

Case Study: Eclipsys

SecureLink Manages Remote Support Complexity and Security Challenges

Customer Description

Eclipsys Corporation is an enterprise healthcare information technology solutions provider to more than 1,500 major healthcare facilities, including academic medical centers, hospitals with pediatric facilities, and community based hospitals of all sizes. Eclipsys offers 14 distinct software applications that enable information flow across a wide range of healthcare functions: financial applications managing patient admission, transfer, and discharge, patient and resource scheduling, and patient financials; clinical applications for patient care and records management; and departmental solutions for surgery, radiology, laboratories, and case management workflow automation. These products deliver workflow and knowledge support to smooth information transfer and patient management between physicians, nurses, managers and other members of the healthcare team.

Eclipsys customers include all of the hospitals on America's Best Hospitals Honor Roll, and nearly half of the more than 100 organizations that have received Magnet Recognition Program status – the highest award an organization can receive for quality of nursing care – use Eclipsys solutions. Eclipsys customers include Boston Medical center, Cleveland Clinic-Easter Region, The National Institutes of Health, and University of Michigan Hospitals and Health Centers.

Key Healthcare Industry Issues

Application Interconnectivity

Hospital departments transfer and share electronic patient data - data that needs to be accessible in real time with views of the information appropriate to the needs of specific departments. Data flow, application interconnectivity and reliability are essential for good health care and efficient operation. Application failure, data corruption, or even slow performance are potentially life threatening and unacceptable for healthcare organizations trying to maintain standards of care. Quality applications and support ensure the continued efficiency, accuracy, and timeliness of information transfer, and all of these lead to better patient outcomes.

Privacy Regulations Compliance

Security, privacy and financial regulations have placed health care providers in an increasingly controlled environment. HIPAA is the most influential, but other regulations such as Sarbanes Oxley, EC 95/46, California SB 1386 and others define requirements for security, managing information, and reporting. Protection of data is extended past the healthcare provider to include the vendors supplying software and systems. Failure to meet statutory requirements can lead to disastrous results. In one case, Choicepoint, an information provider to insurance companies, received the largest civil fine in FTC

history (\$15M) for compromising the personal information of 145,000 US residents. Compliance with these regulations creates requirements for added process, infrastructure, and application features to enable and enforce the process.

Eclipsys Challenges

As an end-to-end healthcare solutions provider, Eclipsys has an extensive product suite that includes a number of server-based software solutions. With over 1,500 customers being supported by 1,000 support analysts, Eclipsys requires remote diagnostics and maintenance of customer systems to meet cost management and customer satisfaction goals.

Like many companies that support complex applications for a large and diverse client base, Eclipsys maintained several remote support solutions and a wide variety of connectivity types. Phone desk, email and chat, and customer initiated web support all required high level of two party (customer and Eclipsys analyst) interaction and were driven by reaction to customer problems instead of proactive management by Eclipsys. A wide variety of connectivity types including modems, point-to-point networks, shared desktops and VPNs were expensive, complex and not all secure. The combination of applications and connectivity made it difficult to define and manage process for security, and had no single audit and reporting capability.

Eclipsys Support Connectivity Requirements:

Scalability: With 1.5M (1,500 customers x 1,000 analysts) potential support connections, Eclipsys needed a scalable solution that minimized the complexity and cost of managing large numbers of connections.

Security: As a solution provider to HIPAA regulated entities, Eclipsys needed to provide solutions that enabled compliance. User control with unique logins for 1,000 employees at 1,500 access points, and audit control to track and record all system access and activities are key features of meeting HIPAA requirements

Platform Independence – In order to reduce the complexity and cost associated with multiple methods of connectivity, Eclipsys needed a single platform to consolidate remote support access and still work with multiple customer platforms. Browser based access with client side

components was needed to provide simple, quick, and inexpensive means of establishing and maintaining remote support connections. A consolidated platform also reduces the hardware and software costs associated with managing remote support. Eclipsys analysts often use proprietary diagnostic tools to aid in remote application support and speed problem resolution. As customers include more and more operating systems, Eclipsys needed a way to control the growing licensing cost of proprietary tools.

“We evaluated several solutions to make support & service more effective. SecureLink scored highest for both security & utility.”
– Jim Reed
SVP, Customer Support

The SecureLink Remote Support Network Solution

In SecureLink, Eclipsys found a solution that provided the perfect combination of control, flexibility and security. The SecureLink Server manages, audits and records all of the remote support connections between Eclipsys and its customers. SecureLink Gatekeepers, installed on customer servers, enable and define the limits for each remote support connection.



The SecureLink server brokers secure access between the Eclipsys technician and the customer's network.



The SecureLink Server runs on a secure hardened platform of Linux and offers a single point of control for support access to customer systems. SecureLink Gatekeeper can be installed and set up in minutes providing simple, customer driven access management by defining the hosts, ports, files, directories and applications that Eclipsys support analysts are allowed to access.

SecureLink Benefits:

- Single platform for managing remote support connections to all OS platforms at all customers, reducing connectivity complexity and cost and improving efficiency.
- Direct, native access to the customer server, allowing Eclipsys support analysts to use their favorite, proprietary resolution tools without paying additional license fees, increasing effectiveness and decreasing time to resolution
- Simple, flexible customer managed access controls allowing compliance conscious healthcare providers to restrict access appropriately and increase security.
- Pre-defined controlled access to customer applications reduces time required by customer IT staff to participate in problem resolution, saving cost and improving customer satisfaction. SecureLink's feature allowing trusted vendor remote access without customer involvement meant Eclipsys could solve problems without requiring customer involvement.
- Multiple remote connections for a single support session allow Eclipsys to apply additional service representatives for faster problem resolution.

- Detailed audit, reporting and real-time monitoring capability for every remote support session, enabling security process definition and proof of HIPAA compliance.

SecureLink and Eclipsys Results – Reduced Costs, Improved Security, Increased Customer Satisfaction

Eclipsys began to see positive results shortly after rolling out SecureLink. SecureLink's platform independence gave Eclipsys the ability to consolidate its remote support connections on a single platform regardless of the customer's operating system. SecureLink ease of use reduced setup costs and improved connectivity response time. As a result, Eclipsys saw its support efficiency increase and the cost of connectivity drop by 87%. SecureLink's direct, native access to customer servers allowed Eclipsys' support analysts to use whatever tools they needed to resolve a service issue, eliminating duplication of license fees, further reducing cost and time to problem resolution.

“Finally, a fast & easy way to remotely connect to a customer's network!”

**– Mike
Senior Support Analyst**

SecureLink's ability to let customers strictly define access for each remote support connection, combined with robust audit and reporting functionality allowed both Eclipsys and its customers to generate historical audit reports and detail log files capturing who accessed the system, what was done (at the command level), and what tools were used. This satisfied the HIPAA concerns of even the most security conscious customers.

Customer Satisfaction, Better Patient Care

Eclipsys uses SecureLink to service hundreds of its customers remotely, securely, and effectively. Since it began using SecureLink, Eclipsys has reduced the cost of managing its remote support connections and the cost of licensing diagnostic tools essential to delivering quick problem resolution. The savings were so significant; the time return on investment in SecureLink was 6 months.

Customers see problem resolution times drop along with the amount of IT resource needed to manage the interaction. Automated, accessible, and detailed audit and reporting offered by SecureLink reduced Eclipsys and customer overhead in meeting security requirements. The net effect: Eclipsys solves customer problems quickly and with less cost using a platform that can easily scale to meet future needs. Eclipsys customers require less IT resources to participate in application support, allowing more focus on improving patient care.

“By converting our customers to SecureLink’s remote support network, we were able to save our customers money on their connectivity costs, enhance the reliability of the connection, improve our response and resolution times, all while increasing the security and auditing capability of the customer’s systems. Not bad for 15 minutes work!”



– Robert Bell
VP, Product Support Services

