Contents

© Mithi Software Technologies

© Mithi Software Technologies

Background

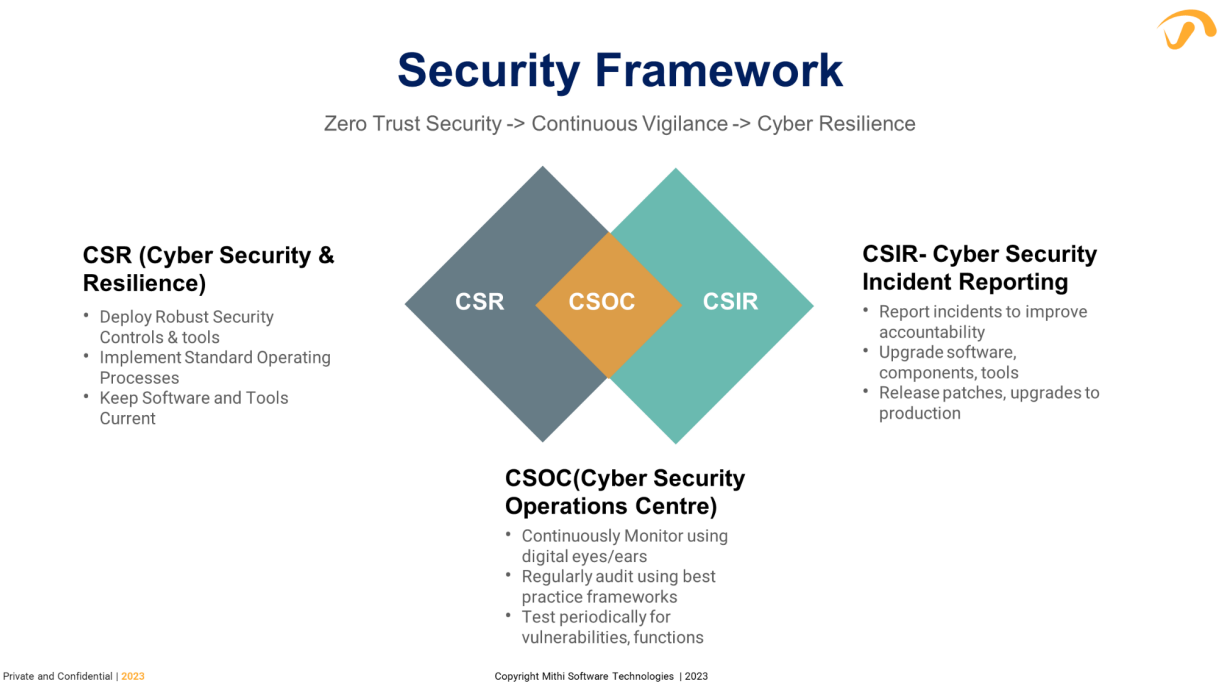
Mithi specializes in Data Protection solutions. The company offers cloud-based SaaS solutions to enterprises. Mithi's solutions are well known for their bulletproof security, rock-solid reliability, and high performance on a massive scale.

This document will give you an idea about our cloud security framework that protects your data with multiple layers, making it nearly impregnable.

Overview

Security framework

Mithi's security framework comprises three core elements, as shown below:



From Infrastructure to Periphery, our multiple-layer security systems cover them all.

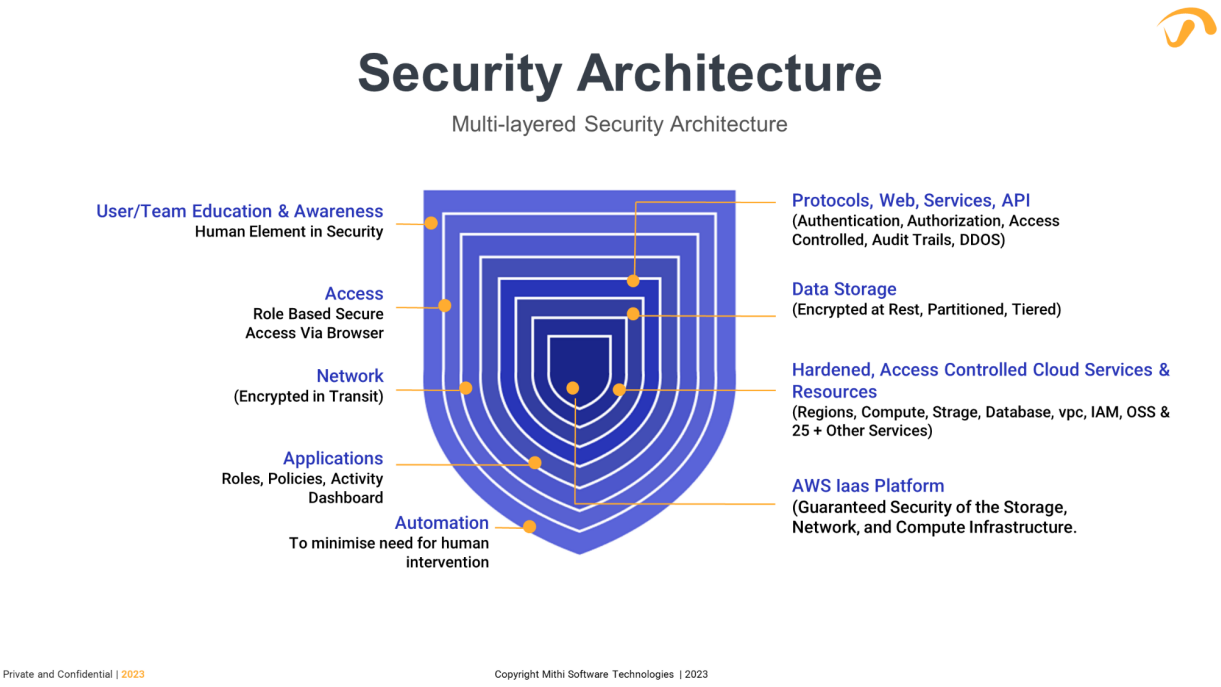
The **CSR (Cyber Security and Resilience)** framework is the foundation that secures the platform using Industry-level best practices and modern solutions.

© Mithi Software Technologies

Our **CSOC (Cyber Security Operations Center)** maintains vigilance on the platform layers to ensure that the platform stays secure. The vigilance includes periodic VAPT scans via independent CERT-IN empaneled vendors and annual FTR (Foundational Technical Review) by independent AWS experts, amongst other initiatives.

If any breach or incident is discovered, our CSOC team takes rapid action to nullify the impact of the incident, neutralize the threat, and report/escalate the incident in a structured manner to the **CSIR (Cyber Security Incident Reporting)** team to build resilience via a time-bound long-term prevention plan.

Security Architecture



Mithi's cloud services are built on the AWS cloud platform and leverage AWS's shared security model.

Security OF the cloud: AWS operates, manages, and controls the IT components from the host's operating system and virtualization layer down to the physical safety of the facilities where the services operate.

Internal and External auditors scan the AWS environment so that the infrastructure and services are of industry certification level. Customers can use these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

© Mithi Software Technologies

Security IN the cloud: Mithi operates, manages, and controls the digital communication, collaboration, and data management platform, services, and applications. This platform comprises the cloud computing, storage, network resources, and operating systems up to the applications and services running on this infrastructure. It secures the platform with multiple layers using industry best practices to achieve cyber resilience.

Mithi ensures adherence to several regulatory standards across industries such as **RBI** (Reserve Bank of India), **SEBI** (Securities and Exchange Board of India), **IRDAI** (Insurance Regulatory Development Authority of India), and **GDPR** (General Data Protection Regulation), which when taken together, create a comprehensive set of security guidelines.

© Mithi Software Technologies

Security Practices and Controls at Each Layer

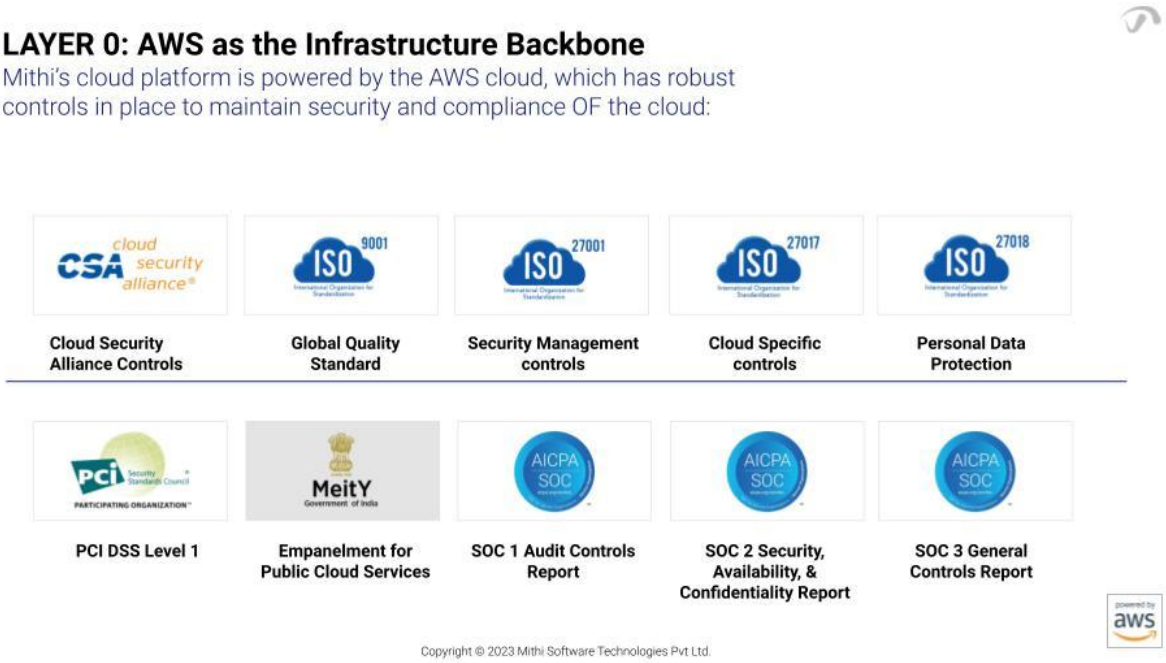
Infrastructure

This Security OF the cloud is the responsibility of AWS. AWS environments are continuously audited to provide Security of the Cloud, and the infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. Customers can use these certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications. The AWS compliance program is based on the following actions:

- **Validate** that AWS services are facilitated across the globe to maintain a ubiquitous control environment operating effectively.
- **Demonstrate** the AWS compliance posture to help customers verify compliance with industry and government requirements. AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and control establishments that are operated by AWS.
- **Monitor**: AWS maintains compliance with global standards and best practices through thousands of security control requirements.

AWS has obtained certifications and independent third-party attestations for various industry-specific workloads such as ISO 27001, ISO 27017, ISO 27018, ISO 9001, PCI DSS Level 1, SOC, and many more.

© Mithi Software Technologies



By tying together governance-focused, audit-friendly service features with such certifications, attestations, and audit standards. AWS Compliance enablers are built on traditional programs, helping customers to establish and operate in an AWS security control environment.

For more information, see the [AWS Cloud Compliance webpage]

By choosing AWS, Mithi has ensured that the core infrastructure platform driving all our applications is highly reliable, secure, and guaranteed.

Resources

Mithi's cloud platform uses AWS services as a host for computing, storage, load balancing, serverless processing, API security, etc. These resources run operating systems, services, and applications to serve the platform's communication, collaboration, and data management workloads.

To maintain the security of these resources IN the cloud, Mithi follows global best practices, some of which are mentioned below:

Control	Description

© Mithi Software Technologies

Region	Delivering to the Data Residency requirement of regulators and laws. Our digital collaboration platform is served from multiple regions of the AWS cloud to support the data residency requirement by our customers. Customers can choose their region during onboarding. This guarantees that the data stored in the region is never moved to another region.
VPC	Logically isolated Virtual Private Clouds for Internet-facing and private resources. Within each region, our platform's resources reside in several logically isolated sections of the AWS cloud (each a Virtual Private Cloud). The resources in each VPC are further layered into Internet-facing and private resources. They are secured using different subnets (public-facing and private-facing), security groups, and network access control lists.
IAM *(Identity and Access Management)*	Granular, multi-level, minimal privilege roles to Teams to minimize the human impact on security. Teams with access to these resources are provided limited privileges linked to their role in the operations. The controls deployed are granular to reduce the human element's impact on security. They include (but are not limited to) time of day access, originating IP address, SSL, and multi-factor authentication.
Operating Systems	Hardened and aligned to that server's role to reduce surface area of exposure. Our compute nodes are configured/hardened and aligned to that server's role to reduce exposure's surface area. Some of the best practices to secure the nodes at this level are role-based user access, minimal services, protected credentials, audit trails, and updated security patches secured by local firewalls on each node.

© Mithi Software Technologies

Security Group Firewall	An additional AWS-level firewall acts as the primary line of defense. This is an AWS-level firewall in addition to the firewalls on our operating systems and acts as the primary line of defense. This is configured in deny-all mode, with ports open based on protocols aligned to the server role, public/private posture, and source IP address. All internal servers are locked to access only from our NOC and service centers to reduce any chance of exposure.
Cloud Storage	All critical data is stored in a highly durable cloud object storage service, controlled with strict IAM policies, and encrypted at rest. All critical data is stored in a highly durable, elastic, redundant cloud object storage service, which offers the durability of 11 9s. The cloud storage buckets are controlled with strict IAM policies and are connected only to the relevant compute instances for access via the applications. The information on the cloud storage is encrypted at rest.

Data

Data comprises customer information, user information, application data (most significantly mail data), logs, etc. To protect and secure all this data in the cloud, Mithi deploys the following controls:

Control	Description
Partitioning	Virtually separate data of each customer. Augmented by introducing the private deep archive, which can reside in the customer's cloud account. Data for each customer is partitioned virtually in the storage and is accessible via authenticated and authorized users of the applications and APIs.
Durability	All data is written to extremely durable cloud storage services, which store each piece of data in multiple redundant locations to achieve 11 9s of durability.

© Mithi Software Technologies

Encryption	Data is encrypted at rest using AES 256-bit encryption to prevent data visibility in the (unlikely) event of unauthorized access or theft.
Tiering	Tiering data across three storage classes optimizes costs, making it three times more difficult to access and steal data. The information/data is spread across Hot, Warm, and Cold storage mediums depending on the frequency of access. This not only improves performance and reduces costs, it also improves security.

Services and Applications

These include all the mailing services, contact management services, calendar services, chat services, etc. Other applications, such as the administrator console, end-user web client, etc, are also included. Only through these tools can a user or an administrator access their data.

The services and applications are protected by ensuring only authorized people can log in to the service using authenticated credentials, which are protected by strict password policies and account lockout policies.

Within the user's or administrator's access, you can finely control the features available to each user or administrator depending on his role in the organization.

Control	Description
Rate Controls	Usage limit thresholds prevent misuse and alerts for abnormal usage patterns.
Audit Trails	A complete record of all activities done by each user ensures full visibility into the use of the services and applications
Immutable and Tamper-proof	The Delete right is off in all roles by default, and there is no way to modify data in the archive. This ensures that the archive account can never be tampered with. At a foundational level, the data is encrypted at rest, further ensuring that tampering is impossible.

© Mithi Software Technologies

Secure Development Practices	We follow secure coding practices to minimize vulnerabilities in the application code and regularly update and patch software to address known vulnerabilities.
Encrypted in Use	Access to each service and API is over secured, encrypted protocols.

Access

At this layer, you can decide which users access which services and applications and from where. By default, all services and applications are accessible from anywhere.

Control	Description
Block services	Granularly block/enable specific services for single or multiple users or the entire domain/organization. This is useful to ensure that your users access the applications using a prescribed method.
Trusted IP ranges	Allow access to services only from trusted IP ranges, such as the office IPs, to ensure that nobody outside the network can access the applications, making them very secure.
Authentication	Users are required to authenticate before they can use any service securely.
Authorization	You can control fine-grained access to the products and their features, services for individual users, groups of users, or the entire domain. By controlling privileges, you are preventing intentional or accidental misuse of the platform.
Strong Password Policies	Strong Password Policies include minimum length, complexity rules to force users to enter a strong password, storing password history

© Mithi Software Technologies

	to prevent reuse of older passwords, expiry to force a password change, etc.
Account lockout	Services are further protected from DDOS attempts using the account lockout capability, where multiple invalid login attempts can result in an automatic account lockout that can be re-opened only through administrator intervention.

Periphery

This is a critical layer since it serves as the entry point for all data into the network. This layer prevents major issues downstream by ensuring only clean mail gets through.

Control	Description
WAFs & Firewalls	Multi-layered firewalls monitor incoming and outgoing traffic to thwart any breach attempts.
DDOS prevention	All internet-facing ports on all computer instances are configured with DDOS throttles to slow down, dissuade and frustrate attackers.
Source binding	Data ingested into Vaultastic is allowed only from trusted sources, which are bound during onboarding or a strict change management process mid-term.
Bare minimum surface area	Resources are layered to minimize Internet-facing surface areas and protect critical data in the (unlikely) event of a breach.

Network

This is the Internet link between our platform, other platforms, and end-users. All network traffic is encrypted using Transport Layer Security 1.2 (TLS, formerly called Secure Sockets Layer [SSL]) with an industry-standard AES-256 cipher. TLS is a set of industry-standard cryptographic protocols used to encrypt information exchanged over the wire. AES-256 is a 256-bit encryption cipher used for data transmission in TLS.

Control	Product	Description

© Mithi Software Technologies

Encryption	All products	All information is encrypted in transit to prevent eavesdropping and data theft during motion. Access by end-users and all inbound and outbound connections are supported only via TLS-enabled protocols to adhere to the "encrypt in transit" policy.
VPN *(optional)*	All Products	Specific use cases in several organizations involve end-users with no Internet access. Typically, these are high-security zones where users have access to highly private and confidential information and, hence, are blocked from using the Internet. Mithi supports deploying a Site-to-Site IPSec VPN tunnel between the customer location/HO and your resources in the AWS cloud.

User Awareness and Education

Shore up your company's first line of defense. Mithi understands that the human is the weakest element in the security chain despite all precautions. The human threat to cybersecurity is broken down into two areas: intentional breaches and unintentional breaches.

Unintentional breaches are the most common type of cybersecurity breach. In most cases, these occur when a user executes some malware on their computer. The malware could be in the form of an e-mail attachment, a link in an email, or downloaded from the Internet.

Intentional breaches are less frequent but usually have a much higher cost for the organization.

> ***In a study done on security breaches in enterprises, it was observed that 50 percent of the breaches had a substantial insider component. What's more, it was not mostly malicious behavior, the focus of so many companies' mitigation efforts. Negligence and co-opting accounted for 44 percent of insider-related breaches, making these issues all the more important. - McKinsey***

We believe the phrase "prevention is better than cure" will help mitigate the 44% inside breaches related to negligence. Mithi provides extensive documentation, videos, and pre-recorded

© Mithi Software Technologies

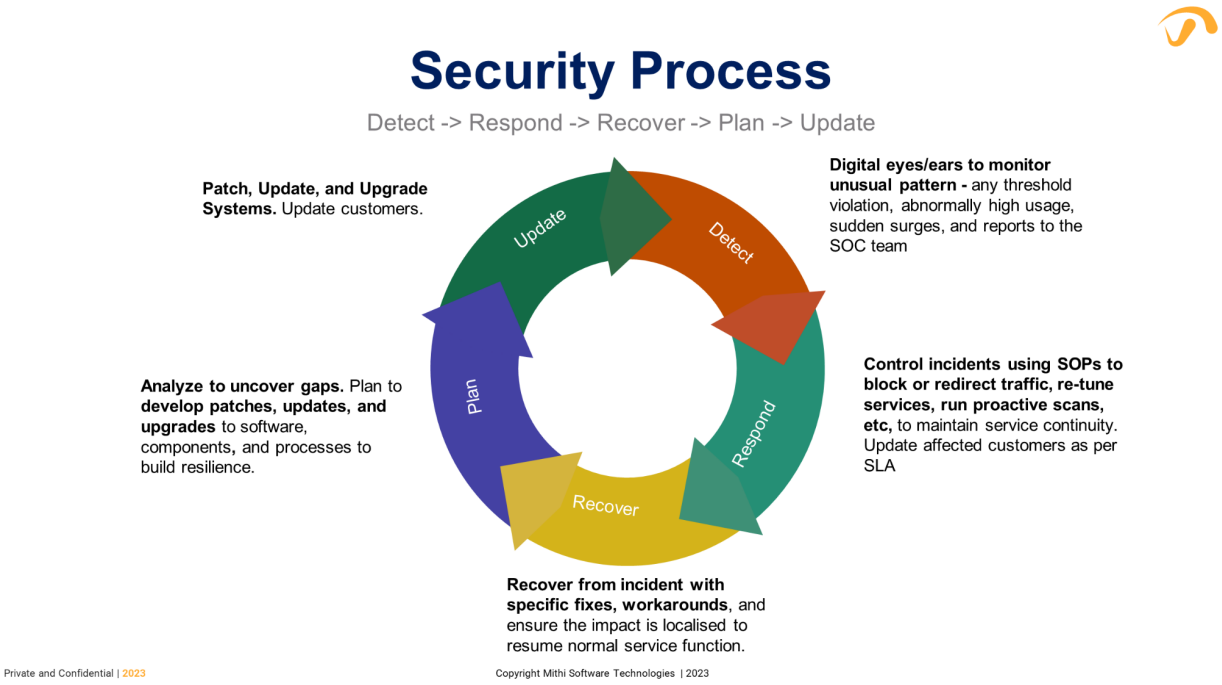
end-user training modules to help educate your end-users about best practices to secure their credentials and cloud accounts.

Too often, cyber security training programs focus only on behavior by educating employees on proper cyber procedures and miss the culture part of the equation. Targeted communications such as periodic alerts on cyber-impact help employees see and feel the importance of "security hygiene." Purposeful reinforcement from senior executives is critical to achieving cooperation from the workforce.

We recommend that you leverage these content pieces to build your content and training programs and run them on an ongoing basis, with assessments thrown in to keep users on their toes.

Security Process

It's not enough to just configure security at all layers. Considering new threats, ongoing software and service upgrades, new usage patterns, etc., monitoring the platform to maintain security levels proactively is essential.



© Mithi Software Technologies

Detection

Visibility is the first fundamental aspect of gaining control of the platform's security. Mithi has created digital dashboards that monitor key parameters of the platform to indicate the security level at all layers.

Any threshold violation, abnormally high usage, sudden surges, etc., are flagged automatically for investigation by the SOC team, which is active 24/7.

Inbound Reports

If an incident is detected by our customers, NOC teams, backend teams, or customer support teams, the same is reported to the SOC team for immediate remediation.

Respond & Report & Recover

The SOC team is trained to control the spread and impact of any detected incident using standard operating procedures. These could involve blocking offending connections, re-tuning services, redirecting traffic, running proactive scans, and more.

Depending on the severity and impact of the incident, the SOC team may choose to intimate impacted customers via email or any other suitable media and may request action from the customers.

Resilience

The SOC team escalates all incidents to the backend & product teams, with detailed supporting resources to help them perform forensic analysis and work out a long-term mitigation and prevention plan. All incidents are tracked in an issue tracker for analysis, audit trail, and reference.

Independent Audits and Certifications

Periodic third-party Audits

Mithi engages a CERT-IN empaneled vendor to periodically perform a security scan on our platform, ensuring closure of all reported points within defined timelines.

© Mithi Software Technologies

Adherence to cyber security guidelines of multiple sectors

Mithi ensures adherence to several regulatory standards across industries, such as **RBI** (Reserve Bank of India), **SEBI** (Securities and Exchange Board of India), **IRDAI** (Insurance Regulatory Development Authority of India), and **GDPR** (General Data Protection Regulation).

The collective guidelines form a comprehensive cyber security checklist covering technology, people, and processes.

Since the effects of these guidelines are to improve the generic security of the platform at all layers, the benefits are seen by all our customers across verticals.

AWS-FTR

The AWS FTR (Foundational Technical Review) has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications.

This independently conducted audit covered a detailed review of all the controls deployed on the cloud platform and the processes we follow to maintain vigilance and build resilience. The audit focuses on security, reliability, and operational excellence. The FTR audit repeats annually.

Learn more: How Mithi builds greater trust & reliability with the AWS FTR audit.

Document Revision:

Created on	***23rd July 2019***
Last Modified	***20th Dec 2023***

© Mithi Software Technologies