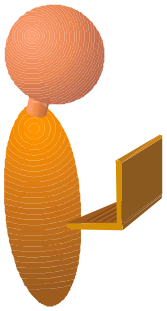

eBLVD™ Online Meetings

Security Guide

Use eBLVD Online Meetings For:

- Application Sharing
- Voice or Text Chat
- White-Boarding
- File Transfer

eBLVD enables secure, browser-based access to your PC from a remote web browser over the Internet. Data, voice, keyboard, mouse and display updates are transmitted over a highly compressed, encrypted stream, yielding "as good as there" experience over broadband and impressive performance over dial-up. eBLVD can be used for:

Application Sharing: Launch any Windows application to share and enable interactive collaboration to any size group.

Voice or Text Chat: Dialog between local and remote users during meetings or collaboration sessions.

White-Board: Draw ad-hoc diagrams and charts using the eBLVD white-board.

File Transfer: Copy and paste text, images, files, folders and directories to and/or from any eBLVD participant PC and meeting HOST.

Technologically, eBLVD is a hybrid-ASP hosted service, composed of three components:

MEETING HOST: A 500K applet is installed on the meeting HOST PC, a home or office PC with always-on Internet access. During the initial registration, the applet registers and authenticates itself with eBLVD's secure 'RELAY' service. The applet is network-aware and does not at any time require manual adjustment or intervention.

REMOTE PARTICIPANT (BROWSER PLUG-IN): Remote users are 'invited' to attend an event by the Meeting Host. The invitation can come in the form of either an email link or a temporary username and password that permits 'admission' to the meeting. In either case, the action launches a browser to eBLVD's secure Web site, which automatically loads a tiny plug-in into the browser. When the participant clicks on the "attend" button, the client sends an SSL- encrypted request to the RELAY.

RELAY: The eBLVD 'matchmaker' service that listens for connect requests and maps them to scheduled meetings on HOST PCs. When a match occurs, the RELAY determines the least-cost and safest connection route. The RELAY then connects each remote participant to the meeting host in the most efficient manner.

 Effective: 1/01/2004

Security from the Ground Up

eBLVD uses a hybrid-ASP model designed expressly to ensure robust, secure operation.

Protecting the integrity of corporate assets
Security is an essential ingredient when extending Internet-based remote access to internal and external users.

Secure Facility
All eBLVD Web, application, communication and database servers are hosted in a highly secured data center. Physical access is restricted using a combination of electronic key and palm-print authentication and monitored by video cameras around the clock.

Secure Network
eBLVD's access routers are configured to monitor denial of service (DoS) attacks and log denied connections. Multi-layer perimeter security is provided by a pair of firewalls: one between the Internet and Web applets, another between the eBLVD RELAY and backend databases. The security of this architecture has been independently confirmed by penetration tests and vulnerability assessments, conducted by an outside organization.

Secure Platform
eBLVD servers run on world-class Operating Systems with the latest security patches installed. The entire service delivery platform is certified for quality, redundancy and reliability. Servers have been penetration tested and system logs are continuously audited for suspicious activity.

Secure Administration
eBLVD servers are administered over a private link to eBLVD's Network Operations Center (NOC). Secure Shell (SSH) supports authenticated, encrypted remote sign-in access to eBLVD's NOC staff. To avoid opening ports and ensure very tight access control, an intermediate applet handles and authenticates all SSH connections.

Scalable and Reliable Infrastructure
This infrastructure is both robust and secure. Redundant routers, switches, server clusters, and backup systems are used to ensure high availability. For scalability and reliability, switches transparently distribute incoming requests among eBLVD Web servers. For optimum performance, the eBLVD RELAY load-balances client to HOST sessions across geographically distributed servers.

Protecting Customer Privacy
eBLVD understands that any enterprise outsourcing service delivery is concerned about privacy. eBLVD has a strong privacy policy that prohibits unauthorized disclosure of personal or corporate information to any third party.

Disclosure of Customer Information

In order to deliver service, eBLVD must collect certain user information, including first/last name, email address, and meeting administrator passwords. Unless expressly authorized, eBLVD will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. For example, email addresses are used only to send service update messages, with the user's express consent. Upon request, eBLVD will also enter into a formal non-disclosure agreement (NDA) with any customer.

Published Privacy Policy
eBLVD's published privacy policy identifies information gathered, how it is used, with whom it is shared and the customer's control over dissemination.

Even when eBLVD is accessed from a public PC, data left behind poses no privacy threat. eBLVD uses an optional cookie to track traffic patterns and retrieve registration information. This cookie is generated on the fly, but does not contain any personally identifiable information or passwords. Users can block this cookie, if desired. After a session ends, browser history indicates that eBLVD was accessed - but history cannot be used to access the account or any PC without a valid sign-in and password.

Access to Customer Information

eBLVD NOC staff are the only individuals with access to eBLVD servers - limited access is granted on a need-to-know basis for the express purpose of customer support.

eBLVD session logs are used by eBLVD to maintain quality of service and assist in performance analysis. eBLVD tracks domain names, browser types and MIME types for traffic management. This data is gathered in the aggregate and is never correlated with an individual user or company account.

Although eBLVD communication servers may relay traffic between client browser and HOST PC, these packets are encrypted. eBLVD cannot decipher this traffic, because it does not possess the access code used to generate encryption keys. Even if an attacker were to gain access to eBLVD's servers, individual session traffic is not recorded and live session traffic cannot be compromised.

Digitally Signed Applications

Software is installed by visiting eBLVD's Web site and launching a signed browser applet and/or executable. Companies that prefer to block or prohibit users from installing software can launch the client via a simple stand-alone installation process.

All eBLVD programs are digitally signed. eBLVD software automatically keeps itself up-to-date. However, no component is ever installed or updated without checking signatures. This prevents "Trojan horses" from masquerading as legitimate eBLVD software.

Effective: 1/01/2004

Firewall Compatibility

eBLVD is firewall friendly. It generates only HTTP/TCP traffic through ports 80 or 443. Because most firewalls are already configured to permit Web traffic over these ports, you won't have to bypass or compromise your corporate, branch office or remote firewall to implement secure remote access with eBLVD.

eBLVD is compatible with:

- Firewalls
- Routers
- Proxy Servers
- NAT/PAT
- DHCP assigned PCs
- Dual-NIC PCs

Many other web-conferencing solutions require applets to receive incoming packets at either a public IP address or by 'tunneling' via HTTP. Most enterprise firewalls (and we believe many other firewalls) will not permit streaming activity over port HTTP, or port 80. This makes eBLVD completely compatible with application proxy firewalls, dynamic IP addresses, and network/port address translation (NAT/PAT).

HOST PC Access

PCs within your network must have the eBLVD HOST applet installed and in order to be accessed remotely. The HOST applet may be turned on and off at will. Installing eBLVD requires physical access to the PC. It is not possible to remotely install or use a Trojan to "plant" the eBLVD HOST on a PC.

PCs are added by visiting eBLVD's Web site from each PC. The PC's owner must enter a valid sign-in and account password to gain access. It is not possible to reset the PC access password without supplying the sign-in and account password used to register the PC.

Protecting Confidential Data

eBLVD uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the eBLVD browser client and PC, including screen images, file transfers, copy/paste operations, keyboard/mouse input and chat text, is protected with end-to-end 128-bit SSL encryption.

Authenticated Access

Secure Service Installation
eBLVD software installation and update procedures were designed with enterprise security in mind.

eBLVD confidentiality between client applet, RELAY, and HOST builds on the strong foundation provided by authentication. Authentication verifies the identity of every party, from the eBLVD RELAY and communication applet to the browser client and PC. This is combined with access controls that ensure only authorized parties can gain access to your web conference or online meeting.

Multiple, Nested Passwords
eBLVD uses multiple, nested passwords to keep intruders away. Cryptographic techniques are used to ensure that sensitive data - sign-ins and passwords - are never sent or stored in plain text.

Password Protection
eBLVD requires that every password be at least six characters. This requirement helps to prevent accounts from being configured with easily compromised passwords.

The eBLVD RELAY authenticates itself to browser clients by supplying a digital certificate, issued by a trusted authority. Clients authenticate themselves to the eBLVD RELAY by supplying an account sign-in and password, exchanged over SSL.

Inactivity Timeouts
Users may walk away from public PCs without logging out or leave home PCs unattended. eBLVD addresses this security issue by applying inactivity timeouts. Users are automatically logged out of the eBLVD.com Web site if their SSL session is inactive for fifteen minutes

OS-Level Access Control
eBLVD leverages the OS-level access controls already in place on the corporate LAN. Simply leave the HOST PC in a screen-locked or logged-out state. When the eBLVD connects, the remote user must enter a Windows sign-in/password to access the PC and be granted file, host, and domain-level permissions associated with his or her account. In other words, the remote user does not have tunneled access to the enterprise network - he or she only has access to a single PC's desktop, and is subject to access controls already in place for that PC.

Controlled Participant Invitation Periods
Meeting Hosts invite others to access their PCs using eBLVD. By accessing the eBLVD Meeting Center, the HOST PC can issue an email invitation that expires after the meeting. The owner must supply his or her account sign-in and password to create invitations. The RELAY then sends an email message to the specified address containing a one-time access URL the guest will follow to get to eBLVD's Web site.

Access “By Permission” is Required
Once at the web site, the guest clicks on a button to download the eBLVD remote plug-in. Once the remote guest requests admission to the HOST PC, a pop-up window is displayed on the HOST PC, requiring manual authorization to complete the process.

Grant/Revoke Control or View-Only Options
Two participant access modes are supported: a view-only mode and a full-control mode. In view-only mode, the remote participant can view, but cannot initiate desktop actions or transfer files. Full-control mode offers the same access normally granted to the PC's owner. The HOST PC can of course end the eBLVD session at any time by disconnecting the guest.

Access Awareness

Whenever a client connects to a PC running the eBLVD HOST, the ‘connected participant’ icon appears on the HOST PC's system tray. This notification makes sure that the PC's owner is always aware of the eBLVD session, preventing a "lurker" from silently watching local desktop activity.

Detailed Session Logs

The eBLVD HOST PC logs additional information for each connection, such as date and time and length of connection period.

Conclusion

eBLVD's security policy is straightforward: Start with a secure hosted service and operational practices that preserve customer privacy. Complement this foundation with secure enterprise-class configuration and monitoring tools to control remote access. Protect online meetings and web conferences with multi-level authentication and state-of-the-art encryption to keep corporate traffic safe. The end result: eBLVD provides world-class, secure, and robust web conferencing services.