Contents

Background

Mithi specializes in Business Communication, Team Collaboration, and 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 at a massive scale.

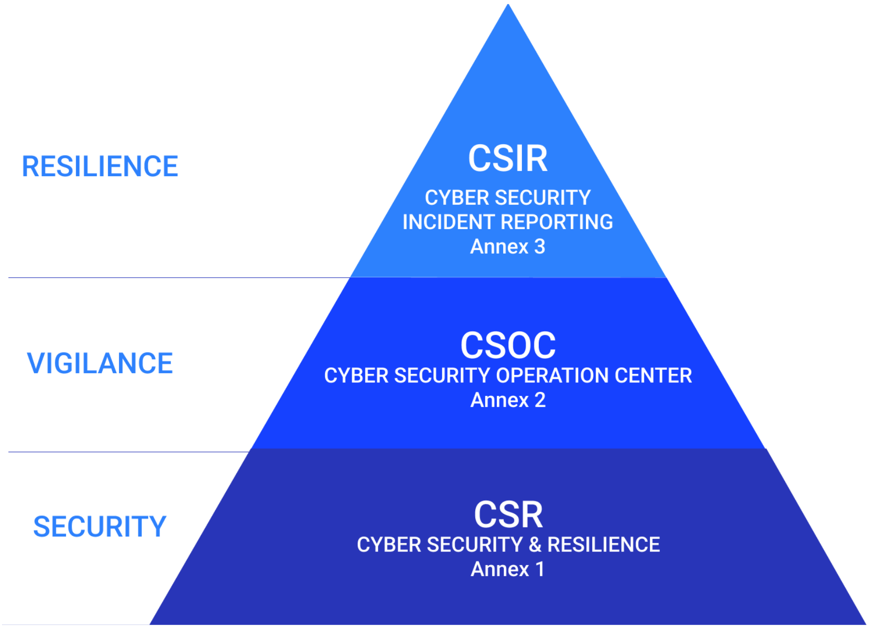
This document will give you an idea about our cloud security framework that protects your data with multiple layers, making it nearly impregnable.

Mithi's cloud platform comprises the following products/building blocks, all covered by the same multi-layered security framework

skyconnect	**Keep your business communication flowing** Secure, Reliable, Efficient Cloud email services for every business
vaultastic	**Data Advantage for Every Enterprise** Agile Data Management for Critical Business data to support Business Continuity and Change Readiness.
Legacyflo	**Cloud Data Migration Tool** Move data easily using Legacyflo's Automatic Migration software.
clrstream	**Fortify your email server setup with ClrStream** Email Security and Disaster Recovery for Uninterrupted business communication
ideolve	**Gain visibility & control on critical business data and processes** Work better with teams and partners through better visibility & collaboration

Overview

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


RESILIENCE
CSIR
CYBER SECURITY INCIDENT REPORTING
Annex 3
VIGILANCE
CSOC
CYBER SECURITY OPERATION CENTER
Annex 2
SECURITY
CSR
CYBER SECURITY & RESILIENCE
Annex 1

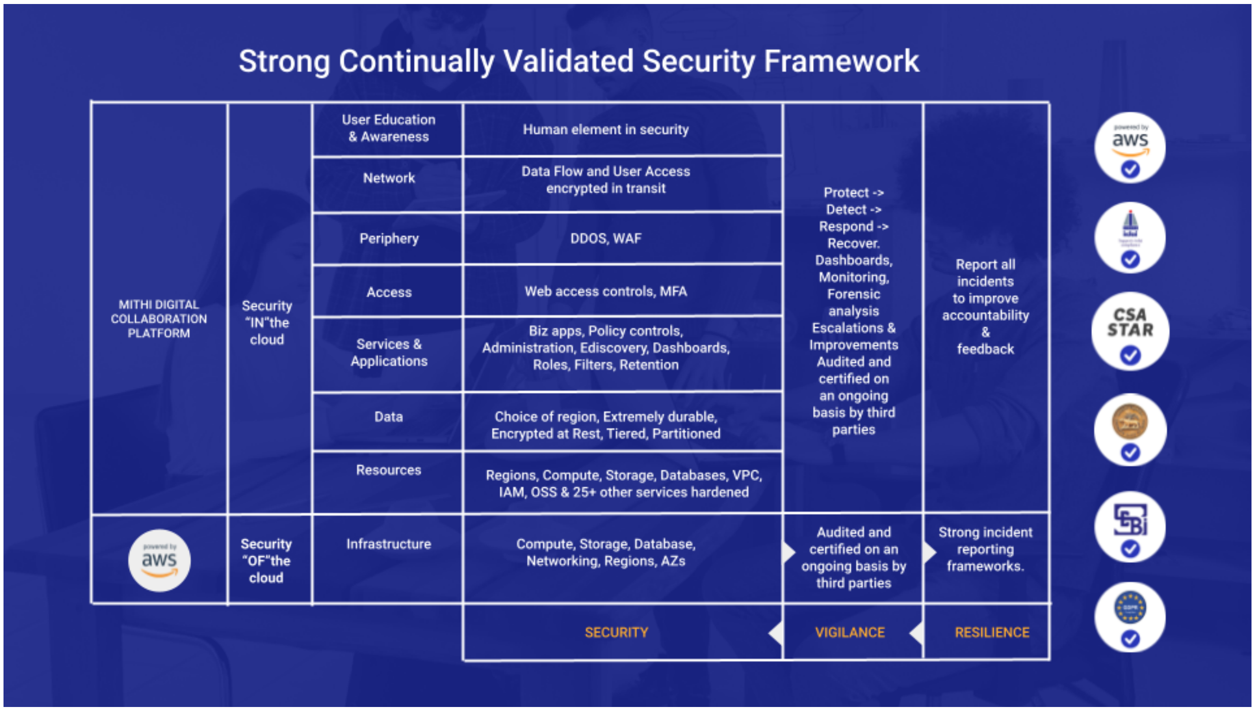
From Infrastructure to Periphery, our multiple layer security systems cover them all.

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

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.

The Cloud Shared Security model at a glance



Strong Continually Validated Security Framework

MITHI DIGITAL COLLABORATION PLATFORM	Security "IN"the cloud	User Education & Awareness	Human element in security	Protect -> Detect -> Respond -> Recover. Dashboards, Monitoring, Forensic analysis Escalations & Improvements Audited and certified on an ongoing basis by third parties	Report all incidents to improve accountability & feedback
		Network	Data Flow and User Access encrypted in transit		
		Periphery	DDOS, WAF		
		Access	Web access controls, MFA		
		Services & Applications	Biz apps, Policy controls, Administration, Ediscovery, Dashboards, Roles, Filters, Retention		
		Data	Choice of region, Extremely durable, Encrypted at Rest, Tiered, Partitioned		
		Resources	Regions, Compute, Storage, Databases, VPC, IAM, OSS & 25+ other services hardened		
powered by aws	Security "OF"the cloud	Infrastructure	Compute, Storage, Database, Networking, Regions, AZs	Audited and certified on an ongoing basis by third parties	Strong incident reporting frameworks.
			SECURITY	VIGILANCE	RESILIENCE

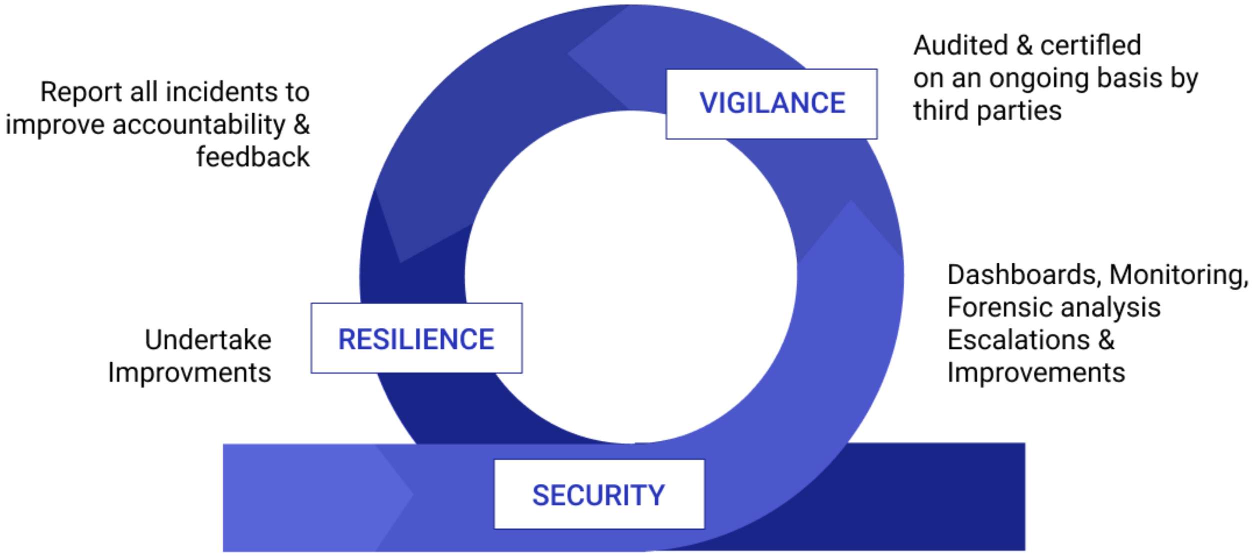
Mithi's Cloud services are built on the AWS cloud platform and leverage the shared security model of AWS.

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.

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 compute, 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.

Security Framework for Mithi’s Cloud Platform


Report all incidents to improve accountability & feedback
VIGILANCE
Audited & certified on an ongoing basis by third parties
Dashboards, Monitoring, Forensic analysis Escalations & Improvements
Undertake Improvments
RESILIENCE
SECURITY

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.

Security Practices at each Layer

Infrastructure

This Security OF the cloud is the responsibility of AWS. To provide Security of the Cloud, AWS environments are continuously audited, 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 controls establishments and is 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.

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 extremely reliable, secured, 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
Region	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	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**)**	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	Our compute nodes are configured/hardened and aligned to that server's role to reduce exposure's surface area. From role-based user access, minimal services, and protected credentials to audit trails, onto updated security patches secured by local firewalls on each node, are some of the best practices to secure the nodes at this level.
Security Group Firewall	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, elastic, redundant cloud object storage service, which offers the durability of 11 9’s. 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	Product	Description
Partitioning	All Products	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 Products	All data is written to extremely durable cloud storage services, which store each piece of data in multiple redundant locations to achieve 11 9’s of durability.
Encryption	All Products	All data at rest is encrypted using the encryption facility provided by the cloud storage service. This prevents data visibility in the event of unauthorized access or theft.
Hierarchy	All Products	The information/data is spread across Hot, Warm, and Cold storage mediums depending on the frequency of access. This not just improves performance and reduces costs, it also improves security. Thus, attempting to steal data would mean gaining unauthorized access to 3 separate storage mediums, making the task near impossible.

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	Product	Description
Authentication	All Products	Users are required to securely authenticate before they can use any service.
Password policies	All Products	Strong Password Policies include minimum length, complexity rules to force users to enter a strong password, storing password history to prevent reuse of older passwords, expiry to force a password change, etc.
Account lockout	All Products	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.
Authorization	All Products	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.

		For E.g. no user can set auto-forward to an external email id, junior admins get access only to limited functionality, etc.
Tamper-proof	Vaultastic	The access to the users is, by default, without "delete" rights. 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.
Data leak prevention	SkyConnect	Mail policies allow you to control mail flow based on rules, which are defined using the mail attributes such as from id to id, cc id, subject content, attachment names, attachments, etc. By defining these rules based on the role of the users in the organization, you would be preventing accidental or intentional leakage of information. E.g. disallow a certain set of users from sending attachments and a certain set of users from communicating with external domains. DLP for inbound and outbound email allows you to intercept, modify and/or monitor email matching certain criteria or carrying private sensitive information, e.g. mails carrying financial or PII (Personally identifiable information) like Aadhar, PAN, Passport numbers, etc.

Spoof prevention	SkyConnect	SkyConnect enables outbound spoof control by default to prevent spam from end-users flooding our platform. This works in a strict form and expects fine-grained a request by the user to have 3 matching elements, viz. the authentication email id = the From ID in the mail = the envelope email id of the sender. This prevents users from authenticating with their credentials but using another's email id to send the email.
Multi-factor authentication	SkyConnect	Baya, the web client of SkyConnect, can be configured for two-factor authentication to tighten the account's security.

Access

The services on Mithi's cloud platform can be accessed from a combination of Web, Mobile, and desktop applications.

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	**Product**	**Description**
Block services	All products	You can block access to certain services for a single user, a set of users, or the entire domain. This is useful to ensure that your users access the applications using a prescribed method. E.g. No user can access POP or IMAP; all should access only over HTTPS (Baya3); disallow POP/IMAP for all users except a few select users who must use a desktop client.

Trusted IP ranges	All Products	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.

Periphery

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

Mithi partners with Trend Micro HES to secure this layer. This layer is called SecureMailFlow in SkyConnect.

The SecureMailFlow service in SkyConnect protects your users' inboxes from spam and virus mails. It also helps prevent recipients from receiving spam or virus mail, which you may send inadvertently.

This service sits in the inbound and outbound mail flow path and ensures that every mail you receive from the Internet is scanned for spam and virus. Any mail detected as spam/virus per the rules and policies defined in the SecureMailFlow service is either rejected or quarantined into a separate storage per domain.

The SecureMailFlow service is an integral part of the SkyConnect service for all our customers and is configured to scan all in and outbound mail.

Control	**Product**	**Description**
Spam Protection	ClrStream SkyConnect	Guaranteed 99.9% spam detection. The detected spam emails are quarantined, held on SecureMailflow, and the digest report is sent to the users. The report has an option to release false positives if any are found.
Virus Protection	ClrStream SkyConnect	Guaranteed 100% protection. The system uses ATP technology to detect viruses and discard them

False Positives	ClrStream SkyConnect	Guaranteed less than 0.003% false-positive rate.
Ransomware and Malware	ClrStream SkyConnect	SkyConnect does an excellent job of protecting your networks from email-borne Ransomware and Malware. The protection is based on an always-on ATP and advanced sandboxing to analyze email content before allowing them through to your network.
DDOS protection	All products	All internet-facing ports on all computer instances are configured with DDOS throttles to slow down, dissuade and frustrate attackers.
Reputation	ClrStream SkyConnect	Inbound mail requests are scanned for the sender's reputation using standard best practice email protocols such as SPF, DMARC, and DKIM, to ensure only emails from highly reputed, well-configured senders are accepted for further scanning. Similarly, for outbound connections, Mithi maintains a high reputation for its domains by configuring best practice protocols for SPF, DMARC, and DKIM. This declares that your domain is a highly reputed email sender, and mail from here should be treated with respect.
ATP	ClrStream SkyConnect	The platform deploys Advanced Threat Protection to provide real-time protection against targeted attacks. A deep discovery analyzer provides custom sandbox analysis to isolate and deal with suspicious URLs and objects. The analyzer detects ransomware, advanced malware, zero-day exploits, and more.

External mail warning	ClrStream SkyConnect	Insert a custom message in all inbound emails (external email) to warn users of potential legit emails posing as spoofs and luring them with clickbait.

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
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. E.g. Use IMAPS instead of IMAP, HTTPS instead of HTTP, etc
VPN	All Products	There are specific use cases in several organizations involving 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 despite all precautions, the human is the weakest element in the security chain. 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 end-user training modules to help educate your end-user 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.

Vigilance

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

Detection: Visibility is the first fundamental aspect of gaining control of the platform's security. Mithi has created digital dashboards, which 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, 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 intimately impact customers via email or any other suitable media and may request action from the customers.

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.

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.

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 set of guidelines forms a detailed, 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 focus of the audit is 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	*1st Aug 2022*