UPLOGIX

LARGE GLOBAL FINANCIAL INSTITUTION

> CUSTOMER PROFILE

As one of the world's pre-eminent financial services companies, this large global bank serves hundreds of millions of customers. Their complex IT infrastructure includes one of the largest deployments of Solaris servers in the world.

"Uplogix' Envoy products deliver the security that we have been looking for in a remote management solution, like the ability to encrypt management access to our Solaris servers and to provide complete reporting for compliance with our internal regulations."

CURRENT CHALLENGES

One of the world's largest financial institutions faces the challenge of managing a highly distributed and complex global infrastructure, while ensuring compliance with strict security and compliance standards. The bank's IT staff found themselves consistently failing internal security audits as a result of vulnerabilities introduced by the terminal servers that were widely deployed throughout their environment to provide remote access to Solaris servers and networking equipment.

The bank was compelled to find a remote management solution that could meet the stringent security requirements that their existing terminal servers failed to satisfy, including:

- *Encrypted management access to Solaris 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, such as ensuring the proper termination of user sessions to prevent unauthorized "piggy-backing" sessions*
- *Centralized management of the appliances*

To find a solution that would satisfy these requirements, the bank sent a request for information to a number of vendors who provide remote access solutions, and after comparing the features that each solution offered, the bank chose to deploy Uplogix' products.

UPLOGIX SOLUTION

Uplogix' remote management solutions provided the secure management features and the always-on compliance reporting required by the bank. Uplogix' Envoy appliances operate on a secure management platform that supports the industry's most stringent AAA requirements and ensures that security and management policies are always enforced, even during a network outage. In fact, the Envoy appliances are so secure that they actually exceeded the bank's security requirements.

UPLOGIX

SECURE ACCESS TO SOLARIS SERVERS

Envoy delivers out-of-the-box support for Secure Shell Version 2 (SSHv2), which leverages powerful encryption technologies to protect management communication with the bank's Solaris servers. Unlike other remote access products, the Envoy appliances provide encrypted access both in-band and out-of-band.

When the network is functioning properly, Envoy appliances use an in-band Ethernet-based connection to connect to the centralized management server, the Envoy Management Station (EMS). If this primary management link becomes unavailable, the EMS immediately establishes remote connectivity using a dial-up modem, cellular network, or satellite communications; this secondary link offers the bank the same secure, encrypted access as the in-band connection.

GRANULAR PERMISSIONING

The Envoy satisfied the bank's need to protect root passwords by providing command-level access control and simple role-based permissions to ensure that the right users get the right access to the right devices. While traditional "dumb" console servers only provide port-level control over permissions, the Envoy can control every command inside the system on a per-user or per-group basis, giving the bank the ability to appropriately delegate responsibilities between the operations, engineering, and security teams in accordance with their management policies.

The Envoy also integrates with remote authentication mechanisms, such as TACACS and Radius; if connectivity is lost, the appliances rely on cached authorization data to maintain permissions even during downtime.

LOGGING AND COMPLIANCE REPORTING

To ensure compliance with internal audits, the bank relies on the Envoy's robust logging and reporting capabilities. The appliance logs three sets of data, including console data from the Solaris servers and other networking devices, session data detailing user interactions with servers and devices, and change data that records any configuration modifications. The Envoy collects this data at all times—even during outages—to provide complete reporting.

Additionally, the Envoy delivers powerful real-time log inspection capabilities. This enables the Envoy to generate alarms or take automated actions when specific patterns are identified in the log data. For example, the Envoy might generate an alert when a user starts or stops a critical network service on a server or when a potentially detrimental procedure is run on a router.

SESSION MANAGEMENT

The Envoy effectively eliminates several severe security gaps that violated the bank's security policies. Automated control of each user session ensures that sessions are properly terminated and users are logged out correctly. Each time a user exits a console session with a Solaris server, the Envoy logs into the Solaris server to clean up and close down the user's session before other users are permitted access to the device. This procedure prevents "piggy-backing" or "ghosting" and eliminates the risk associated with unauthorized access.

The Envoy also enables the bank to configure sessions to time out automatically in accordance with their internal policies. This further ensures proper session termination.

CENTRALIZED APPLIANCE MANAGEMENT

The EMS provides the bank's IT staff with a web-based, centralized point of control for all of the Envoy appliances deployed throughout their environment. Deployed in the Network Operations Center (NOC), the EMS delivers real-time monitoring and management capabilities, offering a unified view of the Envoy appliances and managed devices. Delivering true enterprise-wide management of the Envoy appliances, the EMS fulfilled the bank's final requirement for an out-of-band management platform.

"**Combining secure remote access with intelligent management features that automate support of our Solaris servers and networking devices made the product so compelling that we opted to replace existing traditional terminal servers with the Envoy appliances. We are excited about the reduction in support costs and security improvements that Uplogix offers.**"

ABOUT UPLOGIX // Uplogix provides the first fully-integrated remote management solution. Our co-located management appliances automate routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management requires multiple tools, relies on the network, and remains labor intensive. Uplogix puts the power of your most trusted IT administrator everywhere, all the time.

Uplogix is privately held and headquartered in Austin, Texas with European offices in London. For more information, please visit **www.uplogix.com**.