TATA COMMUNICATIONS

TATA COMMUNICATIONS HELPS CUSTOMERS PROACTIVELY MITIGATE IT RISK

When this international data and telecommunications services provider needed a partner to provide the technical foundation of its vulnerability management service, it chose Qualys.

> *" QualysGuard just works. Once we've shipped and configured a QualysGuard appliance, there's nothing else our customers have to do. We don't think there is another prospective partner out there that could enable us to do what we want the way Qualys does."*

While Tata Communications Limited may be best known for providing innovative voice and communication services within more than 200 countries, the company has expanded far beyond those roots. Tata Communications also makes available network and data services to businesses and other communications firms from its 400 points of presence and nearly 1 million square feet of data center and collocation space. Tata Communications' deep and broad reach within emerging markets includes leadership in Indian enterprise data services, global international voice, and strategic investments in operators in Neotel in South Africa, Tata Communications Lanka Limited in Sri Lanka, and United Telecom Limited in Nepal.

An example would be its Managed Security Services (MSSP) that provides customers 24x7x365 threat detection, evaluation, remediation, and incident response. These services include distributed denial-of-service protection, managed firewalls, authentication, unified threat management and intrusion detection and prevention, proxy, and penetration testing services. In building these offerings, Tata Communications has taken great care to construct its Security Operations Center to meet leading international standards such as the Information Technology Infrastructure Library (ITIL) best practices. It is ISO 27001-certified, SAS 70-audited, and awarded the Cisco MSCP designation. The challenge was to build a vulnerability management service to complement Tata Communications' existing security portfolio of offerings.

Building a World-Class Vulnerability Management Service

As Tata Communications evaluated the best possible options to achieve this, it carefully weighed the benefits of utilizing an existing vulnerability assessment vendor versus building the technology, services, and reporting capabilities in-house. "We have a team that is exceptional with device management and monitoring; we have a team that is excellent with mitigating distributed denial-of-service attacks; and we have a strong understanding of patch management processes," explains Eric Hemmendinger, director of managed security services at Tata Communications. "We also were aware of the many open source tools available, so there was, initially, consideration of an internally developed solution."

However, during the evaluation, it soon became apparent that building the technological underpinnings of a vulnerability management service would require more time, labor, and expertise to develop in-house than initially estimated, and would significantly delay availability of the service as compared to developing a service using commercially available solutions. "When we laid out the requirements for the solution and looked at the time required to develop this internally, we quickly concluded that building the infrastructure ourselves would take too long. In evaluating commercially available, solutions, we found several that we felt were robust enough, but only one that met all of our needs – Qualys", said Hemmendinger.

Today, QualysGuard Vulnerability Management (VM) is the backbone of Tata Communications' Vulnerability Management Service (VMS), which is a white-glove service that provides customers a proactive way to detect, prioritize, and remedy security vulnerabilities. Designed to be just as effective delivering to both large-scale global environments and small or remote offices, VMS is an on-demand service that provides discovery and mapping of IT assets, asset prioritization, vulnerability assessment, remediation tracking, and comprehensive reporting. VMS clients realize hands-free, automated vulnerability management that enforces related security policies and regulatory compliance mandates.

Through Qualys' Managed Services Provider program, QualysGuard MSP, Qualys helps MSPs and others to immediately deploy comprehensive vulnerability assessment services to clients either as a dedicated offering, or as part of an integrated suite of managed services. QualysGuard's software-as-a-service (SaaS) delivery makes it straightforward for MSPs to deliver customized services. The SaaS architecture is ideally suited to meet the needs of MSPs, enabling central operations to securely scan internal and external networks in real time, any time. QualysGuard MSP also supports a variety of branding and customized reporting options, while the simple, extensible APIs make it easy to integrate QualysGuard VM with internal tools and customer portals.

Custom Tailored Vulnerability Management Solutions

Tata Communications now offers a number of different VMS service levels, including its Fast Start for those with modest-sized networks that demand enterprise-class vulnerability management capabilities and its Premium service in which Tata Communications manages the discovery, configuration, vulnerability detection, and reporting tasks to free the time of internal IT staff for more strategic initiatives. Tata Communications also can provide ongoing vulnerability and risk management advisory services that help clients best prioritize their mitigation efforts.

QualysGuard VM enables Tata Communications to deliver flexible, customizable services that fit its exact needs. For instance, large enterprises may want portions of their infrastructure assessed daily, weekly, monthly, and quarterly. "Some segments of a corporate network may not change, or be touched that often, and may require infrequent assessments, while other segments may require more aggressive scanning," says Hemmendinger. "We can help customers prioritize their remediation work and focus on what is important, and bring any new critical vulnerabilities that surface to their attention."

In the two years since Tata Communications has launched VMS, QualysGuard VM has proven itself powerful enough to meet Tata Communications' and all of its customers' needs. It's proven accurate in its ability to find vulnerabilities, with an extremely limited number of false positives, and comprehensive yet flexible reporting. "We can provide the reports our customers need, based on business objectives," he explains. For instance, through Qualys' ability to group assets, Tata Communication's teams can segregate and dispatch the appropriate reports to the internal customer teams responsible for remediation," Hemmendinger explains.

Bringing QualysGuard VM In-house

Following the implementation of QualysGuard VM for service delivery to its customers, Tata Communications realized it also could benefit by leveraging QualysGuard VM for its internal vulnerability assessments. Previously, the internal IT managers had relied on open source assessment software. "The team started looking at QualysGuard's capabilities and comparing it to what they were using for vulnerability assessments across the devices they manage. It seemed QualysGuard would be much more efficient," explains Rathnamala Rajaram, engineering manager for Tata Communications managed security services.

It didn't take long for the team to see that QualysGuard VM would, in fact, be more effective than their open source tools. "QualysGuard enables us to track our own asset inventories and conduct our vulnerability assessments and remediation more efficiently," Rajaram says. "Depending on internal policy requirements, we run assessments on a monthly or quarterly basis," she says.

When Tata Communications embarked on its efforts to offer a vulnerability management service, the company wasn't sure whether to build the technology itself or partner with a market leader. After careful analysis, it decided to partner with Qualys and standardize its service on QualysGuard VM. Shortly thereafter, Tata Communications turned to QualysGuard VM for its own internal vulnerability management demands. "QualysGuard just works," Hemmendinger says. "Once we've shipped and configured a QualysGuard appliance, there's nothing else our customers have to do. We don't think there is another prospective partner out there that could enable us to do what we want the way Qualys does," he says.

FIRM OVERVIEW
Tata Communications Limited
Business: Telecommunications services
Scope: International
Size: 5,825 employees; part of the $62.5 billion Tata Group

BUSINESS PROBLEM
Tata Communications sought a vulnerability management solution that would enable it to build and offer a diverse set of vulnerability management services.

SOLUTION
- QualysGuard MSP
- QualysGuard VM

WHY TATA COMMUNICATIONS CHOSE QUALYSGUARD VM ?

- QualysGuard VM, following extensive consideration, proved to be the most accurate, thereby saving Tata Communication engineers and customers time by avoiding false-positives.

- Comprehensive, insightful reports can be delivered to specific customer internal teams based on business role and objectives.

- QualysGuard VM is centrally managed and maintained by Qualys.

- Qualys' trusted brand and leadership reputation in vulnerability management.

- It provides a streamlined way to identify and mitigate infrastructure vulnerabilities.

- Qualys' network infrastructure scans can be customized so as not to disrupt the critical systems of customers.