

# The IDshield™ SecureAccess Difference

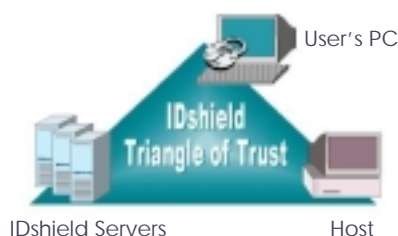
■ ■ ■ ■ ■ Authenticating Business

*IDshield™ SecureAccess guarantees that only those users that have been approved and registered by an enterprise gain access to applications located on that internal network. The patented IDshield technology employs strong two-factor authentication to uniquely identify each user through the combination of user ID, password and “trusted” computer by its hardware components.*

Software-based SecureAccess is transparent to the end-user and requires no additional hardware tokens or readers. Because of the integration of factors, possession of user ID, password and the user’s computer would be necessary to compromise the system. IDshield SecureAccess helps businesses secure their greatest assets, providing transparent enterprise-wide, strong two-factor authentication for internal and remote employees (VPNs), contractors, partners, and customers.

## IDshield Authentication:

1. At initial registration, the client Authentication Agent (AA) is installed on the user’s computer. AA creates a unique digital fingerprint from the user’s computer hardware components and sends to IDshield Servers.
2. Each time a user needs to authenticate, the AA generates unique authentication data from user password-hardware information that is then encrypted and sent to IDshield Servers.
3. The IDshield Servers authenticate the user and generate a unique number which is sent to the user’s computer and then sent from the user’s computer to the host.
4. The host contacts IDshield Servers and verifies the unique number completing an authentication “triangle of trust.” The unique number may be verified as needed — before access or throughout the respective session — continuing dialog between all three systems: AA, host, and IDshield servers.



## IDshield SecureAccess

IDshield SecureAccess assures only “trusted” users and computers gain access to critical internal information and that this interchange occurs with only authenticated employees, contractors, business partners and customers.

- ✓ Software-based solution – No extra hardware to break, misplace, or be stolen
- ✓ Easy-to-use and maintain – No learning curve / fewer help desk calls
- ✓ Low cost and easy to implement – Low cost of ownership and less labor overhead
- ✓ Superior monitoring and reporting – Complete audit trail to track use and misuse

### Advanced Uses:

- ✓ Ensure each PC is updated with latest Anti-Virus signature files
- ✓ Ensure each PC is updated with latest software patches
- ✓ Asset Management / Provisioning
- ✓ Internal chargebacks for IT resources

### External Use

Employees, Contractors, Business Partners, and Customers via VPN or Web

### Internal Use

Employees or Contractors within the Enterprise

