



EpiForce®

Overview

Technology solutions provider to the State of California

Industry: Healthcare

Customer Profile

Based in Sacramento, the California Department of Technology Services (DTS) provides cost-effective computing, network solutions, electronic messaging, training and large-scale information technology project management to state departments, counties and cities throughout California.

Business Challenge

To comply with HIPAA regulations by establishing and maintaining secure communications within a proprietary healthcare records management system, which must scale to support tens of thousands of unique users.

Initial Microsoft IPsec deployment had limited effectiveness and no scalability due to significant management issues and multi-vendor incompatibilities

Solution

DTS selected Apani® EpiForce® to secure internal data flows traveling between multiple platforms. This cost effective approach secured inside the network perimeter using industry proven IPsec encryption technology. With the flexibility to support multiple operating systems and equipment infrastructures, EpiForce enabled DTS to support each of its varied governmental constituencies, ranging from the Children's Welfare Department to the University of California.

Benefits

- Centralized management provides an effective security overview capability
- Cross-platform support to protect heterogeneous environment
- No application rewrites or end user training needed
- Highly scalable architecture satisfies existing needs and future requirements
- Audit trail simplifies HIPAA audit
- Complements existing network infrastructure

California Department of Technology Services (DTS) selects Apani EpiForce to secure data-in-motion and address HIPAA security requirements.

“EpiForce has provided us the flexibility and scalability to effectively support our HIPAA compliance, and ensure confidential patient data remains secure.”

Tom Jones, Chief Information Security Officer, DTS

Established in 1977, the California Department of Technology Services (DTS) provides cost-effective computing, network solutions, electronic messaging, training and large scale information technology project management to state departments, counties and cities throughout California.

The challenge was to maintain HIPAA compliance by establishing secure network communications between multiple hardware and operating system technologies for a proprietary patient records application.

The solution had to be scalable to support the growing number of projected users, estimated to be in the tens of thousands over the next several years.

Initially, a Microsoft IPsec solution was evaluated. However, it lacked scalability and could not handle multiple operating system platforms. EpiForce was selected based on its flexibility, scalability and ability to establish a strong foundation to deploy secure communications within heterogeneous environments. EpiForce will be leveraged for statewide deployment of other sensitive data requiring secure communications



“Establishing security zones with different levels of administrative authority eased deployment and management challenges”

Tim Funk,
Senior Director, IT Security, DTS

SITUATION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a far encompassing act of legislation originally passed to provide health insurance coverage for workers and their families when they changed jobs. The act has been expanded upon to provide the right to confidentiality of sensitive healthcare information.

As part of the act, organizations must protect communications containing health information when transmitted electronically across open networks. They cannot be easily intercepted or interpreted by parties other than the intended recipient. Information systems must be protected from intruders trying to access systems through external communication points.

The DTS plays an important technology leadership role within the state of California. With regards to applying federally mandated HIPAA compliance guidelines within the state of California, their mandate is to recommend viable solutions for each of their departments, including the DTS.

The decision to select EpiForce reflects a comfort level that data-in-motion will be secure and that sensitive healthcare information will be protected while in the custody of the State of California.

DTS delivers services through a powerful network of mainframes and client-server based systems, distributed through a secure statewide network, comprised of systems from multiple leading security vendors. The proprietary healthcare records management application must securely communicate with the distributed servers on different platforms

DECISION PROCESS

Each of the independent agencies within the State of California outsource their IT requirements to DTS, including network solutions, electronic messaging and large scale IT project management tasks. As such, a secure communications solution must be flexible to support the multiple operating systems and equipment deployments in place throughout the state. Scalability and ease of management were key criterion of the selection process.

DTS had deployed small pockets of Microsoft IPsec within their windows environment, however, this had only limited effectiveness as it would not support any ‘non-windows’ devices.

In addition, implementing IPsec between large numbers of internal systems was simply not practical. The fundamental problem with IPsec has always been manageability. While it is relatively simple to set up a single point-to-point encryption tunnel, the challenge grows exponentially when scaling up to just 25 servers, let alone 100, especially when considering varying expiration dates for certificate of authorities.

Another consideration was to deploy all new web-based applications capable of SSL encryption throughout the network. In reality, this option was not feasible, as the cost and use of resources to implement would have been quite tenuous.

Goals

DTS has two stakeholders whose needs must be met when deploying new IT initiatives: (1) the internal agencies within the state of California, and (2) the end users relying on these systems to provide public amenities as part of California residency. DTS works with external systems integration firms to perform these functions; their relationship with CompuCom played an important role in ensuring each of these impacted needs was well addressed.

Internal Requirements

State agencies must be provided a cost effective solution with minimal current year budget impact, while at the same time, minimize technological obsolescence. New IT systems must be compatible with existing communications and the security infrastructure such that systems may be gradually improved upon over time in a well planned manner.

External Requirements

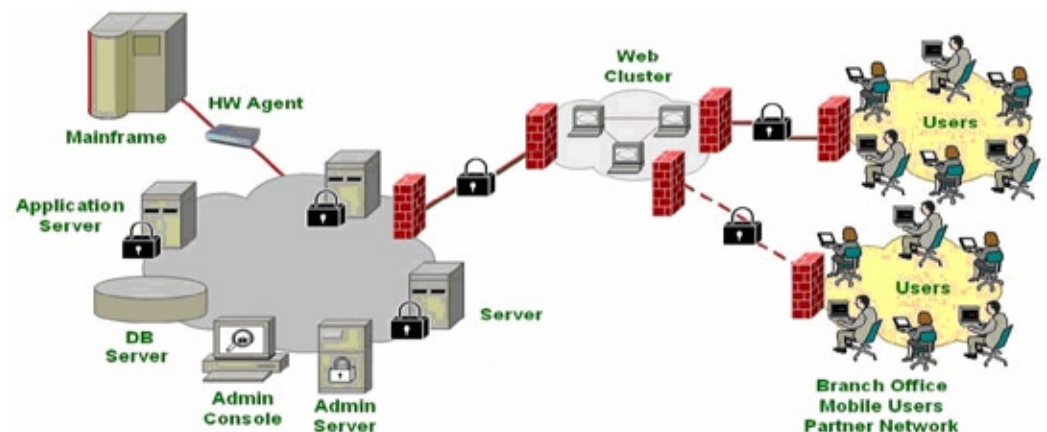
Thousands of users access healthcare information databaes within the state of California, each expecting the utmost of data security. This figure is expected to grow substantially over the next few years to tens of thousands, once deployment is complete. The impact of this project will be far reaching, affecting all health care providers, doctors and pharmacies sharing data with the state's health information data depository. Ease of use and scalability challenges must be addressed to facilitate this ambitious roll out.

SOLUTION

Before selecting EpiForce, DTS performed considerable stress testing within a controlled laboratory environment for over twelve months as part of an evaluation program. The recommended implementation includes a combination of software and hardware based agents to secure communications: (see below diagram)

- Software agents to support multi-vendor server platforms
- Appliance agents to communicate in the mainframe environment

EpiForce ensures secure network-wide communications between each vendor platform and operating system where the proprietary patient records management application is deployed.



Users seeking prescription or medication history, MediCal / Medicare affiliations or other healthcare related information can access the system through SSL secured web-browsers; EpiForce secures back end communications while the sensitive data is in transit.

Not only does the EpiForce secure data flows throughout this heterogeneous environment, but it automatically enforces security relationships defined through a centralized management infrastructure. As new security policies are identified, additional users or servers are added or new associations are established with medical organizations, it is relatively straight forward to adjust the policies to implement the updates in real-time.

EpiForce selectively encrypts data-in-motion and provides machine level access control that is two way: both the sender and recipient must authenticate and approve each other's data transmittals and receipts. This process provides further protection by restricting unauthorized access.

BENEFITS

DTS's implementation of EpiForce contributes to the State of California maintaining HIPAA compliance. By encrypting data flows and providing machine-level access control throughout the network, the highest levels of security are attained, regardless of operating system infrastructure or equipment platforms.

Recognizing legacy systems must be part of the solution, Apani EpiForce made a lot of sense. Not only does EpiForce support MS Windows, Linux, Solaris, HP and IBM, but mainframe applications are easily secured through use of an appliance-hosted agent, capable of providing the same level of protection for devices not capable of running an agent locally on their included OS.

EpiForce's automatic enforcement capabilities offer an innovative solution, through use of logical security zones to address manageability challenges, enabling very large deployments to secure services and endpoints within the corporate network.

EpiForce successfully added a new transparent layer of security, functioning completely in tandem with existing security systems. This compatibility enabled DTS to execute a phased deployment, which will scale to support the typically large configurations of their clients

Benefits of Apani EpiForce - EpiForce vs. Microsoft Provided IPsec		
Cost/Benefit	EpiForce	MS IPsec
Supports multiple platforms	Yes	No
Ease of Management	High	Low
Appliance-based optional deployment	Yes	No
Flexibility to support varying security policies by user-group?	Yes	No
Central management of security policies	Yes	No
Automatic deployment of policy updates	Yes	No

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.

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.