



Neehar Pathare,
Senior Vice President
Corporate IT, Financial
Technologies

INDIA'S LEADING COMMODITY EXCHANGE MCX UPGRADES ITS SECURITY INSIGHT WITH MAXPATROL

THE CHALLENGE

Defend against system downtime with enhanced visibility of vulnerability and compliance across the IT Infrastructure, including an SAP ERP system. Take ownership of security testing to end reliance on third party services

The Multi-Commodity Exchange of India (MCX) facilitates online trading in bullion, metals and agricultural commodities. With 470,000+ remote trading terminals and a platform that can support 40m transactions per day, it has amassed an 84% market share. But profitability, market share and reputation all depend on system availability.

“A stock exchange or commodity exchange cannot go down, so security is very important to us,” says Neehare Pathare, SVP Corporate IT for the company that founded MCX, Financial Technologies. “We work on very low latency networks and downtime is not at all acceptable. We report direct to the Ministries of Finance if anything goes wrong, so we breathe technology and we breathe security.”

Since 2003, MCX has relied entirely on external consultants for vulnerability and compliance testing services. These expensive tests varied in quality and relied on sampling a portion of MCX's systems per month. The exchange never had a comprehensive picture of security levels and the presence of new vulnerabilities or the impact of configuration changes might not be known for several months.

In 2013, MCX began searching for an automated solution that would give it ownership of IT security, performing more frequent assessments of business-critical applications as well as operating systems, databases, networking and security devices. As an ISO-certified organization, measurement of compliance with ISO 27001 and standards such as PCI DSS was also essential.

THE SOLUTION

MaxPatrol Vulnerability and Compliance Management

After testing several solutions, Mr. Pathare says MCX was “completely shocked” to find in MaxPatrol “one enterprise class product which could not only do vulnerability management but also penetration testing and compliance management.”

From a single server in MCX's Mumbai datacenter, MaxPatrol's agentless technology performs black-box and white-box scans of the full IT infrastructure including the SAP-based ERP solution; routers, switches and ASA firewalls from Cisco; Microsoft SQL and Oracle databases; and operating systems such as Microsoft, Red Hat Linux, Oracle Solaris and Ubuntu. MaxPatrol assesses both production and test environments to promote smooth transition of system and application builds from test to production.

The MCX team now has control of security assessments, triggering automated, real-time scans of the entire IT infrastructure or individual systems whenever required. MaxPatrol is used in Audit, PenTest (black box scanning) and Compliance modes, generating a complete picture of the assets and software in use; identifying and prioritizing vulnerabilities and misconfigurations; and giving visibility of compliance with standards including ISO 27001 and PCI DSS as well as measuring conformity with MCX's own custom IT policies.

External security consultants are only used to compile quarterly security audits which are based on MaxPatrol's data.

COMPANY PROFILE

- + Industry:**
Commodity Trading
- + Futures Offered:**
Bullion, metals, energy and agricultural commodities
- + Market Share:**
84.89% (FY 2013-14)
- + Turnover:**
US\$1.3trillion (FY 2013-14)
- + Size:** 2,000+ members,
470,000+ trading terminals
- + Ownership:** Founded by software services firm Financial Technologies. Publicly listed in New York (NSE: MCX) and Mumbai (BSE)



HIGHLIGHTS

- + Expanded visibility of security and compliance for maximum coverage of IT infrastructure including SAP systems
- + Cut risk of system downtime by dramatically increasing the frequency of checks for vulnerabilities and misconfigurations
- + Downsized reliance on external consultants by automating vulnerability and compliance testing under the control of internal security staff
- + Inspired confidence among customers and traders with increased assurance of reliability and compliance with standards including ISO 27001

THE BENEFITS

Expanded visibility of security and compliance; reduced risk of system downtime protects profitability, market share and reputation; dramatic cut in the use of expensive consultants

“MaxPatrol gave us a completely new insight on the network, from an angle that we were not looking at, on live networks in real time,” says Mr. Pathare. MCX can now perform its own on-demand assessments across the majority of its infrastructure, instead of relying on costly consultants using a mishmash of different tools to perform manual audit, compliance and vulnerability tests. “A single product that does everything for us, it has saved us a lot of time,” added Mr. Pathare.

Regular, system-wide checks for vulnerabilities and misconfigurations have replaced the previous sampling methodology, enhancing overall security levels. Weaknesses are caught sooner and MaxPatrol’s joined-up approach highlights flaws in one system that may threaten another, further helping MCX to lessen the risk of downtime that is catastrophic to both reputation and profits.

MaxPatrol’s automated compliance and vulnerability testing of both IT systems and business solutions – in particular the critical, SAP-based ERP platform – has enabled MCX to provide additional security assurance to its customers, traders and stakeholders such as the Ministry of Finance and India’s financial regulators, SEBI.

For Mr. Pathare, another key benefit is MaxPatrol’s flexible reporting: “It has different templates for everyone, from an operational level person managing a single vendor to a report for the CEO. That actually saved us a lot of work.”

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management, and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, banking, telecom, web application, and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of \$20M+.

© 2016 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.