



May 14, 2024

Mr. Rob Lasky
Information Technology Manager
City of Foster City
610 Foster City Boulevard
Forster City, CA 94404

Dear Rob:

Thank you very much for the opportunity to continue to work with you and the City of Foster City. It is with pleasure that we provide this response to your RFP for a data backup system on behalf of Roundstone Solutions and our partner Cohesity.

On the attached pages, please find our response to your RFP. The first page is our agreement to provide products and services per the terms and conditions set forth in the RFP document. Subsequent pages contain our response to your requirements. The final page is our pricing. We've also included an attachment from Cohesity showing the overall Cohesity strategy, which you may find helpful.

Taxes are only owed on hardware supplied, and we've split things out and identified what the tax amount will be.

If you have any questions, please don't hesitate to ask. Thank you again for the opportunity, Rob.

Sincerely,

ROUNDSTONE SOLUTIONS INC.

Timothy J. Joyce
President and CEO

City of Foster City RFP – Data Backup System


The City of Foster City requests pricing for a Data Backup System. Pricing is to include 3 years of software subscription and hardware support (if applicable).

The City invites you to submit a proposal to furnish materials in accordance with the terms, conditions and specifications contained in this document. Please complete the proposal form as instructed below and return it to the specified e-mail address by the due date. No extensions to the deadline will be allowed. All responses must be in an email to:

TO: Rob Lasky
rlasky@fostercity.org
Due Date: 5/14/2024

The undersigned proposes to provide solution and installation services to the City for the stated prices in accordance with the terms and conditions set forth in this document.

VENDOR:

ROUNDSTONE SOLUTIONS INC.	180 VILLAGE SQ. #65
Company Name	Street Address of Company
	ORINDA, CA 94563
Signature of Officer	City, State, Zip
TIMOTHY J. JOYCE	925.217.1177
Printed Name of Officer	Telephone No./Fax Nbr.
PRESIDENT & CEO	94-3485616
Title of Officer	Federal I.D. Tax Number
5.14.24	

Cohesity response

Overall Cohesity Software Strategy

The following section provides a comprehensive overview of the Cohesity platform, called the Cohesity Data Cloud, and explains its key features and functionalities.

Cohesity Data Cloud: Unified data security and management: Cohesity Data Cloud is a software-defined data and application management solution delivered as SaaS, Customer-managed, and/or Partner-managed, or any combination of the three. Regardless of how Cohesity Data Cloud is deployed, it unifies data under a single platform that manages all locations, including on-prem (core), cloud, SaaS, edge, and Mainframe. Cohesity Data Cloud is a multi-tenant, web-scale platform with over 250 patents that outperforms and costs less than competing alternatives.

Cohesity aligns the appropriate solution deployment model to each workload group as follows:

- **On-premises:** Customer-managed physical clusters of hyper-converged Cohesity hardware be deployed at customer-defined locations. This single-tier architecture dramatically reduces the attack surface and management overhead associated with the Data Protection environment
- **Cloud IaaS/PaaS:** For the Cloud IaaS and PaaS workloads, Cohesity proposes that managed Cohesity software running on hyper-scaler VMs/Containers be deployed in each Cloud. These clusters are easily run on commodity Cloud infrastructure, but provide the same native immutability, encryption, air-gap, and granular RBAC as any on-premises cluster since it's the same software, and can be replicated to any other Cohesity cluster, Cloud or On-premises
- **M365:** For M365 applications, Cohesity proposes using Cohesity Cloud Services (CCS) Backup- as-a-Service (BaaS), a turnkey service running in Cohesity's AWS tenant that includes all costs - ingress, egress, infrastructure, software, support, etc. - in one low, per-User price that is fixed for the duration of the term regardless of data growth across various M365 applications (Mail, OneDrive, SharePoint, etc.).

All of these deployments scale up/down linearly in variable increments as needed, and they're "always-on," meaning any expansions, contractions, upgrades, etc. are all done without needing any downtime. In addition, data sites are enabled with seamless replication, archiving, and vaulting, if desired, to any remote site or Cohesity's SaaS Vault called Fort Knox, without any special configuration, hardware, or proxies. All these configurations support DR automation and orchestration, which can be tested and validated on any schedule as needed.

Rapid Recoveries at Scale:

Cohesity's scale shines best when it comes to recoveries. Cohesity can restore operations as much as 50% faster than alternative competitive solutions. This is driven by multiple unique capabilities:

- **Install Mass Restore:** Cohesity's unique ability to instantly recover 1) thousands of VMs, 2) databases such as Oracle etc., and 3) hundreds of terabytes NAS (NetApp for example) data in minutes vs. hours or days. No other provider enables instant recovery of different workloads.
- **Patented snapshot technology:** Cohesity's SnapTree™ takes each incremental backup, and instantly fuses it with the prior fully hydrated snapshot, so that the desired RPO is immediately available as a fully hydrated snapshot, so there's no time lost stitching incremental backups together with a recent full backup. This means data retrieval is just as fast for snapshots from five (5) hours, five (5) days, 15 days, or 45 days ago.
- **Efficient Metadata:** Cohesity retains backups data longer without running out of memory or flash resources. Cohesity I/O is also faster because it's exclusively retained on SSD and deduplicated, and there are no metadata chains to traverse for locating blocks.
- **Parallel processing:** Cohesity's hyper-converged, scale-out file system enables all nodes in a cluster (on-prem, Cloud, SaaS) to participate fully in all operations, including recoveries
- **MegaFile:** Cohesity has the ability to take very large files (e.g., 50MB vmdk files) and break them up into smaller blocks for parallel processing (e.g., recovery) without any data fidelity loss or security risk
- **Restore Flexibility:** Cohesity has the ability to mass restore to a new network, instantly recovering workloads for parallel forensics and clean data validations. Regardless of whether the original VM location can be accessed or not, the VMs are easily brought up and put on any desired network.
- **Restore Resilience:** During instant access, strict consistency and redundancy are maintained, as is expected from primary storage. Crash or loss of a node will NOT lose any cached writes, nor will it interrupt the I/O processing, making it perfectly safe for production use. While Cohesity doesn't perform as primary storage, it outperforms storage solutions designed for backup only. This also means recovered workloads, as well as forensics, dev/test, analytics, etc. workloads all run without interruption, even during software upgrades

2. Security:

Data within Cohesity Data Cloud is secure from the inside out, with in-flight and at-rest encryption, immutability, WORM, natively immutable, encrypted, and air-gapped data and is never exposed by any network protocols or shell access, and it cannot be snooped, deleted, or expired through time-shift attacks.

In addition, the data can be securely shared rather than siloed, stored more efficiently, and made visible rather than kept in the dark to external applications such as ML/AI models, analytics, Dev/Test,

forensics, and to secure applications that run in isolated containers on the Cohesity platform itself, all of which have no visibility, access, or awareness of the original, immutable, encrypted, air-gapped data. Instead, these apps only leverage data clones that consume zero additional storage.

Cohesity's comprehensive anti-ransomware capabilities protect, isolate, detect, and most importantly, rapidly recover, data to reduce downtime and ensure business continuity, regardless of the disruption event - Ransomware, disaster, hacktivism, etc.

Key Benefits Summarized:

- **Reduce Attack Surface** - Collapse your data and infrastructure silos onto a single, software- defined platform that reduces accessible points, running a hardened software stack from OS up to the application, all managed through Cohesity. No Master, Media, Indexing, Deduplication, Reporting, Proxy, etc., servers are needed, dramatically simplifying the architecture, and eliminating multiple components which must be managed - OS versions compatible with Application versions, compatible with firmware, network interfaces, etc.
- **Hardened, Access Controlled, Self-Healing Platform:** The Cohesity Data Cloud is a hardened Linux platform, which comes secure upon installation, with these strict access controls set by default, and includes a built-in posture management capability called Security Advisor. Security Advisor monitors multiple threat vectors in real-time and alerts on any changes, which can then trigger self-healing through automated response actions. In the extremely unusual event that system repair requires shell access, there are no backdoor credentials maintained by Cohesity. Instead, customers must initiate a process with Cohesity Support, who must concur access is needed, and then a one-time-use, time-limited token must be granted before shell access is enabled
- **Natively Immutability** - Prevent external systems or bad actors from targeting your backup data with native immutability, built into the file system by default, such that no block is ever overwritten, and immutable data is never exposed via any protocol, access method, is not mountable to an external system, nor does Cohesity maintain backdoor Vendor Support credentials. The immutable file system can take very frequent, unlimited read-only state snapshots and store them with extremely low overhead, ensuring the longer retention period needed to address increasing Ransomware dwell time can be supported. Data cannot be snooped, deleted, or expired. In addition, virtual air gap, DataLock (WORM - Write Once Read Many), strict granular RBAC, as well as SSO/MFA provide additional protection layers.
- **WORM Protection:** WORM Protections are applied via a Cohesity feature called, DataLock, which ensures immutable, encrypted, air-gapped backup data cannot be altered, expired, or deleted, either by an authorized Administrator, Security Officer role, or authenticated APIs, ensuring data is retained for whatever retention is specified. These WORM protections apply across all the deployment modes recommended - Clouds, On-Premises, SaaS, and Mainframe, without additional infrastructure or specialized storage.

- Strict Access Controls:** Preventing unauthorized access to sensitive data is at the heart of Cohesity's protection vision. Cohesity has very restrictive access controls at the object level (e.g., VM, database, file, etc.), supported by granular RBAC, as well as MFA/SSO and Privileged Access Management (PAM, e.g., CyberArk) integration for keeping your data completely safe. In addition, Cohesity implements Quorum – the ability to define two or more members of a Quorum group, and require two or more of these members to authorize access and actions against backup data, helping to ensure that even if a select number of credentials are compromised along with your data, you can securely backup, access, and recover pristine, clean copies of your data from any location, including the external Fort Knox SaaS vault
- Time-Shift Protection:** To ensure that data locks cannot be expired prematurely, Cohesity leverages NTPSec, triangulates across multiple NTP servers, and an automatic trigger that defaults to the local system time when NTP time shifts more than several minutes. Cohesity not only enables NTPsec and triangulates multiple NTP servers, but even if a malfunctioning NTP server were to try moving time forward too quickly, Cohesity software protections do not allow cluster time changes of more than a maximum of 30 minutes backward or forwards over 14 days, providing better protection than a simple, monotonic clock.
- Data Isolation** - Beyond the native air gap of every cluster, a simple policy-based automated air gap adds an additional layer of protection against modern ransomware attacks, and for further data and management isolation, Cohesity offers the award-winning Fort Knox SaaS vault, which runs in a separate Cloud tenant on AWS and/or Azure, and is secured with additional access controls and restrictions, such as Quorum (2 or more predefined, authorized users that are required to access/operate on Vault data). Quorum groups in control of vaulting operations can be a different people than those performing On-premise or Cloud cluster operations. Fort Knox can be viewed as an additional Isolated Vault or Isolated Recovery Environment (IRE) SaaS service option that augments native immutability, air-gap, and other capabilities previously described.
- ML/AI-based Ransomware Detection:** Cohesity Data Cloud ML/AI Ransomware detection automatically and continuously monitors every backup in real-time as ingested, and responds when an anomaly is detected. If data change rates change, including data ingest is out of the normal range—based on daily change rates on logical data, stored data after global deduplication or historical data ingest, as well as entropy (e.g., the randomness of data). Using Threat Intelligence from Cohesity's Data Security Alliance Partners, these anomalies trigger reactive scans for threat indicators that point to a broader cyber event, as well as sensitive data (e.g., PII, PHI, etc.) scanning to immediately understand the blast radius and event severity (e.g., is reporting to authorities required?). The CyberScan app based on integration with Tenable.io, is also triggered to identify vulnerabilities in the impacted workloads. Based on this consolidated risk assessment, the appropriate Incident Response playbook is invoked. Cohesity Data Cloud initiates API-based automation and orchestration with Security Operations via SIEM/SOAR integration, sending notifications to administrators, and displaying details in the Security Dashboard.

- **Proactive Threat, Sensitive Data Vulnerability Identification** - using advanced ML/AI threat detection models from CrowdStrike and Qualys, Cohesity proactively scans data in parallel, providing proactive protections against many more cyber risks than what can be seen using self-managed YARA rules loaded and run one-at-a-time. By using 200+ industry-leading ML and Natural Language Processing (NLP) models from BigID, more sensitive data is readily identified vs. home-grown, inaccurate regex-based methods. For example, these models enable more accurate detection of names, birth dates, passwords, and street addresses. Collaborating with industry leaders reduces false positives and false negatives, especially important for automated Security Operations workflow automation. In addition, Cohesity works with both Zscaler and Netskope to allow those tools to identify if someone is trying to exfiltrate files Cohesity flags and tags containing PII.
- **Clean Recoveries:** Beyond Cohesity's unique advantages in recovery speed is the ability to ensure clean restores and avoid re-injecting a cyber threat or software vulnerability into your production environment. First, Cohesity protects Directory Services, like Active Directory, and can compare any point in time to the current Identity store down to the attribute level. This enables side-by-side comparison, and recovery at the individual attribute, User, or Tree level, to ensure the compromised credentials leveraged in an attack do not remain compromised after restoring quickly and cleanly. Isolated data clones, with no access, visibility, or connectivity to the original immutable, encrypted, air-gapped data are mounted and scanned by Cohesity's DataHawk and CyberScan services to give deep visibility into the data health and recoverability. DataHawk scans data clones securely mounted on the Cohesity platform for threat indicators using high-fidelity, real-time Threat Intelligence from CrowdStrike and Qualys in parallel vs. individually loaded, self-managed YARA rules run one at a time. DataHawk scans for sensitive data using over 200 NLP and ML patterns from BigID, constantly updated vs. static, false positive-prone Regex rules. CyberScan leverages integration with Tenable.io, and identifies any vulnerabilities, and provides actionable remediation recommendations for review. All of these capabilities can be automated and orchestrated with common SIEM/SOAR tools, using predefined playbooks and integrations delivered by Cohesity's Data Security Alliance, which helps UCOP more quickly, cleanly, and predictably recover from a ransomware attack, or any type of business disruption.

3. Simplicity:

Cohesity Data Cloud enables you to more quickly ramp up and successfully leverage the full capabilities of the platform due to its simplicity, which is broken into several categories:

- Simple to Use: Cohesity intuitive UI is the same for every deployment scenario, and simply having protection groups avoids policy sprawl, re-entering information in mostly-redundant policies, having long policy pick lists
- Simple to Secure: Native immutability, encryption, air-gap, WORM, MFA/SSO and PAM integrations, NTP protections, etc. are all built-in and on by default, and there's built-in posture management with Security Advisor that enables self-healing of the environment
- Simple to Deploy: Cohesity's hyper-converged architecture means simple, flat network deployment of commodity nodes with no need for multiple server types or proxies, nor the need to architect multi-tier data flows, as well as superior space efficiency, results in 30-35% less infrastructure than competitors

- Simple to Integrate: Cohesity provides predefined integrations and Playbooks, as well as jointly developed and supported solutions with Data Security Alliance Partners. Cohesity provides an entire ecosystem dedicated to making integration easy with apps, API example code, videos, and GitHub repository for Ansible, vRA, Terraform, puppet, etc. available at <https://developer.cohesity.com/>
- Simple to Operate: Loads of predefined dashboards, reports, and alerts, as well as integrations, to help automate IT and Security Operations, and a secure Postgres reporting database for integration with standard enterprise reporting tools like Tableau, Qlik, etc. In addition, all cluster expansions, contractions, software upgrades, etc. are done via UI or API and can be run with NO downtime or interruptions to ongoing operations
- Simple to Manage: Unlike other solutions, Cohesity Data Cloud allows IT admins to control all their Cohesity instances located on-premises, in the Cloud, Cohesity-managed (SaaS), or edge all from a single dashboard, including multi-tenancy. ML-based SmartAssist* gives critical global operational data, across all instances, so you can then take action/automate responses to address. This ML engine gives administrators intelligence about all Cohesity environments to enable informed management decisions that ensure you meet business SLAs.

Cohesity Data Cloud Summary:

- Cohesity Data Cloud is a software-defined solution delivered as a customer-managed and/or SaaS offerings to build a modern, unified global data management infrastructure that will
 - Accelerate Digital Transformation and Productivity
 - Provide a unified, simple-to-deploy, operate, and manage a global infrastructure
 - Take advantage of ML/AI to gain security and operational insights, as well as maximize global resource utilization
- With Cohesity Data Cloud you can effectively meet current objectives as well as plan for future requirements, and ensure continuity with
 - Extensive data and platform protections leveraging ML/AI
 - Automation/Integrations to ecosystem partners preserve and extend existing investments
 - Proactive protection and platform wellness through self-monitoring and healing
- And finally, you will be able to –
 - Eliminate data and application sprawl dramatically lowering TCO, while gaining valuable insights into their previously untapped backup data, accelerating critical business decision-making

One Platform. Limitless Potential. Choice – Cohesity Data Cloud - The Industry's First Comprehensive Multi-Cloud Platform for Data Management Services.



**ROUNDSTONE SOLUTIONS INC.
PROPOSAL TO THE CITY OF FOSTER CITY
PRICING FOR DATA BACKUP SYSTEM-COHESITY-36 MONTHS**

Roundstone and our partner Cohesity are pleased to provide updated pricing to the City of Foster City:

PRODUCTS: (1) Cohesity C5016-10G-SFP-4-2 4-node hardware block;
 (4) Intel Xeon CPUs (2.1 GHz, 12 cores each)
 48TB HDD
 6.4TB SSD
 (8) Cohesity ADDP-SFP-10G-SR-2 SFP+ adapters
 (8) Cohesity CBL-10G-LC-010-2 10m optical cables
 (1) CS-P-C5016-10G-SFP-4-2 Premium support
 (15TB) Cohesity SAAS-FORTKNOX-H-AWS-2 Secure and
 immutable Cohesity managed Cloud archival delivered
 as a service
 (10TB) Cohesity SVC-DATAPROTECT-2 DataProtect
 subscription (1TB)

LOCATION: Foster City, CA

DELIVERY: 3-4 weeks after receipt of signed order

IF PURCHASED UPFRONT: **36 MONTHS**

HARDWARE COST: **\$23,164**

HARDWARE SUPPORT: **\$ 7,420**

SOFTWARE LICENSING: **\$39,396**

SUBTOTAL: **\$69,980**

SALES TAX: **\$ 2,172**

GRAND TOTAL: **\$72,152**

4TH YEAR FIXED RENEWAL: **\$16,300 (due at beginning of Year 4)**

5TH YEAR FIXED RENEWAL: **\$16,300 (due at beginning of Year 5)**

NOTES:

1. Taxes are owed on hardware only. Software is all downloadable and non-taxable. We have identified the taxes owed, based on Foster City's sales tax rate of 9.375%.
2. Installation is not included in the pricing above.
3. Cohesity Premium hardware support is what we've proposed, and it's 24/7hours, 365 days.
4. All products are provided from Cohesity through Roundstone's authorized Partner agreement.
5. Support for all Cohesity products is provided directly from Cohesity.
6. Pricing is valid for 90 days from the date of this proposal.