Case Study

FORESCOUT

Rizal Commercial Banking Corporation

Multinational Bank Saves 30 Hours Weekly by Automating Device Compliance and NAC

10-15%
increase in known devices on the network

30-40%
improvement in device compliance

6 DAYS
saved monthly for inventory management

RCBC
We believe in you.

Industry

Banking, finance

Environment

8,000 wired and wireless devices across 550 locations worldwide; 6,770 employees

Challenge

- Empower BYOD and technology advances while defending against millions of cyberattack attempts daily
- Protect every IP-connected thing – PCs and servers as well as IoT devices such as ATMs
- Consistently and sustainably enforce device compliance and NAC policies across a widely dispersed organization

Security Solution

- Forescout eyeSight
- Forescout eyeControl

Overview

Rizal Commercial Banking Corporation (RCBC) began as a small development bank in the Philippines, then rapidly expanded to encompass a wide range of financial services and branches in the U.S., Europe, Australia and New Zealand. To continuously identify and enforce compliance of every connecting thing across its widely dispersed, global enterprise and to control network access (NAC), the company turned to the Forescout platform. In addition to dramatically boosting the bank's security posture, RCBC overhauled asset inventory management, increased security operations productivity and laid the foundation for additional efficiency gains in the future.

Business Challenge

"There will always be cyberthreats. We needed a way to manage the risk, starting with automatically enforcing compliance, followed by implementing robust network access control."

— Jed Lumain, Chief Technology Officer, Rizal Commercial Banking Corporation

A prime target for malicious actors, RCBC fends off millions of cyberattack attempts daily. Yet RCBC Chief Technology Officer Jed Lumain also knows that for the bank to continue to be successful, it must embrace new technologies and adapt as business needs change, such as allowing employees to use their own devices (BYOD) and work from home. To enable such agility yet keep the bank's network secure, implementing robust NAC and device compliance topped his priority list. Devices included everything connected to the network, from ATMs to workstations. Since manually overseeing assets scattered across thousands of Philippine islands and the world was physically impossible and IT staff already stretched thin, the bank needed a way to automate enforcement of compliance policies, followed by NAC.

Use Cases

- Device visibility
- Network access control
- Device compliance

Results

- Uncovered 10-15% more devices than expected on corporate network
- Saved six days each month on inventory management
- Saved 30 hours weekly by automating operational tasks
- Improved device compliance by 30-40%
- Increased security operations productivity 20 hours each week
- Robust "trust no device" network access control
- Accurate, up-to-date asset inventory
- Easier workstation lifecycle management
- Cost savings from reduced operational burden and remediation avoidance
- Greater peace of mind with minimal to no impact on business operations

> "With the increased visibility and control that Forescout gives us, we save a lot of time and reduce complexity, both of which increase overall security operations productivity by roughly 20 hours each week."
>
> — Jed Lumain, Chief Technology Officer, Rizal Commercial Banking Corporation

Why Forescout?

To find the best solution for identifying, assessing and enforcing compliance, RCBC thoroughly evaluated three leading vendor products. In a proof of concept, the Forescout platform stood out for its agentless approach and ease of use. After turning on the solution, the bank's information security team was surprised to discover approximately 1,000 (10-15%) more devices on the network than expected. Although the initial motivation for purchasing the Forescout platform had been device compliance, the team quickly realized that with such comprehensive and granular visibility, they could also use the solution for NAC as well as accurate asset inventory tracking, which had previously been elusive.

Business Impact

Consistent, Sustainable Compliance for Every Network-Connected Thing

Using the Forescout platform's agentless posture and risk assessment, all IT and IoT devices that connect to RCBC's corporate network are automatically discovered, classified and assessed. They are monitored regularly for up-to-date, functioning antimalware or encryption software, appropriate patching and application versions. An exemption report in the Forescout dashboard helps the information security team investigate outliers. Since deploying the Forescout platform, Lumain estimates improvement in device compliance in the range of 30 to 40%. "The Forescout platform consistently and sustainably guards what gets on our network," says Lumain. "It gives me peace of mind that every connected device complies with our security policies."

Agility to Meet New Business Demands Such as COVID-19 Remote Work

"Like most companies across the globe, we were surprised by the speed and magnitude of the changes that we had to embrace overnight when the pandemic hit," recalls Lumain. "We went from 100 at-home workers to approximately 4,000, or two-thirds of our workforce. Thankfully, we had the Forescout platform to provide visibility into this new way of working, to tell us if employees' devices were compliant, and if not, why not, and to let us know when they had safely connected to the corporate network."

Automatically Blocking Network Access for Noncompliant Devices

With the Forescout platform, RCBC actively defends against network access by rogue devices or by authorized but noncompliant devices that could be compromised by malicious actors. For instance, if an employee adds an unapproved application to their PC or their tablet has a broken or missing antivirus agent, the Forescout platform blocks the device from accessing the network. The same goes for IoT devices. If an IoT device violates any RCBC corporate security policy, it will not be able to access the network. The Forescout platform also logs all blocked access attempts so IT personnel can respond appropriately.

In the past, when new PCs were shipped to remote offices and installed by a third party, the obsoleted workstations often remained in use despite instructions to destroy them. Now the Forescout platform blocks the old machines when they attempt to connect to the network. "I knew that this worked well because as soon as we activated the policy, we got complaints!" recalls Lumain.

> “Once an organization gets to a certain size, you just can’t enforce device compliance and NAC manually. The Forescout platform is a fundamental requirement for companies that are serious about protecting everything on their networks.”
>
> — Jed Lumain, Chief Technology Officer, Rizal Commercial Banking Corporation

Significant Time Savings from Reduced Operational Burden

Such automatic policy enforcement not only makes RCBC’s environment more secure, it also significantly reduces time spent on desktop support and remediation. Inventory management also takes 25 fewer hours each week – six days fewer each month – because the Forescout platform provides all the necessary information with just a few mouse clicks – and it’s completely accurate and up to date, unlike the licensing information and spreadsheets used previously. “With the increased visibility and control that Forescout gives us, we save a lot of time and reduce complexity, both of which increase overall security operations productivity by roughly 20 hours each week,” notes Lumain. He estimates that the automation of tasks made possible by the Forescout platform saves 30 hours weekly.

Policy Enforcement That Instills Confidence

“Once an organization gets to a certain size, you just can’t enforce device compliance and NAC manually,” Lumain tells his information security peers. “The Forescout platform is a fundamental requirement for companies that are serious about protecting everything on their networks. Thanks to the automated visibility and control that it provides, we have confidence that threats, which will always be present and ever-evolving, are within the threshold of our ability to manage them.”

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com

© 2021. Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at https://www.forescout.com/company/ legal/intellectual-property-patents-trademarks. Other brands, products or service names may be trademarks or service marks of their respective owners.