

WatchGuard® SSL



Top 10 reasons why WatchGuard® SSL is the smart choice for hassle-free, universal access

When users need to securely connect to the network in order to stay productive, it no longer matters where they are. All that matters is that your infrastructure includes a solution that makes dependable, secure, universal access possible. That solution is the WatchGuard® SSL 500 and SSL 1000, the hassle-free way to extend your network's reach without compromising security. It's the smart choice for businesses that need to provide connectivity to applications and corporate resources for workers on the go, no matter where their work takes them. Here are the top ten reasons why WatchGuard SSL is the right choice for your business.

1. Broadest platform and device support

WatchGuard SSL allows users to connect from more platforms and mobile devices than any other product in its class, providing unsurpassed flexibility and convenience to your mobile workforce. WatchGuard SSL supports all standard browsers, ActiveX, Java, Linux, Mac OSX, Microsoft AirSync, PalmOS, SonyEricsson T68, UNIX, WAP phones, and Windows CE.

2. Access to the widest range of applications and resources

You can provide your remote users with anytime, anywhere access to applications and resources to maximize productivity when they are away from the office. WatchGuard SSL offers client and clientless access for broad device and platform support, and you have the ability to publish applications for users in "kiosk mode" or create tunnels, so they can have an in-office experience no matter where they are.

3. Strong endpoint security

WatchGuard SSL makes it possible to provide remote access to critical resources without compromising the network. It provides robust security from end users to the network, for managed and unmanaged devices. Endpoint health and compliance status is verified before allowing network access by checking device attributes including IP address, firewall settings, OS, patch level, and status of anti-virus software. Client software keeps track of all activities and wipes everything clean when session ends, while session timeout protects corporate information from unauthorized users.

4. Centralized policy management

IT administrators can manage user and group access from a single centralized location across multiple SSL appliances, with integrated logging and reporting. From this centralized management console they can define how incoming and outgoing requests are to be handled, assign granular policies to determine which users and groups have access to specific resources and applications, and control which devices gain network access through built-in endpoint security checks.

5. Flexible network authentication options

WatchGuard SSL offers the most comprehensive set of options for integrating and leveraging an enterprise's existing authentication mechanisms including LDAP, Microsoft Active Directory, RADIUS, IBM RACF, two-factor solutions such as RSA and VASCO, and many others. In addition, SMS and software-based two-factor authentication and federated identity are supported.

6. Single sign-on

WatchGuard SSL includes single sign-on, which allows users to seamlessly access information without having to repeatedly authenticate. This makes remote access a breeze for the end user while reducing help desk issues on the back end.

7. Federated identity

Federated identity allows a single digital identity to be used to access multiple departments or even businesses, without the need for extra, costly user enrollment. Ideal for sharing identities in B2B partnerships.

8. High availability and scalability

Appliances can be clustered for high availability and scalability, so your business has rock solid dependability and room to grow. Simply purchase what you need now, knowing you can easily extend access to more users as business requirements change. Because multiple appliances can be managed from one centralized location, administration remains efficient as your user count expands.

9. Lower total cost of ownership

By seamlessly integrating into your existing network environment, WatchGuard SSL leverages and extends the value of your current technology investment. Thin clients eliminate the hassle of installing client software on every device, while streamlined management minimizes administrative costs. Meanwhile, unmatched ease of use for your end users reduces user support costs and increases mobile workforce productivity.

10. Best support package in the industry

All WatchGuard's products are backed by LiveSecurity® Service, a high-value, innovative support service for IT administrators. LiveSecurity provides hardware warranty with advance hardware replacement, rapid response technical support, software updates, concise threat alerts, and ground-breaking security education resources.

To find out more about the WatchGuard SSL 500 and SSL 1000 appliances, contact your reseller today, visit www.watchguard.com, or call 1.800.734.9905.

ADDRESS: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · WEB: www.watchguard.com · U.S. SALES: 1.800.734.9905 · INTERNATIONAL SALES: +1.206.613.0895

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if-and-when available basis. © 2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66519_032608

