L&T Financial Services Supports Cloud Transformation with Zscaler Zero Trust Exchange

L&T Financial Services

L&T Financial Services

www.ltfs.com

Location: Mumbai, India

Industry: Financial Services

Customer Size: 24,000+ employees with 195+ branches and 1500+ Micro Loans Meeting Centers

L&T Finance Holdings Limited is a leading Non-Banking Financial Company (NBFC). L&T Financial Services is the brand name of LTFH. With more than 24,000 employees at over 195 branches and 1500+ Micro Loans meeting centers, Mumbai-based LTFS offers a diverse range of rural, retail, housing and infrastructure financial products and services, as well as investment management.

Digitalization renders on-premise appliances obsolete

Transforming from a paper-based company to a digital enterprise enabled L&T Financial Services to become a nimble lending leader, but created challenges with its traditional perimeter-based data security approach.

"When the transition began, we had approximately 110 heterogeneous threat management appliances to secure our headquarters, branches and micro loan meeting centers," explained Mohd Imran, Group Head of Information Security at Mumbai-based L&T Financial Services. "Managing, patching, updating and upgrading so many different devices, from different vendors, was becoming unsustainable and, with our workloads moving to the cloud, obsolete."

Securing internet access with zero trust

With executive management keen to leverage cloud technologies for supplying work-from-anywhere (WFA) access to 24,000+ employees spread across 198 branches and 1500+ Micro Loan Meeting Centers, the LTFS infosec team started researching modern solutions for securing internet access.

CHALLENGE

- Support a digital transformation that relies on cloud applications and infrastructure.

SOLUTION

- Zscaler Internet Access™ (ZIA™)
- Zscaler Private Access™ (ZPA™)
- Zscaler Zero Trust Exchange™ platform

OUTCOMES

- Eliminated a heterogeneous security environment comprised of 110 different types of threat management devices
- Achieved close to 40% improvement in endpoint security and reduced access-related support tickets to almost zero
- Realized significant savings on security hardware, software and management with a unified and centralized cloud-based zero trust approach
- Gained granular visibility, data and reporting that enables remediating risks and adopting predictive analytics to drive security improvements

"We needed the ability to enforce a single security policy for all employees and users," Imran said. "We also required one centralized solution to replace all 110 appliances and multiple vendors, making the system easier and more efficient to manage."

Collaborating with its local partner **Solutions Enterprise**, LTFS evaluated multiple offerings and selected **Zscaler Internet Access (ZIA)** as the most comprehensive cloud-based zero trust solution. "Other options were located partially on-premise, making them a hybrid," said Imran. "Only Zscaler was fully cloud-enabled and cloud-delivered, meaning all traffic stayed in the cloud rather than routing through our corporate data center."

ZIA eliminates complexity, reduces cost, and boosts sustainability

Using ZIA, the financial services company is supplying WFA access to SaaS applications and the Internet while centralizing access policies, implementing controls, and achieving visibility. As a fundamental building block of the **Zscaler Zero Trust Exchange platform**, ZIA accomplishes these zero trust tasks via a lightweight application, called Client Connector, deployed on client devices.

With ZIA providing a secure access layer, LTFS eliminated all appliances in the data center and at each of its branch locations. "We're achieving significant savings on security hardware, software and management overhead", Imran said.

In addition, ZIA supplies consolidated and integrated security processes, providing LTFS with visibility that was impossible to achieve before. "Rather than different vendors for firewalls, web proxies, URL filtering, etc., we now have a unified solution with a centralized dashboard and granular, real-time insights," said Imran. "This enables us to establish policies, control traffic, and train users to reduce our risk profile."

Deploying an AI-driven security engine can stop patient-zero attacks

The other benefits include patient-zero attack mitigation, encrypted traffic inspection, and direct cloud platform peering. With over 150 **Zscaler points of presence (POP)**, LTFS offices are experiencing reduced latency and enhanced performance by peering to the POP closest to each office.

Zero-day mitigation can be accomplished by turning on ZIA's AI-driven malware prevention engine, with inline quarantining. This capability, called the **Advanced Cloud Sandbox**, stops patient-zero attacks with protections that are continuously updated from over 135 billion requests per day in real time.

> "Instead of deploying, updating and maintaining 110 different security appliances, we now have a unified solution that provides us with an intuitive centralized dashboard and granular, real-time insights."
>
> – **Mohd Imran**
> Group Head of
> Information Security
> **L&T Financial Services**

Decrypting and inspecting secure internet traffic at scale, whether on or off the LTFS network, is another ZIA advantage. It enables LTFS to identify suspicious files and begin remediation steps.

"Previously, our traffic management capability was mainly limited to blocking certain URLs," Imran said. "Now, we have the visibility to detect suspicious encrypted SSL traffic and take action."

Another ZIA feature LTFS recognizes is **Zscaler's direct peering with Google**. Embracing Google Cloud for infrastructure-as-a-service (IaaS), LTFS and their business users rely on Google Workspace as their primary productivity and collaboration application.

"We began our migration to Google a few years ago and now about 70 percent of our workload runs on Google Cloud," said Imran. "Zscaler's connection to Google, instead of routing traffic through the Internet and back into our systems, provides a direct data path that improves performance and optimizes user experiences."

VPN-free solution quickly supports pandemic remote work

When the COVID-19 pandemic struck, LTFS quickly added **Zscaler Private Access (ZPA)** to support the rapid transition to remote work.

Using ZPA, the company furnished seamless, secure, VPN-free access for private applications running on public clouds, such as Google Cloud, and within its data center.

When a user attempts to access an application, identity and device posture are verified with Client Connector, the same software as ZIA uses. To enable access to private applications, whether on site or in a cloud environment, Zscaler App Connector is installed at an application's location. App Connector is a lightweight virtual machine (VM) that brokers the secure connection between private applications and the Zscaler Zero Trust Exchange.

Further, ZPA ensures neither networks nor applications are ever exposed to the internet. This makes all enabled LTFS infrastructure completely invisible to unauthorized users while still granting authorized users least-privileged access.

"Previously we'd relied on VPNs, which impacted user productivity and permitted broad access to corporate systems," Imran said.

"With ZPA, the user experience is significantly improved," he continued. "We can limit access to only the applications an individual user requires, enhancing network and data security."

> "We've improved endpoint security by almost 40 percent and nearly eliminated access-related tickets completely."
>
> – **Mohd Imran**
> Group Head of
> Information Security
> **L&T Financial Services**

Adopting cloud CSPM to protect workloads

Next on the LTFS security roadmap is the continued expansion of its Zscaler Zero Trust Exchange platform. This includes coordinating consistent cloud security posture management (CSPM) across all of its divisions and branches by adopting **Workload Posture**.

As misconfigurations in cloud applications are a known enterprise vulnerability, Workload Posture will enable LTFS to proactively identify and remediate such defects, as well as prevent them from occurring in the first place.

Implementing Zscaler's Workload Posture will give LTFS continuous visibility of its security, compliance, and risk posture; the ability to enforce standards via guided and auto remediations; the automation of governance by setting policies and exceptions; and the capability to integrate with other IT and risk management solutions. By providing intuitive representations of vulnerabilities and their associated risk level, the solution enables tackling the most serious issues first.

In addition, Workload Posture identifies **compliance** violations across a range of global standards such as GDPR (General Data Protection Regulation) and the Reserve Bank of India (RBI).

"We're constantly examining ways to improve our compliance posture, automate mitigation, and proactively reduce risk," said Imran. "Workload Posture is an attractive solution."

A zero trust approach helps LTFS meet business goals

No matter how LTFS continues to build out its zero trust strategy, partnering with Zscaler is helping the company with securing digital transformation & cloud adoption. "By supporting our company's digital transformation we've not only reduced risk but also significantly improved time to market, while also enhancing user and customer experiences," Imran said.

"For example, a home loan previously required over a month from application to funding," he added. "Now, with our app-based process, the same loan can be funded in less than a day."

From an organizational perspective, LTFS has considerably boosted security and business user productivity. "Endpoint security is up by about 40%," Imran said. "Productivity is also measurably advanced as users no longer encounter access obstacles. This is also reflected in related support tickets, which have plummeted to nearly zero."

> "Simply put, Zscaler has helped us run our business securely."
>
> – **Mohd Imran**
> Group Head of
> Information Security
> **L&T Financial Services**

Moving forward, LTFS expects to net even more value from its Zero Trust Exchange deployment. Using granular data and reports generated by the solutions, the company will start implementing predictive analytics for gaining further insights.

"We'll be able to create multiple types of metrics, such as application utilization, to determine who is actually using which applications and how often," said Imran. "This will help us align access with those who need it and minimize application licensing costs."

Meanwhile, LTFS will continue enjoying its substantially enhanced cybersecurity protections. "Simply put, Zscaler has helped us run our business securely," Imran said. "With Zscaler, it's like we've created a perimeter in the cloud."

Getting critical resources to people faster

To achieve its vision of being an inspirational financial institution and spur economic development, Mumbai-based L&T Financial Services set out on a cloud-enabled digital transformation journey. It relies on a zero trust WFA security model for supplying customers with an app-based, self-service loan application process that puts needed funds into the hands of Indian citizens faster than ever before.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com