPO) to allow business continuance. Virtualized workloads within VMware, or Microsoft Hyper-V environments are supported.

Managed services included as part of the overall DRaaS offering are:

1. Continuity Assessment – A comprehensive continuity assessment to determine the required RTO/RPO and create an inventory of virtual machines and other components of the customer workload to be covered under the disaster recovery plan. The continuity assessment report will provide the customer with the following information:
   - Infrastructure details such as no. of virtual machines and the associated compute, RAM and storage requirements
   - Supporting network information such as IP addresses, DNS, firewalls, VPN, bandwidth etc.
   - Applications hosted on the target environment and relevant interdependencies
   - A high-level disaster recovery plan in order to meet customer specified RTO/RPO

   The price, duration and scope of the continuity assessment would vary for each customer depending on factors such as workload, applications, network and storage requirements etc.

2. Solution Design – Document all solution design aspects including infrastructure, network & storage requirements and key replication/recovery software utilized within the DR solution. Customer will be provided with a detailed runbook, documenting the following:
    - System and network (LAN, WAN) configuration
    - Application details and interdependencies
    - Authorization and access details
    - Roles and responsibilities for TeraGo managed services & customer IT
    - Failover steps – activation of the DR plan
    - Workload failback steps
    - TeraGo support information including escalation steps
3. Implementation - Deployment of disaster recovery solution as determined within the 'Solution Design' step as well as provision of necessary system administration and operational support for:
    - Disaster recovery software & underlying virtualization technologies
    - Storage, network and firewall configurations

    Initial failover testing to be conducted within 30 days of solution implementation.

4. Monitoring & Recovery - Recovery of customer workload upon disaster declaration. One instance of managed recovery (failover & fallback), no longer than 30 days per calendar year is included at no additional charge
    - Monitoring of customer workloads for scheduled replication tasks
    - Ensure replication activities meet recovery point objectives
    - Recover customer workloads in case of disaster declaration within predefined RTOs
    - Perform failback of customer workloads once primary location is available
5. Maintenance & Testing
    - Disaster Recovery test in conjunction with customer IT. Customer to notify TeraGo 90 days in advance of desired DR test date. One instance of a managed testing is included per calendar year at no additional charge
    - Technical support and troubleshooting for all disaster recovery related software and hardware components, including firewalls, DRaaS software and hypervisor layer
    - Maintenance of DR runbook and apply quarterly changes as required due to software, infrastructure or personnel changes

Customer responsibilities:

- Declaration of an outage scenario. Confirmation that workloads are required to be brought online at secondary site
- Management, monitoring & technical support for software applications installed within guest VMs

SERVICES DESCRIPTION

Intended Use-cases

Virtualized workloads hosted on customer premise, co-located with another provider or hosted on the TeraGo cloud can be protected & recovered using the TeraGo DRaaS offering. All workloads will be recovered into TeraGo's VMware powered public cloud environment.

SLA

The standard TeraGo cloud SLA applies here along with any specific RTOs/RPOs agreed upon with the customer.

Billing details

- Continuity assessment – A one-time fee is charged upfront for the continuity assessment.
- Ongoing managed services – Monthly billing for ongoing managed services.

Related Services

- Backup as a Service
- Managed Firewall service
- Infrastructure as a Service (IaaS)

SELF-SERVICE BACKUP & RESTORATION

Backups are delivered using the award-winning Veeam suite of tools. Our services provide fast, flexible and reliable recovery of virtualized applications and data, both on-premise and in our cloud.

Hosted Virtual Machine Backup

Hosted Virtual Machine Backup offers multiple backup options to meet your needs including both image and file level backups. Virtual Appliance (hot add) and Direct SAN Access modes provide direct access to production storage, taking load off of the management network and hypervisor hosts, and maximizing backup performance. Advanced features as source-side deduplication and compression, file-level restore, change block tracking, parallel processing, automatic load balancing and the exclusion of swap files ensure the fastest, most efficient backups possible. This service is powered by Veeam Backup & Recovery Software.

Included in this service are:

- Access to a hosted, multi-tenant environment providing backup management portal to control restores.
- A single restore operator role allows access to their backups and restoration options, with the ability to control permissions.
- System administration and operational support for backup and restore technology, standard provided configurations, and:
  - Managed underlying virtualization and operating system software for host server(s)
  - Created customer user and assigned initial restore permission for Restore Operator role

- Troubleshooting and technical support for:
  - Veeam Backup Enterprise Manager
  - VMware Tools Install
- Management and updates to backup infrastructure, software, and service components as necessary at the sole discretion of the service provider.
- Customer will perform backup job creation using available schedule profiles.
- Maximum of three (3) Custom Directory and/or File Exclusions per VM will be allowed.
- The service provider will review and troubleshoot failed backups, and provide basic assistance in configuration of file-level restore upon customer ticket request only.
- All backups are Off-site Replicated to an alternate cloud site that is geographically diverse from the primary backup location.

The customer is responsible for the following activities:

- Creating and assigning valid backup job.
- Ensuring the accuracy of any exclusions.
- Reporting.
- Automating Notification and Alerting of failed backups.

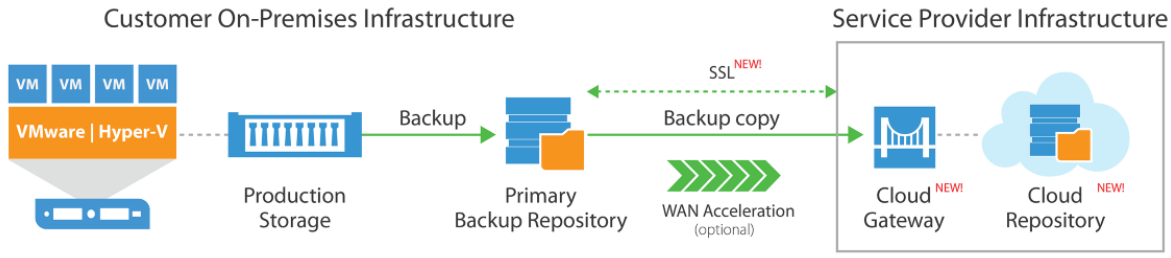
On-Premise Backup using Veeam Cloud Connect

Customer may have on premise compute and storage environments that require backup and recovery objectives. We provide a hosted storage repository that can be utilized by their existing backup implementation as a primary or secondary offsite data repository.

Common objectives for this backup service include:

- **Hosted offsite backups**: Get your backups offsite to a hosted cloud repository through a secure SSL connection with no additional Veeam licensing required.
- **Complete visibility and control**: Access and recover data in hosted backup repositories directly from the backup console; track cloud repository consumption and receive reminders for hosted storage renewals.
- **A modern backup architecture**: Leverage Veeam's modern backup technology, including Backup Copy jobs with Built-in WAN Acceleration, forever incremental backups, GFS (grandfather-father-son) retention policies and more—all built into one product.
- **End-to-end encryption**: Rest easy by encrypting all data at source (before it leaves your network perimeter), in flight and at rest, without negatively impacting the data reduction ratios of built-in compression and WAN Acceleration.

SERVICES DESCRIPTION



The on premise backup service is powered by Veeam Cloud Connect (requires Veeam 8 or newer) and utilizes Cloud Gateway servers enabled with SSL certificates for encryption of both transit and at-rest data, thereby, providing maximum protection for your mission critical data.

Included in this service are:

- Management and hosting of backup storage to support this service. Customers will be allocated storage based on the contracted value. Additional storage can be purchased
- Access to view daily consumption of storage through an online portal
- Troubleshooting and technical support for installation and operational instruction on utilizing the service, including network and software components
- Updates to Veeam cloud connect infrastructure hosted on TeraGo.
- Customers will be assigned with a multi-tenant gateway address, username, password as well as detailed instructions on incorporating the service into their existing backup environment.
- A hosted, multi-tenant Cloud Gateway Server with up to 10Gbit network per gateway. Individual copy jobs to the Cloud Connect service will be restricted to 1Gbit.

The customer is responsible for the following activities:

- Customer site Veeam Backup and Replication software

SELF-SERVICE DISASTER RECOVERY

Disaster Recovery as a Service (DRaaS) is designed to provide customers with the ability to protect on premise or hosted workloads in the case of a disaster. This service provides automated data recovery with tunable RTO and RPO according to available bandwidth, failover and failback to enable full business continuance, allowing you to select any virtual machine in your virtual infrastructure while replicating it to or from our data centers. This service supports both the replication of VMware environments from a single console, allows for data consistency between groups of VM's and also enables migrations between a client's environment and our cloud services.

Disaster recovery is secure and controlled using private connectivity to perform the replication. These include:

- Direct Connect using a Client's private WAN circuit.
- IPsec VPN tunnel.
- Direct peering with our network access points.

Connectivity can be facilitated through a partner or be provided by the customer. The bandwidth required for the service is dependent on the size and change rate of the customer environment, at least 5 Mbit is required. Last, a virtual or physical firewall will be required in order to facilitate direct WAN access for a VPN enabled endpoint on our cloud service.

Included in this service are:

1. Licensing and software to installation on customer premises.
2. Necessary system administration and operational support for virtualization technology and related configurations:
    a. Provide and manage underlying hypervisor/virtualization software.
    b. Provide and manage Operating System for underlying Hypervisors and Hypervisor management systems.
    c. Create and assign one external (1) VLAN; (additional VLANs available for an additional charge).
    d. Management of Hypervisor and Hypervisor management systems.
3. Troubleshooting and technical support for all underlying hardware and software components to deliver this service including firewalls, DRaaS enabling software, and virtualization hosts.
4. Facility security and environmental system monitoring and management and associated data center facility services (including power, cooling and racks).
5. Troubleshooting of hardware components and issues suspected to result from hardware components.
6. Replacement of TeraGo's defective or failed hardware components.
7. Updates to underlying software for hardware components.
8. Virtual Replication Appliance license(s).
9. Disaster recovery protected disks provisioned by the hypervisor to the VM directly (unable to externally mount storage volumes).

The customer is responsible for the following activities:

- Installing a Virtual Replication Appliance (specifications provided upon order acceptance).
- Initial setup time for deploying and licensing the replication software on the customer site.
- Technical support for Guest VMs and installed software applications.
- Management and monitoring of Guest VMs or installed software applications, unless otherwise subscribed to our Managed Services.
- Monitoring of the Virtual Replication Appliance and host machine on the customer premises.
- Disaster Recovery plan creation and testing.

CLOUD NETWORK SERVICES

Connectivity

We provide network connectivity services for Internet and Wide Area Networks (WAN). Included in this service are Bandwidth, support for On-Net WAN connectivity, performance up to 10 Gbps, and a switched Ethernet connection or fiber optic connection with demarcation in our data center. Upon request we can also connect to third-party networks including SuperNet, ORION, all major Candian carriers and customer premises.

SERVICES DESCRIPTION

We provide network gateway services and access to the Internet. Internet services include dedicated and unmetered bandwidth with support for Private Line connectivity and first-hop redundant internet gateway. Internet services support performance up to 10 Gbps and a switched Ethernet connection or fiber optic connection with demarcation in our data center.

Private Interconnections

We provide a virtual local area network that supports Layer 2 connectivity across customer locations, colocation facilities and cloud services, as required. The network supports performance up to 40 Gbps and a switched Ethernet connection or fiber optic connection with demarcation in our data center.

IP Addresses

We are able to allocate additional public (Internet-facing) and/or private host IP addresses for Services, subject to Customer meeting ARIN requirements. We use all reasonable efforts to allocate public host IP addresses on contiguous private subnets in increments of 6, 13, 29, 61, 256, half Class-C and full Class-C blocks, following standard IP subnet allocation methodology.

Private host IP addresses assigned and managed, but are not Internet-facing and cannot be viewed nor referenced from outside our data center. We may allocate IP addresses on subnets that are not contiguous with prior allocations, and thereby, retain ownership of all IP addresses allocated to Customer. Customer may not allocate IP addresses provided to other parties without our written consent.

DNS Service

The Domain Name System (DNS) protocol is an important part of the World Wide Web's infrastructure, serving as the Internet's phone book: every time you visit a website, your computer performs a DNS lookup. Complex pages often require multiple DNS lookups before they start loading, so your computer may be performing hundreds of lookups a day.

TeraGo's DNS service provides a recursive DNS resolver, similar to other publicly available DNS services. It provides many benefits, including improved security, faster performance, and more valid results.

The DNS service does not include the following:

- A top-level domain (TLD) name service.
- A DNS hosting or failover service. TeraGo DNS is not a DNS application service provider, that hosts authoritative records for other domains
- An authoritative name service. TeraGo DNS servers are not authoritative for any domain
- A malware-blocking service

The DNS service includes a number of security, performance, and compliance capabilities. A brief overview of these capabilities are provided below

Performance: Many public DNS service providers are not sufficiently provisioned to be able to support high-volume input/output and caching, and adequately balance load among their servers. The DNS service employs large, optimized caches and load-balances user traffic to ensure shared caching.

Security: DNS is vulnerable to various kinds of spoofing attacks that can "poison" a nameserver's cache and route its users to malicious sites. The prevalence of DNS exploits means that providers have to frequently apply server updates and patches. In addition, open DNS resolvers are vulnerable to being used to launch denial-of-service (DoS) attacks on other systems. To defend against such attacks, TeraGo has implemented several recommended solutions to help guarantee the authenticity of the responses it receives from other nameservers, and to ensure our servers are not used for launching DoS attacks. Besides full support of the DNSSEC protocol, these include adding entropy to requests, rate-limiting client traffic, and more.

Correctness: TeraGo's DNS service does its best to return the right answer to every query every time, in accordance with the DNS standards. Sometimes, in the case of a query for a mistyped or non-existent domain name, an error message is displayed, stating that the domain name could not be resolved.

The following IP addresses are to be used for configuration purposes

- DNS Resolver 1: 69.10.148.19
- DNS Resolver 2: 69.10.148.20

Load Balancers

The load balancer service performs distribution of incoming network traffic across multiple hosts. TeraGo uses the F5® BIG-IP® Local Traffic Manager™ (LTM) to help you deliver your applications to your users in a reliable, secure, and optimized way. You get the extensibility and flexibility of application services with the programmability you need to manage your cloud infrastructure.

TeraGo provides highly-available secure multi-tenant, or dedicated F5 LTM instances with the following capabilities:

- Intelligent Load Balancing
- Application protocol support (HTTP/2, SSL/TLS, SIP, etc.)
- Application Health Monitoring
- Application correction state management
- Advanced routing (BGP, OSPF, BFD, etc)
- Application Delivery Optimization through Compression, RAM cache, TCP express, and HTTP/2 Gateway
- Secure Application Delivery Optimization through hardware accelerated SSL/TLS encryption
- Application Visibility and Monitoring
- · iRules and iRules LX for data plane programmability

The F5 iRules® scripting language—F5's traffic scripting interface—enables programmatic analysis, manipulation, and detection of all aspects of the traffic in your networks. Customers routinely implement security mitigation rules, support new protocols, and fix application-related errors in real time. With robust and flexible iRules, you can easily and rapidly develop solutions that you can then deploy across multiple applications confidently

Included support (from TeraGo) with the Load Balancer service are:

- Creation and enablement of Load Balancer device or context
- Management of underlying technology, firmware/software and warranty
- Management and provisioning of underlying network infrastructure, including private VLAN to customer virtual or physical infrastructure

The customer is responsible for the following with the Load Balancer service:

- Definition and application of Load Balancer settings and configurations for incoming traffic management
- Troubleshooting issues related to configuration settings applied to direct incoming traffic
- Testing of load balancer configuration definitions to be implemented

SOFTWARE

We provide a comprehensive line of software including operating systems for your server, hypervisors for virtualization, and middleware for applications. These softwares are enabled for single-tenant and multi-tenant cloud environments. Although we currently do not allow customers to bring their own licenses to our platform, we are fully enabled for Microsoft Service Provider License Agreements (SPLA) and the VMware vCloud Air Network (vCAN) Program.

CLOUD DRIVE

The TeraGo Cloud Drive – TeraGo's Enterprise File Sync and Share offering – provides the control of enterprise data back in the hands of the customer's IT department, while providing a platform for customer employees to create & retrieve data on the go, easily collaborate with internal teams, and securely send files to external parties. End users may easily create and retrieve content on TeraGo Cloud Drive via a web browser and also via a dedicated endpoint application available on a variety of platforms, including Windows, MacOS, Android and iOS which can be downloaded for free on the TeraGo website. The user has granular control over bandwidth use through selective syncing of content on various devices.

Additionally, the TeraGo Cloud Drive service provides customers with a dedicated tenant portal in which they have full management control to apply their own unique IT policy – ranging from user access, user group creation, device access control, storage quota allocation, and password policy and strength requirements. The customer's data is fully secured through 256-bit AES source-based encryption of data at rest, and 128-bit SSL encryption at transfer. To guarantee the utmost level of data privacy, only the customer owns a copy of the encryption keys – eliminating any risk of sensitive information exposure associated with public cloud offerings. Additionally, the backend of our Cloud Drive is physically protected in our Tier 3 data centre facilities (Kelowna Gigacentre and Tahoe Mississauga) with multi-factor access authentication and 24/7 manned security monitoring.

TeraGo Cloud Drive also includes the following feature set:

- Third-party authentication – Microsoft Active Directory and LDAP Integration
- Storage Segmentation – customer data will not be comingled with other customer content
- Outlook Integration – directly share links to files stored in Cloud Drive via Microsoft Outlook Plug-in

- Desktop Endpoint Application support for Windows and MacOS (includes regular app updates and new features)
- Mobile Application support for Android and iOS (includes regular app updates and new features)
- Web browser support on Windows, MacOS, Linux OS, Android, iOS, Windows Mobile
- 2-factor authentication – ability to require authentication via e-mail for account and device activation, as well as shared link access

The Cloud Drive product also includes the following support from TeraGo:

- 24x7x365 standard support for customer portal administrators
- Redundant power and network connection to ensure high availability
- TeraGo hosted firewall for added security

The customer is responsible for the following activities:

- Application and monitoring of customer IT policy requirements
- End user account provisioning and management, storage quota allocation, and user access control
- End user device monitoring and management
- Configuring monitors and alerts on each device or account

VMware Cloud Managed Cloud Services

We provide managed cloud services hosted at our data center locations. Included with these managed services are support services, which include 24x7x365 availability and monitoring of select managed devices. Managed devices include accountability for network faults, loss of connectivity, automatic detection of threshold violations, assigned a severity level, reporting in our Enterprise Support Ticketing System at our Network Operations Centers.

OVERVIEW

- 24x7x365 monitoring and management of hypervisor and below for multi-tenant services and hardware for single-tenant services
- Hardware resource component maintenance and repair
- Updates to BIOS/Firmware for hardware components that are managed by the service provider
- Management of hypervisor host systems and hypervisor management systems

MANAGED THRESHOLD MONITORING

Threshold Monitoring is an optional service that allows customers to manage and monitor of server operations, and is powered by Nimsoft monitoring technology. Customers utilize this service to monitor and manage virtual for troubling events, such as unexpected high CPU activity or low disk space. Key features such as automated alerting and performance dashboards deliver valuable insight into the state and performance of customer's servers are included.

Included in this service are:

- Coordination with the customer to establish and configure appropriate monitoring thresholds.
- Installation and configuration of monitoring agents as required.
- Automatic ticket creation and proactive electronic customer notification for detected hardware and resource limit alerts.
- Provider initiated critical “call-out” notification of up to five (5) customer supplied contacts for Severity 1 issues (as defined by a service being "hard" down or a critical impact to a customer's business operation with no possible workarounds for the customer, its users, or the service provider).
- Basic monitoring dashboard and historical reporting accessible through portal.

The customer is responsible for the following activities:

- Support or management of Operating System including patching.
- Application management and troubleshooting, including customer provided software.
- Database and information management and troubleshooting.

SERVICES DESCRIPTION

MANAGED OS PATCHING

Patch management is an optional service whereby server management tasks (up to and including the Operating System) are conducted by the service provider. This approach makes customer resources available to focus on their core competencies and their business. Customers receive tailored automated alerting, dashboards and reporting features.

Included in this service are:

- Recommendation of operating system updates and configuration modification with Customer concurrence to apply update;
- Minor upgrades to the server operating system, which includes service packs, minor version upgrades
- Operating system patch updates, including security and integrity patches as required and agreed to by the Customer
- Service Provider retains and manages root access
- Management of problem determination and resolution of server management activities
- Management of existing operating system configuration, by modifying configuration files, documenting system configuration, and controlling access to system configuration files
- Management of operating system files, by creating, maintaining and deleting volumes and directory structures, modifying file system sizes, verifying mount point availability, repairing defective file systems, and modifying file system permissions
- Monitoring of and periodically reducing operating system log files to help prevent file systems from overfilling;
- Management of operating system processes (e.g., continuously running system subtasks); by refreshing processes as required, establishing startup sequences, and changing process priorities as appropriate
- Maintain tools for server management to enable installs, modifications and removals
- Automatic ticket creation and proactive electronic customer notification for detected hardware and resource limit alerts
- Initiate critical “call-out” notification of up to five (5) Customer supplied contacts for Severity 1 issues (as defined by a service being "hard" down or a critical impact to a customer's business operation with no possible workarounds for the customer, its users, or the service provider);
- Evaluation of planned changes to the server environment and advise Customer of any requirements to support such changes
- Administration of file system directory distribution and replication
- Customized monitoring dashboard and historical reporting accessible through portal

The customer is responsible for the following activities:

- Application management and troubleshooting, including customer provided software
- Database and information management and troubleshooting

SERVICES DESCRIPTION

MANAGED FIREWALL

Managed firewall services are available through the Fortigate network security platform, which includes 24x7 monitoring for up/down status, proactive ticket creation, initial trouble-shooting, problem resolution management and specific rule-set changes. The various capabilities of this platform are listed as follows:

Capability	**Specification**
Virtual/Hardware	Hardware
Performance	> 1 Gbps
Concurrent Sessions	600,000
High Availability	Yes
Additional Capabilities	Unified Threat Management (UTM) Services Bundle includes NGFW, AV, Web Filtering, and Antispam Services - IPS/IDS - SSL VPN - Site-to-site VPN

Included support (from TeraGo) with the Managed Firewall service are:

- 24x7 up/down device status monitoring.
- Managed support including updates and patches of the OS or firmware, and device monitoring and interface monitoring.
- Security updates for vendor disclosed vulnerabilities
- Base configuration and implementation of devices
- Management of licensing and warranty
- Proactive support ticket creation.
- Automatic updates from vendor for IDS/IPS patterns and rules, in-line Anti-Virus, Anti-Spam and Spyware definitions (if applicable)
- Initial trouble-shooting of monitoring events or problematic firewall device consisting of:
    - Attempt to ping firewall to confirm device availability or not;
    - Where applicable, attempt remote connection to device GUI through available/standard WAN connection;
    - Observe and note any displayed errors and attempt remote troubleshoot of device if remote connection can be established;
    - Escalation procedures if initial trouble-shooting process is unable to restore normal operation.
    - Problem resolution management consisting of:
        - Relay available trouble-shooting information to authorized technicians and respondents for trouble-shooting, repair and/or replacement of failed firewall appliances;
        - Provide telephone and ticket based support to authorized technicians and respondents to assist in confirming restoration of service for failed firewall appliances;

- Follow up with authorized technicians and respondents to confirm firewall appliances are being attended to and repair/restoration activity is proceeding
- Modify firewall rule-set as directed by customer. Limited to twelve (12) rule set changes per year. Customer to provide specific rule-set change criteria.

The customer is responsible for the following with the TeraGo Managed Firewall service:

- Customer initiated changes to custom firewall rulesets
  - TeraGo to only apply automate updates from the vendor, or customer initiated rule-set change requests as defined by the client
- IPS/IDS rule management
- VPN configuration setup and changes
- Troubleshooting issues related to customer defined settings applied to firewall rule sets
- Testing of firewall rule set changes to be implemented

CUSTOMER MANAGED FIREWALL

The customer managed virtual firewall offering is powered by Cisco Adaptive Security Virtual Appliance (ASAv). Cisco virtual ASA brings the power of Cisco physical ASA appliance to the virtual domain and cloud environments and provides the same level of robust security to cloud workloads.

Included support (from TeraGo) with the customer managed firewall service are:

- Creation and enablement of virtual firewall and portal access
- Management of underlying technology and related configurations

The various capabilities available within the virtual firewall offering is summarized below:

Feature	**ASAv5**
Stateful inspection throughput (maximum)[1]	100 Mbps
Stateful inspection throughput (multiprotocol)[2]	50 Mbps
Advanced Encryption Standard (AES) VPN throughput[3]	30 Mbps
Connections per second	8,000
Concurrent sessions	50,000
IPsec VPN peers	50
Cisco AnyConnect® or clientless VPN user sessions	50
Modes	Routed and transparent
Virtual CPUs	1
Memory	1 GB minimum 1.5 GB maximum
Minimum disk storage[4]	8 GB

The customer is responsible for the following with the Customer Managed Firewall service:

- Firewall rule set base definition and any custom rule set modifications
- Up/down device status monitoring
- Device updates, including but not limited to OS patch update, firmware updates, IDS/IPS rule updates from vendor, Anti-Virus, Anti-Spam, and Spyware definitions
- Base configuration and implementation of devices
- Troubleshooting issues related to customer defined settings applied to firewall rule sets
- Testing of firewall rule set changes to be implemented
- IPS/IDS rule management
- VPN configuration and changes

MANAGED TREND MICRO SECURITY

TeraGo's managed cloud anti-malware and web reputation service is powered by Trend Micro Deep Security. Utilizing Hypervisor Safe APIs, Trend Micro Deep Security provides agentless anti-malware & web reputation to active virtual workloads on VMware's vCloud Enterprise infrastructure.

In Scope

- Trend Micro Deep Security Anti-Malware and Web Reputation service
- Trend Micro Deep Security Tenant Space
- User with View & Computer Edit permission within Deep Security Manager (GUI)
- Necessary system administration and operational support for Trend Micro Deep Security platform and related configurations:
    - Provide and manage components related to the Trend Micro Deep Security platform to ensure portal availability and functionality
    - Create and assign valid server records or IP lists.
    - Assign anti-malware policy to valid server records.
- Management of Hypervisor and Hypervisor management systems.
- Troubleshoot and technical support for:
    - Physical hosts
    - Hypervisor
    - Deep Security Virtual Appliances
    - VMware Tools vShield App Driver
- Access to integrated reports that document prevented vulnerabilities and detected attacks
- Upgrade and patching of Trend Micro Deep Security products as and when vendor patches are released

Customer responsibility

- Malware removal
- Custom Lists (Directory, File Extension, File, IP, MAC and Port lists)
- Custom Rules for Firewall, Intrusion Prevention, Integrity Monitoring and Log Inspection
- Custom Policies

- Automated Notification and Alerting

MANAGED SQL PATCHING

Microsoft SQL Patch management is an optional service whereby MSSQL application patching is conducted by TeraGo. This approach makes customer resources available to focus on their core competencies and their business. Customers receive tailored automated alerting, dashboards and reporting features. Only MS SQL Server 2008 and later versions are supported under this service.

Included in this service are:

- Installation of the Application, at the time of the server provisioning
- Minor upgrades to the Microsoft SQL Server application, which includes service packs, minor version upgrades
- Major release version upgrades for MS SQL Server, as requested by the customer. (ie, 2012, 2012 R2, 2016)
- Proactive notification of patches and requesting of maintenance windows
- Evaluation of planned changes to the server environment and advise customer of any requirements to support such changes

The customer is responsible for the following activities:

- Application management and troubleshooting, including customer provided software
- Database and information management and troubleshooting
- Database content management and periodic data backup

Data Centre Colocation Services

Our colocation services are offered in the following datacenter locations:

- Mississauga, ON
- Kelowna, BC
- Vaughan, ON
- Vancouver, BC

Full descriptions of the capabilities and offerings for each Data Centre location can be found below. All TeraGo data centre facilities are certified to be Service Organization Controls 2 (AT 101 SOC 2) TYPE II compliant.

MISSISSAUGA, ON

As TeraGo's flagship facility, the Mississauga Data Centre is designed to Uptime Institute Tier III standards to provide enterprise grade system availability and resiliency. The data center space resides on the 2nd floor of a complex constructed by Blackberry, providing state-of-the-art design elements not found in similar facilities, including an indoor generator facility located off-grounds of the data center building for added redundancy. All power, cooling, and connectivity infrastructure elements are built with 2N redundancy to provide fault tolerance to the entire system.

Facility and Service Features

FEATURES	DESCRIPTION
Whitespace and Building	• 6,420 sq. ft. of total whitespace for IT • 25" raised flooring, with all sub-floor outlets raised 8" above ground level • Full height and truck-bed height loading docks • Secure room for equipment delivery and storage
Power	**Power Distribution** • In-row Remote Power Panels (RPPs) to allow for more efficient power monitoring and distribution • 2N back-up power infrastructure, from two dedicated municipal hydro substations • A and B side power in every cabinet • 208V Single or 3-Phase, 120V Single Phase available **Generators** • Ten 600kW generators (6,000 kW total) supplying backup power to the complex • 2N generator redundancy • On-site fuel capacity provides >48 hours run time at full load (based on current capacity) **UPS System** • 900kW UPS each for A and B side power • Clean power supplied by double conversion UPS • 2N UPS redundancy

Cooling System	**Chillers** • Fourteen 30-tonne CRAC units, supporting >1MW IT Load at capacity • Independent air-cooled rooftop cooling unit • 2N Cooling redundancy **Cooling System Design** • Alternating warm aisle and cold aisle configuration • Chilled water towers and closed glycol loop
Connectivity	• Carrier-neutral facility • Fully-redundant diverse fibre core fed from multiple providers
Cabinet Space	• Full cabinet includes 42 Rack Units (42U) • In-row cross connects with pre-engineered cable plant to all cabinets • Standard rack PDUs provided; customer supplied PDUs can be supported • Dual cable trays and ladders separating inbounding vs. outbound cabling • Depth-adjustable railings
Security and Monitoring	• 24/7 video monitoring and surveillance by Network Operations Centre • Multi-factor access authentication (access card and biometric)

KELOWNA, BC

As TeraGo's flagship facility in Western Canada, the Kelowna Data Centre is designed to Uptime Institute Tier III standards to provide enterprise grade system availability and resiliency. It is strategically located in the south-central region of British Columbia, with one of the lowest geographic risk profiles in North America. All power, cooling, and connectivity infrastructure elements are built with N+1 and 2N redundancy to provide fault tolerance to the entire system.

Facility and Service Features

FEATURES	DESCRIPTION
Whitespace and Building	• 15,000 sq. ft. of total whitespace for IT • 18" raised flooring • Ground-level loading docks • Secure room for equipment delivery and storage
Power	**Power Distribution** • 2N+1 back-up power infrastructure, from ring bus substations leading to the complex • A and B side power in every cabinet • 208V Single or 3-Phase, 120V Single Phase available **Generators**

	• Two 1,500kW generators (3,000 kW total) supplying backup power to the facility • N+1 generator redundancy • On-site fuel capacity provides >48 hours run time at full load (based on current capacity) **UPS System** • 1,000kW UPS each for A and B side power • 2N+1 UPS redundancy
Cooling System	**Chillers** • Two 250-tonne CRAC units, supporting >1MW IT Load at capacity • N+1 Cooling redundancy • 'Free cooling' capabilities during winter months due to region's climate **Cooling System Design** • Cold aisle containment configuration • Chilled water system closed loop
Connectivity	• Carrier-neutral facility • Fully-redundant diverse fibre core fed from multiple providers
Cabinet Space	• Full cabinet includes 42 and 50 Rack Units (42U, 50U) • In-row cross connects with pre-engineered cable plant to all cabinets • Standard rack PDUs provided; customer supplied PDUs can be supported • Dual cable trays and ladders separating inbounding vs. outbound cabling • Depth-adjustable railings
Security and Monitoring	• 24/7 video monitoring and surveillance by Network Operations Centre • Multi-factor access authentication (access card and biometric)

VANCOUVER VAULT

The Vancouver Vault Data Center is designed to Uptime Institute Tier I standards to provide data centre essentials in a prime location within downtown Vancouver. "The Vault" facility was originally built for the Bank of Canada to protect gold bullion and cash reserves. True to its name, the facility provides the ultimate physical security through its 28" steel-reinforced walls, 1-meter thick ceilings, and 2-meter thick floors. Power is supplied via utility power feed, UPS system, and backup generators to provide power fault tolerance. Cooling and connectivity infrastructure elements are built with N+1 redundancy to provide additional fault tolerance to the system.

Facility and Service Features

FEATURES	DESCRIPTION
Whitespace and Building	• 4,100 sq. ft. of total whitespace for IT • Full height loading dock • Secure room for equipment delivery and storage

Power	**Power Distribution** • Main power delivered from municipal hydro substations • A and B side power available for every cabinet • 208V and 120V Single Phase available **Generators** • 600kW generator supplying backup power to the facility • On-site fuel capacity provides >48 hours run time at full load (based on current capacity) **UPS System** • 560kW UPS for A and B side power • N+1 UPS redundancy
Cooling System	**Chillers** • Total 90-tonne CRAC units, supporting 320kW IT Load at capacity • Chilled water loop system with in-row cooling and outdoor chillers • N+1 Cooling redundancy **Cooling System Design** • Cold aisle containment configuration • Chilled water system closed loop
Connectivity	• Carrier-neutral facility • Fully-redundant diverse fibre core fed from multiple providers
Cabinet Space	• Full cabinet includes 48 Rack Units (48U) • Standard rack PDUs provided; customer supplied PDUs can be supported
Security and Monitoring	• 24/7 video monitoring and surveillance by Network Operations Centre • Multi-factor access authentication (access card and biometric)

VAUGHAN, ON (TORONTO NORTH)

The Vaughan Data Centre is designed to Uptime Institute Tier I standards to provide data centre essentials in a convenient location within the Greater Toronto Area. Power is supplied via utility power feed, UPS system, and backup generators to provide power fault tolerance. Cooling and connectivity infrastructure elements are built with N+1 and 2N redundancy respectively to provide additional fault tolerance to the system.

Facility and Service Features

FEATURES	DESCRIPTION
Whitespace and Building	• 7,500 sq. ft. of total whitespace for IT • 15” raised flooring • Full height loading docks • Secure room for equipment delivery and storage

Power	**Power Distribution** • Main power delivered from municipal hydro substations • A and B side power available for every cabinet • 208V and 120V Single Phase available **Generators** • Four generators (1,300 kW total) supplying backup power to the complex • On-site fuel capacity provides >36 hours run time at full load (based on current capacity) **UPS System** • 660kW UPS total capacity
Cooling System	**Chillers** • CRAC units supporting >900KW IT Load at capacity • N+1 Cooling redundancy **Cooling System Design** • Raised floor cold aisle configuration • Commercial grade modular cooling system
Connectivity	• Carrier-neutral facility • Fully-redundant diverse fibre core fed from multiple providers
Cabinet Space	• Full cabinet includes 42 Rack Units (42U) • Customers to provide their own PDUs • Depth-adjustable railings
Security and Monitoring	• 24/7 video monitoring and surveillance by Network Operations Centre • Multi-factor access authentication (access card and biometric)

COLOCATION SERVICES

In additional to the core colocation services described above, the following one-time services are also available at all TeraGo data centre facilities at an additional one-time cost. Descriptions and requirements of the services are as follows:

Remote Hands and Eyes

Requests for one-time Remote Hands and Eyes support are to be submitted to the TeraGo Network Operations Centre (by phone or via the Customer Service Centre portal), and are billed on an hourly basis. Supported Remote Hands and Eyes services include:

- Racking and stacking equipment into cabinets
- Visual verification for remote troubleshooting including circuits, loops & fiber
- Rebooting, pushing a button, toggling a switch & power cycling equipment

- Swapping removable media / Tape Replacement
- Escorting of staff and approved professional services staff
- Wiring services including moving, securing & terminating cables (requires initial labelling by customer)
- Relaying equipment status & typing commands onto a pre-installed console
- Labelling equipment or providing digital photos
- Diagnostic & signal testing for cross connect circuits
- Receive and store customer equipment
- Move stored customer equipment to staging area (implying a secure storage area with no customer access)

Compliance and Audit Support

Requests for Compliance and Audit support are to be submitted to the TeraGo Account Manager or Account Executive. Advanced notice is required for the following support:

- Client Facility Access Report – minimum 5 business days' notice
- Compliance Questionnaire Response Support – minimum of 5 business days' notice
- On-Site Audit Support – minimum 10 business days' notice, subject to availability of required TeraGo staff

The above services are billed on an hourly rate, with cost estimates provided for Client Access Facility Reports and Compliance Questionnaire Response Support prior to fulfillment.

On-site audit support is subject to a minimum of 4 billable hours, and are subject to additional overage hourly charge as required.

Data Centre Access Services

Data Centre Access Cards are only provided to individuals authorized by the client and TeraGo. A single access card is issued per authorized individual, and cannot be shared among other approved individuals.

To request a new or replacement access card, the individual must complete the Facility Access Control Form and submit to Data Centre Facilities Manager on-site. New and replacement cards are subject to one-time charges.

To re-assign an existing access card to a different authorized individual, the new assignee must complete the Facility Access Control Form and submit to Data Centre Facilities Manager on-site. New and replacement cards are subject to one-time charges.

Equipment Logistics Services

Sending Equipment to the Data Centre

Clients who wish to ship their equipment to a TeraGo data centre must first inform the Data Centre Facilities Manager by completing the TeraGo Shipping & Receiving Form. Requests should be submitted at a minimum of 3 business days prior to shipment arrival.

Shipping Equipment from the Data Centre

Clients who wish to have equipment shipped from the Data Centre to a specified location must submit their request through the TeraGo Network Operation Centre (by phone or via the Customer Service Centre portal). The client is responsible for coordinating shipping arrangements, including:

- Providing required tracking information and waybill
- Providing any required documentation for Customs for international shipment
- Providing required packaging for shipment
- Arranging any required insurance with the logistics vendor

All equipment logistic services are subject to one-time charges billed on an hourly basis.

DATA CENTER SECURITY AND ACCESS POLICY

The following Security and Access Policy (the "**Policy**") regulates activities at data center premises of TeraGo (referred to herein as the "**Data Center**"). All users of Colocation Services, including a Customer of TeraGo, a Customer's employees, agents, vendors and contractors (collectively, "**Users**") must comply with this Policy. Unless otherwise defined herein, all capitalized terms used herein have the meanings ascribed to them in the Master Services Agreement.

This Policy is intended to ensure the safety and security of individuals and equipment at the Data Center. Failure to adhere to this Policy may result in the expulsion of individuals from the Data Center and will result in a breach or violation of the provisions in the Master Services Agreement. Upon such breach or violation, TeraGo may terminate its Services provided to the Customer and/or take any other actions of remedies available to it under the Master Services Agreement, the Order Form, at law or in equity.

Policy Terms and Rules:

1. The Data Center is a secured facility. Access to the Data Center is restricted to those persons with authorization.
2. All Users shall conduct themselves in a courteous professional manner while visiting the Data Center. Users shall refrain from using any profanity or offensive language.
3. Users may not tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
4. TeraGo is not responsible for any loss, damage or theft of vehicle or the contents thereof, while located in a TeraGo parking area.
5. Alcohol, controlled substances, firearms and explosives are not permitted on TeraGo property. Smoking, drinking, and eating are strictly prohibited within the Data Center.
6. Persons under 18 years of age or requiring adult supervision are not permitted within the Data Center without the express written permission of TeraGo.
7. All visitors to the Data Center must wear appropriate footwear and attire.

8. Unless permitted by TeraGo in writing, storage of combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) are prohibited within the Data Center.
9. Customers may use cellular phones inside the Data Center but may not use cellular phones for picture or video capture. Two-way radios are not permitted in the Data Center.
10. Skateboards, skates, scooters, bicycles or other types of vehicles are prohibited in the Data Center.
11. Sharing TeraGo proprietary information, without the express written permission of TeraGo, is strictly prohibited.
12. TeraGo does not accept mail/post/courier packages on behalf of Customers at the Data Center. All mail/post/courier packages should be directed to Customer's own business address.
13. Customers must cooperate and obey all reasonable requests of Data Center personnel, including immediately addressing any violations of rules when brought to the Customer's attention.
14. Upon activation of a smoke detector or emergency alarm, all Users must be prepared to evacuate the Data Center and to receive further instructions from the TeraGo staff.
15. Any use of cameras, video and other photographic equipment including audio monitoring and audio capture devices is strictly prohibited within or immediately outside the Data Center. If pictures or video are required for insurance or marketing purposes, please contact TeraGo for assistance and consent. Web cams may be permissible as long as they are fixed-mount placements with no pan-tilt-zoom capabilities and the field of view is limited to Customer's Colocation Space only. The camera manufacturer and model number shall be submitted through the change order process so that Data Center staff may review the equipment. Web cameras found not to be compliant will not be permitted for use in the Data Center.
16. Customers are restricted to authorized areas only in the Data Center, including the Customer's Colocation Space, the lobby, customer lounge, and any conference rooms (collectively referred to as the "**Common Areas**").
17. Exterior and interior Data Center doors may not be propped open. These access doors are monitored and alarmed.
18. TeraGo reserves the right to access any part of the Data Center at any time for safety and security reasons and Customer may not install any devices that prohibit such access.
19. Customers are responsible for maintaining and updating their list of Authorized Representatives who will have access to the Data Center. TeraGo requires a written submission for additions and deletions to the Customer's Authorized Representatives list. Individuals identified on this list will be granted access to the Customer's Colocation Space. Customers may grant temporary access to their Colocation Space for an employee, vendor or technician by completing the Facility Access Control Form (FACF).
20. The Common Areas within the Data Center are for the common use by all TeraGo Customers with Colocation Space within their respective Data Centers. Extended use or exclusive use of the Common Areas for more than 2 hours (total) in a 24-hour period is not permitted. Internet access in Common Areas is provided as a courtesy to Customers and may only be used in accordance with TeraGo's Acceptable Use Policy.
21. Customers must take all necessary precautions to ensure the physical security of property contained within their Colocation Space. Cage and cabinet doors must be secured at all times when a Customer is not physically present.
22. Customers must remove all refuse materials (which include, but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are non-essential to the operation of Customers' equipment) from Customer's Colocation Space and the Common Areas. Materials must be placed in designated disposal areas.
23. The creation of "office space" within the Customer's Colocation Space or anywhere on the Data Center floor is prohibited.
24. All Customer Equipment shall be stored in a cabinet or must be kept in approved plastic or metal containers. Containers must be sealed, stacked neatly and cannot impede ingress/egress or cooling.
25. "Un-racked", operating equipment outside of cabinets or racks, is strictly prohibited.
26. Customer may not hang or mount anything on the cage mesh walls or cabinets unless authorized by the Data Center staff. The tops of the cabinets or ladder rack may not be used for physical storage.
27. Unsecured cabling across aisles or on the floor of the Data Center is strictly prohibited. Ladder racking must support all cabling between rows.

28. Cable wrapping, wire management, zip ties and/or Velcro, must be used to organize cabling in a rack or cabinet. Cabling must not obstruct airflow/ventilation/AC (perforated tiles) or access to power strips. TeraGo expects Customers to adhere to the cabling standards of the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA), 568 and 569.
29. Remote Hands service requests or change orders may be denied should Customer's cage, cabinet or Colocation Space be identified as non-compliant with this Policy. TeraGo's Service Level Agreement does not apply to a Customer who is not in compliance with this Policy.
30. If Customer intends to use Remote Hands services, all devices and cabling must be clearly labeled in a unique naming fashion. In order to reduce confusion, two devices or cables should not share the same name. TeraGo recommends that the Customer should not use its name as a naming convention to protect Customer privacy and confidentiality. For additional security purposes, external IP addresses should not be visible from outside of the Customer's Colocation Space.
31. Non-compliance with any of the cage, cabinet or cabling requirements will result in notification to Customer and a request that the Customer promptly take action to remedy the situation. Customer failure to remedy the situation will result in assessment of time and material fees if TeraGo takes correction actions on behalf of Customer.
32. Customer may not climb onto cabinet and or scale cage walls. Customer must request Data Center Staff assistance when needing to access cabinet / rack tops.
33. Customer may not make physical alternations or modifications to the Colocation Space without prior written consent from TeraGo.
34. Cabinet doors may be removed while Customer is working within a cage and must be replaced before Customer exits the Data Center.
35. Customers are prohibited from lifting or moving floor tiles where applicable. The sub-floor area is restricted area, accessible by TeraGo staff only.
36. Data Center equipment such as tools, dollies, carts, server lifts, monitor and keyboards will be available to Customers on a first-come, first-served basis. Customer is responsible for all loaned equipment while it is checked out and shall return the equipment immediately upon completion of use.
37. Customer may bring small "hand carry" equipment through the lobby. Large equipment, shipments or large devices must enter the Data Center through the applicable shipping/receiving dock. Customers must notify TeraGo staff in advance of any such deliveries.
38. Hand carried equipment brought into the Data Centers may require TeraGo technician assistance with the installation to determine the additional power draw of any new equipment being added to a customer's rack.
39. All packages shipped to the Data Center and previously approved by TeraGo must have the Customer's name and site ID on the shipping label. Any unidentified packages delivered to the Data Center will be refused for security reasons.
40. Customer is responsible for unpacking, uncrating, and movement of heavy equipment to the Data Center floor, including all associated costs.
41. Customer, in coordination with the Data Center staff, must implement appropriate protection plans to prevent damage to Data Center infrastructure (plywood on raised floors, cage wall removal, overhead clearance, etc.).
42. The Data Center will not pack and ship any Customer owned equipment. The Customer may open a ticket to authorize temporary access for their shipping company to enter their cage and cabinet, or to have the Data Center staff de-rack a device and make it available to the Customer's shipping company. Customer is responsible to ensure their shipper provides all packing material and physically packs the devices for shipping them. TeraGo shall not be liable for improper packing and shipping of Customer owned devices.
43. Upon termination or expiration of the Colocation Service(s), the Customer must leave the Colocation Space in as good condition; normal wear and tear accepted, as it was at the Commencement Date. Unless otherwise agreed to in writing, Customer will have all Customer Equipment removed from the Data Center no later than the effective cancellation/termination date.
44. Readings from any Customer environment sensing device installed in a Colocation Space shall be considered secondary to TeraGo's own environmental monitoring devices.

45. Individual or free-standing electrical devices such as humidifier/dehumidifier, fans, air circulators, or air filters are not permitted in cage areas or cabinets. Fans integrated into racked equipment (servers, routers, switches) and customer provided racks are permitted. Should Customer need assistance with environmental conditions, Customer may open a trouble ticket with TeraGo's Network Operating Center (NOC).
46. Use of customer provided power strips must be discussed and reviewed with Data Center staff. Power strips or PDU's (power distribution units) must be CSA / UL or industry approved, provide for over-current protection and must be mounted in the racks. If TeraGo determines that receptacles need to be changed to accommodate the Customer-provided power strips, additional charges may apply.
47. Customers are prohibited from daisy-chaining power strips or any other violations of electric and safety codes.
48. Customer requested power audits must be conducted by contacting the TeraGo NOC.
49. TeraGo may conduct periodic power audits of Customer Space. Any violation of power limitations must be addressed immediately.

REVISIONS TO THIS DATA CENTER SECURITY AND ACCESS POLICY

TeraGo reserves the right to revise, amend or modify this Data Center Security and Access Policy from time to time. It is the responsibility of the Colocation Services Customer to access and inform itself and its Users, from time to time, as to the provisions of this Data Center Security and Access Policy. This Data Center Security and Access Policy is posted on our website at www.TeraGo.ca. The Customer acknowledges having read and accepted this Data Center Security and Access Policy prior to executing the Master Services Agreement.

NETWORK SERVICES

Wide Area Network

We provide network connectivity services for Internet and Wide Area Networks (WAN). Included in this service are Bandwidth, support for On-Net WAN connectivity, performance up to 10 Gbps, and a switched Ethernet connection or fiber optic connection with demarcation in our data center. Upon request we can also connect to third-party networks including SuperNet, ORION, and customer premises.

We provide network gateway services and access to the Internet, as well. Internet services include dedicated and unmetered bandwidth with support for On-net LANx connectivity and first-hop redundant internet gateway. Internet services support performance up to 10 Gbps and a switched Ethernet connection or fiber optic connection with demarcation in our data center.

Local Area Network

We provide a local area network that supports Layer 2 connectivity between colocation and cloud services, as required. The network supports performance up to 10 Gbps and a switched Ethernet connection or fiber optic connection with demarcation in our data center.

IP Addresses

We are able to allocate additional public (Internet-facing) and/or private host IP addresses for Services, subject to Customer meeting ARIN requirements. We use all reasonable efforts to allocate public host IP addresses on

contiguous private subnets in increments of 6, 14, 30, 62, 126, half Class-C and full Class-C blocks, following standard IP subnet allocation methodology.

Private host IP addresses assigned and managed, but are not Internet-facing and cannot be viewed nor referenced from outside our data center. We may allocate IP addresses on subnets that are not contiguous with prior allocations, and thereby, retain ownership of all IP addresses allocated to Customer. Customer may not allocate IP addresses provided to other parties without our written consent.

DNS Service

The Domain Name System (DNS) protocol is an important part of the world wide web's infrastructure, serving as the Internet's phone book: every time you visit a website, your computer performs a DNS lookup. Complex pages often require multiple DNS lookups before they start loading, so your computer may be performing hundreds of lookups a day.

TeraGo's DNS service provides a recursive DNS resolver, similar to other publicly available DNS services. It provides many benefits, including improved security, faster performance, and more valid results.

The DNS service does not include the following:

- A top-level domain (TLD) name service.
- A DNS hosting or failover service. TeraGo DNS is not a DNS application service provider, that hosts authoritative records for other domains
- An authoritative name service. TeraGo DNS servers are not authoritative for any domain
- A malware-blocking service

The DNS service includes a number of security, performance, and compliance capabilities. A brief overview of these capabilities are provided below

Performance: Many public DNS service providers are not sufficiently provisioned to be able to support high-volume input/output and caching, and adequately balance load among their servers. The DNS service employs large, optimized caches and load-balances user traffic to ensure shared caching.

Security: DNS is vulnerable to various kinds of spoofing attacks that can "poison" a nameserver's cache and route its users to malicious sites. The prevalence of DNS exploits means that providers have to frequently apply server updates and patches. In addition, open DNS resolvers are vulnerable to being used to launch denial-of-service (DoS) attacks on other systems. To defend against such attacks, TeraGo has implemented several recommended solutions to help guarantee the authenticity of the responses it receives from other nameservers, and to ensure our servers are not used for launching DoS attacks. Besides full support of the DNSSEC protocol, these include adding entropy to requests, rate-limiting client traffic, and more.

Correctness: TeraGo's DNS service does its best to return the right answer to every query every time, in accordance with the DNS standards. Sometimes, in the case of a query for a mistyped or non-existent domain name, an error message is displayed, stating that the domain name could not be resolved.

The following IP addresses are to be used for configuration purposes

- DNS Resolver 1: 69.10.148.19
- DNS Resolver 2: 69.10.148.20

Voice Services

OVERVIEW

We have been deploying enhanced business voice solutions since 2010, servicing organizations of all sizes regardless of complexities or technical limitations. Our dynamic organization staffs IT and network professionals that strive to create predictable, positive client experiences.

Our geographically diverse platform offers:

- Ability to run from multiple, high-availability data centers.
- Session Initiation Protocol (SIP) – the de facto standard for IP-based voice communications.
- Interoperability with a wide range of PBX's, desktop handsets, softphones, and applications.
- Support for custom application development, leveraging the API to our platform.

LAN / WAN REQUIREMENTS

As our services are standards compliant they are not dependent upon any specific LAN or WAN manufacturers products. We do recommend best practices be observed and respectfully requests an opportunity to collaboratively discuss network design in detail prior to implementation.

SERVICE LIMITATIONS

Usage charges will be billed individually in 6 second increments, subject to a 30 second minimum. Call timing will be determined by TeraGo's network systems. Any fraction of an increment will be treated as an entire increment.

The Equipment and the Service

- Includes 9-1-1 emergency service, will not work during a power outage, broadband service outage, interruption or slow-down, or other service interruption or problem with the relevant computer apparatus. Customer may be required to reset or reconfigure the Equipment, as the case may be, prior to utilizing the Service following a power outage, broadband service outage or other service interruption or rectification of the computer apparatus problem.
- Does not support 900/976 calling, and therefore Customer will not be able to make 900 calls using the Service.
- Does not support collect calling.
- Does not support operator services (dialing 0).
- Does not come with a telephone directory.
- Only works on a high-speed Internet connection and service quality may vary depending on the quality, upload speed and service level of the high-speed Internet connection and other factors/third party service providers extraneous to our organization.

Available Special Needs Services

The Equipment and the Service has the following special needs services:

- Message Relay Service (MRS)/7-1-1
- Tele Typewriter (TTY)

Message Relay Services (MRS)/7-1-1 allow hearing-impaired subscribers to communicate with others connected to the PSTN by providing operator intermediation. A hearing-impaired person who wishes to communicate with a hearing-impaired person dials a toll-free number to be connected to an operator who contacts the hearing-impaired user and relays the communication using a teletypewriter (TTY). Conversely a hearing impaired person, with a TTY, contacts a hearing person through the relay operator by dialing 7-1-1. MRS service is provided.

Standard LD minute charges apply for this service. There is no service fee per call.

9-1-1 VoIP Service Conditions and Limitations

Customer acknowledges that we utilize VoIP for the delivery of the Services. This is an important difference from traditional wireline local services and affects the quality and nature of 9-1-1 services available. As a result, the VoIP 9-1-1 services provided by us, have certain limitations compared to Enhanced 9-1-1 services ("E 9-1-1") available for most wireline local services. These differences include, but are not limited to:

- A bilingual call center agent will answer the 9-1-1 emergency call, request the caller's location and the emergency service required and route the call to the 9-1-1 public service answering point ("PSAP") serving the location provided by the caller.
- Unlike traditional E 9-1-1 service, the caller's location information and phone number will not be automatically delivered to the VoIP 9-1-1 call center and may not enable call control features that provide the PSAP agent with control over the line on which the 9-1-1 emergency call is made.
- The caller's location and telephone number may not be automatically transmitted with the 9-1-1 emergency call. The caller must be able to verbally communicate his/her location to the call center agent.
- VoIP 9-1-1 emergency calls made from locations outside of Canada cannot be completed by the call center agent. The caller will be told to use an alternate service to VoIP 9-1-1.
- Traditional wireline 9-1-1 is not available in all locations within Canada. VoIP 9-1-1 services within Canada are subject to the availability of traditional wireline 9-1-1 service at the caller's physical location. If traditional 9-1-1 is not available from User's location, User should contact emergency services such as fire, police or ambulance directly.
- VoIP 9-1-1 service will not function if the Equipment is not configured properly or if Customer's Service is not functioning for any reason.
- VoIP 9-1-1 service will not be available during a power outage and will be unavailable during a broadband Internet outage.
- VoIP 9-1-1 services will not be available if Service is suspended or terminated.
- Customer understands the 9-1-1 limitations of our services and Customer acknowledges that it is their obligation to make all other Users, or potential Users, of the Service aware of these limitations.

Connectivity Services

WIRELESS AND FIBRE ACCESS

Private Line Data Services (formerly known as VLAN)

The Company's Layer II data connectivity services provide businesses with the ability to connect their multiple sites within a city or across our geographic footprint through a Private Virtual Local Area Network ("VLAN"). Our Private Line services are available with speeds from 5Mbps to 10Gbps and are ideal for companies with multiple offices, requirements for connection into TeraGo's data centres and large interoffice data requirements. Our data services are symmetrical, and include our premium service level agreement.

Internet Services

The Company's wireless broadband network provides businesses with high performance Internet access with upload and download speeds from 5Mbps to 1000 Mbps. To enhance the performance of the service, we minimize the number of network hops between our customers and their audience by connecting to the Internet through peering arrangements with multiple tier-one carriers. All of our services are symmetrical (allowing customers to experience the same high speed broadband performance when uploading or downloading). We provide static IPs with all of our Internet services; up to 5 usable IPs requiring no additional paperwork with a standard contract.

Technical Infrastructure

We own and control a national MPLS network from Vancouver to Montreal. This is a next generation, carrier-grade, broadband IP network that utilizes core fibre as well as licensed wireless spectrum to deliver ubiquitous broadband connectivity.

Symmetrical Speeds

In telecommunications, the term symmetrical refers to any system in which data speed or quantity is the same in both directions, averaged over time. All our Internet and Private Line services are symmetrical and offer maximum burst speeds for both inbound and outbound traffic.

Full Duplex Service

All Internet and Private Line services are deployed as full duplex connections. Full-duplex data transmission means that data can be transmitted in both directions on a link at the same time.

DISTRIBUTED DENIAL OF SERVICES (DDOS)

TeraGo's DDoS Mitigation Services monitor all traffic entering the TeraGo network for large-volume flood and intrusion attacks, among other anomalies.

The service is composed of two key systems: a detection system and an attack mitigation system. The detection system is inserted in front of the TeraGo Gateways and is configured towards host detection. From there, it monitors traffic. Host detection can trigger an alert for an enabled misuse type. If excessive traffic is detected for multiple misuse types that are enabled, then a single alert is created instead of separate alerts for each misuse type. The alert includes each misuse type that had excessive traffic. This provides continuous threat detection against

Volumetric and SYN Attacks. Once a threat is detected, and the traffic exceed high severity rate and latency period, then the attack mitigation system will automatically automatically use local blackholing until the attack is ended. If the attack lasts longer than 15 minutes and his higher than 5Gbps, upstream blackholing is activated, until the attack ended . DDoS protected clients are identified by their IP address. Their traffic is protected and routed to clean their data. Those without DDoS protection may be quarantined.

TeraGo DDoS Mitigation Services is offered in a several packages.

	Attack Type Protection (Refer to table for exact types)	**DDoS Reporting Available?**	**TeraGo Managed Service Included?**
Bronze	Volumetric	None available	Yes - no report per customer
Silver	Bronze + Low and Slow, SIP Attacks, Memory attacks, DNS Query Floods, etc.	Yes, Generalized and not at a single IP	Yes
Gold	Bronze + Silver + Application-specific attacks, HTTP Get floods, Session attacks, concurrent connection attacks, etc.	Yes, individualized to the user	Yes

Attack Protections by Package

Bronze	Zero Minute Volumetric / Reflection Attacks	Full behavioral dynamic protection	No
Bronze	Zero Minute Flood Attacks	Full behavioral dynamic protection	No
Bronze	TCP Syn Floods	Full behavioral dynamic protection	No
Bronze	TCP SYN+ ACK Floods	Full behavioral dynamic protection	No
Bronze	TCP Reset Floods	Full behavioral dynamic protection	No
Bronze	TCP Fin floods	Full behavioral dynamic protection	No
Bronze	TCP Fragment Floods	Full behavioral dynamic protection	No
Bronze	ICMP Floods	Full behavioral dynamic protection	No
Bronze	UDP Floods	Full behavioral dynamic protection	No
Bronze	UDP Fragmented Floods	Full behavioral dynamic protection	No
Bronze	IGMP Floods	Full behavioral dynamic protection	No
Bronze	L3 / L4 Black Listing	On-demand (only during event if needed)	No
Bronze	RFC Violation Attacks / Packet Anomaly	Yes. (limited to 15 most common violations and best effort on demand)	No
Silver	Low and Slow attacks	Yes; known attack tools like LOIC and HOIC	High level shared report

Silver	TCP Stack Resource Floods	Limited (to known one fragmented stateless attack and best effort on demand)	High level shared report
Silver	DoS Vulnerability Attacks	Yes. (limited to 32 most common violations and best effort)	High level shared report
Silver	Memory Allocation Attacks	Limited (only 3 know stateless buffer overflow type of attacks and best effort on demand)	High level shared report
Silver	SIP Attacks	Limited (Limited to 10 known stateless SIP attacks and best effort on demand)	High level shared report
Silver	DNS Query Floods	Included (very small query floods will not be covered)	High level shared report
Silver	ACK Floods	On-demand (only during event if needed. Rate limit only)	High level shared report
Gold	Zero Minute Volumetric / Reflection Attacks	Included, full behavioral dynamic protection	Detailed Reporting
Gold	Zero Minute Flood Attacks	Included, full behavioral dynamic protection	Detailed Reporting
Gold	TCP Syn Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	TCP SYN+ ACK Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	TCP Reset Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	TCP Fin floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	TCP Fragment Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	ICMP Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	UDP Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	UDP Fragmented Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	IGMP Floods	Included, full behavioral dynamic protection	Detailed Reporting
Gold	L3 / L4 Black Listing	Always on	Detailed Reporting
Gold	RFC Violation Attacks / Packet Anomaly	Full coverage (1000's signatures plus custom signatures)	Detailed Reporting

Gold	Low and Slow attacks	Full coverage (1000's signatures plus custom signatures)	Detailed Reporting
Gold	TCP Stack Resource Floods	Full coverage (1000's signatures plus custom signatures)	Detailed Reporting
Gold	DoS Vulnerability Attacks	Full coverage (1000's signatures plus custom signatures)	Detailed Reporting
Gold	Memory Allocation Attacks	Full coverage (1000's signatures plus custom signatures)	Detailed Reporting
Gold	SIP Attacks	Full coverage (1000's signatures plus custom signatures)	Detailed Reporting
Gold	DNS Query Floods	Full coverage including small query floods of all types	Detailed Reporting
Gold	ACK Floods	Always on, full coverage	Detailed Reporting
Gold	Concurrent Connection Attacks	Full coverage including connection-limiting and signatures	Detailed Reporting
Gold	TCP Out of State Floods	Full coverage	Detailed Reporting
Gold	Stateful Protection Challenge Response	Full coverage, including L4/L7 challenges	Detailed Reporting
Bronze	Zero Minute Volumetric / Reflection Attacks	Full behavioral dynamic protection	No
Bronze	Zero Minute Flood Attacks	Full behavioral dynamic protection	No
Bronze	TCP Syn Floods	Full behavioral dynamic protection	No
Bronze	TCP SYN+ ACK Floods	Full behavioral dynamic protection	No
Bronze	TCP Reset Floods	Full behavioral dynamic protection	No

REDUNDANCY

TeraGo offers a suite of Internet services by means of wireless microwave antennas or fibre facilities where wireless is not feasible. This allows for customers to have bandwidth speeds of anywhere from 5Mbps to 1 Gbps and beyond. By offering customers this service, we provide them the ability to have a committed, symmetrical connection to the Internet to service all their business needs.

Many customers host mission critical applications on their networks that must be reachable at all times. Using multiple Internet connections across multiple mediums and providers can increase uptime. To combine these connections and to remain connected, TeraGo offers failover and redundancy options. Depending on their needs, customers may move from a primary connection to a secondary when the first has failed, or use multiple connections at the same time. To accomplish this, TeraGo uses a Border Gateway Protocol (BGP) peering session with one or multi-homed Internet Service Providers (ISP).

This redundancy service has the ability to offer the full internet routing table or default route only.