ExaGrid Tiered Backup Storage

Fastest Backups

Fastest Recoveries

Unparalleled, Cost-effective Scale-out

Comprehensive Security and Ransomware Recovery

ExaGrid Tiered Backup Storage

Security, Reliability, and Redundancy

ExaGrid Reliability and Redundancy Architecture

ExaGrid's architecture and implementation have multiple facets of reliability and redundancy protecting the customer's data at every step, allowing organizations to make informed vendor selections. Organizations using backup storage to hold their invaluable backup data should carefully consider how the solution is architected for reliability and redundancy. Compromises in a product's architecture or implementation may reduce product cost, but those savings are quickly dwarfed by the risk and real cost to an organization of a loss of some or all backup data.

Retention Time-Lock for Ransomware Recovery

Retention Time-Lock is a revolutionary approach to protecting backup retention data to enable fast and easy recovery from ransomware.

- ExaGrid's two-tier architecture includes a network-facing tier and a non-network-facing tier. ExaGrid alone controls the non-network-facing tier, creating a tiered air gap
- Backups are written to the network-facing-tier for fast backup performance. The most recent backups are kept in their full undeduplicated form for fast restores
- Data is adaptively deduplicated (for storage cost efficiency) into the non-network-facing tier for long-term retention data. Organizations can have as many days, weeks, months, or years of retention as they require. There is no limit to the number of version retention copies that can be saved
- If data is deleted in the network-facing tier, that data is not deleted for a set period of time in the non-network-facing Repository Tier. This allows for all data to be recoverable after a ransomware attack or other security event
- If encrypted data is sent to the network-facing tier, or if any of its data is encrypted, ExaGrid's repository tier is protected as all the deduplication objects are immutable because they are never modified

ExaGrid assumes the threat actors/hackers will take control of the backup application or the backup storage and will issue delete commands for all backups. ExaGrid has the only non-network-facing Tiered Backup Storage solution (a tiered air gap) with delayed deletes and immutable deduplication objects. This unique approach ensures when a ransomware attack occurs, data can be easily recovered or VMs booted from the ExaGrid Tiered Backup Storage system. Not only can the most recent primary storage data be restored, but all retained backups remain intact.

ExaGrid alerts on large delete attempts above the set threshold and also on data deduplication ratio change due to encryption. These act as an early warning detection of an attack.

For a more in-depth look at the Retention Time-Lock feature, please download the ExaGrid Retention Time-Lock for Ransomware Recovery data sheet.

Server Hardware and Platform Software

RAID6 Internal Storage with Consistency Checking

ll ExaGrid internal storage is accessed using an industry-leading PCIe RAID controller configured to RAID6 (e.g. double-parity) with a global "hot spare" disk. In normal operation, your data is additionally protected because the RAID controller does consistency checking of the data on its disks in the background, correcting any disk media errors using the parity disks.

Because there are two parity disks, each ExaGrid appliance can tolerate the simultaneous loss of up to two disk drives. The first lost disk drive will automatically initiate a parity rebuild operation using the global hot spare. Administrators and (optionally) ExaGrid customer support are informed via alerts of the failure. A replacement disk drive is dispatched quickly, typically allowing replacement of the failed disk the next business day. Loss of the second disk does not result in loss of data since the remaining parity disk allows for data regeneration; providing more time for the important task of replacing the failed disk(s). Over 90% of ExaGrid 's customer have alerts also sent to the ExaGrid Health Reporting system.

Flash-Backed RAID Cache

The industry-leading PCIe RAID controller has an onboard volatile memory writeback cache that is backed up to flash memory when system power is lost or interrupted. The RAID controller's super-capacitor provides ample power to allow all writeback cache data to be transferred to flash until system power is restored.

Redundant Power Supplies

All ExaGrid models include redundant power supplies monitored by the system software, producing an alert and optionally an e-mail notification of any power supply issues. When Health Monitoring (see below) is enabled, ExaGrid customer support is made aware of the issue and can immediately arrange for the shipment of replacement power supply. Power supplies, like disk drives, are hot-swappable.

Securing Data on the WAN

Replication of deduplicated backup data can be encrypted when transferred between ExaGrid sites using 256-bit AES, which is a FIPS PUB 140-2 Approved Security Function. This eliminates the need for a VPN to perform encryption across the WAN.

Encryption at Rest

ExaGrid offers FIPS 140-2 Validated hardware-based disk encryption on all SEC models. Self-encrypting hard disks with RAID controller-based key management and access control secures your data during the storage process.

Up to Date with Industry Standards

- ExaGrid supports IPv6
- ExaGrid is up to date with industry security features in CentOS 8

ExaGrid Specifications

- Uses FIPS 140-2 Validated Self-Encrypting Drives (SEDs) to ensure that data at rest is always efficiently encrypted with 256-bit AES and is never in the clear on the disk storage. All data, configuration settings, etc. are encrypted
- Drive theft protection – The drives cannot be read outside of the host system where encryption was enabled
- System theft protection – System booting and access to data can be restricted with a password. This can be enabled as an option (no extra charge)

Operating System Patches

Current ExaGrid server platform software is based on the CentOS Linux distribution. We release critical and relevant OS security patches as a part our regular ExaGrid software releases. Relevant CVEs will be included at least quarterly, with critical fixes included more quickly.

ExaGrid Software

Management Interfaces

- ExaGrid software is managed through a web interface and will, by default, accept connections from a web browser on both ports 80 (HTTP) and 443 (HTTPS). ExaGrid software supports disabling HTTP for environments that require HTTPS (secure) only. When using HTTPS, ExaGrid's certificate can be added to web browsers, or a user's certificates can be installed onto ExaGrid servers via the web interface or provided by a SCEP server
- Windows Active Directory (AD) domain credentials can be used to control access to the ExaGrid management interface, providing authentication and authorization to the web GUI

- Two-factor Authentication (2FA) can be required for any user (local or Active Directory) using any industry-standard OAUTH-TOTP application. 2FA is turned on by default is for both the Admin and Security Officer roles and any login without 2FA will create a warning prompt and an alarm for greater security.
- Role-Based Access Control using local or Active Directory credentials and Admin and Security Officer roles are fully compartmentalized
  - ***Backup Operator*** role for day-to-day operations has limitations such as no deletion of shares
  - ***Security Officer*** role protects sensitive data management and required to approve any changes to the Retention Time-Lock policy, and to approve the viewing of or changes to root access
  - ***Admin*** role is like a Linux super-user – allowed to do any administrative operation (limited users given this role) Admins cannot complete sensitive data management action (such as deleting data/shares) without the Security Officer's approval
  - Adding these roles to users can only be done by a user that already has the role – so a rogue admin cannot bypass Security Officer approval of sensitive data management actions
  - Key operations require Security Officer approval to protect against internal threats, such as share deletes and de-replication (when a rogue admin turns off replication to remote site)
- Automatic user interface logout after a period of inactivity
- Although access via SSH is not necessary for user functions, some support operations can only be provided over SSH. ExaGrid secures SSH by allowing it to be disabled, allowing access via randomly generated passwords, or customer-supplied passwords, or only SSH key pairs
- Security checklist for quick and easy implementation of best practices
- Each ExaGrid server runs a proper firewall and a customized Linux distribution that opens just the ports and runs just the services necessary for receiving backups, web-based GUI, and ExaGrid-to-ExaGrid replication

Share Access

- Common Internet File System (CIFS) – SMBv2, SMBv3
- Network File System (NFS) – Versions 3 and 4
- Veeam Data Mover – SSH for command and control and Veeam-specific protocol for data movement over TCP
- Veritas OpenStorage Technology protocol (OST) – ExaGrid specific protocol over TCP
- Oracle RMAN channels using CIFS or NFS

For CIFS and Veeam Data Mover, AD integration allows using domain credentials for share and management GUI access control (authentication and authorization). For CIFS, additional access control is provided via an IP whitelist. For NFS, and OST protocols, access control to backup data is controlled by an IP whitelist. For each share, at least one IP address/mask pair is provided, with either multiple pairs or subnet mask used to broaden access. It is recommended that only the backup servers that regularly access a share are placed in a share's IP whitelist.

For Veeam shares using the Veeam Data Mover, access control is provided by username and password credentials entered into both the Veeam and ExaGrid configuration. These can be AD credentials, or local users configured on the ExaGrid site. The Veeam Data Mover is automatically installed from the Veeam server onto the ExaGrid server over SSH. The Veeam Data Mover runs in an isolated environment on the ExaGrid server which limits system access, has no root privileges, and runs only when activated by Veeam operations.

Backup Data Checksums with Automatic Repair

As backup data is deduplicated, checksums are added to the deduplicated data as it is placed into the portion of the ExaGrid storage referred to as the repository. These end-to-end checksums cover the deduplicated backup data itself, and are used to verify the backup data during processing and as it is read from disk. The deduplicated backup data can optionally be replicated to a remote site; these checksums are used to validate the replicated data as well. During backup restore operations on shares that have been replicated to a DR site, the rare case of an invalid checksum is automatically handled by using the deduplicated data kept at the DR site.

External syslogging and SNMP

ExaGrid software can be configured to send operational information to an external syslog receiver and/or SNMP server for further integration into enterprise management systems. Examples of operational information sent to a syslog receiver include web access audits, configuration audits, hardware issues, significant software events, etc.

Deduplicated Metadata Transactional Consistency

Metadata that tracks all of the deduplicated data is kept in a database and on internal storage. Software techniques are used to ensure transactional integrity of all metadata changes, including flushing filesystem pages into the flash-backed RAID controller's onboard cache. The data flow of deduplicated backup data is protected end-to-end by the combination of checksums (above) and metadata transactional consistency.

Logging Filesystem

Backup data is kept in the ExaGrid internal storage on an industry-standard logging filesystem where file activity is logged for integrity and quick repair after an unclean shutdown.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

Replication and Inter-server Security

Replication of deduplicated backup data from one site to another can be optionally encrypted using internally-managed keys. The ExaGrid software uses a combination of Kerberos, TLS and SSH with 256-bit AES keys, which is a FIPS PUB 140-2 Approved Security Function, to secure all communications between ExaGrid servers in a site. A unique Kerberos domain is configured per site, and all sites have trust relationships automatically configured and enforced between them. All API communications are authenticated using Kerberos to ensure that commands and data cannot be tampered with while traversing the network.

Insulation from Ransomware

When ransomware strikes, it is critical to have backups insulated from the malicious encryption/damage since they may be your last line of defense. In addition to ExaGrid's Retention Time-Lock (see above), ExaGrid helps insulate backups from ransomware in the following ways:

- Comprehensive access security
  - ExaGrid shares can be accessed only from designated backup/media servers. While those servers may also be subject to rampant ransomware, the fewer servers that have access to your backups, the better. If those servers are affected by ransomware, ExaGrid's Retention Time-Lock will allow full recovery of any and all retained backups.
  - Windows Active Directory domain credentials can be used to control access to ExaGrid shares (CIFS and Veeam Data Mover) and management GUI, requiring Windows account credentials to be authenticated and authorized before access is granted to an ExaGrid share, further reducing the chance of malicious access to backups.
  - Veeam Accelerated Data Mover shares require a separate Veeam password and are accessible only via SSH, with optional key pairs, which also reduces the chance of malicious access to Veeam backups.
  - All accounts used to manage the ExaGrid software are protected using non-default passwords. This includes the backup "admin" account, the special ExaGrid customer support account, and root access.
- ExaGrid software is updated at least quarterly with the latest appropriate CVE fixes, reducing the ways ransomware can gain access to ExaGrid servers. Software may be updated more frequently as dictated by CVE severity.
- Each ExaGrid server runs a proper firewall and a customized Linux distribution that opens just the ports and runs just the services necessary for receiving backups, web-based GUI, and ExaGrid-to-ExaGrid replication.
- Communications between ExaGrid servers is secured using Kerberos authorization and authentication, protecting from a "man in the middle" attack from malicious users or software.

Periodic Assessments Using a Network Vulnerability Scanner

A complete vulnerability assessment is run periodically against ExaGrid's software. Vulnerabilities flagged by this assessment are evaluated and tracked and mitigated as appropriate.

Windows Active Directory

ExaGrid's support for Windows Active Directory allows:

- Authentication and authorization of the ExaGrid Web GUI using Active Directory user accounts and/or groups
- Authentication and authorization of ExaGrid CIFS shares using Active Directory user accounts and/or groups
- Authentication and authorization of ExaGrid Veeam shares using Active Directory user accounts and/or groups
- Access to all ExaGrid shares can continue to be controlled via an IP "whitelist"

Key behaviors include:

- Active Directory membership of ExaGrid Server(s) is defined and performed at the ExaGrid Site level. No need to configure each and every ExaGrid Server individually.
- Each ExaGrid Site can be joined to only a single Active Directory Domain (just like Windows computers).
- All ExaGrid Servers in a multi-server ExaGrid Site must join and belong to the same Active Directory Domain.
- Different ExaGrid Sites in a multi-site ExaGrid System can be joined to different Active Directory Domains.
- Once an ExaGrid Site is added to a domain, AD user(s) and/or groups – from any trusted AD Domain – are mapped to ExaGrid management role(s) for the Web GUI – e.g. administrator, backup operator, view only, etc. This mapping is done in the ExaGrid Web GUI. Any user can then login to the ExaGrid Web GUI with their AD account/password and will only be able to perform the management actions permitted by their assigned role – a.k.a. Role-Based Access Control (RBAC).
- Once an ExaGrid Site is added to a domain, AD user(s) and/or group(s) – from any trusted AD Domain – can be used to control access to the CIFS and/or Veeam shares in that Site. The AD user/group/password is generally configured into the backup application which then presents those credentials to ExaGrid when accessing share(s).
- If an ExaGrid Site is not in an Active Directory Domain, then a locally-managed set of "local users" can be used to control access to the ExaGrid user interface and shares, including allowing "guest" access to shares.
- Microsoft supports a wide range of characters in Active Directory usernames and passwords. However ExaGrid's user interface login is currently limited to: Active Directory usernames and passwords that contain any printable, 7-bit ASCII character including special characters and spaces.

ExaGrid Support Facilities

Health Monitoring

ExaGrid servers deliver data to ExaGrid Support (phone home) using both health reporting and alerting. Health reporting includes statistics data for trending on a daily basis and automated analysis. Data is stored on secure ExaGrid servers with trending databases used to determine the overall health over time. Health reports are sent to ExaGrid using FTP by default, but can be sent using e-mail with some decrease in the depth of analysis. Alerts are momentary notification that could indicate actionable events, including hardware failures, communications issues, potential misconfiguration, etc. ExaGrid Support promptly receives these alerts via e-mail from ExaGrid Support servers.

Secure Remote Support Access

ExaGrid Support provides a secure remote access solution so customer support engineers can provide unattended monitoring and corrective action on customer ExaGrid servers. Using a secure outbound TLS connection, tunnels are connected back into ExaGrid servers. The tunnels are secured using the highest security ECDHE and AES cipher suites, use certificate pinning for authentication, and can utilize an HTTP proxy.

Internal Database Backups and Self-Describing Metadata

The database used to keep metadata that tracks deduplicated data is periodically dumped to internal storage. These dumps are used to quickly restore the metadata database in the case of massive failure. The database dumps are used as an optimization; the metadata kept on disk is self-describing and can be used to completely rebuild the deduplicated data in the internal repository both at the local and remote ExaGrid sites.

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

exagrid.com