Remote Support Network
Table of Contents

I. Introduction - Executive Summary...........................................................................................................................1
   Managing Remote Support in a Secure Environment..................................................................................................1
The Increasing Complexity of Remote Support...........................................................................................................1
   Growth of Complexity........................................................................................................................................1
Enterprise Software Vendors and Privacy Legislation..................................................................................................2
   Security Lapses Frequent and Sometimes Spectacular............................................................................................2
   Data Privacy and Financial Regulations Include Software Vendors.................................................................3
The Problem (and Characteristics of A Solution).........................................................................................................3
The Solution - SecureLink remote support network..................................................................................................4
II. Managing Remote Support Connections with SecureLink - A Single Secure Platform.................4
   Platform Consolidation Reduces Complexity and Simplifies Security.................................................................4
   SecureLink Design Goals.......................................................................................................................................5
III. SecureLink Architecture – Single Platform Server and Simple Client.........................................5
   SecureLink Overview........................................................................................................................................5
   SecureLink Server.............................................................................................................................................6
   Administration....................................................................................................................................................6
   Reporting...........................................................................................................................................................7
   Services................................................................................................................................................................8
   SecureLink Gatekeeper.......................................................................................................................................9
   Connecting the Gatekeeper to SecureLink Server............................................................................................9
   Gatekeeper Registration with SecureLink............................................................................................................9
   Customer Controlled Access................................................................................................................................10
   Gatekeeper Enables De Facto Security Policy....................................................................................................11
IV. Summary............................................................................................................................................................11
   Technical Specifications........................................................................................................................................12
   SecureLink Server.............................................................................................................................................12
   SecureLink Gatekeeper.......................................................................................................................................12
   SecureLinkJava................................................................................................................................................12
   Encryption........................................................................................................................................................12
   User Interface....................................................................................................................................................12
Appendix 1: Case Study.............................................................................................................................................13
   Eclipsys – Managing Remote Support for Healthcare Providers..................................................................13
   Support Connectivity Requirements..................................................................................................................13
   SecureLink........................................................................................................................................................13
I. Introduction – Executive Summary

Managing Remote Support in a Secure Environment
Enterprise software vendors strive to maximize support efficiency – log on to the customer system, diagnose, then fix the problem, log off and close the ticket. Fast, easy network access to all the systems and tools needed to solve the problem delivers quick resolution times and satisfied users. For a lot of enterprise customers however, this is a security nightmare. Concerns over data privacy have created a class of businesses that have significant legal obligations for keeping systems and data secure, including remote access to systems for support. Privacy regulated businesses can’t afford to trade rapid problem resolution for data and system security. For these businesses and for their software vendors, strictly controlled system access with detailed auditing is requirements for remote support. The challenge for the software vendor is to deliver secure support in the wide range of networking, software, and customer systems that make up the typical enterprise computing environment.

The Increasing Complexity of Remote Support

Growth of Complexity
Although the methods of delivering remote support have evolved, the economics remain fundamentally the same. Whether it’s by telephone, chat, email or networked access to customer systems, remote software support is far more cost effective and timely than onsite support. The problem is that the complexity of managing remote support connections grows at an increasing rate as a vendor adds customers and products. The situation is made even more acute when security considerations are added. Consider the following example when a company adds products, personnel and customers over a three year period:

Year One:
- Company A sells 2 products, has 2 support technicians, and 20 customers
- 2 different systems are used for remote connectivity (e.g. dial up modems and VPN)
- In the very simplest scenario, Company A manages all of remote support with 2 unique connections (based on type of connection) shared between technicians, products and customers
- When security considerations are added (unique technician/product/customer combinations) the possible number of connections for customer support grows dramatically: 2 products x 2 technicians x 20 customers x 2 connectivity types = 160

Year Three:
- Company A has released new versions of each of its products and acquired Company B. There are now:
  - 4 products (2 versions each), 4 technicians and 40 customers with 4 types of connectivity
  - Total unique connections = 4 x 2 x 4 x 40 x 4 = 1280
- By doubling the number of customers products, technicians, etc., the complexity of managing remote service connections increases by 700%
This simple example illustrates how quickly administering remote support connections can become an exercise in complexity management.

In the real world, the problem is even more challenging. Enterprise software vendors may have hundreds of support technicians, thousands of customers, and several suites of products with support contracts covering multiple versions of software. Customers acquire and upgrade technology in a piecemeal fashion – software applications, servers, and networking are added and changed as market conditions require or budget allows (and occasionally according to a CIO’s long term plan). Whether it’s VPNs, telnet, FTP sites, browser access, point-to-point networks, or dial up modems, software vendors need to work with whatever the customer has. The result is an environment where complexity can grow so quickly that software vendors spend more on managing connectivity than solving customer problems.

**Enterprise Software Vendors and Privacy Legislation**

**Security Lapses Frequent and Sometimes Spectacular**

News releases about losses or outright theft of personal information have become almost commonplace. Recent examples include the chairman of the UK revenue and Customs service (the UK equivalent of the IRS) resigning after his agency lost the “Personal and bank details” of 25 million people. In another incident, the FTC levied a record fine of $15M against ChoicePoint for “unwittingly selling the records of 163,000 US citizens to fraudsters”. The problem has been growing for years, prompting privacy legislation and more IT resources focused on data and system security.
Data Privacy and Financial Regulations Include Software Vendors
The data privacy and financial regulations arising from security concerns (HIPAA, Sarbanes Oxley, EC 95/46, California SB 1386 and others) have created a class of businesses that must manage data and access to data in a demonstrably secure way. Security processes must be defined, implemented and audited for banks, hospitals, and other companies handling private personal information in order for them to meet legislated requirements. And, it’s not just the companies holding the data that have security requirements. Under HIPAA (Health Insurance Portability and Accountability Act), for example, the data security obligation is extended past the healthcare provider to include vendors supplying systems and software. Software vendors providing support must operate in the same security environment as their enterprise customers.

The Problem (and Characteristics of A Solution)
Economics and efficiency drive the requirements to provide remote support. Enterprise software vendors support customers with widely varied (and constantly changing) computing and networking environments, and an increasing number of those customers have substantial data security and system access control obligations that they must meet. The problem for the software vendor is to manage the complexity and deliver quality service in a highly secure environment.

The general characteristics of a solution to this problem include:

- **Complexity Management** – Support a wide variety and large number of remote connectivity alternatives without adding management overhead.
- **Security** – Provide simple and detailed auditing and reporting. Enable customer defined and controlled system access for remote support.
- **Flexibility and Scalability** – Add customers, users, and applications easily and offer the tools required to effectively perform remote support.
- **Simplified Customer Participation** – Reduce customer resources required for providing and supporting remote access.
The Solution - SecureLink remote support network

SecureLink’s remote support network is the first system designed specifically to address the issues involved in managing remote support connections for secure enterprise customers. Over 15,000 organizations including hospitals, financial institutions, public sector entities and the vendors that supply them software use SecureLink to provide secure remote support connections. The remainder of this paper will provide an overview of the key architectural components and features of SecureLink and how these combine to simplify managing remote support.

II. Managing Remote Support Connections with SecureLink - A Single Secure Platform

Platform Consolidation Reduces Complexity and Simplifies Security

The solution to meeting the challenges of managing remote connectivity when supporting secure enterprises fortunately involves a synergy – reducing the complexity of remote connection management provides security benefits. By consolidating connection types, application management and remote access to customer systems onto a single platform, the problem of tracking, auditing and reporting on support technician activities on customer systems becomes greatly reduced – all of the remote connection session data is in one place.

Security in a legislated environment requires systems that are technically secure (password protection, access restrictions, encrypted communications, etc.) and demonstrably secure (auditing and reporting). Without a single platform to manage access, providing detailed auditing and reporting (users, applications, servers, dates, actions taken, etc.) each time a support technician accesses a customer system is problematic. The audit and report functions are either unique to each application, built as an add-on, or built as entirely separate applications (with ad-hoc integration). And, it’s likely to be different for each customer. For the enterprise software vendor in this situation, managing security is difficult and implementing an efficient overall process for helping enterprise customers meet their security obligations is nearly impossible.
By consolidating remote system access onto a single management platform, both problems of managing connection complexity and enabling security are solved. Even with a large numbers of applications, customer systems, and connection types, auditing and reporting functions can be handled with a single interface.

SecureLink Design Goals
To provide some background for the product features, it’s helpful to first review some of the design goals that identified for SecureLink. The overall design goal was to deliver a system that enabled software vendors to a) reduce the cost and complexity of providing remote support, b) help security conscious customers meet their data and system access requirements, and c) deliver higher quality application support. Some of the key components of that overall goal include the following:

- Reduce the requirement to support a large number of remote connectivity types.
- Take advantage of widely available technology – connect to everything using the Internet and use browsers as the primary interface for customers and support technicians.
- Deliver the infrastructure to manage large numbers of clients, applications and support technicians.
- Provide support technicians with a set of tools to allow them to effectively diagnose, repair and maintain customer’s applications.
- Make remote support connections secure with encryption and tunneling.
- Make access to the management infrastructure secure for both users and administrators.
- Provide detailed audit and reporting functions for both the software vendor and the enterprise customer.
- Let the customer (the enterprise managing the data) define the rules for accessing the host system and the tools provided to the support technician for performing remote support.

III. SecureLink Architecture – Single Platform Server and Simple Client

SecureLink manages all of the remote connections between the software vendor and its customers. SecureLink is made up of two main components: SecureLink Server and SecureLink Gatekeeper. The SecureLink Server provides a single point of control for identifying customers, connections specific to the customer, and the groups of support technicians allowed to access those connections for support. The SecureLink Gatekeeper resides on the customer’s server and defines access rules for remote support connections (when, which systems, and what activities can be performed by the vendor support technicians). SecureLink also includes a reporting feature (for both Servers and Gatekeepers) that records the details of each support session, providing a single source of auditing and reporting.

SecureLink Overview
SecureLink utilizes encrypted SSH tunneling and proprietary port-forwarding technology to broker secure, audited remote connectivity. SecureLink is specifically designed to provide control, security and audit capability while simultaneously providing the tools technicians need to deliver timely and effective remote support.

SecureLink operates on a dedicated server located within the software vendor’s secure network – not a hosted server in the cloud. Login access to the SecureLink server is only available to authorized vendor support and services personnel authenticated to the vendor’s network. Within the SecureLink application, users are segmented by different user groups that in turn have access privileges to designated customer groups on an as needed basis.
The SecureLink Gatekeeper is a client application installed on remote servers and PCs with outbound Internet access that acts as a secure access point for vendor technicians. Once installed and enabled, the Gatekeeper sends an outbound “ping” over SSH on regular polling intervals to the SecureLink server checking to see if anyone at is requesting a remote connection.

**SecureLink Server**

The SecureLink server manages all remote support connections between the software vendor and its customers, and provides administrative functions to create users and user groups, customers and customer Gatekeepers. Access to SecureLink server functions is provided through a simple browser interface.

**Administration**

SecureLink administrators can create user accounts (support technicians and other administrators), user groups, and Gatekeeper groups. Support technicians (standard user account) can add customers and Gatekeepers and determine to which group a Gatekeeper is assigned.

Graphic of hierarchy – gatekeeper groups, customers, users, ...

SecureLink server provides all the tools needed by the support technician to create and maintain remote support connections including:

- Customer lists
- Gatekeepers associated with each customer
- Session history for each customer
- Detailed activity from each session

Technicians can easily identify customers and associated Gatekeepers, keep track of live remote connection sessions, and review report detail from previous (and ongoing sessions).
Reporting
Details of each remote connection session are recorded by SecureLink and available in both summary (by user and customer) and detailed form.

Detail recorded for each session includes:

- Session and Gatekeeper information and status
- Owner
- Registration code
- Creation date, completion date, session duration
- Which support technicians participated during the session
- What services were accessed by the support technician, what happened, and how long it took:
  - Start and end time of each activity
  - Telnet logs
  - Files transferred
  - Bytes sent and received during desktop sharing
  - Chat history
The history of each remote connection session is available to both the software vendor (through SecureLink Server) and to the customer (through the Gatekeeper). Both the vendor and the customers have the detail they need to provide evidence of compliance with security regulations.

**Services**

Support technicians need more than a secure Internet connection to remotely diagnose and repair applications. They need access to the server hosting the application and a set of services to perform the diagnosis and repair. Each Gatekeeper installed on a customer server enables a set of default service that provide most of what a software vendor will need to remotely support applications. These services include:

- **File Transfer** – FTP services allow the transfer of files between the vendor and customer including log files for diagnosis, software updates, and shell scripts. File transfer can be read only or read/write.

- **Desktop Sharing** – Remote graphical desktop sharing allows the support technician to access the customer’s desktop, see what the customer is seeing, and take over mouse and cursor control.

- **Command Prompt** – The remote command shell interface provides the support technician with the ability to access a command prompt for supporting Unix of Linux based systems.

- **PowerPrompt** – PowerPrompt is an enhanced command prompt on Window systems with much more flexibility than a standard DOS prompt (what’s an example?).
SecureLink also provides support for proprietary tools, allowing support technicians to use their favorite tools to provide quick problem resolution. (Does this mean that SecureLink allows easy installation of proprietary tool on the vendor’s host, or running the proprietary tool on the Linux server?) Services can be added or deleted and temporarily enabled or disabled.

All access to customer systems and services available during remote support connections are controlled by the customer using the SecureLink Gatekeeper.

SecureLink Gatekeeper
The Gatekeeper is the SecureLink client software that resides on the customer’s server and defines the remote connection between the SecureLink Server and the customer’s system. The Gatekeeper includes a simple browser based interface that allows customers to identify the host system, ports, connectivity settings, services, and security settings governing the software vendor’s access. The Gatekeeper runs on systems with outbound access to the Internet that acts as a secure access point for support technicians. Once installed and enabled, the Gatekeeper sends an outbound “ping” over SSH on regular polling intervals to the SecureLink server checking to see if anyone is requesting a remote connection. When a request for a remote connection has been made, the Gatekeeper establishes and initiates a secure, encrypted tunnel to the SecureLink server forwarding the ports that are configured on the Gatekeeper to the remote technician that has requested remote access. Detailed reports of each support session are available through the Gatekeeper, providing customers the data they need to establish and maintain security compliance.

Connecting the Gatekeeper to SecureLink Server
The Gatekeeper utilizes port 22 (SSH) by default to make outbound connections to the SecureLink server. If port 22 is not open, the Gatekeeper will then attempt to connect over port 80 (http) and if this also fails, it will then attempt to auto-detect the machine’s proxy settings. The vast majority of the time, the Gatekeeper will detect and use the most efficient available port to access the Internet.

Because the Gatekeeper makes an outbound connection to the Internet, no firewall or network security adjustments need to be made on your end. As long as the machine that the Gatekeeper is installed on has access to the Internet, nothing else needs to be done.

The Gatekeeper’s Windows installer can be launched and installed with 2-clicks. The Gatekeeper will go through a short connectivity test to ensure it can find its way to the Internet. Once the Gatekeeper passes the connectivity test, it will prompt for a registration code. The registration code is generated and provided by an authorized vendor support technician. The registration code is generated by the SecureLink server and uniquely identifies the customer profile and the machine it is installed on. The new Gatekeeper will only communicate and establish connections with the SecureLink server where it is registered.

Once the Gatekeeper has been installed, registered and enabled, it is now available to be remotely accessed by authorized vendor technicians. When a technician requests access, the SecureLink server brokers an encrypted tunnel between your gatekeeper and the technician. The Gatekeeper then forwards its available ports to the technician’s desktop.

Gatekeeper Registration with SecureLink
The Gatekeeper does not automatically register itself with the SecureLink Server when installed. It registers itself when a registration code (generated within the SecureLink server and provided to the customer by a vendor technician) is entered at the prompt following installation and the connectivity test.

When this registration key is entered, the Gatekeeper makes an outbound SSH connection to the server. Contained in this connection is the registration code, which syncs the Gatekeeper to its matching entry in
the SecureLink Server, but the public and private SSH keys are totally separate from this code. So, the SSH authentication only takes place when the gatekeeper is manually set up to connect to the server or allow anytime access through a polling interval.

**Customer Controlled Access**
Any connection to the customer from the SecureLink server must approved first by the customer (through the enabling of the Gatekeeper). Customers have a great deal of flexibility and control to define Gatekeeper access:

- **Connectivity Settings**
  - Gatekeeper access is either enabled or disabled. A remote connection can be made to the customer system only when the Gatekeeper access is enabled.
  - Gatekeeper connection status can be managed in three ways
    - On a defined schedule (day, date, hour)
    - Disabled after an elapsed time access (within n hours)
    - Manually – customer enables or disables access
  - The Gatekeeper has optional HTTP tunneling modes to address connectivity issues with firewalls and proxies.
  - Proxy servers can be defined for Gatekeepers if the host must go through another system to access the Internet

- **Security Settings**
  - **Password** – Access (to enable or disable Gatekeepers) and administration (to configure Gatekeepers) can be restricted by password
  - **Encryption** – Users can choose between four encryption options to secure the communications between SecureLink server and the system hosting the Gatekeeper AES (Rijndael block cipher, the current Advanced Encryption Standard) in 128, 192, and 256 bit modes, Blowfish, or Triple-DES.
  - **Updates** – The Gatekeeper can be configured to download a newer version if one is available. Upgrades are installed automatically after the support session is complete and the connection is closed.

- **Notification Settings**
  - Customers can select an email address to receive notifications whenever a connection is made through the Gatekeeper.
  - **Vendor Privileges** - The services used by the support technician to diagnose and resolve software issues (FTP, shared desktop, command prompt) are included in the Gatekeeper and enabled (or disabled) by the customer.
  - When configuring the Gatekeeper, customers build an access list that contains hosts or IP addresses and ports the vendor is allowed to access.
  - Using the Gatekeeper access list (shown on next page), the customer controls a) the host and ports accessible to the software vendor and b) the services available on those hosts.

- **Vendor Defined Services** – SecureLink has a feature that allows vendors to add services to a host. When Vendor Defined Services are enabled, the vendor can add services needed for support to host that are available for access. The vendor is only able to add services on hosts and accessed through ports that are allowed in the access list.
Gatekeeper Enables De Facto Security Policy

One of the key security features in the SecureLink design is that the entity whose systems are accessed (and who has the obligation of protecting the data) defines and enforces the rules of remote access. Remote support connections are managed through the SecureLink server, but are enabled and defined by the Gatekeeper. The customer sets levels of security on the Gatekeeper, defines which systems can be accessed and what services are available to the support technician, and sets the schedule for remote access. The SecureLink Gatekeeper enables the establishment of a de facto security policy for remote support with minimal customer overhead (no code to write, no additional applications to integrate).

IV. Summary

This paper has highlighted some of the key issues that define the challenges enterprise software vendors face when supporting security conscious customers:

- Legislation and business requirements have created a class of enterprises that must maintain a high level of security. This includes well defined processes for how systems are accessed by vendors providing remote support.
- Enterprise technology acquisition occurs over time, resulting in a diverse computing and networking environment and an increasingly complex connectivity problem that must be solved by the software vendor to provide support.

When considering large numbers of customers and support technicians, and the variety of connectivity types, application versions, and hosting servers, the problem of managing remote support connections becomes immense and potentially creates significant security risk.

SecureLink manages complexity and enables security by providing a single platform from which to manage remote support connections. The single platform approach has delivers many benefits to the software vendor:

- **Reduced Complexity** – All remote support connections are managed the same way – from a common platform.
• **Improved Scalability** – With a common interface and consolidated information on all remote support connections, adding customers doesn’t add complexity. The hierarchy and interface are simple to understand and use. SecureLink can easily scale to handle large numbers of support technicians, applications, and customers.

• **Reduced Cost** – SecureLink replaces the ad hoc manual creation of support connections, services, authentication requirements and reporting. The cost of establishing and maintaining connections to customer systems is reduced dramatically. A single platform also reduces the cost of maintaining multiple versions of hardware and software required to support the customer base. A multi-platform Gatekeeper means SecureLink server can provide native access to a customer system regardless of operating system. Cost is reduced for the customer as well. Customers require considerably fewer resources to interact with vendor support technicians because the terms of the connection (what the support technician can access and do) have been defined in advance and the reporting function is automatic.

• **Improved security** – Detailed audit, reporting and real-time monitoring capability for every remote support session enables security process definition by the customer and provides easily verifiable proof of compliance.

The real gain provided by SecureLink is that software vendors can reduce the amount of resources required to manage remote support connections and redirect them to increasing the quality of customer support. Time to connect and time to repair drop. Detailed records of session activity provide data required to determine security compliance and offer a knowledge base resource for future problem solving. Enterprise customers spend less time involved in support calls and see the level of service and quality of reporting improve. SecureLink empowers the vendors support technicians and reduces the burden on the customer, cutting support costs and improving customer satisfaction.

### Technical Specifications

**Hardware Appliance Option**
- Dell PowerEdge™ R220
- OS: CentOS 6
- Intel Core i3-34130 3.30 GHz Processor
- 8 GB RAM – 1600MHz
- 2x 500GB SATA Hard Drive (RAID)

**Virtual Appliance Option**
- Available File Formats: .OVA or .ISO
- OS: CentOS 6
- 1 vCPU
- 3 GB vRAM
- 30 GB Disk Space – this is a minimum based on RDP session storage preference.

**GateKeeper Application**
- Supported Operating Systems: Windows, Solaris, Linux, AIX, HP-UX, Tru64
- 1G MHZ CPU
- 50 MB Disk Space
- 30 MB RAM
- Outbound Internet Connection (DSL - 128 kpbs is optimal)
- Inbound network access to additional servers required on requested ports
- Java-capable browser (Internet Explorer, Firefox; etc.)

**Encryption**
- Up to and including AES, Blowfish, and 3DES
Appendix 1: Case Study

Eclipsys (now Allscripts) – Managing Remote Support for Healthcare Providers

Eclipsys is a healthcare information systems provider with 14 unique software applications, over 1,500 customers and 1,000 support technicians. With customers including hospitals, clinics and other HIPAA regulated entities; Eclipsys needs to provide solutions and support that enable HIPAA compliance. Like many companies that support applications for a large client base, Eclipsys maintained several remote support solutions and a wide variety of connectivity types including modems, point-to-point networks, shared desktops and VPNs that were expensive, complex and not all secure. The range of connectivity types and support solutions were challenging to maintain and made it difficult and expensive for Eclipsys to provide consistent and detailed information to its customers about system activity during remote support sessions.

Support Connectivity Requirements

With 1.5 million potential support connections (1,500 customer x 1,000 support technicians), Eclipsys needed a scalable solution that minimized the complexity and cost of managing large numbers of connections. Eclipsys also needed solutions that enabled compliance, including unique logins for each technician/customer access point, and audit control to track and record all system access and activity.

SecureLink

In SecureLink, Eclipsys found a solution that provided the perfect combination of control, flexibility and security. SecureLink consolidated the management of all of the remote support connections between Eclipsys and its customers. Security was enhanced by making it simple for customers to define and manage Eclipsys support access using a SecureLink client installed on the customer server. And, SecureLink recorded the details of each support connection session, greatly simplifying reporting, auditing, and compliance with customer’s security requirements.