Zadara Cloud Services Security Brief

Revision history:

Ver	Date	Author	Description
12.04	April 2012	Yair	Security considerations in Zadara Cloud 12.04 version
13.07	July 2013	Yair	Adding Remote Mirroring Authentication and Encryption
16.05	May 2016	Yair	- Some updates on Mirroring encryption - B2S3 encryption brief description
16.05- SP2	January 2017	Oded	Updates for 16.05 SP-2
17.11	January 2018	Oded	Updates for 17.11
18.11	December 2018	Oded	Updates for 18.11
20.12	January 2021	Oded	Updates for 20.12
22.06	October 2022	Oded	Updates for 22.06, adding zCompute
23.09	January 2024	Oded	Updates
23.09	May 2024	Oren	zCompute updates
23.09-SP1	June 2024	Oded	Added “shared responsibility”
23.09	September 2024	Oren	zCompute updates
25.07	March 2026	Oded	Added: securing clouds access
25.07	May 2026	Oded	Restructure. Adding Corporate Security

Contents

Introduction

At Zadara™ we take security concerns seriously and have made security an integral part of our cloud services offering. We have architected security into our system and software from the ground up.

In this brief, we discuss our approach to security. It covers the controls we implement across several security domains, both in securing Zadara's public and private clouds and our own systems and environments. It also covers the processes we have in place to ensure we create secure products for our partners and customers.

With multiple layers of security, our customers can enjoy full, end-to-end data privacy and protection.

Zadara Cloud Services come with the following commitments:

● **Encryption**: All data is encrypted at transit and can be encrypted at rest.

● **Access Controls**: Tenant admin has full control over users' access permissions. Only authorized Zadara employees will ever access your cloud for the purposes of resolving incidents, recovering user's data with your explicit permission, or where required by applicable law.

● **Data Privacy**: Each customer's data is logically and physically separated from all other customers.

● **Redundancy**: Zadara provides several levels of local and remote data redundancy to ensure data availability. This includes RAID protection, Snapshots, Mirrors, and built-in backup/recovery.

Data Classification

Generally speaking, Zadara maintains 3 types of data:

1. **Customer Data** - Customers using Zadara clouds keep their data in volumes/containers they create on Zadara Cloud. Since Zadara has no visibility into the customer data, we treat it all as most sensitive and critical information. Access is restricted to the data owner only, while the customer administrator controls users and access rights to the data. It is the customer's responsibility to define the data protection and high availability requirements for this data. Zadara provides the tools to ensure data privacy, availability, and protection.

2. **Customer Configuration Data** – This category is the metadata for the above Customer data, and the system configuration information. Zadara uses this data to maintain and protect the customer data. This data is critical for system operation but does not contain any sensitive information. Zadara is responsible for protecting it and backing it up.

3. **Customer Information** – This is the database of Zadara customers that contains details like contact information, email addresses, and billing details. This is highly sensitive data. Zadara is responsible for protecting it and backing it up. This information is stored, maintained and protected within Salesforce.com, Zendesk.com and Oracle NetSuite.

Shared Responsibility

Zadara Clouds security follows the “shared responsibility” model where the responsibility for securing different aspects of the cloud-computing environment is shared between Zadara and the partner/customer. In this model Zadara secures the infrastructure, including virtual machines, storage, and networks—while customers secure everything hosted on the cloud infrastructure, such as the operating system, runtime, applications, and data.

Security of the cloud: Zadara is responsible for securing the data centers hosting public clouds, Compute and Storage nodes and networking equipment. Zadara also handles tasks such as patching and updating the above nodes and networking devices as well as ensuring the availability and reliability of the cloud services.

Security in the cloud: Partners/Customers’ security responsibilities include physical security of on-premises clouds, setting up secure access controls, encrypting data, backing up the data, managing user accounts and credentials, and application-specific security.

Zadara’s Responsibilities:

- Physical security and physical access to public clouds
- Host-infrastructure security, proper configuration, patching and upgrades, ensuring availability and reliability of the services
- Network-infrastructure security, securing the cloud-network infrastructure: FWs, switches, and load balancers
- Securing remote management access
- Engaging independent audits to certify compliance with industry standards

Customers’ Responsibilities:

- Physical security and physical access of private, on-prem clouds
- Ensuring data protection by implementing effective data access controls, encryption, and backups
- Keep user access secure by managing permissions, enforcing strong passwords and MFA, or using Key Pairs
- Protecting cloud resources from unauthorized access by implementing networking controls such as VPCs and Security Groups
- Securing and hardening virtual machines OSs, upgrades and security patching
- Securing the specific cloud-hosted applications

The rest of this document describes the controls implemented by Zadara to secure its clouds, as well as security tools available for partners/customers to use.

Infrastructure Security

Physical Security

The Zadara Public Clouds are hosted in the most secure data centers of the leading providers of colocation services. As of the writing of this document, Zadara clouds are hosted at CSquare (Cyxtera) Ascenty and Equinix datacenters. Zadara Federated Edge is also used by many Service Providers and enterprise customers around the globe, where Zadara clouds are hosted at customer or partner datacenters. These data centers feature, at minimum, the following important physical security attributes:

- Dedicated cages
- Biometric access controls
- 24x7 surveillance
- Redundant power feeds and generators
- Robust fire suppression
- Carefully monitored climate control (to protect the servers that store customer data)

In OPaaS (On Premises) deployments, the customer/partner takes full responsibility for the physical security, physical health and physical access to the Zadara systems.

Secure Communication

- The Zadara Provisioning Portal, Command Center, zCompute Console and Zadara VPSA® (Virtual Storage Array and Object Storage) expose RESTful API calls via the **HTTPS** protocol. This requires **TLS 1.2** or higher encrypted communication and securely identifies the Zadara web server with which the client is communicating.
- Zadara GUI clients also communicate with the Storage or Compute web server's RESTful API via HTTPS to ensure the same level of security.
- For HTTPS communication, users can use the built-in Zadara certificate or provide their own certificates.

Protecting the Clouds

Each Zadara cloud is a separate network, connected to the internet for remote management

purposes.
The cloud is protected by a FortiGate firewall with modern capabilities such as Intrusion Detection and Prevention (IDP/IPD). All firewalls are monitored and managed centrally using FortiManager, that also manages centralized deployment of access policies to devices worldwide. These firewalls are upgraded as needed and run the latest approved version that includes security patches. The FW opens only necessary ports. It blocks traffic from known malicious IP addresses and uses Geo-IP filtering to restrict access from specified countries (e.g. Iran, North Korea).
FortiAnalyzer provides real-time visibility, automated threat detection, forensics, and compliance reporting.
Customers have full control over the IP address whitelist to manage and secure remote connections.

System Hardening

All Zadara clouds nodes (both Compute and Storage) are installed from pre-approved server images that are tested and verified by our QA. These images are digitally signed. OS hardening is an integral part of the release development life cycle. Node hardening is done for the purpose of reducing the attack surface and eliminating vulnerabilities:

- Disabling unused network ports and services
- Removing unneeded OS components
- Frequent recycling of complex random passwords
- Applying latest patches for known vulnerabilities

Bug Bounty Program

Via Inspectiv (https://www.inspectiv.com/), Zadara invites security researchers and ethical hackers to report security issues via our Bug Bounty Program. The program offers safe harbor for good faith security testing and cash rewards for vulnerabilities based on their severity and impact. Pen testing findings are addressed according to the severity of the discovered vulnerability.

Data Security and Privacy

We treat all customers' data as highly sensitive and have implemented stringent controls governing this data.

VPSA Architecture

The VPSA architecture provides the basic building blocks for granting complete data privacy for

Zadara Storage users on a multi-tenant cloud:

- Each VPSA Virtual Controller is granted dedicated compute resources (RAM and CPU vCores) and dedicated networking resources (NIC VFs) to partition IO stack data handling per-tenant.
- Physical drives are the basic storage allocation unit. As a result, drives are dedicated to only a single VPSA and hence a single tenant.
- Physical drives are exposed as iSCSI LUNs to the VPSA Virtual Controllers via a separate back-end network, which is internal to the Zadara Cloud.
- IQN-based SCSI **LUN Masking** is used to ensure that physical disk drives are exposed only to the authorized VPSA system.
- Each tenant can look up the physical location (Node) of the drives assigned to that tenant.
- VPSA Block Virtual Volumes are presented as iSCSI/FC/NVMe LUNs and are 'attached' to selected Cloud Servers. Again, LUN Masking and FC zoning is used to prevent access to those Virtual Volumes from other Cloud Servers.
- From the networking perspective, the VPSA is isolated in the customer's VLAN that is connected to the customer's Virtual Private Cloud (VPC) within the public cloud.
- VPSA *requires* the usage of **Challenge-Handshake Authentication Protocol** (CHAP) over iSCSI to authenticate a Cloud Server to a VPSA. CHAP requires that both the Cloud Server and VPSA know a shared **CHAP Secret**. This secret is never sent over the wire.
- The VPSA Supports optional **Mutual CHAP** authentication and **CHAP secret per Server.**

VPSA Data Encryption

Zadara Storage supports Encryption of **Data-at-Rest** (DAR) and **Data-in-Flight** (DIF). Because data encryption requires compute overhead, we leave it up to Zadara users to evaluate the trade-off between security and performance. Hence both DAR and DIF encryption are optional.

Encryption of Data-at-Rest

- Encryption of Data-at-Rest is done at the VPSA Virtual Controller and is defined on a Volume-by-Volume basis, i.e. a user can decide that some Volumes are encrypted, while others are not.
- A VPSA generates a unique random 256-bit **Encryption Key** per encrypted Volume and uses the Advanced Encryption Standard (AES) to encrypt and decrypt the Volume data.
- The Volume Encryption Keys are stored on disk as ciphertext, using AES-256 **Master Encryption Key**, which is generated from a *user-supplied* **Master Encryption Password**. Alternatively, the master password can come from a compliant Key Management System integrated over the KMIP protocol.

The Master Encryption Password is *not* saved on any persistent media. Therefore, each user is fully responsible for retaining and protecting the Master Encryption Password. During VPSA operation, the Master Encryption Password itself is held in kernel memory of the VPSA and the cloud controller. Core-dumping any User Mode process within the VPSA will not reveal the Master Encryption Key.

- The above method ensures that encrypted Data-at-Rest cannot be accessed without explicitly knowing the user-supplied Master Encryption Password.

Encryption of Data-in-Flight

- For advanced security needs, Zadara Storage supports encryption of Data-in-Flight between the hosts and the VPSA storage using **Internet Protocol Security** (IPSec).
- Zadara uses **Internet Key Exchange** (IKE) protocol to negotiate the IPSec encryption keys with a user's host. The encryption keys used to encrypt Data-in-Flight are stored in kernel memory only and are *never* stored on any persistent media. Periodically, encryption keys are renegotiated by VPSA and Cloud Servers' IKE daemons.
- Users of SMB file systems on Zadara storage can use "SMB Encrypt" to secure file traffic of Windows servers.
- A user can configure the renegotiation trigger for each Cloud Server.

VPSA Data Mirroring

Remote Mirroring is the VPSA's Disaster Recovery (DR) service.
Volumes are mirrored from a source VPSA to a remote VPSA. Typically, the remote VPSA resides in a different region, and the data is synchronized over the network.

Authentication

The first step is to establish trusted communication between the VPSAs. It is done by exchanging encrypted secrets using a **public-key encryption protocol** (RSA). Each VPSA generates public and private keys and passes the public key to the other VPSA. The keys are session-based. i.e. re-generated for every new session.

Encryption

VPSA Remote Mirroring is snapshot-based. It creates and deletes snapshots at defined intervals and then mirrors the modified data between two snapshots to the remote VPSA.

For encrypted Volumes on the source VPSA (AES-256), the data is mirrored as-is to the destination VPSA. The Volume encryption key is mirrored as well. It is then stored in encrypted form in the destination VPSA, using the user-provided master password which can be different

than the user-provided master password used on the source VPSA.

For Volumes which are not encrypted at-rest on the source VPSA, the mirrored data is encrypted using AES-256 before it is shipped to the remote VPSA to ensure that the in-flight data is always encrypted.

Like the authentication process, a **public-key encryption protocol** (RSA) is used to exchange random keys for stream encryption.

Note:
For better efficiency, mirroring traffic between 2 VPSAs which are connected via a local FE network rather than via Public IPs is not encrypted.

Object Storage Architecture

Zadara Object Storage provides multi-tenancy at both the Object Storage and Account levels. It uses both 2-Way and Erasure Code data protection to ensure data availability.
Its architecture provides the basic building blocks for granting complete data privacy for Zadara Users. The Object Storage system organizes data in a hierarchy, as follows:

- **Account** (also referred to as Tenant), represents the top-level of the hierarchy. The account admin owns all resources in that account. Accounts are also used to control users' access to objects and containers.
- **Container** (also referred to as Bucket), defines a namespace for objects. In addition to containing objects, you can also use the container to control access to objects.
- **Object** stores data content, such as documents, images, log files etc.

The Cloud Orchestrator assigns dedicated drives for each Object Storage instance, like the VPSA. The drives are provisioned from different Storage Nodes (SNs) for maximum redundancy and performance. Each drive is exposed as a separate iSCSI target from the SN and is LUN masked only to the Object Storage virtual controller (VC). The instance QoS is guaranteed, because neighbors, with provisioned adjacent drives, cannot access the Object Storage drives, impact performance, or compromise privacy and security.

Object Storage Data Encryption

Data-at-Rest encryption is applied by the Object Storage on a per-Container basis. Encrypted and unencrypted Containers can coexist in the same account.

Zadara Object Storage generates a random 256-bit unique Encryption Key per encrypted Container and uses the Advanced Encryption Standard (AES) to encrypt and decrypt the objects data.

The Encryption Keys are stored on disk as ciphertext, using AES-256 with a Master Encryption Key, which is generated from a user-supplied **Master Encryption Password.**

The User owns the Master Encryption Password. It is *never* stored in any persistent media.

Instead, the master password can come from an integrated compliant Key Management System over the KMIP protocol.

Data-In-Flight encryption is implemented by the Object Storage API. Data transfer to and from the Object Storage is done by REST API over https. TLS 1.2 or higher is used.

Compute Architecture

Protecting Virtual Machines

In addition to the standard authentication provided by the VM operating systems (Windows/Linux), the following are provided by the Zadara compute architecture:

- Key pairs are used for ensuring the identity of a user connecting to a VM instance. When a VM instance is created, the user has the option to provide a key pair which will be used for authentication when logging in to the VM.
  zCompute encourages the use of key pairs instead of passwords by providing machine images (VM templates), which authenticate users only when using key pairs, eliminating the use of default passwords.
- With zCompute Security Groups, virtual machines are protected behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing and restricting incoming connections to customer specified IP addresses and ports.
- Each account in zCompute may have multiple projects, isolated from each other.
  zCompute Projects provide the ability for account administrators to manage access permissions to their account's cloud resources, with some users and groups granted permission to a set of projects and other users and groups granted permissions to other sets of projects.
- zCompute projects may have one or more Virtual Private Clouds (VPCs), which are an isolated and closed networking environment.
  VPCs are isolated by design from each other, which also implies they're isolated from other accounts' VPCs, unless explicitly configured by end users, e.g. by assigning an elastic IP to a VM within the VPC and setting security group rules to allow network traffic through that elastic IP.

Protecting Compute Block Storage

One of the key services zCompute provides is block storage.
zCompute users may create block storage volumes (virtual disks) with an arbitrary size as they require and attach these volumes to VMs. Users may also take snapshots of such volumes to allow fast recovery.

zCompute also provides protection groups, which are a service that automates taking snapshot backups of protected resources (volumes and whole VMs) for fast recovery.

Block storage in zCompute leverages Zadara VPSA technology, with some additional security measures:

- Data-at-rest:
    - Volumes created on VPSAs assigned to zCompute block storage are always encrypted, with the encryption key managed internally within zCompute only. This setting is enforced and validated internally to make sure all volumes are encrypted and to prevent any use of non-encrypted volumes.
- Data-in-transit:
    - iSCSI CHAP authentication is always used between the zCompute nodes and the VPSAs' interfaces.
    - The VPSA REST API access is always authenticated and TLS encrypted.
    - The VPSA iSCSI network interfaces are isolated, inaccessible outside the zCompute cloud boundaries, accessible only internally from the zCompute cloud's hosts over an internal dedicated VLAN assigned for this purpose.

Data Retention

Zadara retains the customer data for as long as the customer uses the service and doesn't delete the data. With Zadara Object Storage, users can set an expiration date for each object, after which the object is automatically removed.

Data Deletion

Zadara allocates dedicated drives for each customer. This allows drives to shred when the customer removes data or stops the services. When customers delete the data, they can either use logical shredding in accordance with the DoD 5220.22-M standard, or buy the used drives from Zadara and physically destroy them.

Data Protection

VPSA Data Backup to Object Storage (B2OS)

Data copied to or from S3 or any other equivalent object storage such as Zadara Object Storage, is transferred using the HTTPS protocol, so that the data in-flight is encrypted using SSL.
The data which is stored in S3 is encrypted using S3 server-side encryption.
If the data is encrypted at-rest on the source VPSA, it is decrypted before it is sent over HTTPS to the object storage.

VM Backup to Object Storage (B2OS)

zCompute Backup to Object Storage (B2OS) is an integral feature of zCompute. It provides full backup and recovery functionality without requiring third-party software or installing software agents on protected VMs.
B2OS extends backup and restore capabilities beyond local block storage. It enables backing up and restoring VMs and volumes that are protected by protection-groups to and from Zadara Object Storage systems.
These Zadara Object Storage systems can also reside in different physical locations than the source zCompute cloud, allowing recovery to any zCompute cloud in the event of a site-level failure.
Protection Groups also provide VM-level crash-consistent backups. Backup snapshots are taken as an atomic operation on all volumes of a protected VM, treating the VMs volumes as a consistency group.

Access Control

Cloud Identity Management

- Each Zadara user creates an account within the Zadara Provisioning Portal. A cryptographic hash value is stored for further login authentications. The user's **Password** is *not* kept. MFA can be enabled on an account.
- Zadara Provisioning Portal supports Dual Factor Authentication using an authenticator mobile app.
- The Cloud Console provides an initial temporary access code via an email. The user must enter a strong **User Password** to replace the temporary access code.
- The Zadara Provisioning Portal password, the zStorage password and the zCompute user password can be different from each other. This enables support for different permission levels (roles) within an organization.

- Once customers login to the Provisioning Portal, they can only view their existing Compute account and VPSAs. A customer's access is limited to their provisioned systems, with no visibility into the rest of the Zadara Cloud. The customer can create new services and modify and delete existing cloud services.
- In the event of a user forgetting their password, an email will be sent to the user with a new temporary access code. The existing user password will secure access until the new access code is used.

VPSA Identity Management

- Only a cryptographic hash value of the user password is stored in the VPSA database for further login authentication.
- VPSA admins can control the user password policy, such as password expiration, password length and history retention. An admin can also enforce MFA.
- Users can change their passwords and reset their API access keys at any time
- VPSA admins can create additional users and assign their roles that define access rights.
- All Zadara Web applications support Dual Factor Authentication using an authenticator mobile app.

NAS Users Access

File system access is granted to each user according to the defined permissions.
VPSA supports both local users and Active Directory central user management.

Object Storage (NGOS) Identity Management

Object Storage Users and Roles

There are 3 types of roles assigned to VPSA Object Storage (ZIOS or NGOS) Users:

- The user registered in the Zadara Provisioning Portal who orders the VPSA Object Storage is assigned as its Administrator.
- **ZIOS Administrator** is a super-user with the privileges to create accounts and users of any role. Users with the ZIOS Administrator role can perform container and object operations across accounts.
- **Account Admin** can create an account using the Self Account Creation Wizard, and can manage their own accounts. They can perform any user management and container and object operations. An Account Admin can set password policies and enforce MFA for all members.

- **Member** can do Object Storage operations according to the permissions granted by the Account Administrator, within the limits of that account. These operations include creating, deleting and listing containers, and creating, deleting and listing objects.

Object Storage Access

Buckets and objects can be accessed either via OpenStack Swift or AWS S3 interfaces.

- **OpenStack Swift** (V3 Authentication) – Authentication via the V3 Auth Endpoint, using a username and password
- **AWS S3** – Using Access Key and Secret Key pairs

Compute Identity management

The zCompute architecture provides the basic building blocks for granting complete data privacy for Zadara Users:

Zadara zCompute is designed, top-down, as a multi-tenant platform.

Accounts in zCompute are fully isolated from each other, providing tenancy isolation. Each account has its own set of resources such as users, groups, and projects, which are fully isolated from any other account, i.e., permissions can be granted within an account to users of that account only, and account users have no visibility into other accounts, including their very existence.

Any zCompute user may be assigned the following roles:

Member role allows the user to use the console, policies and APIs for creating, viewing, modifying and deleting virtual resources such as VMs and belonging to projects to which the user has been assigned. This is the standard role for most users.

Tenant Admin role holders can use all functions which are granted to a Member role holder. In addition, users with the Tenant Admin role can use policies and APIs for creating and managing new projects and users within a specific account. The user that is registered on the Zadara Provisioning Portal for Compute services, has the role of Tenant Admin and is responsible for managing the account on behalf of their organization. The Tenant Admin can create additional Tenant Admins. They can also control the user password policy, such as password expiration, password length, history retention and enforce MFA.

Cloud Admin/MSP Admin role holders can do everything on the cloud including creation of new accounts and users of these accounts. The Cloud Admin role is used by Zadara to manage the cloud resources, settings, etc.

Roles define the maximum permission level a user may be granted.

Roles work in conjunction with Symp API Policies and AWS API Policies, which may be used to further **limit** users' permissions in a granular fashion. For example, a user may be assigned a Tenant Admin role with a Symp API StratoReadOnlyAccess policy and an AWS API ReadOnlyAccess policy, which will result in the user having read-only access to all aspects and objects created within their account, without the ability to change any of them.

Corporate Security

Policies

The Zadara security program consists of a series of security policies covering the domains listed in both the ISO 27001 standard and the requirements of System and Organization Controls 2 (SOC 2) by AICPA. The security policies and procedures are available internally to all employees to ensure they understand the bar they are expected to meet when it comes to security. All employees are required to confirm they have read and understood the related policies and the consequences of not following them. The policies are updated annually, and when we observe new threats and risks that require modifications to our security approach.

Background Checks

Zadara clearly understands the importance of protecting information that belongs to our customers. This influences our hiring processes and employee onboarding.
To maintain trust in Zadara's employees, all candidates are subject to background checks. Candidates are accepted as employees only after background checks have been completed, and references are checked.

Onboarding and Offboarding

Zadara's Onboarding process ensures new hires have the necessary tools to be productive while immediately enforcing security hygiene.

- **Access Control Implementation:** Applying the principle of least privilege, granting access only to systems necessary for the specific job role.
- **Device Security:** Employees are provided with company-approved devices encrypted with solutions such as BitLocker and FileVault, along with security software such as endpoint protection and Endpoint Detection and Response (EDR).
- **Security Training:** Security training is conducted to cover phishing, passwords, and data handling policies.
- **Identity Verification:** All employees are required to use MFA.
- **Policy Acknowledgement:** Employees are required to sign Security and Acceptable Use Policies.

Offboarding is a critical security function that, if skipped, can lead to lingering access and data breaches.

- **Prompt Access Revocation:** We revoke access to cloud applications, email, VPNs, OpenOTP and SaaS tools on the employee's last employment day.
- **Asset Recovery:** We retrieve all company property, including laptops, keys, and access badges.
- **Credential Rotation:** Shared passwords are rotated and user access to secrets management systems is removed.
- **Data Backup:** Document ownership is transferred to the manager or another employee. Email and critical data from the user's account is backed up.
- **Exit Interview:** HR conducts an exit interview and reminds employees of their ongoing obligation to keep company information confidential.

Training

Awareness training is provided to our employees annually. We advance and reinforce data protection guidelines and technologies through ongoing security training. Secure coding training is also part of our SW development lifecycle.

Operations Access control

Zadara Operations and Support teams access the cloud infrastructure for monitoring and maintenance purposes. Access to production clouds and to Compute or Storage Nodes and Virtual Controllers is restricted only to authorized Operations and Support personnel.
To ensure comfort that people who have access to Zadara's production clouds can always be trusted, Zadara takes the following measures:

- Employees are subject to background checks
- Employees must respect the company security policy and code-of-conduct
- Employees perform professional and security training courses

All incoming and outgoing traffic from the Zadara Cloud to the Internet is protected by complex firewalls. Access is allowed from Zadara's IP addresses only and requires either Teleport permission or VPN login using MFA with a one-time password (OTP). Teleport access is based on outgoing traffic only from the cloud into Zadara. Managers can grant Teleport access to specific employees for a limited period of time, as needed.
Access to Virtual Controllers also requires MFA with OTP. This access is allowed with a limited command set with no visibility into the customer's file systems. Zadara personnel access is limited to the cloud and VPSAs metadata (Configuration Data).

Whitelist access to the Command Center cloud management tool is controlled by the customer and requires MFA with OTP.
Access to the VPSA GUI for Zadara cloud administrators is controlled by the customer's VPSA admin.
Zadara maintains full auditing track for the cloud and the VPSAs in its Access Log. These logs are kept within the cloud, backed up to AWS S3, and never expire.

Mobile Devices

Laptops are centrally managed and are secured with full disk encryption. All laptops are protected by Bitdefender Endpoint Security featuring Endpoint Detection and Response (EDR) capabilities to detect and remediate threats. We apply updates to employee machines on an ongoing basis and monitor employee workstations for malware and anomalous activity. We also can apply policies or remotely wipe machines. Wherever possible, we use MFA to further secure access to our corporate systems and infrastructure.

Software Development

Development Process

Zadara practices its own version of agile software development.
Our goal is to maintain the agile pace of development, while introducing security in ways that accommodate simple and efficient processes. As a provider of enterprise storage, our product must be highly available and maximally secured.
Information security and privacy is part of every level of the Agile process: Vision, Roadmap, design, Release, Iteration or Sprint, and QA.
Developers are responsible for identifying security and privacy risks and considerations when designing and implementing new features and application architecture.
For every change that might affect the integrity of data, the test plan is updated.
Manual code-reviews and automated static and dynamic scans are performed against critical code modules, such as authentication, encryption, session management, and other sensitive code pieces.
Vulnerabilities and flaws are tracked and tested in regression tests.

Source Code Security

All code for Zadara products is managed via GitHub, with enforced access controls and change controls ensuring only those with an approved business need to modify this code are granted such access. Access to GitHub requires MFA, and employees need to be on a company-issued and managed laptop to access the codebase. All code changes require code review, and automated tests must pass before any code is merged into the main tracking branch.

Business Systems

Zadara Storage uses cloud services (SaaS) for all its business applications, such as CRM, HR and finance.
Zadara protects its SaaS (Software as a Service) business systems by implementing a multi-layered security strategy that combines technical controls, rigorous vendor assessment, and continuous monitoring, often under a **shared responsibility model**.

Access Management

- **Multi-Factor Authentication (MFA):** Requiring MFA for all SaaS applications.
- **Single Sign-On (SSO):** Centralizing authentication using Google SSO wherever possible.
- **Role-Based Access Control (RBAC):** Implementing the principle of least privilege ensures that employees only access data necessary for their roles.

Data protection

- **Encryption at Rest and in Transit:** Ensuring sensitive data is encrypted using protocols like TLS 1.3 to prevent interception.
- **Backup and Recovery:** Using cloud-to-cloud backups to protect against data loss caused by human error or ransomware.
- **Credit Cards:** Zadara does not store credit card info.

Vendor Assessment

- **Compliance:** Evaluating SaaS vendors for security and privacy controls and certifications (ISO27001, SOC2, GDPR). Introducing a new system to Zadara requires CISO approval.

Compliance

Zadara Storage services are compliant with most of the common security standards and regulations.
Zadara goes under annual audits to maintain the following certifications:

- **SOC1 Type II / SOC2 Type II**
  SOC 1/2 compliance provides businesses with confidence and peace of mind that their data is secured and highly available.
- **ISO27001 / 27017 / 27018**
  ISO27001 is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

The ISO27017 standard provides guidance on the information security aspects of cloud computing.
The ISO27018 standard provides guidance aimed at ensuring that cloud service providers offer suitable information security controls to protect the privacy of their customers' clients.

- **IRAP**
  Infosec Registered Assessors Program (IRAP) is the security standard of the Australian government.
- **HIPAA**
  The Health Insurance Portability and Accountability Act (HIPAA) is a standard for sensitive patient data protection.
- **GDPR / ISO27701**
  The General Data Protection Regulation (GDPR) is the European privacy law that protects European Union (EU) citizens' right to privacy.
  Zadara is an active participant in the EU-U.S. DPF and UK-U.S. DPF programs.

More information about Zadara certification can be found at our site:
https://www.zadara.com/edge-cloud/compliance/

More information about Zadara Cloud Services can be found at our site:
http://www.zadara.com