

# Access to Customers with SecureLink's Customer Connect

In today's environment of near constant cyber attacks, threats from every side, and most companies having already experienced a third-party data breach, organizations are wary of the risk their vendors and third-parties can introduce. Gone are the days of relying solely on trust and reputation; they are now requiring the highest levels of security from their partners, especially when it comes to remote access to their critical assets.

Only SecureLink's Customer Connect meets - and even exceeds - these high security standards. It both meets the remote access requirements of technology vendors and partners to provide innovative support and services, and provides their customers with the control and visibility they demand.

## What control and visibility over access do customers have?



### ELIMINATE THE RISKS OF SHARED, PRIVILEGED CREDENTIALS

Privileged credentials are stored, obfuscated and passed directly into sessions, with options to:

- Manage credentials in the customer's own PAM solution
- Have customer-managed credentials on their side in their Gatekeeper
- Manage credentials at the administrator level in the Customer Connect vault



### IMPLEMENT ACCESS CONTROLS

Customers maintain control over when and what users can access, with options to:

- Define access per application, down to the specific host and port
- Turn access on or off at any point
- Implement granular access controls, including access approvals workflows, access schedules, and just-in-time access.



### MONITOR SESSION ACTIVITY

Customers gain total visibility into access, with options to:

- Receive notifications upon connection, as well as upon disconnection, with an included summary of activity
- Review detailed audits of all activity, with contextual information such as: individual user, start and end time, services accessed, reasons for access, who approved access and stored credentials utilized
- View complete text audit log for text-based services
- Watch HD videos of activity for graphical protocols

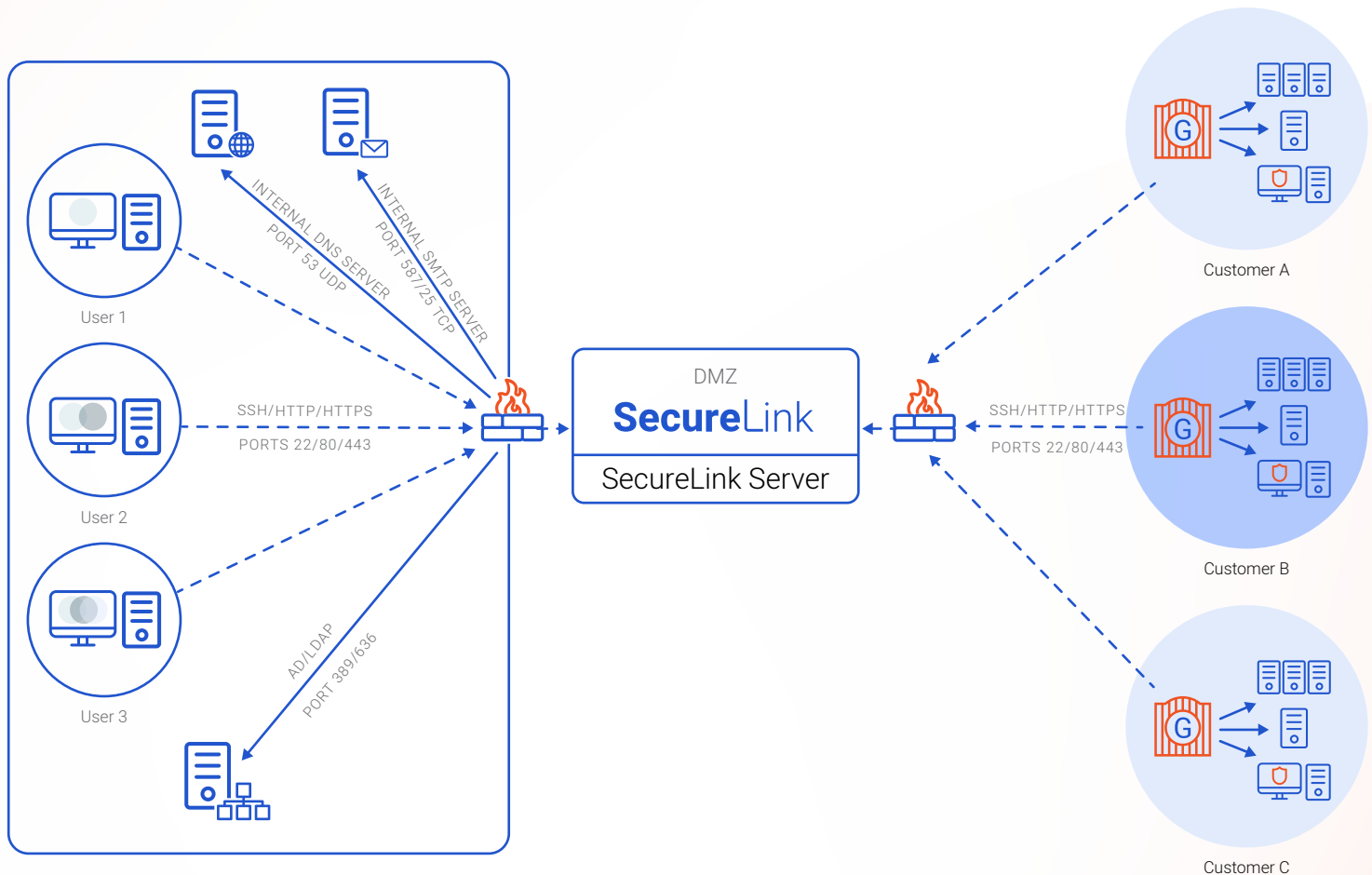


### SECURE, ENTERPRISE-GRADE, AND COMPLIANT ACCESS:

How Customer Connect facilitates this connectivity is highly secure, with:

- Outbound connections only to the Customer Connect server, with no required firewall changes
- Minimum encryption level of 128-bit AES, with options for 192-bit AES and 256-bit AES
- Users are never a node on the network
- Meets the compliance requirements of the most regulated industries, including HIPAA, CJIS, PCI and NIST

## SecureLink Customer Connect Architecture



Over **14,000** organizations utilizing SecureLink for secure access

Reduces time spent establishing connections to customers by **75% on average**

Includes dedicated SecureLink team to directly help customers with training and support

Customers are demanding higher levels of security, visibility and control from their third parties' access. With Customer Connect, technology vendors and partners can meet the requirements of their strictest customers to achieve security, standardization, and efficiency—no compromises.

For more information on **Customer Connect**, contact our team.