CASE STUDY

State-wide Co-operative Bank

K7 secures bank endpoints across hundreds of remote rural branches

K7 SECURITY

The State-wide Co-operative Bank wishes to provide safe and secure banking to customers in urban and rural locations. K7 assists them by enabling safe and secure computing in all their branches.

Client Snapshot

- 2,300 Endpoints
- 600 Add-on Servers
- 400+ Remote Rural Branches
- 2,000+ Employees
- 50,00,000+ Customers

The state co-operative bank serves a region that covers more than one third of the area and over half the population of its state. Cybersecuring such widely distributed operations across locations with varying sophistication of IT infrastructure is critical in helping the bank provide undisrupted banking services to its customers.

Cybersecurity that Overcomes Connectivity Constraints

The Bank's Challenges

- Protecting operations with world-class cybersecurity
- Maintaining cybersecurity standards across the organisation
- Limited connectivity in remote rural locations – as low as 24 kbps
- Lack of IT talent in remote rural locations

The K7 Solution

K7 Security's Endpoint Security (EPS) is designed to be efficient and flexible, which allowed K7's team to address the bank's challenges and secure their most connectivity constrained branches.

Add-on Servers

K7 add-on servers were installed at the bank's branches. The add-on servers act as secondary K7 web servers that link the primary K7 web server in the head office to individual endpoints in remote branches, avoiding the need for multiple endpoints to link directly with the primary server.

Compact Update Size

K7 Security's emphasis on efficient design ensures that malware definition and solution updates are very small in size and don't choke networks. The compact updates reach the add-on servers even when connectivity is just 24 kbps without affecting other banking operations. This ensures that all endpoints, including those in remote rural areas, are protected against the latest cyberthreats and comply with updates to cybersecurity policy.

Local Update Distribution

Each branch's add-on server receives updates from the primary K7 server and distributes them using the local network to individual endpoints. This ensures that multiple endpoints do not congest available bandwidth to download the same updates from the primary server.

Remote Management

K7's EPS enables 100% remote cybersecurity management with granular, centralised control over installed applications and devices connected to individual endpoints at any location. On-site IT personnel are not required to enforce enterprise cybersecurity policy.

Why The Bank Chose K7

- International award-winning cybersecurity solution and malware research
- Enables policy-based centralised control across all endpoints
- Updates and management are not hindered by limited connectivity
- Reliable remote management mitigates need for on-site IT talent

K7 Security's Endpoint Security enables the co-operative bank to create a secure computing environment for banking operations without investing in expensive bandwidth and equipment upgrades in remote locations. Contact Us to learn more about our enterprise cybersecurity solutions that are designed to provide robust protection and adapt to the unique requirements of and constraints faced by organisations operating in diverse environments.

www.k7computing.com