eBLVD enables secure, cloud-based access to a PC or server over the Internet. Data, 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 Host software: A 500K applet is installed on the Host PC – a home or office PC or server with always-on Internet access. During the initial installation, the applet stores an encrypted password locally, then registers and authenticates itself over SSL with eBLVD's secure service. The password is never stored or passed to eBLVD servers. The applet is network-aware and rarely requires manual adjustment or intervention.

eBLVD Client software: Remote users connect to an eBLVD Host PC via an SSL connection from their web browser. There is no installation procedure, and configuration is typically not needed. 2 factor authentication (2FA) is available using mobile apps that support TOTP protocol such as Google or Microsoft Authenticator. If 2FA is enabled, access to a host is checked for authorization on every connection attempt.

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

Security from the Ground Up
eBLVD uses a hybrid-ASP model designed expressly to ensure robust, secure operation.

Secure Facility
All eBLVD Web, application, communication and database servers are hosted in redundant, highly secured data centers. Physical access is restricted using a combination of electronic key and biometric authentication and monitored by human personnel around the clock.

CONTACT US care@eBLVD.com | 877.438.3258

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 private network 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 systems with the latest security patches installed. The entire service delivery platform is certified for quality, redundancy and reliability. Servers and networking apparatus are penetration tested and system logs continuously audited for suspicious activity.

Scalable and Reliable Infrastructure

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

Protecting Customer Privacy

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.

eBLVD understands that any enterprise providing business communication is concerned about privacy. eBLVD has a strong privacy policy reviewed by TrustE™ that prohibits disclosure of personal or corporate info to any third party.

CONTACT US care@eBLVD.com | 877.438.3258

Disclosure of Customer Information

In order to deliver service, eBLVD must collect certain user information, including first/last name, email address, and 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.

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 routers and servers. Login access is provided via 2-party authentication. Limited access is granted on a need-to-know basis for the 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 gateway routers may relay traffic between client browser and HOST PC, these packets are encrypted. eBLVD cannot

decipher this traffic, because it does store these packets, nor possess the access code used to generate encryption keys. In the unlikely event that an attacker were to gain access to eBLVD's servers, live session traffic could not be deciphered or compromised.

Digitally Signed Applications

Software is installed by visiting eBLVD's Web site and launching a signed browser plug-in and/or applet.

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.

eBLVD is compatible with:

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

Firewall Compatibility

eBLVD is firewall friendly. It generates only HTTP/TCP traffic through ports 80 and 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.

Many other remote access solutions require applets to receive incoming packets at a public IP address. The eBLVD applet sends an outgoing HTTPS "update" to the eBLVD system at regular intervals, checking to see if any connect requests have been received. This makes eBLVD completely compatible with application proxy firewalls, dynamic IP addresses, and network/port address translation (NAT/PAT).

CONTACT US care@eBLVD.com | 877.438.3258

HOST PC Access

PCs within your network must have the eBLVD HOST applet installed and running 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 (or reseller web site) from each PC. The PC owner can only install eBLVD using valid credentials, setup code, or encoded URL. The PC owner then assigns a second password that is encrypted only on the host itself. It is therefore not possible to reset the PC access password without reinstalling the software.

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.

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

Authenticated Access

eBLVD confidentiality between client applet and HOST builds on the strong foundation provided by authentication. Authentication verifies the identity of every party, from the eBLVD client applet to the PC to be accessed. This is combined with the local PC and network access controls that ensure only authorized parties can gain access to the HOST.

Multiple, Nested Passwords

eBLVD uses multiple, nested passwords to keep intruders away. Cryptographic techniques are used to ensure that

Password Protection
eBLVD requires that every password be a minimum number of characters. This requirement helps to prevent accounts from being configured with easily compromised passwords.

CONTACT US care@eBLVD.com | 877.438.3258

sensitive data - sign-ins and passwords - are never sent or stored in plain text.

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

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 or Domain/LAN credentials 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.

Access “By Permission” Can be Required

Once at the web site, the guest clicks on a button to download the eBLVD applet. Access is only allowed to the PC owner or via “remote guest” access. 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 remote user access modes are supported: a view-only mode and a full-control mode. In view-only mode, the remote user 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.

CONTACT US care@eBLVD.com | 877.438.3258

Access Awareness

Whenever a client connects to a PC running the eBLVD HOST, the ‘connected user’ 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 your PC resources 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 remote access services.

CONTACT US care@eBLVD.com | 877.438.3258