Core expertise, tireless paranoia.
Security is of paramount importance. Avalara understands this from the top of the organization. The CEO and COO previously held high-level management positions at Check Point Software Technologies, the worldwide leader in securing the Internet. We know that in a service environment, where Avalara is hosting your business information, your data must never be compromised. From its inception, the AvaTax ST service was designed with this in mind. Our internal development team worked in conjunction with experienced security consultants to architect and build a world-class, secure network service implementation. Ongoing, we actively review our systems and procedures, enlisting the efforts of penetration assessment and auditing firms. In addition, we have an advisory group that contains security experts who have worked in major security organizations like Check Point, Cisco and Watchguard. In short, the Avalara design team has extensive enterprise-level experience, and approaches data security with tireless paranoia.

Macro-view security highlights.
Avalara’s approach to security includes the following:
• Experienced, professional design, implementation and on-going maintenance
• Industry-leading technologies deployed in multi-layered architecture with overlapping checks and correlation algorithms
• Ongoing assessment and deployment of new, proven security technologies
• Monitoring and evaluation of emerging Internet security developments and threats
• Redundancy at all points within the infrastructure, increasing both security and reliability

Physical security.
The stability and security of AvaTax ST is far greater than that of the Internet, your client’s computer systems, or any specific location. Our datacenters are co-located in carrier-class networking facilities that provide 24-hour security, photo and biometric ID, redundant power and HVAC, and other services needed to ensure that our systems are up 24x7.

Data encryption.
All communications between your systems and the AvaTax ST service use the strongest encryption available, including 128-bit VeriSign SSL and 1024-bit RSA public keys. Our service will not respond without first instantiating this secure “pipe” and then validating identity via our User Authentication scheme.
AvaTax ST Client Authentication.
The AvaTax ST client uses a one-way hash algorithm that ensures the identity of the client and eliminates spoofing. The client ID and password are passed securely via the data encryption pipe.

User authentication.
Access to the AvaTax ST Administration Console is available through a two-step authentication process with two distinct username/password pairs. First, a user must be authenticated into the Avalara User Center. Once authenticated, the user initiates a second level login process with a new username/password combination to the AvaTax ST administration Console. The applications enforce the use of strong passwords. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Access control and defense.
AvaTax ST employees a multi-layer firewall architecture with technology from industry-leading vendors. Client access to the AvaTax ST service is controlled through a first-layer of firewalls. Access between AvaTax ST front-line web services and historical data stores is controlled through a second-layer of defense with another layer of firewalls. Additionally, users can never directly access any resources behind the second-layer — all requests are managed by application logic and security from the first-layer. In addition, Avalara actively monitors log and traffic activity looking for active security threats.

Attack detection and monitoring.
To monitor potential threats inside the first-layer defense, Avalara uses intrusion detection systems (IDS) from leading vendors. IDS technology offers sophisticated threat-correlation detection to detect and protect against the sneakiest, most stealthy and advanced, security risks.

Application security.
The Avalara ST system software was designed with independent, discrete components with minimal, clearly defined points of interaction. This design eliminates common vulnerabilities and protects against the most sophisticated exploits. In addition, authenticated users in the ST service only have access to their data — access to other customers is not possible.

Systems and internal network security.
Operating system and Database security has been designed following industry Best Practice guidelines for security hardening. Internal networking uses Network Address Translation, Port Redirection, non-routable IP addressing schemes, IP masquerading and more for additional safeguards.

Data Security — The algorithm for creating user account passwords can only be used one time ensuring that data is only accessed by that authorized users. Avalara employees do not have the ability to access customer information directly via servers or

We’re the strongest link in your chain.
The Avalara co-location sits directly on a trunk line, the fastest possible Internet conduit. Regardless of traffic volume, the speed of data interaction between your accounting system and AvaTax ST is limited only by the speed of your computer and Internet connection — not AvaTax ST.
How AvaTax ST Works:

**A:** When a new invoice is created, the AvaTax ST Client (a small file which runs in the background of your accounting system) connects to the AvaTax ST service farm via SSL. AvaTax ST checks the customer’s address against Avalara’s US Postal Service certified (CASS) address database (updated weekly) and corrects any errors in the address, automatically puts the address into correct format including zip + 4, and verifies that it is indeed a deliverable address. This is called Address Validation, and it is the key to correct identification of the customer’s tax jurisdiction.

**B:** SSL encryption passes your ID and key securely to the AvaTax ST service farm ensuring your identity and protecting your real-time validation and calculation transactions.

**C:** Historical transaction data is then moved to the AvaTax ST reporting database that resides behind another layer of firewall security. Your data and surrounding transactions are stored layers away from hackers.

**D:** Security tools continually watch for intrusion attempts, actively blocking intruders from reaching critical services or data.

**E:** Within Avalara’s service farm and datastore, data is continually backed up locally, as well as off-site, following industry standards for best-practice. Complete disaster control and recovery procedures ensure 7/24/365 protection and uptime.