



INDUSTRY:

Banking/Financial

TECHNOLOGY PARTNER FOR SECURE AUTOMATION
OF CRITICAL BANKING DATA CENTER INFRASTRUCTURE



Case Study Overview

As one of the world's pre-eminent financial services companies, this large global bank serves hundreds of millions of customers. Its complex IT infrastructure includes highly-distributed mission-critical servers at data centers worldwide. For over 15 years and three hardware refreshes, it's chosen Lantronix's advanced out-of-band management platform and technical services to securely automate critical data center infrastructure.

CHALLENGE: Enforce Security Policy While Enabling Admin

Access

The SWIFT banking system powers international money and security transfers. The bank's IT team needed to access and manage servers that are on the SWIFT network while ensuring compliance with strict security and compliance standards. After years of using Lantronix out-of-band solutions for other data center applications, the bank approached Lantronix about designing a solution.

Success Highlights

- Encrypted management access to remote servers, both in- and out-of-band
- Granular, role-based permissioning with port- and command-level authorization controls
- Logging and compliance reporting of all user interactions, keystrokes and changes
- Session management, including proper termination of user sessions
- Level Technical Services that provide trusted network engineering support

SOLUTION: Lantronix LM83X Secures Physical and Virtual Ports

With unique, dedicated Ethernet connections, the LM83X console server is used to connect to baseboard management (lights-out) ports to enable primary functions, such as powering on and off the servers. This connection is isolated, allowing no access to these ports except through Lantronix by admins who have logged in using multifactor authentication and have appropriate rights to access the port, all while logging the session for audit.

Virtual ports allow server guest OS access available only to the LM83X IP address. The LM creates a reverse SSH tunnel and forwards the port to the authenticated user, providing a unique solution that meets the bank's security policies.

LEVEL Technical Services

Longstanding Technical Partnership

In addition to the advanced out-of-band management technology, a key part of the Lantronix partnership with this financial institution is the ongoing Level Technical Support.

Lantronix serves as a banking network subject matter expert assisting the bank's network admins with writing rules and automated controls for the LM83X console servers as well as custom reporting for compliance assurance. Over years of providing these "concierge services," Lantronix support engineers have become trusted partners.



Lantronix LM83X Console Server

Lantronix's LM83X is a modular, scalable platform designed to act independently from the network to remotely monitor, manage and control from 8 to 104 devices. Connectivity options include dual Ethernet management, an SFP port, modular out-of-band modem options and three expansion bays for serial and dedicated Ethernet connections. It includes dual power inputs.

For more information, visit:
lantronix.com/products/lm83x/

“ The Lantronix out-of-band management platform delivers the security that financial institutions need in a remote management solution, including encrypted access to our remote servers and complete reporting. ”

RESULTS: Secure Automation of Critical Data Center Infrastructure

Delivering true enterprise-wide management, Lantronix's LM83X and Control Center fulfilled the bank's requirement for an ultra-secure out-of-band management platform.

Benefits include:

Encrypted Management Access to Servers

Delivering out-of-the-box support for Secure Shell Version 2 (SSHv2), the solution leverages powerful FIPS 142-2 Level 2 encryption technologies to protect management communication with the servers, both in-band and out-of-band.

Granular, Role-based Permissioning

To ensure secure access, Lantronix solution provides granular, role-based permissioning with port- and command-level authorization controls. While traditional "dumb" console servers only provide port-level control over permissions, the LM83X can control every command inside the system on a per-user or per-group basis.

“ We are excited about the reduction in support costs and security improvements provided by Lantronix. ”

Logging and Compliance Recording

To ensure audit compliance, the bank relies on the LM83X's robust logging and compliance reporting to record all user interactions at all times, even during outages.

Three sets of data are logged:

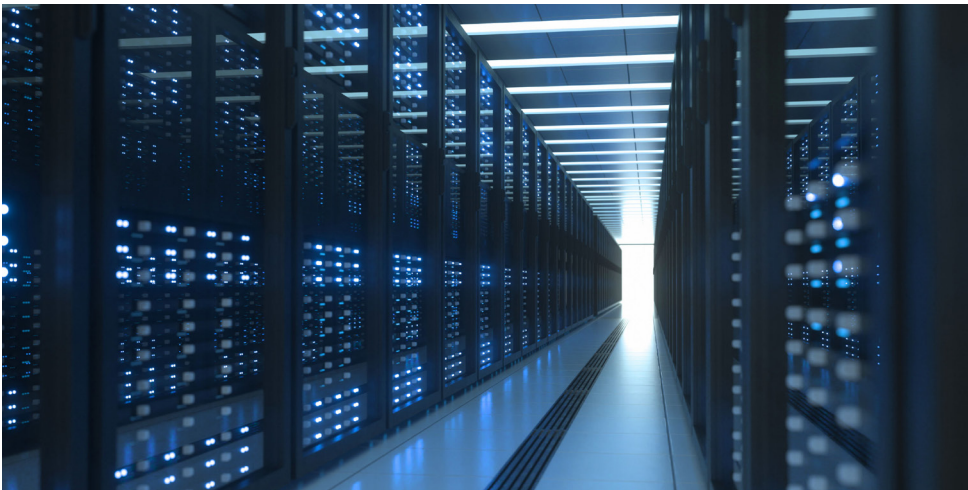
- Console data from the remote servers and other networking devices
- Session data detailing user interactions with servers and devices
- Change data that records any configuration modifications

Secure Session Management

Lantronix's LM83X security eliminates gaps that had previously violated the bank's security policies. Automated control ensures that sessions are properly terminated and that users are logged out correctly which helps prevent unauthorized access.

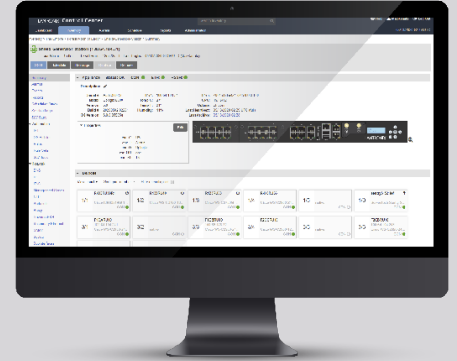
Control Center Provides Centralized Management

Deployed in the bank's Network Operations Center (NOC), the Lantronix Control Center delivers a real-time point of control with 24/7 monitoring and management capabilities.



Lantronix Control Center

The Lantronix Control Center enables out-of-band management by providing a centralized point of control for all Lantronix LM Series console servers and through this, of managed devices deployed throughout the distributed IT environment.



With its Web-based graphical user interface (GUI), the Control Center puts IT administrators in control of real-time data to easily manage, configure, and control all connected network devices and servers.

About Lantronix

Lantronix Inc. is a global provider of secure turnkey solutions for the Internet of Things (IoT) and Remote Environment Management (REM), offering Software as a Service (SaaS), connectivity services, engineering services and intelligent hardware.

LANTRONIX[®]

lantronix.com/about-us