

# EpiForce®

## Overview

International organization operating in 100 countries

**Industry:** Financial Services

## Customer Profile

Global enterprise with 200+ million customers including several of the most well known and respected investment banking, insurance and brokerage firms of the world. For security reasons, anonymity was requested for this case study

## Business Challenge

To comply with government regulations requiring encryption of sensitive customer data, user names and passwords when transferred within the network, while at the same time **without** modifying existing applications

## Solution

Initiated deployment of Apani® EpiForce® to secure internal data flows traveling between multiple platforms utilized by existing applications

## Benefits

- Transparent to existing applications, requiring no code rewrites
- Cross-platform support to protect heterogeneous environment
- No end user training required
- Centralized management
- Highly scalable architecture
- Complements existing network infrastructure
- Scalable design supports phased deployment

## Global financial institution achieves regulatory compliance without the cost of replacing legacy applications – sets foundation for next generation security architecture

“EpiForce’s ability to work with our existing applications and operating system platforms was a significant decision factor.”

Vice President , Information Technology Security

## OVERVIEW

With roots extending back nearly 200 years, this organization represents a myriad of large, international companies delivering every type of financial service to each of its 200+ million customer accounts. Global business units include consumer banking, credit cards, loans, insurance, wealth management, investment banking and asset management services.

## CHALLENGE

Specific provisions within privacy regulations, including Gramm-Leach-Bliley Act and California SB 1386, required that personal information including user names and passwords be encrypted while in transit. Existing legacy applications needed this data to be sent in the clear.

A solution was needed to address encryption requirements without replacing or modifying the existing applications. At the same time, the approach must complement plans for a ‘next generation’ network with enhanced security architecture, rather than simply block security threats at the perimeter.



“EpiForce was the only product capable of adequately scaling to support our need to encrypt data flows within the perimeter...”

Global Security Architect

## SITUATION

In response to increased network attacks and customer information thefts, multiple government agencies adopted regulations on how to best secure against data theft. What exists today is a patchwork of regulations, each with its own set of minimum security requirements.

One such regulation, the Financial Modernization Act of 1999 (“Gramm-Leach-Bliley Act” or GLBA), was enacted to protect the privacy of customer records specifically within the financial services industry. The act’s importance today has significantly expanded, based in part on the rapid growth of phishing, pharming, identity theft and online fraud. Financial organizations must deploy tight security surrounding customer records to thwart criminal activity.

This presented a substantial challenge for the IT security administrators within the organization. They faced a paradox whereby legacy applications required personal information including user names and passwords to be sent ‘in the clear’ in order to function, however, regulations now required this communication to be encrypted.

The objective was to establish a “defense-in-depth” strategy, applying strong security controls at multiple levels throughout the network infrastructure. In essence, the desire was to shift from a “crunchy on the outside, chewy on the inside” security model to an environment where all aspects of the company’s information processing environment were hardened.

Securing the network inside the perimeter was a must. The value and criticality of Personally Identifiable Information (PII) is climbing rapidly. As the value of this data has increased, so too has the temptation for theft.

## DECISION PROCESS

Several years ago, the Chief Security Architect wrote a position paper calling for a new security architecture from the then current perimeter model to one resembling a “medieval keep” where the most precious information was surrounded by multiple layers of defense. Instead of relying primarily on a hardened edge, the

“The encryption problem is particularly challenging for organizations like ours that have legacy systems that often authenticate using clear text transmissions”

Global Security Architect

idea was to insure each aspect of the information processing environment was secure including the communication paths between them.

When that paper was written, key technologies needed to realize the vision were still immature – most security at the time was focused on either establishing the perimeter or securing remote access through it.

As new privacy regulations were enacted, the priority of this initiative was significantly altered. It became clear that protecting information – both from the inside and the outside – would become a central requirement of these regulations.

Several approaches were evaluated. The use of VPN technology within the perimeter was tested, but performance and management challenges prohibited deployment. Microsoft’s embedded IPSec functionality was explored, however, as new servers were added, it became quickly apparent that the management complexity would eliminate this as an effective solution.

Secure Socket Layer, or SSL was also assessed. Testing, however, revealed a significant performance impacts. And, as so few applications were SSL enabled, it was just not a practical solution for them.

After all their testing, it was clear that a network layer encryption solution like IPSec would be the best solution for them. By securing data at the network level, irregardless of software application, operating system or user interaction, the best security architecture could be applied with minimal software application disruption or modification expense.

But the challenge was how to overcome the deployment, manageability and scalability issues inherent in IPSec.

## SOLUTION

Apani EpiForce was selected to allow the bank to take advantage of the benefits of IPSec while suffering none of the management and deployment challenges typical in a large scale enterprise installation.

EpiForce secures network-wide data flows between multiple vendor platforms and operating systems by utilizing a combination of software and hardware-based agents:

- Software agents secure multi-vendor server platforms, including those running HP-UX, AIX, Linux, Solaris and MS Windows
- Hardware agents will secure communications to other devices not capable of running IPSec, including mainframes and printers

The first implementation phase was aimed at securing information flowing during batch jobs that use FTP, or command channels when passing a User ID and Password, as well as telnet (TN3270) going back to the mainframe while sending a CICS password over an insecure channel.

Compartmentalizing the network into logical security zones utilizing application, port and geographic regions greatly simplified the overall management task accounting for phased deployments and minimized costs.

Security policies, including access control and encryption, are managed by EpiForce software agents. Each agent is visible through a central administration console to monitor and manage activity between servers. Groups of agents are aggregated to easily apply network-wide policy changes and updates.

Agents automatically enforce security relationships while providing reporting on “out of bounds” activity, providing a clear audit trail to assist in compliance audits. Audits are a necessary requirement to achieve regulatory compliance within this security implementation.

Hewlett-Packard (HP) was retained as a global systems integrator due to the size and scope of the installation as well as their expertise at implementing such security solutions. A phased deployment plan was established allowing sufficient time to establish appropriate security policies and implement through a project team.

## BENEFITS

The fact that the existing applications will be secured 'as is' was a very important factor in the final decision-making process. The cost to rewrite and then integrate multiple applications across many business units in over 100 countries would have run into hundreds of millions of dollars.

Specific provisions within GLBA dictate encryption of customer data, including user names and passwords, while in transit. This requirement has now been addressed.

Overall security has now been augmented by adding a new transparent layer of protection for inside the perimeter. The risk of unauthorized access to in-the-clear communications of sensitive information has been eliminated.

In summary, EpiForce enabled this institution to:

- Meet regulatory security requirements without having to rewrite existing applications
- Centrally manage both the encryption of sensitive customer data while in transit and the protection of this data while at rest
- Create closed user groups to ensure access to corporate applications is allowed only from authorized nodes
- Logically segment the network through a centralized console without modifying any existing hardware; this enabled the IT organization to reap the benefits of traditional network segmentation (increased security and lower operating costs), without having to sacrifice network flexibility
- Provide a strong audit trail for regulatory compliance audits
- Implement a solution that can scale to true enterprise levels while allowing phased deployments

EpiForce's automatic enforcement of security policies offered a cost effective, innovative solution through use of logical security zones to address manageability challenges. It's transparency to existing infrastructure and applications enabled very large deployments without rewriting code.

## ABOUT APANI

Apani is the preeminent provider of cross-platform server isolation solutions for large enterprises. Apani's solution isolates and secures the communication between servers and endpoints without regard to operating system or physical location.

Apani EpiForce, the company's flagship product, is a software-based alternative to using firewalls and VLANs inside the corporate network. EpiForce enables two powerful disciplines – logical security zoning and policy-based encryption of data in motion. EpiForce is a distributed, centrally-managed solution that is transparent to users, applications and infrastructure – making it quicker to deploy and less costly to manage than hardware-centric solutions. Policy enforced by EpiForce is persistent, which enables protected resources to be relocated without compromising security.

Providing an evolutionary improvement in efficiency, flexibility, manageability and total cost of ownership, Apani technology is used by much of the Fortune 500.

Based in Southern California, Apani was founded in 2003 and is privately held. More information about the company may be found at [www.apani.com](http://www.apani.com).

### For More Information

To learn more about EpiForce and Apani, please call (866) 638-5625.

Outside the United States, please call  
+1 (714) 792-1875.

Apani is accessible on the web at  
[www.apani.com](http://www.apani.com).

08-007 05/08