The game changer for South Africa's oldest bank

Size: 44,000 employees | Industry: Financial Services | Location: Johannesburg, South Africa

First National Bank (FNB) is the oldest bank in South Africa and one of the country's "big four" financial institutions. It is a division of FirstRand Limited, a large financial services conglomerate, which trades on the Johannesburg Securities Exchange under the symbol FSR. FNB is also listed on the Botswana Stock Exchange under the symbol FNBB and is a constituent of the BSE Domestic Company Index. To learn more, visit fnb.co.za.

Challenges

- Increase data center visibility
- Improve problem identification and troubleshooting
- Defend against persistent, multifaceted cyber attacks

Solutions

- Application connectivity and dependency mapping
- Integrated, multi-layered security from the core to the edge
- Application-centric, software-defined network

Results

- Attained a detailed picture of application connectivity, dependencies, and data flows
- Accelerated problem resolution from tens of hours to minutes
- Reduced malware infection rate from 9 percent to 0.1 percent

For More Information

- Cisco® Tetration platform
- Cisco Security
- Cisco Nexus® 9000 Series Switches
- Cisco Application Centric Infrastructure (Cisco ACI™)
- Cisco Network Assurance Engine (Cisco NAE)

Challenge: Accelerate problem resolution in the data center

Eugene Pretorius was tired of the blame game. Every time FNB experienced a service disruption or dip in application performance, fingers would point at the networking team.

"The network doesn't discriminate. It's either working or everything is down. It's not going to pick and choose things to disrupt," says Pretorius, CIO of Infrastruture and Security Services at FNB. "But whenever something went wrong, the network was always blamed."

In these circumstances, representatives from FNB's network, data center, and server teams would gather in a "war room" to troubleshoot the issue. It would take hours—sometimes days—to find a solution. And many times, a root cause was never identified, leaving the distinct possibility of problem recurrence and the blind troubleshooting that followed.

"It was clear we needed better visibility in the data center," Pretorius recalls. "We needed the ability to see exactly what was happening, where it was happening, and why."

To improve data center visibility, troubleshooting, and security, FNB deployed Cisco Tetration platform, which provides a detailed view—both real-time and historical—of application connectivity, dependencies, and data flows across a hybrid IT environment.

"The game changer," as Pretorius calls Cisco Tetration, has indeed altered the playing field on which FNB competes.

From blindness to 20/20 vision

FNB was the first company in the world to adopt Cisco Tetration, which is now installed on half of the bank's servers, including its DNS and Active Directory systems. Pretorius, a self-described "nerdy, hands-on CIO," has become a power user and says Tetration is his favored tool whenever problems occur.

"If something goes down, we immediately use Tetration to see what's happening," he says. "We have very large, very complex applications that have been around for decades, and Tetration shows us things we've never seen before. If an IoT device is misconfigured, or if a server is in distress, or if an endpoint is causing issues, we can immediately see it and isolate the problem."

Anomalies and outages that used to take a roomful of specialists and tens of hours to troubleshoot are now characterized in minutes using Cisco Tetration, which is integrated with Cisco Nexus 9000 Series switches.

As Pretorius has long asserted, the network has rarely been the culprit of such problems. In one case, a DNS issue was quickly exposed. In another, a failing front-end web server was easily detected. And in a situation that would have otherwise proven baffling to FNB's IT staff, Cisco Tetration pinpointed a user-generated query that had been running for 197 hours inside a data warehouse, slowing down the entire environment.

"We never would have been able to see or understand these problems without Tetration. It's the only tool in the world that can show what is happening across the network, application, and server planes all on one screen," Pretorius claims."Tetration gives me 20/20 vision in the data center."

> "Tetration gives me 20/20 vision in the data center. It's the only tool in the world that can show what is happening across the network, application, and server planes all on one screen."

Eugene Pretorius
CIO of Infrastructure and Security Services, First National Bank

Thwarting persistent cyber attacks

In addition to better data center visibility, Cisco Tetration—along with an entire suite of Cisco security products—has dramatically improved the bank's cyber defenses. Like all of South Africa's "big four" banks, FNB is under persistent, multifaceted attacks by cybercriminals and malware.

Cisco Stealthwatch® and Cisco Tetration work in tandem to provide continuous, real-time monitoring of all network traffic. Cisco Umbrella™ and Cisco Advanced Malware Protection (AMP) scour the traffic to detect anomalies, malicious behavior, and malware. And Cisco Identity Services Engine (ISE) takes action when problems are identified.

"All of our Cisco security products are tightly integrated, giving us multi-layered protection from the core to the edge," Pretorius says. "Stealthwatch identifies anomalies, ISE immediately quarantines them, and then we use Tetration to get an incredibly detailed picture of what happened and what was affected. In the past, we had to comb through firewalls, hundreds of logs, and dozens of network devices just to get a fraction of the picture."

With Cisco Tetration working in concert with Cisco security products, FNB's malware infection rate has dropped from 9 percent to 0.1 percent. Whereas the bank used to have thousands of infected endpoints at any given time, Pretorius says FNB now has less than 100 compromised machines on average.

> "All of our Cisco security products are tightly integrated, giving us multi-layered protection from the core to the edge. Stealthwatch identifies anomalies, ISE immediately quarantines them, and then we use Tetration to get an incredibly detailed picture of what happened and what was affected."
>
> **Eugene Pretorius**
> CIO of Infrastructure and Security Services, First National Bank

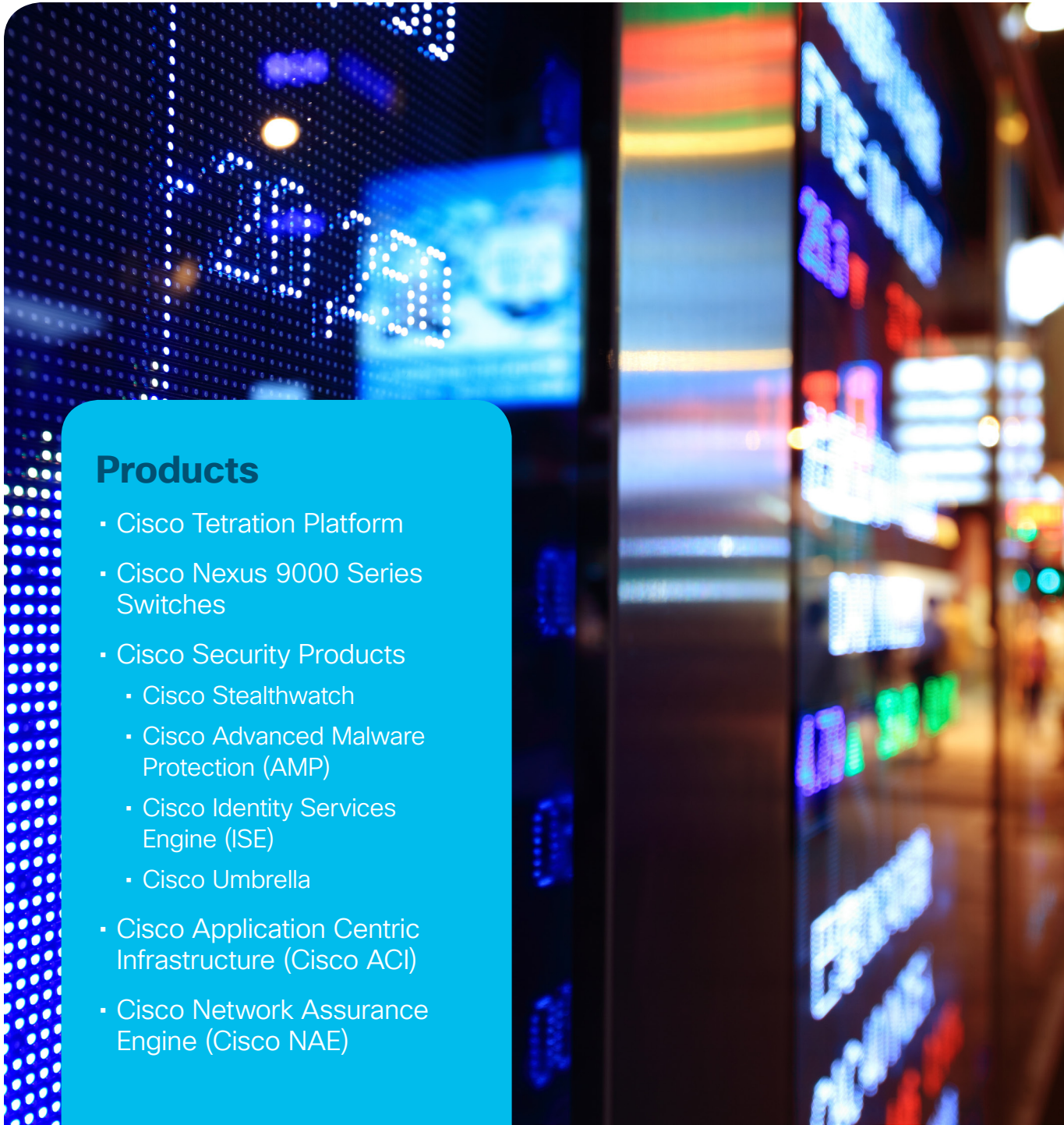
Looking ahead

With vastly improved troubleshooting and security, Pretorius is now working to enhance the automation and compliance reporting of FNB's three data centers. Key to those efforts are Cisco ACI, the industry's leading software-defined networking (SDN) solution, and Cisco Network Assurance Engine, or NAE, a comprehensive intent assurance solution that mathematically verifies the entire data center network for correctness.

"Cisco ACI will help us automate our processes, enforce network and application policies, and segment our data," Pretorius explains. "Once ACI is fully installed, Cisco NAE will give us assurance and show compliance, which will stop auditors from running scripts in our environment."

Cisco ACI will also help FNB move to a DevOps model of continuous application development and deployment. Instead of working two weekends every month—in the middle of the night—to implement changes and deploy new applications, Pretorius' team will be able to do so at any time, without disrupting service availability.

"In addition to security, visibility, and availability, Cisco technologies give all of us the ability to sleep at night," Pretorius says. "And ever since Tetration was launched, not a single outage has been blamed on the network."



Products

- Cisco Tetration Platform
- Cisco Nexus 9000 Series Switches
- Cisco Security Products
  - Cisco Stealthwatch
  - Cisco Advanced Malware Protection (AMP)
  - Cisco Identity Services Engine (ISE)
  - Cisco Umbrella
- Cisco Application Centric Infrastructure (Cisco ACI)
- Cisco Network Assurance Engine (Cisco NAE)