



Enterprise remote support network

whitepaper

I. Introduction – Executive Summary

Managing Remote Support in a Secure Environment

Enterprise computing environments often include dozens, even hundreds of different software applications. Each application is critical to the ongoing operation of a business unit, department or division and each may be maintained by a different software vendor. Each vendor will have multiple technicians providing support depending on geography, time of day, product expertise, account knowledge, or availability.

Remote support for the typical enterprise involves a wide variety of connection types – modems, VPNs, desktop sharing, point-to-point networks, and more. In addition to raw connectivity, vendors need diagnostic tools and utilities specific to their application in order to quickly repair application problems. The enterprise CIO is faced with a tremendous amount of complexity in dealing with large numbers of applications, different types of network connections, different support tools and functions, and hundreds or thousands of remote 3rd party users needing access to enterprise systems for support.

For organizations in healthcare, financial services, government and other heavily regulated industries, this remote vendor support clutter is a security and compliance nightmare. Concerns over data privacy have created a class of business 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, strictly controlled system access with detailed auditing is an absolute requirement for remote support.

The Challenge

Economics and efficiency drive the requirements to provide remote support. The challenge for the enterprise CIO is to enable secure remote support in a way that is simple to implement and manage, and that can scale as the number of applications and remote support connections grow. There are no easy solutions – a permanent onsite support technician is prohibitively expensive, and setting up network access on a case-by-case basis in response to system outages would create unacceptable resolution times. Supporting a large number of applications, network connections and remote technicians in a haphazard (non-standardized) manner creates a complexity management challenge and makes the remote support environment impossible to scale. Worse, it severely compromises any attempts to implement a workable security policy. Audit and reporting become ad hoc application add-ons at best, or, in many cases, security audit for remote support is completely absent.

Security in a regulated 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 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 application. For the enterprise CIO in this situation, managing security is difficult and implementing an efficient overall process for meeting security obligations is nearly impossible.

The Solution

The solution to the problem is to standardize remote support access with a system that allows an enterprise CIO to easily manage the variety and number of remote support connections needed to keep applications up and running and the business operating effectively. Standardization also enables a uniform security policy for remote support access. The characteristics of such a solution include:

- **Complexity management** – Support a wide variety of applications and vendors without adding management overhead
- **Security** – Enable strictly defined and controlled system access for remote support
- **Audit** - Provide simple and detailed auditing and reporting of all system activity
- **Flexibility and scalability** – Add vendors, users, and applications easily and offer the tools required to effectively perform remote support
- **Ease of Use** – Reduce IT staff resources required for providing and supporting remote access

II. SecureLink Enterprise – Secure Managed Access for Remote Support

SecureLink Enterprise 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.

SecureLink – A Single Secure Platform

Platform Consolidation Reduces Complexity and Simplifies Security

The solution to meeting the challenges of remote application support involves a synergy – reducing the complexity of remote connection management provides benefits to both the organization and its vendors. By unifying remote, 3rd party connectivity, time and effort of managing secure network access is reduced for both the organization and the software vendor.

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, vendors and connection types, auditing and reporting functions can be handled with a single interface. Security process can be defined for all connections instead of application by application (or connection by connection).

III. SecureLink Architecture

SecureLink is made up of two main components: SecureLink Server and SecureLink Gatekeeper. The SecureLink Server provides a single point of control for identifying vendors, connections specific to the vendor, and the groups of support technicians allowed to access those connections. SecureLink Gatekeepers reside on application servers in the enterprise and define access rules for remote support connections (when, which systems, and what activities can be performed by the 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 Server

The SecureLink server manages all remote support connections, and provides administrative functions to create technician accounts (users) and user groups, vendors and Gatekeepers. SecureLink utilizes encrypted SSH tunneling and proprietary port-forwarding technology to broker secure, audited remote connectivity. SecureLink Server operates on a dedicated system located within the enterprise secure network – not a hosted server in the cloud. Login access to the SecureLink Server is only available to authorized vendor support personnel authenticated to the enterprise network.

Administration

SecureLink administrators can create user accounts, user groups, and Gatekeeper groups. IT staff (standard user account) can add vendors and Gatekeepers and determine to which group a Gatekeeper is assigned.

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

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

IT staff can easily identify vendors and associated Gatekeepers, keep track of live remote connection sessions, and review report detail from previous (and ongoing sessions).

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 an application server enables a set of default services that provide most of what a software vendor will need to remotely support applications. These services include:

- **FTP Services** – 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.
- **Power Prompt** – The remote command shell interface provides the support technician with the ability to access a command prompt for supporting Windows, Unix and Linux based systems.

SecureLink also provides support for proprietary tools, such as database clients, debuggers and other applications, allowing support technicians to use their favorite tools to provide quick problem resolution. Services can be added or deleted and temporarily enabled or disabled.

SecureLink Gatekeeper

The Gatekeeper is client software that resides on an application server and controls all access to systems and services available during remote support connections. The Gatekeeper includes a browser-based interface that allows enterprise IT staff to identify the host system, privileges, connectivity settings and security settings governing the software vendor's access. 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 machines proxy settings. The Gatekeeper will detect and use the most efficient available port to access the Internet.

The Gatekeeper is available for native installation on servers running Windows, Linux, Solaris, AIX, HP-UX and other operating systems.

The Gatekeeper’s Windows installer can be launched and installed with 2-clicks. The Gatekeeper will go through a short connectivity test to insure 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 IT staff or a SecureLink administrator. The registration code is generated by the SecureLink server and uniquely identifies 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 the Gatekeeper and the technician. The Gatekeeper then forwards its available ports to the technician’s desktop.

Authentication

Each individual technician must be authenticated for each connection with SecureLink Enterprise’s unique two-factor authentication methodology. Each application is associated with one or more vendors who are authorized to access it. Within the individual profile for each vendor, one or more authorized e-mail domains are identified. For example, xyz software company may use the domain xyzsoft.com. Each technician is assigned an individual account that must use this approved domain. System administrators have the ability to modify this approved domain or add an additional authorized domain for this vendor, while a standard user may only have the ability to add a user account for an individual technician. Typical distribution list domains, such as “support@” or “info@” can be automatically forbidden from use.

After providing their individual login (always their individual e-mail address) and password, the SecureLink server automatically e-mails a session access key to the e-mail address for that individual user. This second factor of authentication ensures the technician is still employed by the vendor, since a typical policy is to immediately remove a terminated employee from corporate e-mail access.

Access Restriction

Any connection to the application server from the SecureLink server must approved by the IT staff (through the enabling of the Gatekeeper). IT staff have a great deal of flexibility and control to define the rules governing the Gatekeeper:

- Connectivity Settings

- Gatekeeper access is either enabled or disabled. A remote connection can be made to the 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 – IT staff 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
 - IT staff can select one or more email addresses to receive notifications whenever a connection is made through the Gatekeeper. These notifications include pertinent details about that individual connection.
- Vendor Privileges
 - Each application is uniquely defined with the hosts and privileges approved for the support of that application. The Gatekeeper includes built-in services for FTP, desktop sharing and a command line utility. This list of privileges can be modified with a simple interface.
 - A single Gatekeeper can enable access to additional servers. Each host has its own unique privileges available for the support of that application.

Audit

Details of each remote connection session are recorded by SecureLink and available in both summary (by user and vendor) 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

IV. Summary

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

SecureLink Enterprise reduces 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 on a unified platform that benefits both the organization and the software vendor
- **Improved scalability** – With a common interface and consolidated information on all remote support connections, adding vendors and applications 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 vendors.
- **Reduced cost** – SecureLink replaces both the hard dollar costs of access infrastructure (modems, telephony, networking equipment) and the labor associated with managing ad hoc network connectivity.
- **Improved security** – SecureLink improves security by consolidating vendor network access on a single platform, as well as by its security features, including encryption, dual-factor authentication, granular access controls and more.
- **Accountability** – All technicians are required to register and connect with an individual account (validated by their corporate e-mail) and all system activity is tied to that individual accounts, which eliminates finger pointing and confusion about who may have used an account shared among multiple technicians.
- **Compliance** – Industry regulations, such as HIPAA, PCI, CJIS, Sarbanes, etc. are all different, yet share a common theme: the organization must have a defined process for managing access to information AND an audit trail of system utilization. SecureLink meets both needs.
- **Improved service levels** – More than 70% of the total cost of enterprise software ownership is ongoing support. SecureLink helps organizations maximize the value of this investment.