

## Overview

Enexity's SecureLink Virtual Support Network enables on-demand network connectivity between secure organizations and their software vendors. SecureLink VSN is used by over 10,000 organizations including technology vendors, hospitals, banks, government agencies and others to replace modems and as an easy, secure and auditable alternative to desktop sharing and VPNs.

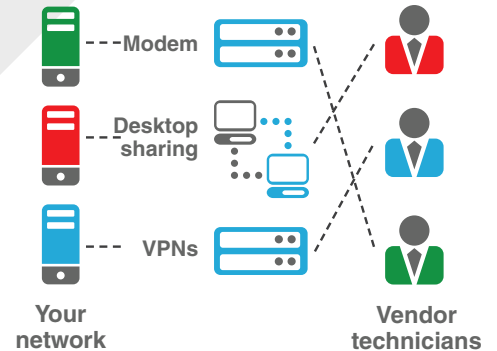
### Your challenge: Enabling remote access for your software vendors

Enterprise software applications are the backbone of business operations. Mission critical applications are complex and require frequent support and service delivered from the software vendor's support center.



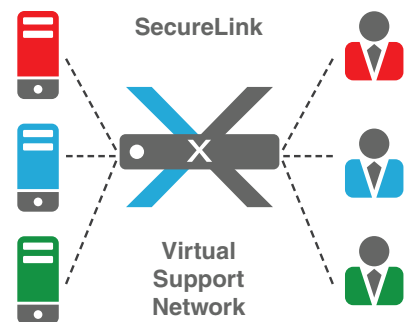
### Before – vendors access your network with modems, VPNs, desktop sharing

Traditionally, vendors dialed in with modems. Today, they are using a mix of modems, VPNs, desktop sharing and other ineffective, insecure and un-auditable methods. This burdens your IT staff, creates security vulnerabilities and violates industry regulations. Service levels and uptime suffer.



### After- Unified vendor connectivity: secure, simple and auditable

SecureLink VSN was specifically designed to address the unique challenges of enabling remote network access for your software vendors. The SecureLink Enterprise VSN server enforces the rules you set, authenticates the remote users and delivers a high definition audit trail to ensure individual accountability and compliance with industry regulations.



#### Secure.

- Dual-factor authentication
- Granular privilege control
- End-to-end encryption
- Access scheduling

#### Simple.

- Browser based
- No key fobs
- Online tutorials
- Dedicated support team

#### Auditable.

- Email connection notifications
- High definition audit trail of individual activity
- Real-time monitoring

## SecureLink Enterprise VSN - How it works

SecureLink Enterprise VSN is used by security conscious and highly regulated customers to enable remote access for their software vendors. Similar to a VPN, but designed with specialized features for the unique requirements of 3rd party network access, the SecureLink Enterprise VSN server enforces the rules you set, authenticates the remote users and delivers a high definition audit trail to ensure individual accountability and compliance with industry regulations.

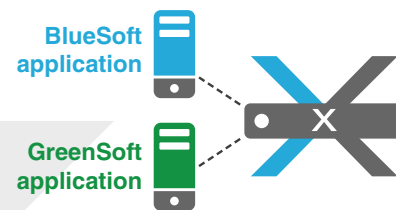
### Step 1 – Install SecureLink Enterprise VSN server

Installed in your DMZ, the SecureLink Enterprise VSN server is fully under your control.



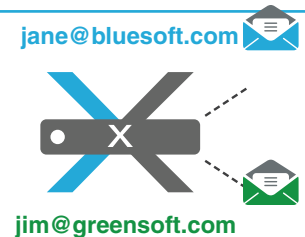
### Step 2- Install and configure application Gate-keeper software

Each application is configured with specific access rules for one or more vendors. Rules include when access is available, who can connect, what privileges are granted and more.



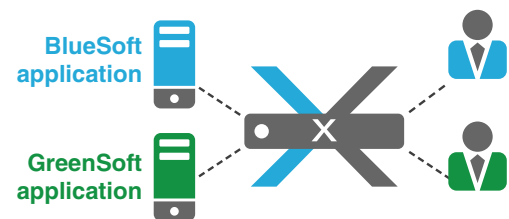
### Step 3- Support technicians authenticate

Each technician authenticates with their corporate e-mail, ex: greensoft.com. After logging in, a one-time key is e-mailed to this authorized domain.



### Step 4- Access granted, notification, rules enforced, audit

Support technicians gain access to the privileges you've granted. A notification e-mail is sent to you. All traffic is encrypted, your rules are fully enforced. Detailed audit is available in real-time.



## Technical specs

Supported platforms	Windows, Linux, Solaris, AIX, OS400, HP-UX, Tru64, Mac OSX, VMWare, Java Applet and more
SecureLink VSN server	Operating system: RedHat Linux, Fully J2EE compliant Recommended hardware: Dell PowerEdge, hosting available in our data center
Encryption	Up to and including 256 bit AES, configurable by application
Supported services	Any TCP-based service, including: SSH, telnet, RDP, desktop sharing, FTP, database, HTTP
Access Options	Access can be enabled on-demand, via a schedule or always on
Report data format & export	HTML, ODBC, syslog export

## Why SecureLink Enterprise VSN is more secure than a VPN for vendor access

Network access for your software vendors has unique requirements, including; authenticating a user that is not an employee at your organization, the ability to enable restrictive access to non-standard network services, and a requirement for a detailed audit of individual activity. SecureLink Enterprise VSN was specifically designed to address these unique needs.

**Remote, dual-factor authentication-** The support technician login is authenticated remotely using SecureLink Enterprise VSN's unique authentication methodology. When an account is created for a vendor, one or more authorized domains are associated with the account (ex: vendorname.com). Each time a technician accesses your network, they must supply an individual login and password. Once the login is verified the SecureLink Enterprise VSN server automatically e-mails a session key to the individual at this certified domain. The key must be entered to access your network and is good for a single session only. This methodology ensures that the technician is still employed by the vendor and is much more secure and simple than mailing key fobs or security tokens to the vendor.

**Individual accountability-** With a VPN account it's common for VPN credentials to be stored in the vendor's CRM system (or written on a sticky note) and shared among multiple technicians. SecureLink Enterprise VSN requires individual accounts for each technician.

**Encryption-** SecureLink sessions are encrypted from end-to-end. You may select your preferred encryption, including 128 AES, 3DES, 256 and others.

**Granular permission control-** Your vendor's technicians will only be able to access the services which you permit. Access rights are administered at the port level per machine. For example, you may only enable RDP to a single server, or may wish to enable multiple services, such as FTP, telnet, HTTP, databases on one or more servers. Different permission can be granted to each application / vendor.

**Credential privacy-** The SecureLink Gatekeeper can store network credentials (logins) for your network resources. The support technician may access these permitted network resources without ever seeing the login & password. This protection is clearly superior to having secure customer credentials stored in the vendor's CRM system or on sticky notes.

**Application grouping-** Each of your applications can be configured with unique rules for the type of access permitted, the vendors and individuals who may access the application and other controls to ensure a technician has access to everything they need and nothing they don't.

**Single session access:** If desired, access can be enabled for a single session over a distinct period of time. For example access can be enabled for just the next 4 hours.

**Access scheduling-** The SecureLink Gatekeeper can be configured to enable access via a schedule, such as Monday – Friday from 8:30 AM to 5:00 PM and Saturday from 9:00 AM to Noon.

**Connection notification-** Each application can be configured to send e-mail notifications every time a support technician connects. These notifications can include additional information, including the name of the technician, the server being accessed and relevant information about the support ticket being worked. These notifications can be sent to one or more individuals or distribution lists.

**Monitoring-** SecureLink VSN sessions can be monitored via a browser from anywhere within your network.

**High definition audit trail-** The Gatekeeper maintains a detailed audit trail of all activity at the individual user level, ensuring individual accountability. These detailed reports include services accessed, durations, files viewed or transferred and commands entered. The Gatekeeper can also be configured to store a local copy of RDP and desktop sharing sessions.

**Audit export-** The Gatekeeper audit trail can be easily exported to syslog or another local reporting repository.

## SecureLink Enterprise VSN implementation

Enexity's Customer Success Team is dedicated to ensuring a successful deployment of your SecureLink Enterprise VSN. With more than five years of successful deployments, Enexity has the experience and a proven methodology to ensure a successful rollout with minimal effort from your team.

Existing relationships with your vendors- Many of your vendors may already be using SecureLink VSN to support you and their other customers & can be quickly transitioned to your new VSN.

Professional services- Enexity offers consulting services that leverage our knowledge and experience in managing secure and compliant network connectivity for your software vendors. From a basic implementation and training to a turn-key package, our Professional Services team can help you quickly attain the benefits of your SecureLink VSN system.

Examples of services offered:

- ▶ **Audit of current vendor access platforms-** This service identifies how each of your software vendors connects to your network, including modems, desktop sharing and other backdoors that should be closed immediately.
- ▶ **Network access control for your vendors-** Enexity can help configure each application with the appropriate access privileges per vendor. This service ensures that the vendor's technicians have access to everything they need and nothing they don't.
- ▶ **Reporting & audit integration-** SecureLink VSN's audit information can be delivered into customized reports and/or exported into your own reporting structure.
- ▶ **Employee remote access services-** This service can determine what products & methods your employees may be using to access their PC from a remote location. SecureLink Enterprise VSN can also be used as a secure and cost effective alternative to GoToMyPC™ or other products.

Typical SecureLink Enterprise VSN rollout:

- ▶ Establish contacts & agree on measurable project goals & timelines
- ▶ Review existing software vendor connectivity & requirements
- ▶ Train system administrators
- ▶ Enexity develops messaging for introduction to vendors
- ▶ Deploy application Gatekeepers and vendor profiles
- ▶ Full launch, including Enexity hosted webinars & phone calls with key vendors
- ▶ Measure progress versus plan, modify deployment strategy as necessary
- ▶ Upon completion of deployment transition to Enexity support and ongoing account management

*“Our vendors have been quick to accept and utilize SecureLink Enterprise. Even our most inflexible vendors recognize SecureLink as a far superior solution to their entrenched and outdated support methodologies.”*

- Kay Warner  
Computer Security Officer  
Medical Center Hospital

## SecureLink Enterprise VSN Frequently Asked Questions

### Q: What is the SecureLink Enterprise VSN & how does it work?

A: SecureLink VSN is a Virtual Support Network solution made by Enexity. SecureLink Enterprise VSN is specifically designed to help security conscious and highly regulated customers manage software vendor and other 3rd party access to their secure networks.

### Q: How does using SecureLink VSN benefit me?

A: SecureLink Enterprise VSN helps you get issues solved faster, without sacrificing security or compliance. Over 70% of the total cost of enterprise software ownership is the ongoing maintenance and support. SecureLink Enterprise VSN helps you maximize the value of this investment in a very secure, simple and auditable way. SecureLink Enterprise VSN also reduces strain on IT departments who may be managing VPN and site-to-site networks and eliminates modems, desktop sharing and other backdoors that create security vulnerabilities and issues with industry compliance.

### Q: Who else is using SecureLink VSN?

A: SecureLink VSN is used today by more than 10,000 highly secure and heavily regulated organizations. SecureLink has been reviewed and accepted by organizations in healthcare, financial services, government, pharmaceutical, legal, manufacturing and other secure industries.

### Q: Why is SecureLink Enterprise VSN secure?

A: SecureLink Enterprise VSN was designed from the ground up to give you a superior level of security, control and audit. SecureLink Enterprise VSN has features specifically designed to meet the unique requirements of enabling 3rd party network access, including: individual accounts for each support technician, remote dual-factor authentication, a detailed audit trail of individual user activity, manually initiated sessions or access scheduling, real-time connection notifications delivered to your e-mail, granular access controls at the host and port level, real-time reporting and monitoring from anywhere in your network and audit export to syslog or other reporting repositories.

### Q: We enable access for our vendors with our VPN. How is SecureLink VSN similar to, or better than a VPN?

A: SecureLink Enterprise VSN is similar to a VPN in that it enables remote network access. However, for enabling remote access for your software vendors and other 3rd parties, SecureLink Enterprise VSN offers additional security, control and audit with less effort and infrastructure. With a VPN account, it's typical for more than one support technician (sometimes hundreds) to share a login, making accountability and compliance impossible. While you may issue individual VPN accounts and key fobs to each individual, but these burdensome policies don't typically last when the support technicians must provide a drivers license, social security number, etc. Additionally, unless the software company provides a daily list of employees who have been hired & fired, it's impossible to be certain if an account should still be active. SecureLink Enterprise VSN authenticates the support technician with a unique, dual-factor approach that ensures security and individual accountability. SecureLink Enterprise VSN also offers unique features, such as access scheduling, connection notification delivered via e-mail, real-time monitoring and an audit trail that captures detailed activity (including files accessed, commands entered) at the individual technician level.

### Q: We use WebEx to allow our vendors to support us, how does this compare to SecureLink?

A: Desktop sharing services, like WebEx or GoToMyPC are excellent for supporting desktop applications, and are also quite useful for training purposes. SecureLink VSN includes full desktop sharing capabilities, but also includes the functionality required to support enterprise applications in high security environments. These include access to non-Windows environments, the ability to restrict access to individual ports on individual machines, access scheduling, remote authentication, connection notification, high-definition audit trails and much more.

### Q: What do I need to install on my network?

A: The SecureLink Enterprise VSN Server is typically installed in your DMZ. This server communicates with individual VSN software called Gatekeepers that control unique rules for each vendor and application.

### Q: Where do I install the Gatekeeper?

A: The Gatekeeper is typically installed on one of your servers running the software vendor's application. Depending on your use-case, we may recommend that you install more than one Gatekeeper, or a single Gatekeeper may be utilized to enable access to multiple servers. Native Gatekeepers are available for virtually any operating system.

### Q: Does the Gatekeeper put a load on my server?

A: The Gatekeeper requires an absolute minimum of memory and processor while waiting for a connection, running as a background service requiring about 3K of memory.

**Q: Will my vendors accept using SecureLink Enterprise VSN?**

A: Almost all vendors will welcome the opportunity to work with SecureLink Enterprise VSN, as it gives them rapid, native access to the services they require to perform their job. Since only a browser is required remotely, there is no need for the vendor rep to involve IT departments or drive to the office in the middle of the night to access a VPN machine. Many leading enterprise software vendors have already standardized on SecureLink VSN themselves for all customer connectivity.

**Q: What other software is required for the vendor?**

A: The vendor only needs a browser and access to their e-mail.

**Q: Who can have access to my Gatekeeper?**

A: Only the support technicians with the appropriate credentials may access your network. At the vendor's support center, each technician must log into your SecureLink Enterprise VSN with an individual login. Once the login is verified the SecureLink Enterprise VSN server automatically e-mails a session key to the individual at this certified domain. The key must be entered to access your network and is good for a single session only. This methodology ensures that the technician is still employed by the vendor and is much more secure and simple than mailing key fobs or security tokens to the vendor.

**Q: When can they have access to my network?**

A: Access can be enabled manually by you for a certain period of time (ex: turn on access for 2 hours or 2 days), can be scheduled for certain days and times (ex: Monday – Friday from 8:30 – 5:00 and Saturday from 9:00 – 12:00) or can be enabled for access any time.

**Q: What can the vendor's support technician do once connected?**

A: The Gatekeeper enforces the network access rules you set, which can be configured at the port level. For example, you may want to enable access to RDP on a Windows server, telnet on a Unix server and an Oracle database port on the database server. Enexity works with software vendors every day and will assist you in configuring the appropriate services for each application.

**Q: How will I know when one of the vendor's technicians is accessing our network?**

A: The Gatekeeper can be configured to e-mail connection notifications to one or more people. The connection notification will indicate who has connected, what server they're connected to and may also contain relevant information about the support ticket number, reason for connecting or specific issue being worked.

**Q: How will I know what's been done?**

A: The Gatekeeper maintains a detailed historical audit of all activity at the individual user level. This information is available in real-time from anywhere inside your network and can also be exported to syslog or another local reporting repository.

**Q: Is SecureLink Enterprise VSN compliant with HIPAA, GLB, PCI, FIPPS or other industry regulations?**

A: Products themselves can't be compliant with any regulation. It's the proper implementation of a product like SecureLink Enterprise VSN that achieves compliance. Each of these regulations has unique language, but all of them have the same principles: protect the privacy and security of information with well defined procedures and a detailed audit trail. SecureLink Enterprise VSN, properly utilized, fully meets the most stringent interpretation of each of these regulations, and more importantly, the purpose for which they were enacted.

**Q: How long does it take to implement SecureLink Enterprise VSN?**

A: The SecureLink Enterprise VSN Server can be deployed in about 2 hours. Full system deployment timing is dictated by the goals set by the customer. For example, some customers decide to eliminate all other forms of vendor connectivity immediately, while others decide to simply stop issuing new VPN accounts to vendors, moving them gradually to SecureLink Enterprise VSN. Enexity professional services, including on-site discovery, training & deployment can accelerate the timing of any deployment.

**Q: I have additional questions that we not addressed here. Who should I contact?**

A: Please contact Enexity online at [www.enexity.com](http://www.enexity.com) or by phone at 512-637-8700 or 866-ENEXITY.