The GateKeeper wireless authentication system allows organizations to enhance workflow and achieve higher levels of security without inconveniencing the user.

ACCESS MANAGEMENT & REPORTING
GateKeeper Enterprise allows real-time data collection on a central server that runs on your network. This database will allow the administrator to generate detailed access logs for all computers on the network.

The centralized admin console also allows the administrator to deploy security policies such as mandatory two-factor authentication, access control lists for specific computers, and assigning user to workstations.

WIRELESS AUTHENTICATION FOR EVERY USER
GateKeeper uses a computer’s built-in Bluetooth, or a USB dongle that serves as non-intrusive authentication detectors.

Each user is provided with a GateKeeper Halberd or Smart Badge. Plus with the Trident App, users can use their smart phone as a wireless key. Wireless keys (tokens) are registered for each person on the server and serve as a unique identifier for that individual. The Tokens will be detected and used for authentication when the individual logs into their computer.
GateKeeper Enterprise: The key to centralized access management.

No other access management system provides such a wide range of features and benefits.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Feature</th>
<th>Function</th>
<th>Benefit</th>
<th>Stakeholder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of security at workstations</td>
<td>Enhanced, seamless security</td>
<td>Prevents users from leaving sensitive data open when they leave the workstation</td>
<td>Helps protect the practice from breaches and PHI exposure that could result in fines or loss of reputation</td>
<td>IT, Security Team, Owner</td>
</tr>
<tr>
<td>The organization does not meet compliance standards/policies</td>
<td>Individual authentication</td>
<td>Individual authentication</td>
<td>The organization doesn’t have to worry about being penalized in an audit for using shared passwords</td>
<td>Compliance Officer, Owner</td>
</tr>
<tr>
<td>The organization would like to increase efficiency</td>
<td>Touchless authentication</td>
<td>GateKeeper unlocks machines when a user approaches, saving time with: • overall authentication process • forgotten passwords • mistyped credentials</td>
<td>The organization has more time to devote to seeing patients, which increases revenue</td>
<td>CFO, Finance, Operators</td>
</tr>
<tr>
<td>The company wants more information about how employees spend their days</td>
<td>Business Intelligence Reporting</td>
<td>The company can make profit-enhancing decisions using the time and motion data gained from using GateKeeper</td>
<td>The organization has more time to devote to seeing patients, which increases revenue</td>
<td>Operations, Administration, Employees</td>
</tr>
</tbody>
</table>

FEATURES & BENEFITS

- Automatic lock (100% Security).
- Fast login with optional 2-Factor Authentication.
- Regulatory compliance (e.g. HIPAA, HITECH, CJIS).
- Centralized credentials management.
- Richly detailed audit logs for workplace optimization and security audits.
- Web-browser based user interface.

CENTRALIZED MANAGEMENT

- Many-to-many matching of GateKeepers to computers.
- Group computers/users according to access control needs.
- Revoke/Delete GateKeeper credentials from the server admin console.

AUDIT LOGS FULL OF RICH DATA

- Powerful analytics to measure efficiency and time secured.
- Detailed access logs from each GateKeeper-enabled computer.
- Identify users even on shared computers.
- Filter data based on GateKeeper credentials, computers, and activity.

SPECIFICATIONS

- Client Software supports Windows devices with Win 7, 8, 8.1 & 10, and Mac OSX version 10.13 or above.
- Enterprise Hub requirements: Windows Server 2012 & SQL Database
- Adjustable range from inches to 30 feet.
- State-of-the-art AES256 encryption to secure credentials.
- Regulatory compliance (e.g. HIPAA, GDPR, DFARS, CJIS, NIST).