TeraGo Products and Services Description

May 22, 2019

TeraGo

Contents

TeraGo Products and Services

TeraGo is a leading Canadian IT technology service provider, with dedicated lines of business in Cloud, Connectivity and Colocation. This document provides an overview of the products and services in each one of these areas.

1 Software

TeraGo provides a comprehensive line of software including operating systems for servers, hypervisors for virtualization, and middleware for applications; both single-tenant and multi-tenant cloud environments are supported. Presently, customers may not bring their own Microsoft Operating System licenses to our multi-tenant cloud platform only (due to restrictions imposed by Microsoft licensing), however TeraGo is fully enabled for the Microsoft Service Provider License Agreements (SPLA) and the VMware vCloud Air Network (vCAN) Program.

2 TeraGo Cloud and Managed Services

2.1 Multi-tenant Cloud

TeraGo's Multi-tenant infrastructure and services are powered by VMware technology. TeraGo deploys VMWare vCloud Director, vSphere, vCenter Server, Operations Manager Enterprise, NSX and a myriad of other Enterprise Plus licensed features. All cloud services are offered out of TeraGo's western and eastern geographically dispersed data centers.

Clients are also provided with access to TeraGo's Network Operations Center ("NOC") and web portal access to create, view, respond and manage any trouble tickets. Additionally, if issues are detected, TeraGo's systems will automatically trigger email notifications and send alerts to the NOC team to be addressed.

This service includes:

- Preconfiguring virtual machines with vCPU, RAM and base storage OR allocation of vCPU, RAM and base storage for self-service virtual machine management.
- VMware Enterprise Plus Edition.
- Installation, troubleshooting and reinstallation of the Operating System selected.
  Note:
  - A detailed list of supported operating systems is available here: https://www.vmware.com/resources/compatibility/pdf/VMware_GOS_Compatibility_Guide.pdf
  - Clients may provide a custom OVF image.
  - Windows or RedHat Operating System licenses are available for an additional charge.
  - Client may supply, install and support their own Operating Systems upon approval
- Operational support for Virtual Machines (VMs).
- Parameter configuration for VMs or logical partitions with assistance from the client 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.
- Managed Network Service.
- Managed Security Patching Service.

TeraGo's Network Operations Center ("NOC") provides the following support:

- 7x24x365 availability to respond to client calls and trouble tickets.
- Proactive monitoring of security, fire detection, cooling and electrical systems of TeraGo's Kelowna and Mississauga data centers.

2.2 Managed Core Monitoring Service

With the Managed Core Monitoring service, TeraGo will ensure client systems are healthy by constantly monitoring for anomalies. The performance and availability of a client's servers, on a per VM (virtual machine) basis will be monitored around the clock by TeraGo. TeraGo will detect and resolve potential issues that may impact performance 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 client VMs.

Included in this service are:

- Coordination with the client to establish and configure appropriate monitoring thresholds.
- Installation and configuration of monitoring agents as required.
- Automatic ticket creation and proactive electronic client notification for detected hardware and resource limit alerts.
- TeraGo initiated critical "call-out" notification of up to five (5) client supplied contacts for Severity 1 issues (as defined by a service being "hard" down or a critical impact to a client's business operation with no possible workarounds for the client, its users, or the service provider).
- Assignment of any reasonable number of users and privileges on a per account basis. User privileges include: create tickets, read tickets, read and post to tickets, and full user admin.
- Portal view of internet transfer and power utilization amounts (when applicable).
- Portal view of general account details, assigned IPs, and manage server canonical name.

Client responsibilities:

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

Assumptions

TeraGo does not provide a consumption-based cloud, i.e. the client is responsible for requesting additional resources based upon capacity management recommendations.

2.3 Dedicated Private Cloud

TeraGo's Dedicated Private Cloud is designed to meet the demanding needs of resource intensive cloud workloads or of applications requiring secure single-tenant infrastructure. Powered by enterprise grade hardware from Cisco Systems and VMware's leading virtualization technology, TeraGo's dedicated private cloud solution provides clients with complete flexibility to assign compute resources to the various workloads. Additionally, clients can create/remove VMs and create private networks as desired. A dedicated private cloud means the underlying cloud hardware is dedicated to the client's workloads and is not being shared with other users, i.e. no resource bottlenecks, no noisy neighbors.
TeraGo will manage the hardware infrastructure and the hypervisor software (patching, monitoring, etc.) and provide a 99.99% SLA.

Clients are also provided with access to TeraGo's Network Operations Center ("NOC") and web portal access to create, view, respond and manage any trouble tickets. Additionally, if issues are detected, TeraGo's systems will automatically trigger email notifications and send alerts to the NOC team to be addressed.

2.3.1 Product benefits include:

- Dedicated computing resources for resource intensive application.
- Consistent performance for all workloads (no 'noisy neighbors' sharing the same cloud infrastructure).
- Stringent security and compliance requirements.
- Allocation of processor and memory resource to VMs.
- Establishment of minimum, maximum and proportional resource shares for CPU, memory, disk and network bandwidth.
- Dynamic resource allocations, even while VMs are running.
- Unlimited number of VMs.
- Inclusion of VMware NSX.
- Internet connectivity at 200Mbps.

TeraGo's Network Operations Center ("NOC") provides the following support:

- 7x24x365 availability to respond to client calls and trouble tickets.
- Proactive monitoring of security, fire detection, cooling and electrical systems of TeraGo's Kelowna and Mississauga data centers.

2.3.2 Product features

Feature	Benefits
Trusted Platform	VMware vSphere platform, one of the industry's most trusted virtualization stacks enables you to create and manage your own cloud environment quickly and easily. TeraGo is a VMware Gold Partner.
Full control over resource pools	Full access to vCenter environment allows the creation of virtual machines based on unique resource needs.
Dedicated infrastructure	Single tenant dedicated environment powered by industry leading Cisco hardware.
Hybrid IT platform	Seamless integration with TeraGo's multi-tenant public cloud, colocation and connectivity services.
NSX	Provides logical network components to connected workloads—logical switches, routers, firewalls, load balancers, VPNs and more…
Security & Compliance	TeraGo's facilities are SOC 2 Type I and II compliant. TeraGo is PIPEDA compliant and can also help clients achieve other compliance requirements such as PCI-DSS, HIPAA, etc.

Included in this service:

- Provisioning private cloud infrastructure with TeraGo best practices.
- Client access to a vSphere environment (vCenter access).
- A preconfigured network topology.
- Management and monitoring of compute and underlying hardware.
- Multi-Path 10Gbps network connectivity between server hardware components and storage.

Client's Responsibilities:

- Creation and management of virtual machines.
- Management of applications and workloads.
- Manage firewall rules (for NSX).

Optional Managed Services are available to the client for configuring and managing Guest VMs, operating system images and licenses, and installed software applications.

2.4 Managed Private Cloud Monitoring Service

With the Managed Private Cloud Monitoring service, TeraGo will ensure client systems on a *per node* basis are healthy and performing optimally by constantly monitoring for anomalies. TeraGo will detect and resolve potential infrastructure issues that may degrade system performance thereby minimizing any business disruptions.

Included in this service are:

- Coordination with the client to establish and configure appropriate monitoring thresholds.
- Automatic ticket creation and proactive electronic client notification for detected hardware and resource limit alerts.
- Assignment of any reasonable number of users and privileges on a per account basis. User privileges include: create tickets, read tickets, read and post to tickets, and full user admin.
- Portal view of internet transfer and power utilization amounts (when applicable).
- Portal view of general account details, assigned IPs, and manage server canonical name.
- Service Provider initiated critical “call-out” notification of up to five (5) client supplied contacts for Severity 1 issues (as defined by a service being "hard" down or a critical impact to a client's business operation with no possible workarounds for the client, its users, or the service provider).

Client responsibilities:

- Support or management of the Operating System including patching.
- Application management and trouble shooting, including client provided software.

Assumptions

TeraGo is not providing a consumption-based cloud, i.e. the client is responsible for requesting additional hardware based upon capacity management recommendations.

2.5 Managed Security Patching Service

Managed Security Patching is an infrastructure service whereby management tasks such as hardware and hypervisor updates are proactively conducted by TeraGo. All updates are thoroughly tested before being pushed live. This ensures that systems are not being left vulnerable or compromised to any new security threats.

Included in this service are:

- Hardware resource component maintenance and repairs.
- Updates to BIOS/Firmware for hardware infrastructure.
- Applies to all hosted servers/nodes (not virtual machines).

Client responsibilities:

- Support or management of Operating System including patching.
- Application management and troubleshooting (above the operating system), including any client provided software.

2.6 Managed Network Service

With the Managed Network service, TeraGo will manage, monitor and troubleshoot the underlying network infrastructure as it relates to the client's allocated resources, to achieve and exceed all SLAs. At the core of this service, TeraGo will monitor:

- Network availability / uptime – availability of systems at all time.
- Network utilization – real-time traffic monitoring and alerting.
- Management and provisioning of network infrastructure.

2.7 Managed OS Patching

OS Patch management is a service whereby TeraGo monitors for and applies critical OS patches. Clients receive tailored automated alerting and reporting features via the TeraGo Client Service Center (CSC).

Included in this service are:

- Recommendation of operating system updates and configuration modification with client concurrence to apply update.
- Minor upgrades to the server operating system, which includes service packs, minor version upgrades.
- Critical operating system patch updates, including security and integrity patches as required and agreed to by the client.
- Schedule maintenance window proactively.
- TeraGo will work with all parties involved to select a preliminary environment within the CP solution to patch first. Upon confirmation of success, patching in further environments will be scheduled.
- Rollback of failed or impacting patches.
- Patching reports.

Client responsibilities:

- Application management and troubleshooting, including client provided software.

Assumptions

- Client will validate application functionality post-patch rollout.
- Client will request any patch rollbacks.

2.8 Managed Firewall Service

Perimeter security is of the utmost importance in any cloud solution. TeraGo's Managed Firewall service leverages TeraGo's 24/7 Network Operations Team to monitor and manage the client's perimeter device. As part of this service, TeraGo specialists will monitor the device for issues and events, and configure the appliance based on vendor best practices.

TeraGo offers either a multi-tenant (hardware) device from Fortigate, or the option to select one of four virtual (software) devices from amongst the Cisco ASAv50 series as well as NSX Edge from VMware.

2.8.1 Hardware Firewall

The capabilities of the Fortigate firewall are as follows:

Capability	Specification
Virtual (Software) / 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

2.8.2 Software Firewall – Cisco ASAv

Cisco Adaptive Security Virtual Appliance (ASAv) 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. The Adaptive Security Virtual Appliance is a single-tenant device that runs as a virtual machine inside the hypervisor in a virtual host managed environment.

The capabilities of Cisco's ASAv products are as follows:

Feature	**ASAv5**	**ASAv10**	**ASAv30**	**ASAv50**
Stateful inspection throughput (maximum)[1]	100 Mbps	1 Gbps	2 Gbps	10 Gbps
Stateful inspection throughput (multiprotocol)[2]	50 Mbps	500 Mbps	1 Gbps	5 Gbps
Advanced Encryption Standard (AES) VPN throughput[3]	30 Mbps	125 Mbps	1 Gbps	3 Gbps
Connections per second	8,000	20,000	60,000	120,000
Concurrent sessions	50,000	100,000	500,000	2,000,000
IPsec VPN peers	50	250	750	10,000
Cisco AnyConnect® or clientless VPN user sessions	50	250	750	10,000
Modes	Routed and transparent			
Virtual CPUs	1	1	4	8
Memory	1 GB minimum 1.5 GB maximum	2 GB	2 GB	16 GB
Minimum disk storage[4]	8 GB	8 GB	16 GB	16 GB

2.8.3 Software Firewall – VMware NSX Edge

NSX Edge provides network edge security and gateway services to isolate a virtualized network. The NSX Edge gateway connects isolated, stub networks to shared (uplink) networks by providing common gateway services such as DHCP, VPN, NAT, dynamic routing, and Load Balancing. Common deployments of NSX Edge include in the DMZ, VPN Extranets, and multi-tenant Cloud environments where the NSX Edge creates virtual boundaries for each tenant.

NSX Edge Services	
Dynamic Routing	Provides the necessary forwarding information between layer 2 broadcast domains, thereby allowing you to decrease layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to where the workloads reside for doing East-West routing. This allows more direct virtual machine to virtual machine communication without the costly or timely need to extend hops. At the same time, NSX also provides North-South connectivity, thereby enabling tenants to access public networks.
Firewall	Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for all protocols.
Network Address Translation	Separate controls for Source and Destination IP addresses, as well as port translation.
Dynamic Host Configuration Protocol (DHCP)	Configuration of IP pools, gateways, DNS servers, and search domains.
Site-to-Site Virtual Private Network (VPN)	Uses standardized IPsec protocol settings to interoperate with all major VPN vendors.
L2 VPN	Provides the ability to stretch your L2 network.
SSL VPN-Plus	SSL VPN-Plus enables remote users to connect securely to private networks behind a NSX Edge gateway.
Load Balancing	Simple and dynamically configurable virtual IP addresses and server groups.
High Availability	High availability ensures an active NSX Edge on the network in case the primary NSX Edge virtual machine is unavailable.

NSX Edge supports syslog export for all services to remote servers.

Note that TeraGo currently offers NSX Edge in the large size but upon request can offer the other sizes.

NSX Edge (Large)	
vCPU	2
Memory	1GB
Disk	512MB
Interfaces	10
Sub Interfaces (Trunk)	200
NAT Rules	2000
FW Rules	2000
FW Performance	9.7Gbps

DHCP Pools	25
Static Routes	2048
LB Pools	64
LB Virtual Servers	64
LB Server / Pool	32
IPSec Tunnels	1600
SSLVPN Tunnels	100
Concurrent Sessions	1,000,000
Sessions/Second	50,000
LB Throughput L7 Proxy)	2.2Gbps
LB Throughput L4 Mode)	6Gbps
LB Connections/s (L7 Proxy)	46,000
LB Concurrent Connections (L7 Proxy)	8,000
LB Connections/s (L4 Mode)	50,000
LB Concurrent Connections (L4 Mode)	600,000
BGP Routes	50,000
BGP Neighbors	20
BGP Routes Redistributed	No Limit
OSPF Routes	50,000
OSPF Adjacencies	20
OSPF Routes Redistributed	5000
Total Routes	50,000

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

- 24x7 up/down device status monitoring.
- Troubleshooting issues related to client defined settings applied to firewall rule sets.
- Testing of firewall rule set changes to be implemented.
- Creation and enablement of virtual firewall and portal access.
- Management of underlying technology and related configuration.
- Managed support including updates and patches of the OS or firmware, and device monitoring and interface monitoring.
- Security updates for vendor disclosed vulnerabilities and workaround solutions where no patches are available.
- Base configuration and implementation of devices.
- Management of licensing and warranty.
- Proactive support ticket creation.
- Apply updates from vendor for IDS/IPS patterns and rules, in-line Anti-Virus, Anti-Spam and Spyware definitions (if applicable).

- Modify firewall rule-set as directed by client. Limited to twelve (12) rule set changes per year. Client to provide specific rule-set change criteria. Rule-set change is any requested change to the configuration. Changes are implemented within 24 to 72 hours generally.
- *Further* rule changes can be made at an additional cost after the environment has achieved "steady state".
- 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:
        - Trouble-shooting information to authorized technicians and respondents for trouble-shooting, repair and/or replacement of failed firewall appliances.
        - 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.

Client responsibilities:

- Firewall rule set base definition.
- Change requests to custom firewall rulesets; must provide specific rule-set change criteria. Limited to twelve (12) rule set changes per year.
- IPS/IDS rule management (for hardware firewall).
- Client premise VPN configuration setup and changes.

2.9 Managed High-Availability Service

High Availability (HA) is critically important if you need a reliable and fault-tolerant system in the cloud that delivers optimal performance and guaranteed uptimes. Especially if your business operates around the clock, you want to ensure your client experience is not negatively impacted in anyway. Therefore, a high availability architecture becomes a fundamental requirement to deliver optimal customer experiences and maximizing revenue potential of your organization.

2.9.1 Load Balancers

Load balancers distribute incoming network traffic across multiple hosts at throughput increments of 100mbits/sec. 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
- Throughput increments of 100mbits/sec
- 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. Clients 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 in this service:

- Initial environment creation.
- Creation and enablement of Load Balancer device or context.
- Underlying load balancer infrastructure management and maintenance.
- Management and Creation of Load Balancer Virtual Servers.
- Management of underlying technology, firmware/software and warranty.
- Management and provisioning of underlying network infrastructure, including private VLAN to client's virtual or physical infrastructure.
- Security group and policy configuration.
- 24x7x365 environment monitoring and management.
- 24/7 Service Desk to support client reported incidents.

Client responsibilities:

- 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.
- Management of client data.
- Requesting configuration changes through the TeraGo Client Service Center.

2.10 Managed Backup & Restore

TeraGo offers clients the opportunity to backup both hosted virtual machines or on-premise physical servers/workstations. Each Virtual Machine is pre-configured by TeraGo by default to be backed up daily with the last 6 restore points available for restoration.

Backups are delivered using the award-winning Veeam suite of tools. This service provides fast, flexible and reliable recovery of virtualized applications and data, both on-premise and in TeraGo's cloud.

The detailed Service Level Agreements (SLA) is available on-line at https://terago.ca/company/legal/.

2.10.1 Hosted Virtual Machine Backup

Hosted Virtual Machine Backup offers multiple backup options to meet your needs including both image and file level backups. Advanced features such 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 & Replication software.

Included in this service are:

- Backup management portal to enable self-service and TeraGo managed restores.
- A single restore operator role that allows access to backups and restoration options, with the ability to control permissions.
- System administration and operational support for backup and restore technology, and standard provided configurations. Also included is management of underlying virtualization and operating system software for host server(s).
- Troubleshooting and technical support for all backups and restore operations.
- Last 6 restore points are available for restoration.
- Management and updates to backup infrastructure, software, and service components as necessary and at the sole discretion of TeraGo.
- Maximum of three (3) Custom Directory and/or File Exclusions per VM.
- Review and troubleshooting of failed backups with basic assistance to configure file-level restore (upon client ticket request only).
- Off-site backups that are replicated to an alternate cloud site that is geographically diverse from the primary backup location.
- Creating and assigning valid backup jobs.
- Notification, alerting and resolution of failed backups.

Client responsibilities:

- Procuring required software licenses (available through TeraGo).
- Capacity planning and purchase of additional backup storage space as required.
- Ensuring the accuracy of any exclusions.
- Testing of restored data/VMs.

2.10.2 On-Premise Physical Machine Backup

TeraGo provides an agent-based backup solution for on-premise virtual and physical servers/workstations, creating snap shots in TeraGo's geographically diverse Cloud Connect repository. Veeam Agents (End-Point Backups) enable efficient and secure backup to offsite locations using industry leading technology.

Included in this service are:

- 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.
- Clients 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.
- Creation and management of backup schedules.

Client responsibilities:

- Procuring required software licenses (available through TeraGo).
- Installing Veeam agents to client's on-premise servers or workstations.
- Determine backup rules and schedules in collaboration with TeraGo.

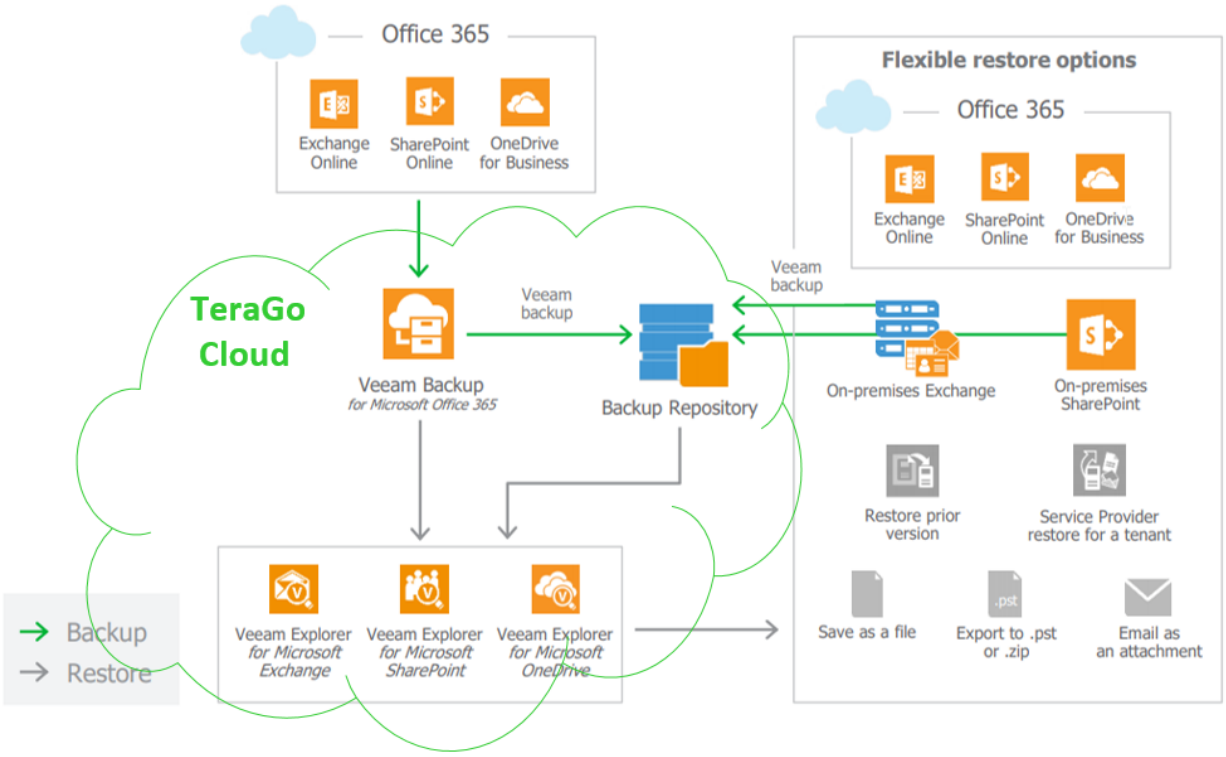
Operating systems supported include:

- Windows
- Linux
- IBM AIX
- Oracle Solaris

2.11 Managed Microsoft O365 Backup

TeraGo provides and manages offsite backup of SharePoint, OneDrive, MS Teams and O365 data - specifically email, contacts, and calendar items at an individual level. As depicted below, TeraGo can restore mailbox items:

- directly back to O365
- to an on-premise Exchange server
- to an email attachment
- to a file
- to a PST file



Included in this service:

- Storage of Office 365 data (email, contacts, calendar), OneDrive and SharePoint data in a secure offsite storage (within TeraGo Cloud) and separated from Microsoft's platform.
- Long term and unlimited retention of data.
- Restoration of data to its full and original state – including folder structures, categories, and more;
    - data includes email, contact, OneDrive and SharePoint files.
    - up to 2 restores / user / year
- Enablement of scheduled and on-demand backup.
- Quick search and recovery of individual mailbox items residing in archived Office 365 content.
- Recovery directly back to Office 365, on-prem Exchange Server, email attachment, file, or .pst file.
- Alert notification of storage nearing capacity threshold.
- Management of Veeam O365 Backup licenses.
- Monitoring and ensuring software is running optimally.
    - includes patching and installing latest updates.

Client responsibilities:

- Veeam Backup for Microsoft O365 license (available separately).
- Defining retention period, and backup schedule.
- Requesting on-demand backup.
- Requesting recovery of any 0365 data.
- Capacity planning and purchase of additional backup storage space should more storage be required
- Management of MS Office 365 environment.

TeraGo currently supports Veeam Backup for MS O365 v3.

2.12 Managed Resiliency / Disaster Recovery as a Service (DRaaS)

To support your critical business functions against any disruption caused by unplanned events, such as natural disasters, ransomware attacks, server crashes or just simply maintenance updates, a good IT resiliency strategy is essential and should be part of the overall business continuity plan. The benefits include minimal disruption to business operations, preventing impacts to revenue, and retaining a good client experience amongst other things.

For businesses whose virtual IT infrastructure resides *on-premise*, within *TeraGo's cloud*, AWS, or *Azure* TeraGo provides managed resiliency (DRaaS) for the following use-cases:

Production site / *Recovery site options*	*TGO Data Center*	*Azure*	*AWS*
TGO Data Center	✓	✓	✓
Client's on-prem	✓	✓	✓
AWS	✓		✓
Azure	✓	✓	

Fully managed DRaaS enables 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.

Included in this service:

Solution Design – Determination and documentation of all solution design aspects including infrastructure, network & storage requirements and key replication/recovery software utilized within the DR solution. Client 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 & client IT.
- Failover steps – activation of the DR plan.
- Workload failback steps.
- TeraGo support information including escalation steps.
- Recovery Time and Recovery Point Objectives (RPO/RTO).

Implementation - Deployment of disaster recovery solution as determined within the 'Solution Design' step above, as well as provisioning of necessary system administration and operational support for:

- Disaster recovery software & underlying virtualization technologies
- Storage, network and firewall configurations

Initial failover & failback testing is to be conducted within 30 days of solution implementation. For every subsequent year, one additional failover & failback test is included at no extra charge. Note that DR tests will run within a period of 30 days or less.

Monitoring & Recovery - Recovery of client workload upon disaster declaration. This includes:

- Monitoring of client workloads for scheduled replication tasks.
- Ensuring replication activities meet recovery point objectives.
- Failing-over client workloads (as described in the runbook) in case of disaster. declaration and within predefined RTOs.
- Completing failback of client workloads once primary location is available.

Maintenance & Testing - includes:

- Disaster Recovery test in conjunction with client's IT staff. Client is to notify TeraGo 90 days in advance of desired DR test date. As described previously, one instance of a managed DR test is included per calendar year at no extra charge.
- Technical support and troubleshooting for all disaster recovery related software and hardware components, including firewalls, DRaaS software and hypervisor layer.
- Quarterly maintenance of DR runbooks capturing any changes or updates required due to software, infrastructure or personnel changes.

Client responsibilities:

- Procuring required software licenses (available through TeraGo).
- Declaration of an outage scenario. Confirmation that workloads are required to be brought online at secondary (DR) site.
- Management, monitoring & technical support for software applications installed *within* guest VMs.
- Advising TeraGo of updates or changes to systems/applications/configurations, etc., via ticketing system.

Detailed SLAs with regards to this service are available in TeraGo's Service Level Agreements (SLA) available on-line at https://terago.ca/company/legal/.

Additional DR Tests

Additional DR tests can be purchased per virtual machine (VM) and are executed on a per availability group (i.e. group of VMs). DR tests are performed according to the most current runbooks as maintained by TeraGo. Execution reports will be provided by TeraGo and will outline the actual RTOs and RPO, with potential remedies proposed.

2.13 Managed SQL Patching

Microsoft SQL Patch management is an optional service whereby MSSQL application patching is conducted by TeraGo. This approach allows clients to focus on their core competencies and their business. Clients 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 client (e.g. 2012, 2012 R2, 2016).
- Proactive notification of patches and requesting of maintenance windows.
- Evaluation of planned changes to the server environment and advise client of any requirements to support such changes.

Client responsibilities:

- Procuring required software licenses (available through TeraGo).
- Application management and troubleshooting, including client provided software.
- Database and information management and troubleshooting.
- Database content management and periodic data backup.

2.14 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 anti-malware & web reputation to active virtual workloads on VMware's vCloud Enterprise infrastructure.

Included in this service are:

- 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.
- In-guest agent installation and troubleshooting.
- 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.

Client responsibilities:

- Custom Lists (Directory, File Extension, File, IP, MAC and Port lists).
- Custom Policies.
- Automated Notification and Alerting.

2.15 Standard Monthly Reporting

After all resources are provisioned and operational, it becomes crucial to ascertain the usage levels to ensure all resources are functional and running optimally. These reports provide insights into:

- CPU utilization.
- Memory utilization.
- Number and type of storage, and the amount utilized in GB.
- Network utilization.

Included in this service:

- 24/7 Service Desk to support client reported incidents.

2.16 Advanced Monthly Reporting

TeraGo's Advanced Monthly Reporting provides a dedicated account support manager to be the liaison between TeraGo and the client. As part of this service, a TeraGo Specialist will gather best practices and recommendations pertaining to your TeraGo Cloud environment.

A TeraGo specialist will gather the appropriate information and organize it in a readable format. These advanced reports will be delivered to you in an email on a monthly cadence. A follow up meeting may be scheduled to discuss the report content and document any resulting actions.

2.16.1 Reports

- Cloud Capacity Report: describes the current cloud utilization, and provides recommendations based on the last 30 days of growth in memory, CPU and network.
- VM's CPU/IOPs/Memory Report: a 30-day list view report of the performance of the virtual machines on the cloud.
- Network Traffic Report: Network utilization of the environment and VMs.

Included in this service:

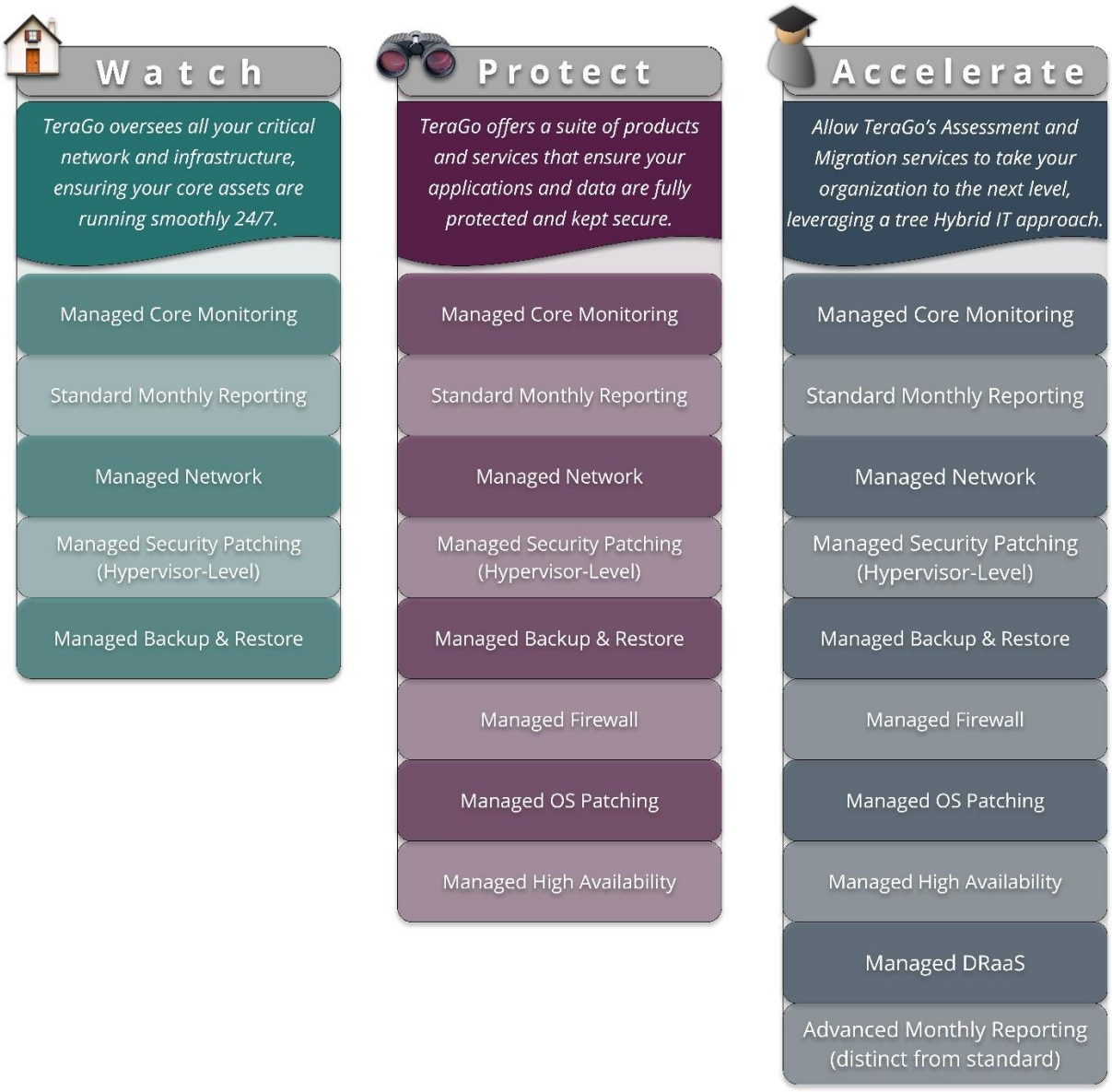
- Monthly reports as stated above.
- Walkthrough of the reports on monthly cadence.

Client Responsibilities:

- Contact the assigned TeraGo specialist and request details of a particular report.

2.17 Managed Services – Packages

TeraGo's Managed Services are available in one of three packages to help deliver a collective value of services that address escalating needs at reduced price-points. Watch, Protect and Accelerate packages have been designed to provide the best value for a defined set of requirements aimed at alleviating your burden on infrastructure maintenance and letting you focus on your core business services.



3 Enterprise Cloud Storage

Enterprise Cloud Storage is delivered using highly reliable and performing persistent data stores. To keep data secure and private, TeraGo's storage services do not have a data collection nor any data processing components. Four types of storage are offered; these are targeted at archiving, development, production, and disaster recovery workloads that vary in terms of performance. The types of storage available are:

1. Provisioned IOPS Storage.
2. Block Storage.
3. Object Storage.
4. Archival Storage.

3.1 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, 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. This tier is securely presented to private cloud environments and suitable for customers requiring guaranteed IOPS for their application requirements. Provisioned IOPS storage is encrypted using state-of-the-art technology.
Ideal use cases include virtual machines running heavy workloads such as database applications or ERP systems.

3.2 Block Storage

Block storage service utilizes SAS disk with a read and write caching layer for improved performance. Block Storage can also be provisioned as utilizing a file gateway to provide an 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.
Block storage is most suitable for mid-level I/O workloads. Most operating systems and applications are recommended for this storage service.

3.3 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. 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. Object Storage is currently available only in TeraGo's western data center.
It is ideal for low I/O web and mobile applications as well as backup storage.

3.4 Archival Storage

Archival Storage is a cost-effective solution for adding to the clients dedicated storage within TeraGo's Cloud ecosystem. Archive storage can be presented as NFS or SMB and is delivered on SATA disk infrastructure for quick access. **This storage type is designed for infrequent access type data and archival storage for files, images, or VM templates.**

3.5 Storage Inclusions / Exclusions

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.

Client responsibilities:

- Management of proprietary data.
- Requesting any configuration changes through TeraGo's ticketing system.

4 Data Centres

TeraGo offers colocation services in its datacenter facilities at the following 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. TeraGo data centre facilities are certified to be Service Organization Controls 2 AT 101 SOC 2 compliant.

4.1 Mississauga, ON

As TeraGo's flagship facility in Eastern Canada, 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 from 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.

Mississauga 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)

4.2 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.

Kelowna 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)

4.3 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.

Vancouver Vault 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)

4.4 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.

Vaughan 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)

5 Colocation Services

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

5.1 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).

5.2 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 is subject to additional overage hourly charges as consumed.

5.3 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 amongst other approved individuals.

To request a new or replacement access card, the individual must complete the Facility Access Control Form and submit it to the 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.

5.4 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.

5.5 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.

6 Connectivity Services

6.1 Internet and Private Networks

6.1.1 Network

TeraGo combines high speed wireless networks with a Canada wide fiber optic network to provide businesses with secure, reliable and scalable Internet and Private Networking solutions. TeraGo's network supports connectivity speeds up to 10 Gbps across a variety of access mediums, including licensed and unlicensed wireless, fiber, cable and DSL.

6.1.2 Private Line Services

TeraGo's Private Line Services allow business customers to connect sites together leveraging Layer 2, Ethernet connections. TeraGo can support point-to-point, point-to-multipoint and bridged Ethernet topologies with dedicated bandwidth speeds up to 10Gbps. Private Line Services provide secure, low latency connections - ideal for companies with multiple offices, large interoffice data requirements or connections to data centers.

6.1.3 Internet Services

TeraGo provides scalable, business grade Internet services with speeds up to 1000 Mbps. To enhance reliability and performance, TeraGo maintains diverse peering arrangements with multiple tier-one carriers across Canada. All TeraGo Internet services are provisioned with dedicated, symmetrical, bandwidths and static IPs.

6.1.4 Data Center Connectivity

TeraGo Data Centers are fully integrated with the TeraGo national network. Businesses with TeraGo cloud or colocation services can seamlessly connect leveraging TeraGo's Internet and Private Line Services.

TeraGo Data Centers are also carrier-neutral facilities, with fully-redundant diverse fiber cores fed from multiple connectivity providers.

6.1.5 TeraGo Cloud Connect

TeraGo Cloud Connect provides customers with secure, private connectivity to AWS Direct Connect and Microsoft Azure ExpressRoute. TeraGo Cloud Connect supports connections from customer-owned facilities, third-party facilities, customers collocated in TeraGo's Data Centers or customers leveraging TeraGo's Cloud services. TeraGo Cloud Connect is provided as a Layer 2, Ethernet connection with available bandwidths from 50Mbps to 10Gbps. TeraGo Cloud Connect from customer-owned or third-party facilities will only be supported across fiber or TeraGo provided wireless connectivity.

6.1.6 IP Addresses

All TeraGo Internet services are provisioned with a public /30 subnet. TeraGo can allocate additional public IP addresses, subject to the customer meeting ARIN requirements. TeraGo will make reasonable

efforts to allocate public IP addresses to customers on contiguous subnets, following standard IP subnet allocation methodologies.

Private IP addresses assigned by TeraGo cannot be viewed and are not routable outside the customer's Private network (i.e., they cannot be viewed and are not routable on the Internet, or on other Private networks). Private IP addresses may be allocated on subnets that are not contiguous with prior allocations. TeraGo will retain ownership of all Private IP addresses allocated to the customer. Customers may not allocate IP addresses to other parties or customers without TeraGo's written consent.

6.1.7 Dedicated Bandwidth

All TeraGo Private Line and Internet services are provisioned with a dedicated bandwidth. Dedicated bandwidth means that a customer's service is guaranteed a specific bandwidth or speed (in Mbps) through the TeraGo network. The customer's service is also capped at the dedicated bandwidth, meaning that the customer's service cannot exceed the dedicated bandwidth or speed through the TeraGo network.

6.1.8 Symmetrical Speeds

All TeraGo Internet and Private Line services are symmetrical. Symmetrical means that the average bandwidth or speed of the service (in Mbps) will be the same in both the Incoming and Outgoing directions.

6.1.9 Full Duplex Service

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

6.1.10 DNS Services

TeraGo provides fast, highly-reliable recursive DNS services for business customers. Fully compliant with IETF DNS standards, TeraGo's DNS servers are optimized to provide fast and accurate responses. TeraGo DNS servers are highly secure, employing DNS Security Extensions (DNSSEC) to help guarantee the authenticity of the responses it receives from other nameservers and prevent cache poisoning attacks and employing a variety of best security-practices to protect against DDoS attacks.

TeraGo DNS services are available through the following IP addresses:

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

6.2 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 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

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

7 Voice Services

With dedicated IT and networking professionals, TeraGo has been providing enhanced business voice solutions since 2010, servicing organizations of all sizes regardless of complexities or technical limitations.

TeraGo's geographically diverse platform offers:

- 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.

7.1 LAN / WAN Requirements

As TeraGo services are standards compliant, they are not dependent upon any specific LAN or WAN manufacturers products. TeraGo will provide best practice recommendations based on collaborative discussions for network design.

7.2 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.

7.2.1 Inclusions and Exclusions

The Service includes 9-1-1 emergency service, but will not work in the following situations:

- Power outage.
- Broadband service outage.
- An interruption or slow-down, or other service interruption or problem with the relevant computer apparatus.

Customers may be required to reset or reconfigure their phone equipment, as the case may be, prior to utilizing the Service following any of the above scenarios.

Not supported in the Service are:

- 900/976 calling i.e. customers will not be able to make 900 calls.
- Collect calling.
- Operator services (dialing 0).
- A telephone directory.

Assumptions

The Service will only work with a high-speed Internet connection and the quality may fluctuate according to:

- upload/downloads speeds.
- service level of the high-speed Internet connection.
- other factors/third party service providers extraneous to TeraGo.

7.2.2 9-1-1 VoIP Service Conditions and Limitations

TeraGo utilizes 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 have certain limitations as 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 who 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, the 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 the 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 the Service is suspended or terminated.
- The Customer understands the 9-1-1 limitations as described above and the Customer acknowledges that it is their obligation to make all other Users, or potential Users, of the Service aware of these limitations.