



## Alpine Secure Remote Solutions

At Alpine Access, we know your brand is the most important asset you own. Security breaches of sensitive customer data can cost tens of thousands of dollars and quickly harm your reputation. Alpine Secure Remote Solutions provide the ultimate in data protection and were specifically developed to address the needs of securing a home-based workforce. Our solution gives Customer Care Professionals (CCPs) secure access to the resources, applications and tools they need. At the same time you have peace-of-mind knowing your customer information is safer than in a traditional center.

### OUR SECURITY MAKES THE DIFFERENCE

- :: Uncompromising security helps you preserve customer goodwill and protect your brand.
- :: PCI Level 1 compliance gives you and your customers confidence that their sensitive data is protected.
- :: Increased security and risk reduction with granular access control and industry-leading desktop security

### SECURE, SCALABLE AND INTEGRATED

Alpine Access' security approach is straightforward: start with a secure client environment, extend this environment to our hardened collocation facilities and deliver it to our CCP's desktop using best-in-class operational practices and technology to preserve customer privacy. Limited access is granted on a need-to-know basis with dual-factor authentication and state-of-the-art encryption. Connectivity is established via a secure SSL VPN tunnel and a standard web browser. This solution is complemented with secure, enterprise-class configuration and monitoring tools. Our integrated solution seamlessly supports your existing network and security infrastructure with flexible administrative controls. These controls support and enforce a wide variety of security policies and hierarchical groupings, enabling the highest quality, most secure, lowest cost and completely scalable security solution.

### PCI LEVEL 1 COMPLIANT

Alpine Access solutions utilize dual-factor authentication complying with Payment Card Industry Data Security Standards (PCI DSS) for home-based CCPs across America. As a Level 1 compliant service provider, Alpine Access has controls and procedures in place to protect customer privacy and reduce the risk of security breaches in accordance with the 12 requirements put forth by the PCI DSS. This standard requires Alpine Access to secure thousands of home-office locations along with its entire corporate network and data infrastructure. Additionally, we are audited by a third party who also performs quarterly network scans.

# Alpine Secure Remote Solutions



Rest easy with the highest levels of security available. Our security solutions are best-in-class, easy to use, integrated and fully scalable.

## STRONG, COMPREHENSIVE SECURITY

The Alpine Access solution delivers outstanding performance, scalability and availability. Our granular policy management, ease-of-use and desktop security ensure high productivity for our home-based CCPs while maintaining the highest levels of security for you and your customers.

### Desktop protection

- > Risk reduction with strong desktop security
- > Desktop integrity validation detects the presence of required processes (e.g. virus scan, personal firewalls, OS patch levels, registry settings, etc.) and the absence of other processes (malware, spyware, etc.) before allowing full network access
- > Automatically disable CCP machine if unauthorized changes occur
- > CCPs run authorized apps only
- > Lock down PCs by granting or denying access to host PC devices such as printers, USB memory keys, or DVD/CD/floppy drives
- > Desktop trust management
- > Disable copy/paste
- > Monitor all active processes
- > Active monitoring of CCP machines for changes
- > Disable save files to anywhere
- > BIOS password protected
- > BIOS password change monitored
- > Complex admin passwords
- > Security Account Manager (SAM) monitored
- > User profile monitored
- > Users have non-admin account
- > No changes to security settings allowed
- > Active, password protected screen saver

### Connectivity protection

- > Rules-based network access enables desktop compliance by identifying and quarantining expired, unauthorized or out-of-date environments
- > Disable access to external storage and non-authorized network locations
- > Secure SSL VPN tunnel
- > Disable IR Ports
- > Disable wireless
- > Disable COM and LPT ports
- > Disable LANMAN hashes

### Application protection

- > Flexible desktop lockdown tightens security policies while simultaneously giving CCPs the freedom to be productive
- > Secure and easy-to-use access to client applications (email, web portals, network file services, terminal services, CRM, etc.)
- > Restrict internet access to authorized websites only
- > Dual-factor authentication
- > Dynamic policy-based access with granular control over network and application resources
- > Secure business and worker continuity



For more information call Alpine Access

866.279.0585 | 303.279.0585  
www.alpineaccess.com

