SECURELINK

SecureLink for Government

SECURE THIRD-PARTY REMOTE ACCESS FOR GOVERNMENT ORGANIZATIONS

> “Because of strategic partnerships with industry leaders like SecureLink and their secure vendor access product, Gilbert can streamline support activities, allowing IT staff to focus more time on the issues that matter. The payoff is better vendor access management and improved services for our customers and citizens.”
>
> –Mary Goodman, Deputy Town Manager for the Town of Gilbert

With SecureLink, state and local government agencies and law enforcement departments can securely provide remote access for their third parties. At the same time, organizations can decrease the amount of time spent managing vendor access and accounts while demonstrating compliance to regulations or other security requirements.

Individually identify the third parties accessing your network.

Know exactly what vendor and vendor rep is accessing your network, when, and why. Using a vendor management platform that is designed specifically to manage your vendors identities and their access increases your team’s operational efficiency and decreases the time spent managing and troubleshooting vendor access.

SecureLink ROI

For an average city or county, we’ve seen:

A **50% reduction** in time spent creating and tracking vendor accounts..

A **90% reduction in time** in time spent managing, support and troubleshooting vendor access.

An **implementation** time of under **60 days.**

Control exactly what and when your third parties can access your network.

With access schedules, approval workflows, and connection notifications you have control down to the port and host level. By adding a level of security with masked credentials, you will have a greater peace of mind knowing that your network usernames and passwords can’t be stolen or phished because vendors do not have access to them.

Gain complete visibility into all of your third party access with audit of all activity via video recordings, as well as keystroke logs. Easily demonstrate compliance to your relevant regulations such as CJIS, HIPAA, PCI, or meet security best practices from NIST or ISO 2700.

Key product features to increase the security of your third-party remote access and the efficiency of managing that access

Credential vault for privileged network credentials

- Ensure vendors never know network usernames or passwords, and therefore cannot leap-frog into other areas of your network, or accidentally compromise those credentials via phishing attacks.
- Use either SecureLink's built-in credential vault to store credentials, or integrate with your existing PAM solution.

Access schedules, or disabled-by-default access, with approval workflows

- Control when vendors can access systems via a schedule, allow access any time, or require approval for each unique session access on a vendor-by-vendor basis.
- Receive notifications when a vendor connects as well a summary of access activity when a session ends.

Remove generic and shared accounts

- Creating individual user accounts is streamlined and simple to manage on an ongoing basis.
- Automatic deprovisioning of accounts after a defined time period or of inactivity.

Full audit of all activity, including HD video recordings

- Audit all vendor activity on your network for RDP, SSH, Telnet, and any other TCP- or UDP-based protocols.
- View HD video recordings and/or keystroke logs, services accessed, files transferred, commands performed, and time stamps.

Self-registration for large vendors

- Simplify vendor account management processes by removing vendors from your corporate directory.
- Save valuable time by delegating vendor rep account creation to the vendors. Now just simply approve or deny the request of new accounts when they are submitted.

Decentralized approvals for application owners

- Allow your business application owners to approve vendor access, receive access notifications, and view their vendor's audit trail.
- Allow new vendor account creation requests to be submitted by the application owner.

Demonstrate compliance or security requirements to auditors around vendor activity

- Easily share the documentation on vendor approval workflows, restrictions, and past activity that external audits for CJIS, HIPAA, PCI, and other mandates.
- Ensure compliance with built-in security and compliance checklists and any necessary workflows or access rules.

Multi-factor authentication

- Deploy multi-factor authentication for all individual vendor reps via any time-based one-time (TOTP) authenticator.
- Verify current employment at the vendor company of the individual vendor rep that's requesting network access.

SecureLink's All-In-One Offering for Government

Tailored, configured product specifically for government organizations

To ensure you're adhering to all necessary regulations, like CJIS, HIPAA, or PCI, the SecureLink product is configured to meet these regulations with in-product security checklists.

Full implementation

Tailored implementation services specifically for government agencies includes product configurations and workflow customizations with a dedicated implementation project manager.

Training and support

In-person and online training courses within SecureLink University, as well as unlimited phone and email support.

Vendor onboarding

Help with onboarding all third parties, including any training or connectivity testing as needed.

Managed appliance

SecureLink managed appliance, including unlimited upgrades and patches, OS management, and performance and security monitoring comes with the life of your subscription.

How governments typically buy SecureLink:

Most Governments choose

To purchase SecureLink through their preferred value-added reseller (VAR) rather than directly, and we can go through most state contracts via that route. We have worked with many common resellers, such as:

SHI · CDWG · Insight · Presidio

Dell · SoftChoice

We will need

To know your preferred VAR and their contact information

Be prepared

And plan for a legal review of terms in the purchasing process, as you will still need to sign SecureLink's terms and conditions, even when purchasing through your VAR.

Governments that trust SecureLink

About SecureLink

SecureLink is the leader in managing secure vendor privileged access and remote support for both highly regulated enterprise organizations and technology vendors. More than 30,000 organizations across multiple industries including healthcare, financial services, legal, gaming, and retail rely on SecureLink’s secure, purpose-built platform. SecureLink is headquartered in Austin, Texas.

securelink.com | 888.897.4498 | contact@securelink.com