egenera | xterity cloud services

SERVICE DESCRIPTION - Premier DRaaS

Leverage Xterity Premier Disaster Recovery-as-a-Service (P-DRaaS) to provide your clients a critical component of a comprehensive business continuity strategy.

Xterity Disaster Recovery Services: Premier Disaster Recovery as a Service (P-DRaaS)

The intended audience for this document includes all Xterity channel partners, including but not limited to businesses typically referred to as:

- Managed Service Providers
- Technology / Service Resellers
- Technology / Service Distributors

All the business types mentioned above are referred to as "partner" or "partners." The end users, consumers, or beneficiaries of a service originating from Xterity are referred to as "client(s)" or "partner's client(s)."

The term "server" is meant to encompass any number of servers. The use of "server" implies one or more servers.

The term "desktop" is meant to encompass any number of traditional end user personal computer devices such as desktops, towers, and laptops.

All references to "end user devices" implies traditional personal computer devices such as desktops, towers, and laptops. Mobile devices (e.g. smartphones, tablets etc.) are not currently supported with the services referenced in this service description document.

To meet the needs of businesses requiring business continuity protection the following Xterity Business Continuity Cloud Services are available:

- Premier Business Continuity Services for servers:
  - Premier Disaster Recovery as a Service **(P-DRaaS)**
  - Premier Backup as a Service **(P-BaaS)**[1]

- Essential Business Continuity Services for servers and end user devices:
  - Essential Backup as a Service **(E-BaaS)**[1]

This document specifically pertains to the P-DRaaS service.

[1] The Backup as a Service (BaaS) products (E-BaaS and P-BaaS) mentioned above are described in detail in the Xterity Backup Services service description document.

The terms On Cloud and Off Cloud are used to represent the scenarios described below, and are depicted in the diagram.

- **ON Cloud:** Services that are operational within, and between Xterity cloud platforms. Both the source and recovery resources reside within Xterity datacenter locations.

- **OFF Cloud (Hybrid):** Services that are operational between an Xterity cloud, and any other infrastructure platform. The source resource is not located within an Xterity cloud but the recovery (target) resource is.

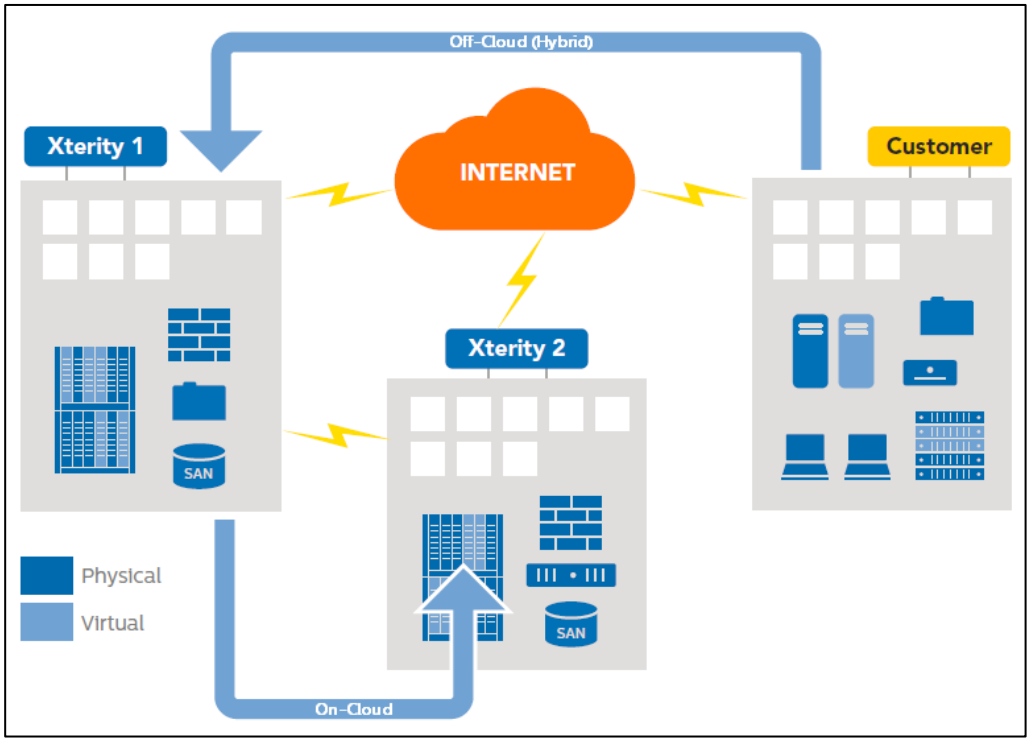


Table of Contents

P-DRaaS description

Xterity P-DRaaS provides protection for physical and virtual **servers** to ensure that in the event a protected server becomes inaccessible at a primary (source) location**, the server can be recovered and made accessible in an Xterity (target) datacenter** while the primary location or server is off line.

Xterity P-DRaaS uses storage device (block/disk/LUN) backup technologies, highly available hardware platforms, and Tier 3 / 3+ datacenters to ensure that server recovery can be accomplished at any time. Xterity P-DRaaS enables partners to provide disaster recovery support for their client's servers without the need to duplicate hardware, software, licenses or develop skills for disaster recovery configuration or management processes. Xterity P-DRaaS configures, maintains and monitors the DRaaS environment 24x7x365 to ensure it is ready to perform server recovery procedures when needed.

Utilizing server-based (agent) software provided by Xterity, partners can specify which servers are to be protected. Xterity P-DRaaS is a constant data protection (CDP) service maintaining full backup of identified servers constantly. Xterity P-DRaaS delivers a 4-hour Recovery Time Objective (RTO)[2] and can provide Recovery Point Objectives (RPO)[2] as short as 15 minutes, depending on the network connectivity selected between the primary (source) location and the chosen Xterity (target) datacenter.

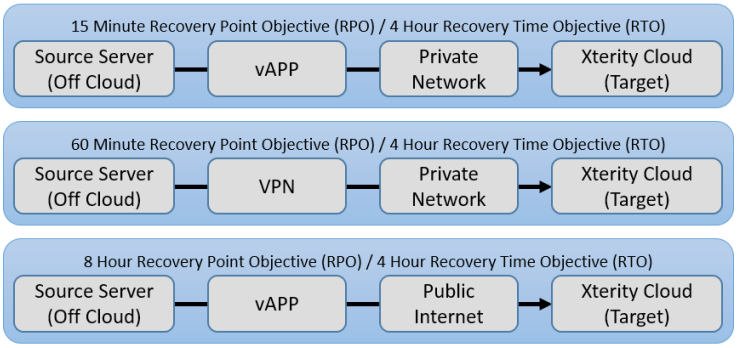
Xterity P-DRaaS supports two disaster recovery models: On Cloud and Off Cloud

- **ON Cloud:** Services that are operational within, and between Xterity cloud platforms. Both the source and recovery servers reside within Xterity clouds.

- **OFF Cloud (Hybrid):** Services that are operational between an Xterity cloud platform, and any other infrastructure platform. The source server is not located within an Xterity cloud but the recovery (target) server is.

For Off Cloud P-DRaaS there are (source) server configuration choices required for compatibility and performance reasons:

Source Servers: Off Cloud



For **off-cloud** environments with available hypervisor (VMware, Hyper-V, XenServer) cluster resources: A virtual appliance (vAPP) configuration is available that includes WAN optimization and utilization of secure sockets layer (SSL) connectivity over public networks resulting in simple network connectivity, and performance levels that support an 8 hour RPO at economical network costs. The vAPP configuration is also compatible with private network connectivity for the highest performance, and is capable of delivering an RPO of 15 minutes.

[2] Please refer to the FAQ and definitions sections of this document for additional RPO and RTO details.

Off-Cloud P-DRaaS features & requirements:

	Off-Cloud P-DRaaS with vAPP
Agents	Agent installed on all physical or virtual (VM) servers to be protected
Fully managed and monitored	Yes, with alerts and notifications 24x7x365
WAN optimization	Yes
Charges	Per GB per month of storage allocated to each protected server, plus networking charges

Technical requirements	• Virtual appliance (vApp) deployed (by partner or partner's client) on-premise, on active hypervisor (VMware, Hyper-V, XenServer) cluster
	• Partner (or partner's client) are required to have skills to administer the active hypervisor
	• 4GB RAM
	• 4 vCPU
	• 72 GB boot disk space
	• Additional storage:
	  - Minimal size of 120% of total protected space
	• 1 dedicated Public IP Address
	• Ability to modify firewall rules to allow access to the following ports:
	  - 11575-11590(tcp)
	  - 113 (tcp)
	  - 81 (tcp)
	  - 623 (tcp)
	  - 80 (tcp)
	  - 443 (tcp)
	  - ICMP
	• Internet connectivity of at least 1.5 Mbps

- For **On Cloud P-DRaaS:** A single recovery point with a dataset that is no older than 15 minutes is maintained constantly. The RPO for On Cloud (source) servers is 15 minutes, and the RTO is 4 hours.

Xterity clouds are hosted in Tier 3 / 3+ datacenters that are monitored, managed and maintained by some of the most respected, and experienced datacenter operators in the world. Xterity cloud platforms build on the availability features of these world-class datacenters to deliver a 99.99% availability service level agreement (SLA). The Xterity cloud platform extends the focus on availability by utilizing enterprise-class hardware, redundant power, networking, and management technologies. Xterity cloud recovery (target) sites are always ready to recover your client's physical and virtual servers.
After you install the Xterity DRaaS agent on each of the source servers, you then configure network connectivity. Once network connectivity is verified, Xterity cloud operations will set up your client's

specific solution with our disaster recovery technology that automates failover and failback operations. Xterity cloud operations will create jobs to manage the recovery processes to ensure rapid recovery of files, databases, systems, and entire sites.

Rapid recovery is achieved by mapping servers, applications, storage, and failover procedures from source sites to recovery sites. These processes automate the logistics involved in resuming server availability via the recovery site. With Xterity P-DRaaS, partners aren't required to have in-depth disaster recovery technical skills or expertise in order to build a reliable DR solution for their clients.

The Xterity cloud operations team will perform a trial connectivity test to ensure the basic networking parameters are correctly setup. Then, the Xterity cloud operations team will perform the initial synchronization of data and verify that the recovery point has been created successfully. Once verified, Xterity cloud operations will perform a complete end-to-end test verifying that the protection of source servers is operational. Once this occurs, Xterity cloud operations will notify you that the source servers have disaster recovery protection. Xterity DRaaS constantly monitors the solution by verifying communications with the DRaaS agent running on the source servers, and confirming that the recovery points satisfy the desired RPO.

Recovery point dataset creation processes capture all data contained in the block volume/disk/LUN for the servers selected for protection. Xterity DRaaS automatically manages recovery point dataset updates and retention, helping to optimize the service and minimize costs. You determine the location of the recovery site from a selectable list of Xterity's global cloud locations. Charges are based on the total monthly allocated storage volume in gigabytes assigned to protected (source) servers. In the event of server recovery, standard server charges will commence for any recovered server operating in the Xterity cloud for the duration that they are active in the Xterity cloud.

Xterity P-DRaaS includes 24x7x365 support. In the event of a situation that interrupts access to a primary (source) server, and requiring a recovery; your designated (authorized) representative must notify Xterity cloud operations either via the Xterity support ticketing system or direct phone call. This communication to Xterity cloud operations indicates that your designated representative is fully authorizing Xterity cloud operations to begin the recovery process. Once the recovery request is confirmed with your authorized partner representative, **the RTO clock starts**. The Xterity cloud operations team:

- Initiates the automated recovery software
- Builds a VMDK (virtual machine disk) for each server with virtual compute resources as the target
- Identifies the physical compute resource server profile for servers with physical compute resources as a target
- Provisions the server or servers

Depending on the specifications entered at DRaaS setup time the recovery servers are deployed on virtual or physical compute resources with processor, memory, network/connectivity and storage specifications that match the production (source) server.

Once a recovery server is successfully booted (Booted Server) and operating system console access is verified, the Xterity cloud operations team notifies you (partner) that the server has been recovered. This

notification indicates server recovery completion, and **the RTO clock stops.** Standard charges commence for processor, memory, storage, networking, and any other services utilized by the recovered servers. The servers are ready for the partner or client to load applications and validate the computing environment. The partner then notifies the Xterity cloud operations team that the recovery environment with applications has been validated, and all required networking modifications (e.g. DNS configurations) have been deployed to redirect their client's end users to the recovery server(s).

There is no time limit for how long the Xterity recovery site can function as the "new" primary site, however, since there may be capabilities in the (original) primary site that are not available in the recovery site, it is expected that the recovery site will be "failed back" to the original primary site. The Xterity cloud operations team will provide partner support for the failback process.

Frequently Asked Questions (FAQ):

Q: What does the recovery server use for public IP addresses?

For OFF Cloud and On Cloud DRaaS, recovered servers will have different public IP addresses than those used in production. These different public IP addresses will be assigned during the set-up process and will remain unchanged during the term of this Agreement.

Q: How is redirection of IT users handled?

Partner is responsible for any external networking management and configuration including redirection of networking names, public IP addresses, shortcuts, or other routing configurations for client compute environments.

Q: What can be recovered?

Xterity DRaaS recovers servers. The recovery point used to recover a server is a replication of the entire storage volume specified for the server. Xterity DRaaS does not recover individual files.

- For On Cloud DRaaS: A single recovery point with a dataset that is no older than 15 minutes is maintained constantly. This recovery point is used for server recovery.
- For Off Cloud DRaaS, recovery point times vary from 15 minutes (using vAPP technology with a private network), to 8 hours (using vAPP with a public network).

Q: Can I select from a list of multiple recovery points to recover a server?

Xterity DRaaS uses an intelligent Constant Data Protection (CDP) technology that enables near synchronous updating of the recovery point dataset. Rather than creating individual archived volumes, a single volume is constantly updated and provides the ability to deliver access to a recovery point no older than the specified RPO. This technology provides cost savings by minimizing the amount of storage needed to support your client's disaster recovery requirements.

Q: Does network connectivity impact the dependability, reliability or availability of the DRaaS solution?

OFF Cloud DRaaS can consume a significant amount of bandwidth between the production (source) location and the Xterity cloud. Xterity assists with this by specifying configurations available in the agents that can help control bandwidth demands. Managing the cost, performance, and priority of bandwidth used by such services in the production location is the partner's responsibility. If OFF Cloud DRaaS is being used, we strongly recommend you work with your networking teams to tune these network configuration settings along with any router or connection settings to find an optimal configuration that works efficiently for you and your client.

Q: How long does the initial data synchronization (seeding) process take to complete?

The amount of time required for initial synchronization is dependent on the amount of data to be synchronized, and network bandwidth.

To avoid potentially long initial synchronization times, the (optional) Xterity Dock Service provides a secure, efficient solution. For a one-time charge, the storage dock service allows for copying the seed data to a local media device (e.g. USB, HDD), and sending the device to Xterity cloud operations where it is loaded into Xterity cloud storage.

Q: How long will it be until my clients will be able to use their recovered server(s)?

Once a partner authorizes Xterity to initiate a recovery, Xterity will recover the specified server(s) within the 4 hour RTO. At this point you (partner) have:

- A server with an operational operating system
- Access to the dataset
- Communications for accessing the server

You or your clients can now deploy applications and workloads. Actual access time varies and is dependent on how long the application/workload deployment process takes.

Q: What do Xterity RPO and RTO mean?

Recovery Point Objective (RPO) indicates a duration of time that is acceptable for experiencing data loss. For example, an RPO of 15 minutes means that the recovery dataset will be updated every 15 minutes to capture the last 15 minutes worth of data changes. If a dataset was updated at 2:45PM and then the server goes off-line at 2:52PM the 7 minutes of data changes that were made on the primary (source) server do not get propagated to the recovery dataset because the next sequential recovery dataset update wasn't scheduled to occur until 3:00PM, 8 minutes after the server went off-line. In this scenario 7 minutes worth of source server data updates are not recoverable.

Recovery Time Objective (RTO) indicates how much time a business can tolerate a server not being available. For example, an RTO of 4 hours indicates that the business can sustain a server outage of 4 hours. See the example below:

Specified Recovery Point Objective (RPO)	15 Minutes	
Specified Recovery Time Objective (RTO)	4 Hours	
Initial Restore Point Dataset create time	1:00 PM	
Most recent Restore Point Dataset update time	2:45 PM	7 Minute Recovery Point
Server off-line time	2:52 PM	
Server off-line discovery time	3:00 PM	
Partner authorizes Xterity Cloud Operations to commence recovery - RTO clock starts	3:15 PM	2 Hour Recovery Time
Recovery complete (OS console access is verified & partner is notified) - RTO clock stops	5:15 PM	
The 15 minute RPO was met		
The 4 hour RTO was met		
The data updates made on the source server between 2:45PM and 2:52PM were not propagated to the Restore Point Dataset		

Tasks and Responsibilities:

P-DRaaS TASK	RESPONSIBILITY
Maintain access by Partner to the download for DiskSafe Agent.[3]	Xterity
Maintain instructions for installing the DiskSafe Agent at the source site.	Xterity
Fill out Direct Connection form, or vAPP form and submit to Xterity (OFF Cloud DRaaS only). Forms are accessed via the partner portal.	Partner
Create definition of the DR environment with details specifying server(s) build specifications, Public IP requirements, network connectivity from information provided by Partner (OFF CLOUD only).	Partner
Deployment, maintenance, management, and administration of on-premise hypervisor environment for use in Off-Cloud DRaaS configurations where virtual appliance (vAPP) technology is used	Partner / Client
Install Off Cloud DRaaS vAPP and setup SSL connectivity	Xterity
Provide IP address of Storage Server and logon and password for the partner.	Xterity
Download/install and configure DiskSafe agent on each (physical or virtual) source server.	Partner
Using the POV ticket system, notify Xterity Cloud Operations that DiskSafe agent(s) have been installed on source servers.	Partner
Verify communications between DiskSafe Agents installed on source servers and Xterity Cloud.	Xterity
Perform and verify a successful initial synchronization.	Xterity
Setup DR solution in the Xterity Cloud recovery automation system mapping servers, applications, networks and storage between the primary (source) site and the Xterity recovery site.	Xterity
Notify Partner via POV ticket system that initial synchronization is complete and (source) server is now protected. This is done on a per server basis, not multiple servers. Provide PUBLIC IP Addresses to be used during a DR event for servers that need public access.	Xterity
Using the POV ticket system request Xterity Cloud Operations to perform a DRaaS Verification Test (DRVT).	Partner
Perform DRaaS Verification Test (DRVT) and notify the partner through the POV ticket system that the recovery is complete and the recovery server(s) are accessible for 5 calendar days after which the server(s) will be deleted.	Xterity

[3] "DiskSafe Agent is the Xterity P-DRaaS agent installed on each protected server"

P-DRaaS TASK	RESPONSIBILITY
Partner or partner's client determines that a DR event has occurred — Partner notifies Xterity Cloud Operations via POV ticket system or phone call that a DR event has occurred and a DR restore is requested.	Partner
Xterity Cloud Operations confirm the DR restore request from Partner with the identified Partner contact by phone including identification of all servers that require resto- ration. The RTO clock starts.	Xterity
For recovery servers targeted for deployment on virtual compute resources, create VMDK for each server, create each server in DR cloud, build the server(s), copy VMDK and start the server. Verify server availability through successful access of an OS login screen via the server's console.	Xterity
For recovery servers targeted for deployment on physical compute resources, identify the physical server profile (pServer) for each server, provision each server in DR cloud, build the server(s), start the server(s). Verify server availability through successful access of an OS login screen via the server's console.	Xterity
Verify all restored servers are communicating over the prescribed VLAN. Any publicly facing servers are available at the PUBLIC IP addresses specified. Completion of RTO. All charges for servers in Xterity Cloud initiated.	Xterity
Notify Partner via POV ticket system that the DR environment is available and verified and ready for software validation by the partner or partner's client.	Xterity
DR environment is validated and issues are reported to Xterity Cloud Operations via POV ticket system. Notification of DNS modification to settings and network re-directs to enable environment for client user access.	Partner
Monitor ongoing communications with DiskSafe, success of data replication and compliance with the RPO schedules contained in DiskSafe configuration— notify Partner of any anomalies via POV ticket system.	Xterity

Service Level Agreement:

1) Server Recovery will be completed within the RTO of four (4) hours. If recovery is longer than 4 hours and less than 5 hours, the partner will receive a credit equal to 5 days/16% of the server DRaaS monthly charges. If recovery is longer than 5 hours, the partner will receive a credit equal to 1 month/ 100% of the server monthly DRaaS charges.

2) Server Recovery for an Xterity Cloud OFF CLOUD DRaaS solution utilizing *Private Network* connections purchased by the partner or partner's client and determined by the partner to support an RPO of 15 minutes will present the recovered server's storage dataset in a state reflecting the RPO of 15 minutes maximum.

3) Server Recovery for an Xterity Cloud OFF CLOUD DRaaS solution utilizing public Internet network connections will present the recovered server's storage dataset in a state reflecting the RPO of 12 hours maximum.

4) Server Recovery for an Xterity Cloud ON CLOUD DRaaS solution will present the recovered server's storage dataset in a state reflecting the RPO of 15 minutes maximum.

5) Server Recovery for protected servers that are deployed on a virtual compute resource will be recovered on a virtual compute resource designated by the partner during DRaaS setup.

6) Server Recovery for protected servers that are deployed on a physical compute resource and are designated for recovery on virtual compute resources will be recovered on a virtual compute resource designated by the partner during DRaaS setup.

7) Server Recovery for protected servers that are deployed on a physical compute resource and are designated to be recovered on a physical compute resource will be recovered on a physical compute resource designated by the partner and purchased by the partner as a reserved Xterity Cloud physical compute resource.

8) Application Recovery is not the responsibility of Xterity Cloud DRaaS, P-DRaaS, or Xterity Cloud Operations.

9) DRaaS Verification Test (DRVT) can be requested by partners and will be fulfilled in 3 to 10 calendar days after receipt of the request. One DRVT per subscription year is included with the DRaaS service. Additional DRVT tests are available for purchase.

Definitions

1) **Application recovery:** All activities required to recover any workloads and/or applications including their configurations, settings, and access protocols that utilize protected servers.

2) **Booted Server:** A server that has attained an operational state whereby it is accessible remotely from designated network address(es).

3) **End User Device:** Personal computing devices including workstations, towers, and laptops. Does not include mobile (smartphones, tablets).

4) **Physical compute resource:** A computer that includes all hardware elements (processor(s), memory, communications, storage, power, mechanical enclosure) to support deployment of operating systems and hypervisors.

5) **Private Networks:** Network connections between Xterity Cloud External Network Interfaces and any other compute infrastructure whose network capacity, security, performance, features, supplier and maintenance are designated and purchased by the partner or partner's client(s). These networks are not part of the Xterity Cloud infrastructure.

6) **Server downtime:** The time span that starts with the event that interrupts the protected server operation and includes the elapsed time to:
   - Identify the server is off line plus
   - Authorize a server recovery at Xterity Cloud plus
   - Perform server recovery at Xterity Cloud plus
   - Perform application recovery

7) **Server Recovered:** For a single instance of a server designated for protection by Xterity DRaaS, recovery is completed when:
    - The operating system as specified in the setup of the DRaaS for the server, including specified network address(es), storage device(s), and file system(s) are accessible by the designated Xterity partner or client representative located in the designated remote location
    - The state of the recovered server's storage device represents the dataset version as defined by the recovery point objective (RPO)
    - The server is recovered on the specified compute resource (virtual or physical)
    - The recovered server is accessible through the specified public IP address(es)
8) **Server:** A server is software that includes an operating system and the operating system configuration settings necessary to enable the operating system to attain an operational state that is capable of supporting application software workloads and is accessible remotely through designated network address(es).

9) **Server Recovery Authorization:** Communication via POV ticket or phone by the designated partner representative(s) to Xterity Cloud operations that server recovery for the specified server(s) is authorized.

10) **Virtual compute resource:** A virtual computer that includes virtual processor(s), virtual memory, virtual network and virtual storage to support deployment of operating systems.

11) **Xterity Cloud DRaaS Verification Test – DRVT:** Partner requests a DRVT for a client and Xterity Cloud operations performs the DRVT as soon as commercially possible but in no case sooner than 3 calendar days or later than 10 calendar days after receipt of the request. Xterity Cloud operations perform the disaster recovery by creating server(s) at the disaster recovery site using the most recent recovery point dataset and notifying the partner when the server(s) are online and accessible for testing by the partner or partner's client(s) through an Xterity Cloud defined IP address. The server(s) remain accessible for 5 calendar days after notification by Xterity Cloud personnel. There are no charges for virtual server(s) CPU and Memory during the DRVT time period. The DRVT provides a method for partners or their clients to verify the effectiveness of their disaster recovery plan without affecting production operations at the primary site.

12) **Xterity Cloud external network interfaces/ports:** For connecting Xterity Cloud infrastructure to external networks such as the public Internet or private networks.

13) **Xterity Cloud network(s):** Communications network within the Xterity Cloud infrastructure for communications within the Xterity Cloud resources.

14) **Xterity Cloud / ON Cloud Services:** Services that are operational within and between Xterity Cloud datacenters.

15) **Xterity Cloud / OFF Cloud Services:** Services that are operational between Xterity Cloud datacenters and any other infrastructure platform or datacenter.

16) **Xterity Cloud Recovery Point:** The storage volume(s) that are a replication of the storage volume(s) specified for a DRaaS protected server with a data state representing the state of the protected server's storage volume at the time of replication.

17) **Xterity Cloud Recovery Point Objective (RPO):** The specified maximum age, in minutes, hours or days, of the recovery point dataset to be used in the Server Recovery. The age of the recovery point dataset is determined by the time between the successful completions of two (2) sequential recovery points.

18) **Xterity Cloud Recovery Time Objective (RTO):** The time span in hours that starts with the email/ phone confirmation timestamp from the partner to Xterity Cloud operations that an event requiring recovery has occurred and ends with the completion of the Server Recovery. The RTO for Xterity Cloud DRaaS is four (4) hours.

To learn more about Egenera's Xterity Cloud Services please contact us at

USA - Headquarters
Egenera, Inc.
80 Central Street
Boxborough, MA 01719 USA
phone: 978-206-6300
www.egenera.com
email: info@egenera.com

Asia/Pacific
Egenera, K.K.
Park Side Annex BLDG 1-17
Sanban-cho, Chiyoda-ku,
Tokyo, 102-0075 Japan
phone: +81-3-6261-6301
japan.egenera.com
email: info-jp@egenera.com

EMEA - Dublin
Egenera, Ltd.
4033 Citywest Avenue
Citywest Business Park
Dublin 24
Ireland
phone: +353 (0) 1 485 3473
www.egenera.com
email: sales@xteritycloud.ie

EMEA - London
Egenera, Ltd.
21 St. Thomas Street
Bristol, BS1 6JS
United Kingdom
phone: +44 (0) 203 808 5563
email: emea@Egenera.com

EMEA - Germany
Egenera, GmbH
Dornhofstrasse 34
63263 Neu Isenburg
Germany
phone: +49 6102 812230
email: emea@egenera.com