Contents

Background

Mithi is a Communication, Collaboration and Data Security specialist, offering cloud-based SaaS solutions to enterprises. Mithi's solutions are well known for their bullet proof Security, rock solid reliability and high performance at massive scale.

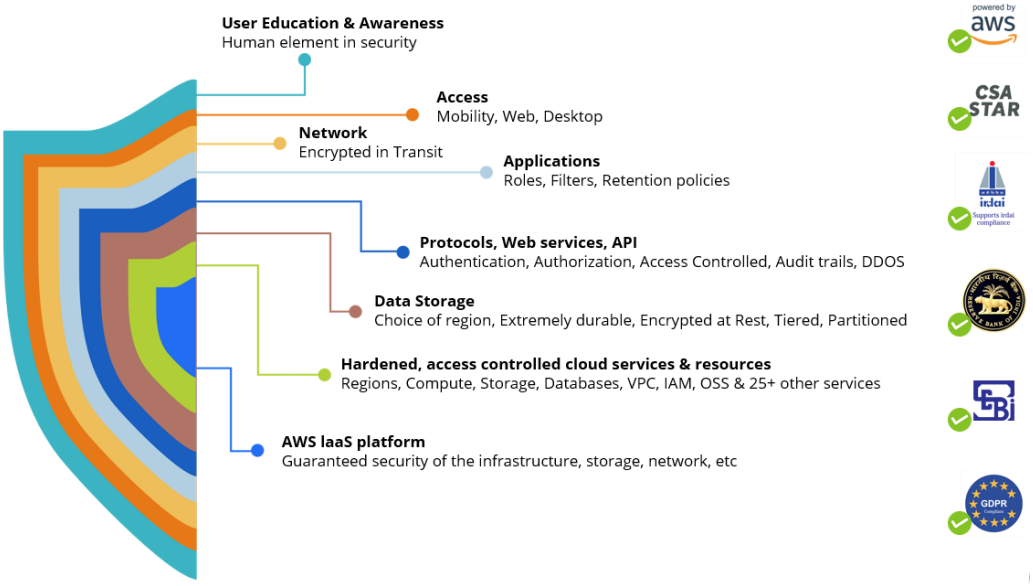
This paper documents the security framework deployed in our cloud platform, across all our products, to protect your data at multiple layers, making it near impregnable.

Overview

Mithi's security framework comprises 3 core elements as shown below:

The foundation of the entire security system is the act of securing the platform at all layers from the Infrastructure to the Periphery onto the Network. Once this foundation is in place and the platform is secured using best practices, the CSOC maintains vigil to ensure that the platform stays secure. This vigil includes periodic VAPT scans via CERT IN empaneled vendors. In case on any breach or incident discovered, rapid action is taken to arrest the impact of the incident, neutralize the threat and report/escalate the incident in a structured manner with a time bound long-term prevention plan.

The Security Framework at a glance

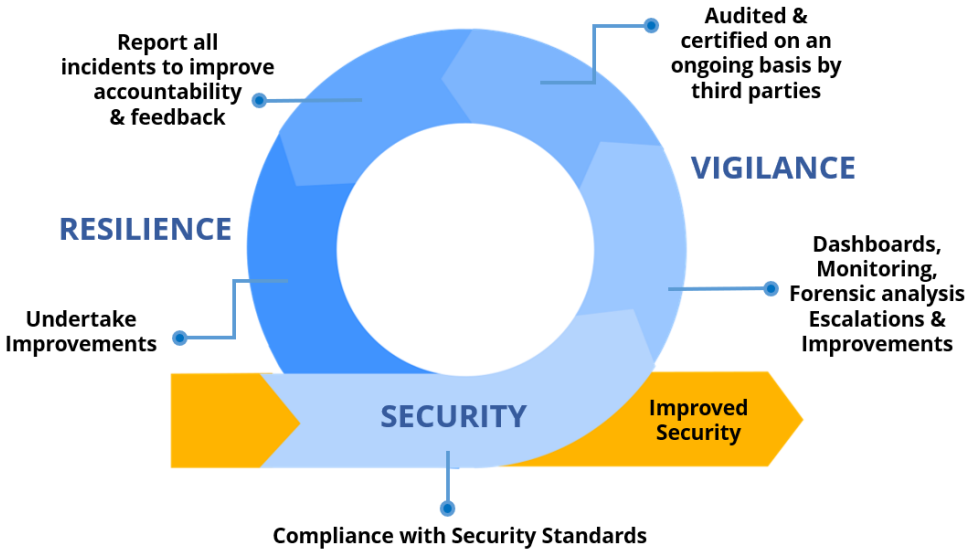


Mithi's Digital Collaboration Platform is built on the AWS cloud platform and leverages the shared security model of AWS.

Security OF the cloud: AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

In order to maintain vigilance, 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.

Security IN the cloud: Mithi operates, manages, and controls the digital collaboration platform, which comprises the cloud compute, storage, network resources and their operating systems right up to the applications and services running on this infrastructure. Mithi secures the platform at multiple layers using industry best practices to achieve cyber resilience.



To maintain vigilance, Mithi deploys a Cyber Security Operations Center to continuously monitor and audit the platform environment to ensure compliance to several standards across verticals such as RBI (Reserve Bank of India), SEBI (Securities and Exchange board of India), IRDAI (Insurance Regulatory Development Authority of India), HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), which when taken together, create a comprehensive security guideline.

Security Practices at each Layer

Infrastructure

This is Security OF the cloud and is the responsibility of AWS. In order 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 and facilities across the globe maintain a ubiquitous control environment that is 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 established and operated by AWS.
- **Monitor** that, through the use of thousands of security control requirements, AWS maintains compliance with global standards and best practices.

AWS has obtained certifications and independent third-party attestations for a variety of 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 build 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, secure and guaranteed.

Resources

Mithi's digital collaboration platform uses a host of AWS services for compute, storage, load balancing, server less processing, API security etc. These resources run operating systems, services and applications to serve the communication, collaboration and archival workloads of the platform.

To maintain 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, resources of our platform reside in several logically isolated sections of the AWS cloud (each a Virtual Private Cloud). In each VPC, the resources are further layered into Internet facing resources and private resources and are secured using different subnets (public facing and private facing), security groups and network access control lists.

IAM	Identity and Access Management - Teams having access to these resources, are provided limited privileges that are linked to their role in the operations. To reduce impact of the human element in security, the controls deployed are granular and include (but not limited to) time of day access, originating IP address, SSL, and multi factor authentication.
Operating Systems	Our compute nodes are configured/hardened aligned to the role of that server to reduce surface area of exposure. From role-based user access, running minimal services, protected credentials, to audit trails, onto updated security patches, secured by local firewalls on each node, are some of the best practices followed to secure the nodes at this level.
Security Group Firewall	This is an AWS level firewall, which is in addition to the firewalls on our operating systems, and acts as primary line of defense. This is configured in deny-all mode by default, 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 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 its unauthorized access or theft.
Hierarchy	All Products	The information/data is spread across Hot, Warm and Cold storage mediums depending on frequency of access. While this improves performance, 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 and applications such as the administrator console, end user web client, etc. Its only via these tools, can a user or an administrator access their data.

The services and applications are protected by ensuring only people who are authorized can login to the service using authentication 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, which 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 an administrator intervention.
Authorisation	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. E.g. no user can set auto forward to an external email id, junior admins get access only to a 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.
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, content of the subject, 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, disallow a certain set of users from communicating with external domains. DLP for inbound and outbound email allow 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 numbers, PAN numbers, 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 each email send request by the user to have 3 matching elements, viz. the authentication email id = the From ID in the mail = the envelop email id of the sender. This prevents users from authenticating with their own credentials but using another's email id to send the email.

Access

The services on Mithi's digital collaboration platform can be accessed from Baya3 (responsive web client platform), mobile applications and desktop applications.

At this layer, you can decide which users get access to 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 for the entire domain. This is useful if you want to ensure that your users will 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 email into the network. By ensuring only clean mail get through, this layer prevents major issues downstream.

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

The SecureMailFlow service in SkyConnect is designed to protect the inbox of your users from spam and virus mails. It also helps prevent your 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 which you receive from the Internet is scanned for spam and virus. Any mail detected as a spam/virus as 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 inbound mail and outbound mail.

Control	Product	Description
Spam Protection	ClrStream SkyConnect	Guaranteed 99.9% spam detection. The detected spam mails 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 mail content before allowing them through to your network.
DDOS protection	All products	All internet facing ports on all compute instances are configured with DDOS throttles to slow down, dissuade and frustrate attackers.
Reputation	ClrStream SkyConnect	Inbound mail requests are scanned for reputation of the sender using standard best practice email protocols such as SPF, DMARC, DKIM, to ensure only email from highly reputed, well configured senders are accepted for further scanning. Similarly, for outbound connections, Mithi maintains a very high reputation for your domains by configuring best practice protocols for SPF, DMARC and DKIM. This declares to the world that your domain is a highly reputed email sender and mail coming from here should be treated with respect.
ATP	ClrStream SkyConnect	The platform deploys Advanced Threat Protection to provide real time protection against targeted attacks. 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 email (external email) to warn users of potential legit email that is posing as spoof and luring them with click bait.

Network

This is the Internet link between our platform and other platforms and the 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 for encrypting information that is 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, 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, which involves 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 the deployment of 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 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 e-mail, or downloading 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 that the adage "prevention is better than cure" is what will help mitigate the 44% insider 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," and 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

Its 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 ensure that the security levels are maintained.

Detection: Visibility is the first fundamental aspect of gaining control on the security of the platform. 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 intimate impacted 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 perform a security scan on our platform, periodically and ensures closure of all reported points within defined timelines. These reports are available as artifacts for our customers, upon request.

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 has ensured compliance with industry specific cyber security guidelines by agencies across sectors, viz. RBI (Reserve Bank of India), SEBI (Securities and Exchange board of India), IRDAI (Insurance and Regulatory Development Authority of India), GDPR (General Data Protection Regulation), CSA Star (Cloud Security Alliance).

The collective set of guidelines form 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 organizations, across verticals, who adopt our platform

Well-Architected for AWS

The AWS Well-Architected Framework has been developed to help cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars —

operational excellence, security, reliability, performance efficiency, and cost optimization — the Framework provides a consistent approach for customers and partners to evaluate architectures and implement designs that will scale over time.

Our cloud architecture is periodically reviewed by solution architects from AWS to confirm compliance to their "Well-architected for AWS" framework. This ensures that we are using the AWS platform in its most optimal form, most secure form and we are up to date on all the latest technologies in the AWS platform.

Document Revision:

Created on	*23rd July 2019*
Last Modified	*27th Aug 2019*