

Infraon NCCM helps one of the top five banks in India take control of Compliance, Configuration and Change Management across its vast network.

The Challenge

With one of the largest large spread of banks and branches, this bank is ranked amongst the top five in India and is headquartered in Bengaluru. The Bank's IT network was huge, complex and spanned multiple technologies and vendors. Without a proper management system, such a massive network could become prone to attacks, vulnerabilities and management issues. The network uses a "Centralized Tree structure Network" where the Data Centres (DC and DRC) exist at the root of the Network hierarchy. The Zonal Offices, Regional Offices and Branch Offices reside at the second, third and fourth levels respectively in the Network. The Bank's IT Operations had defined a "local management scenario", where a given office's network is managed at its specified hierarchical level in the defined tree structure. The branch offices located within a specific Region would be managed from that Regional Office and same would apply for Regional Offices managed by the Zonal Office.

Infraon NCCM

EverestIMS Technologies Singular Approach

With such a deep-dive architecture the bank's network had to be managed at both the macro and micro levels spanning software, hardware and infrastructure to maintain the overall performance integrity. With an avalanche of assets in operation, the need of the hour was to have a complete and comprehensive snapshot of the devices, operating systems and configurations. The coverage had to span updates, backups, security, configurations, vulnerability, etc. Relevant policy management regarding baselines and compliance had to be structured and applied to all branch and remote offices.

Regular Configuration Backups taken from 10000+ Branch offices, Regional Offices, Data Centers and DRC Network devices from a Centralized Location.

Infraon NCCM Solution

Infraon NCCM was deployed in both the Bank's Data Centre and the DRC site. The NCCM deployment was a centralized design where devices at all locations would be managed from the main Data Centre. NCCM was sized to manage 15000+ devices. Infraon NCCM's Policy Management "Baseline Policy Check" and "Compliance Policy Check" runs on all branch and remote office devices at defined intervals to identify the devices with policy breaches. A single click Auto Remediation process clears the violations quickly and easily.



Key Benefits & Outcomes

Task Scheduling, Automation & Backups

NCCM scheduled Network Automation Tasks which comprised Daily Backups of Devices Configurations and Critical Inventories from NCCM's Application Database to a Secured External storage in zipped format for purposes of Compliance pertaining to storage adherence and device configurations backups for 7 years.

Daily Backups were taken of all Check Point Devices Messages, Traffic logs and migration snapshots (in Megabytes size) for detailed troubleshooting and Device Recovery purpose during failure situations.

700+ HP Branch Devices operating systems were upgraded to the latest version to enable security features & supporting centralized device authentication and authorization feature using TACACS+ protocol
100+ Cisco Branch Devices operating system were upgraded to a newer version helping in resolving Security Vulnerabilities and upgrading of features

Vulnerability Management, Reporting & Remediation

NCCM's Vulnerability module pulled all the vulnerabilities published by vendors from their cloud services (Cisco API & NIST), every quarter and matched the vulnerable devices OS version against NCCM's device OS version. This helped quickly identify of vulnerable devices available in the Bank's network. All of them were resolved through a single and easy remediation action.

Policy Management

NCCM's Baseline policy check is configured with all Cisco, HP and Aruba security hardening rules and runs daily on 10,000+ devices. Email notifications with auto remediation templates are configured to resolve the violation in case security hardening is identified. 6000+ rule violations were identified and the resolving process runs continuously to remediate the same.

The Bank

The Bank is one of the largest public sector banks owned by the Government of India. It was established at Mangalore and is now headquartered in Bengaluru. The bank has a network of over 6,700 branches and more than 11,000 ATMs which is spread across all over India.

Highlights

- Daily Backups of Devices Configurations and Critical Inventories
- Device configurations backups taken for 7 years.
- Daily Backups of all Check Point Devices Messages, Traffic logs and migration snapshots
- 700+ HP Branch Devices OS upgraded to the latest version
- 100+ Cisco Branch Devices OS upgraded to a newer version

Infraon NCCM automates change management, network automation, disaster recovery, configuration auditing, for networks of all sizes. Enterprises & Banks can Audit, Authorize, Automate, Compliance, Vulnerability on any network Infrastructure. NCCM empowers banks and FIs to adhere to norms set out by RBI on guidelines addressing Cyber Security Frameworks.