



Shubhendu Dutta,
Head of Governance,
Information Security and
Alliances for SSTL

MOBILE OPERATOR MTS INDIA GETS INSTANT CLARITY ON ITS ASSETS WITH MAXPATROL™

THE CHALLENGE

Control risk from undisclosed IT assets with automated inventory and vulnerability management; protect system availability and meet group governance targets by determining compliance with corporate and industry standards, particularly ISO

With over a billion potential customers and more than 257 million mobile handset shipments per year*, India’s mobile telecoms market is amongst the toughest in the world. To develop its market share, MTS India continuously introduces new services and applications, but this rapid product lifecycle requires the constant commissioning and decommissioning of new application platforms.

“The HTTP applications themselves are only part of the picture,” says Shubhendu Dutta, Head of Governance, Information Security and Alliances for SSTL. “The infrastructure behind each application includes databases, OS, network devices and web services, making it difficult to keep track of assets on our network. That’s really bad news from a security perspective because we can’t secure IT assets if we don’t know about them. So our biggest challenge was to get better visibility of every asset in our infrastructure, starting with our perimeter.”

Vulnerability management needed to be more robust. “Our internal security team used several black box testing tools, but we knew it wasn’t enough,” adds Mr. Dutta. “We wanted a single tool for all our IT assets that would provide high-quality, automated vulnerability detection and prioritize the most serious threats to our business.”

To satisfy the demands of both internal and group-level governance teams, MTS India also needed more effective and efficient measurement of compliance with the security policies of its parent company, Sistema Corporation, as well as industry standards including ISO 27001, the 3GPP security specifications and regulations imposed by India’s authorities.

THE SOLUTION

MaxPatrol Vulnerability and Compliance Management

Following a detailed assessment of MTS India’s needs, MaxPatrol server was deployed in its primary data center near Delhi, in conjunction with MaxPatrol scanner at the secondary site in Chennai. MaxPatrol’s low-privilege, agentless technology automatically scans the telco’s entire infrastructure, supporting an unlimited number of IP addresses.

MaxPatrol’s PenTest mode provide visibility over network assets and server-side vulnerabilities. MaxPatrol’s Audit mode delves deeper and provides a full inventory of every IP-enabled asset on the MTS network, including any unauthorized devices added by staff, contractors or intruders. These white-box scans reveal the hardware type, installed software (including version numbers) and configuration settings for each asset. Technologies scanned include Juniper and Cisco networking and security devices; multiple OS including Windows, Oracle Solaris, IBM, HP UX and RedHat Linux as well as databases such as Microsoft SQL and Oracle.

COMPANY PROFILE

- + Name:** Sistema Shyam TeleServices Ltd (SSTL), trading as MTS India
- + Industry:** Mobile Telephony
- + Service Offering:** Wireless voice, broadband & data services
- + Revenue:** 11.8bn INR (2013-14)
- + Ownership:** Subsidiary of the Sistema Corporation (sistema.com)



* Source: India Monthly Mobile Handsets Market Review by CyberMedia Research — February 2015

HIGHLIGHTS

- + Eliminated blind spots in a constantly-changing infrastructure with automated inventory of all IT assets
- + Cut risk of fraud and data breach by rapidly identifying and prioritizing vulnerabilities and misconfigurations across the entire IT infrastructure
- + Revolutionized governance processes by automating checks for compliance with internal security policies as well as industry standards such as ISO and 3GPP
- + Supported the secure, rapid deployment of value-added services

Several departments utilize MaxPatrol. “Our Security Vigilance team reports directly to Sistema headquarters,” explains Mr. Dutta. “With MaxPatrol, they can automatically measure conformity with standards including ISO 27001 and 3GPP security specifications and also check performance against Sistema’s own custom IT Security policies. A separate Operations Security Team uses MaxPatrol to track vulnerabilities and compliance for ongoing development projects, so there are no nasty surprises at project launch.”

THE BENEFITS

Increased visibility across a constantly-changing infrastructure; reduced risk to network availability, customer data and profitability; simplified compliance processes

“MaxPatrol improved our visibility from day one,” says Shubhendu Dutta. “The audit mode immediately identified all the assets in our infrastructure, including settings and installed software. We can perform a new real-time asset inventory as often as we want, so we no longer have to worry about unmanaged devices posing a risk to our network.”

“To keep our existing customers and attract new subscribers, we must maintain 100% system availability and give the public confidence that personal data, emails and messages are safe with us. So preventing downtime and data breach is our top priority,” says Mr. Dutta. “MaxPatrol’s automated scans rapidly identify and prioritize vulnerabilities and misconfigurations in all our systems, so we can eliminate them more quickly and get better protected against external attack.”

“A big factor in our selection of MaxPatrol was its support for compliance and vulnerability management in a single solution and its ability to meet the needs of all our governance teams,” adds Mr. Dutta. “MaxPatrol not only makes it easier to continuously enforce our corporate IT security standards across all our assets, it also means we can demonstrate to our board, our parent company and the relevant regulators that we comply with local, internal and international security standards.”

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.