Asia's Oldest Stock Exchange Relies on Forcepoint to Protect 8 Million Trades a Day

This stock exchange is committed to ensuring its traders are playing fairly and safely, using Forcepoint DLP as a pillar of its security posture.

Founded in 1875, the oldest stock exchange in Asia and tenth largest in the world is still always eager to learn new tricks—especially when it comes to cracking down on fraudulent financial practices. It stops insider trading and safeguards the up to eight million orders made per day on its screen-based and online trading platforms with the help of Forcepoint DLP.

CUSTOMER PROFILE:
Established in 1875, Asia's first stock exchange and the world's 10th largest.

INDUSTRY:
Financial Services

HQ COUNTRY:
India

PRODUCT:
Forcepoint DLP

India's oldest and biggest stock exchange is responsible for maintaining the security and integrity of the seventh-largest capital market in the world. That's not hyperbole—the exchange is listed among the Indian institutions protecting the country's "most critical infrastructure" by the National Critical Information Infrastructure Protection Center.

The scale of the trading that must be protected is just the beginning of the exchange's security challenge. Securities markets where stocks, bonds, equities, debt, and derivatives are traded face the highest level and number of cyber threats among all financial markets, according to BAE Systems researchers.

Stock exchanges have more daily activity, market infrastructure operations, and participants than securities-issuing institutions, making them easier to attack by various methods and vectors.

Protecting 8 million trades a day

Trades on stock exchanges can involve long chains of custody and unstructured communications between many different parties, presenting challenges to both threat prevention and post-incident forensics. For extremely large exchanges, those challenges are exponentially greater.

With a market cap of $2.2 trillion and some 5,500 listings on its exchange, the exchange oversees up to eight million trades per day made over both its automated, screen-based trading platform and its centralized, exchange-based internet trading system.

Working closely with the Securities and Exchange Board of India (SEBI), the exchange must facilitate ease of trading for brokers while also ensuring that all trading on its floor and online platform is above-board and 100% secure. SEBI, India's top financial regulator, is also a Forcepoint customer.

Indeed, the stock exchange must serve as a role model in how it conducts its own security operations, which directly impact the integrity of the securities market it oversees as a whole.

The rising threat of data loss via exfiltration

One area that has become a growing concern for the stock exchange is data loss through exfiltration, said the exchange's Chief Information Security Officer.

Several years ago, when the stock exchange decided it needed a different dedicated data loss prevention solution than the one it was using, it turned to Forcepoint Data Loss Prevention (DLP).

"Being a national critical infrastructure, data loss is a major concern. Forcepoint DLP has helped us gain much better visibility and control over our data, strengthening our overall security posture," he said.

Proof of concept shines a light on data leak risks

The IT security team leaned on Forcepoint to help build a stringent, round-the-clock monitoring system in order to secure critical data from both external and internal threats. Through a proof of concept (POC), Forcepoint was able to show that DLP added the necessary protection against data exfiltration to the existing security framework in a seamless integration.

Challenges

Ensure that all information traded on its floor and online platform is secure by preventing data loss through exfiltration.

Approach

Replace existing data loss prevention tool with Forcepoint DLP.

The POC demonstrated how data leaks and their sources can be identified by DLP and included:

→ A data leak risk assessment

→ Monitoring of live traffic for emails and web uploads

→ Identification of users attempting to send data via Gmail and other unauthorized accounts to public domains

→ Real-time recommendations for actions to take during the running of the POC

The demonstration was enough to determine the switch to Forcepoint.

"While we had invested in a solution to address these challenges, the existing controls were not sufficient to defend against advanced data theft mechanisms such as data exfiltration in the form of images and slow-and-low leaks the way Forcepoint enabled us to do," the CISO said.

A more secure stock exchange, a safer trading floor

Today, through stringent monitoring that's strengthened by a 24/7 support model with locally available, on-call technicians, Forcepoint DLP is helping keep track of how and where data travels in and out of its organization. The exchange is now able to prevent any unauthorized access of data, both accidental and malicious, the CISO said.

When a user tries to access and copy unauthorized data to an endpoint device like a laptop or an external storage drive, the system blocks the action and then sends an email or SMS alert to IT. If a user tries to send unauthorized data over email, a similar alert is generated and necessary action is taken, plugging all possible data loss points—endpoint, network, and email—and thwarting any possible security breach.

The CISO also called out behavior-based elements of Forcepoint DLP like Incident Risk Ranking (IRR), which builds behavioral baselines for organizations and individual employees to better identify anomalous activity that might point to a meaningful data loss activity or event.

> "With their human-centric approach to security, Forcepoint DLP is helping us address this key piece of our security strategy."
>
> CHIEF INFORMATION SECURITY OFFICER

"Tackling the human element within the overall security roadmap is critical for organizations in today's environment. With their human-centric approach to security, Forcepoint DLP is helping us address this key piece of our security strategy," he said.

Results

Prevent any unauthorized access of data, both accidental and malicious.

Forcepoint