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.

The encrypted data transmission is forwarded only, it is never stored on the eBLVD platform.

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 the client called from their web browser. There is no installation procedure, and configuration is typically not needed. IP Access Control and 2 factor authentication (2FA) is available using mobile apps that support TOTP protocol such as Google or Microsoft Authenticator. If IP Access Control or 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.

Cloud-based Topography

eBLVD uses the Amazon Web Services (AWS) platform. AWS cloud services offers high performance IT infrastructure in the form of compute power, database storage, content delivery and other functionality .

AWS provides advanced security capabilities and services that include:

- Network firewalls built into our Virtual Private Cloud (VPC), and application firewall capabilities that allow us to create private networks with controlled access to applications across regions.

CONTACT US care@eBLVD.com | 877.438.3258

- Encryption in transit with TLS across all services
- Connectivity that enables private connections from eBLVD offices

Inherited Security
eBLVD inherits from Amazon important security characteristics for data storage, encryption, access control, archiving and others. Detailed description of underlying Amazon security concerns are well documented in Amazon whitepapers: https://aws.amazon.com/security/.

All eBLVD Data (Amazon RDS) and Snapshots reside on the AWS platform and are encrypted. We manage these encryption keys through the AWS Key Management Service (https://aws.amazon.com/kms/). AWS Data storage complies with PCI DSS, ISO, SOC and HIPAA requirements (https://aws.amazon.com/compliance/programs/).

Physical Security
eBLVD leverages the sophisticated AWS physical security infrastructure. Amazon AWS is the largest cloud provider on the market. eBLVD runs in AWS's highly secure data centers, which utilize state-of-the art electronic surveillance and multi-factor access control systems.

Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. All personnel must be screened when leaving areas that contain customer data. Environmental systems in the datacenters are designed to minimize the impact of disruptions to operations.

Data Security and Encryption
In transit
All transport channels go through the HTTPS protocol with the latest security policies of AWS (https://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-security-policy-table.html)

CONTACT US care@eBLVD.com | 877.438.3258

Note: The PCI Security Standards Council has chosen the arbitrary date of June 30, 2018 for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged).

After June 30 2018, the PCIS DSS specifies that termination points which POI/POS devices connect to that can be verified as not being susceptible to any of the known exploits (POODLE and BEAST exploits) for SSL and early versions of TLS may continue to use SSL /early TLS.

We verify that eBLVD has been patched to current specifications as to not be susceptible to any of the known exploits (POODLE and BEAST exploits) for SSL and early versions of TLS.

Thus, TLS 1.0/1.1 currently needs to be enabled on eBLVD end-user termination points for backwards compatibility of our eBLVD version 7 hosts running on XP. We have notified all customers running version 7 hosts that we will retire this version by year-end 2018. At that time we can deploy TLS 1.2 end-to-end in conjunction with our version 10 release.

Data backup and archival

Data backups are stored in Amazon S3 storage and archived in Amazon Glacier by the automatic S3 life-cycle management process (https://aws.amazon.com/s3/details/). Only the customer account, host identification and audit data is backed up – client-to-host session data is not recorded or stored.

At rest

All data residing on eBLVD regardless of location (S3 storage, RDS) are encrypted. Keys are stored and managed by AWS Key Management Service (https://aws.amazon.com/kms/ and CloudHSM (https://aws.amazon.com/cloudhsm/.

CONTACT US care@eBLVD.com | 877.438.3258

Scalability
AWS has been architected to be one of the most scalable cloud computing environments in the world today.

eBLVD cloud instances 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.

Availability
eBLVD leverages the availability of Amazon services. Amazon, in the case of EC2, EBS, and RDS claims to "use commercially reasonable efforts to make each available with a Monthly Uptime Percentage (defined below) of at least 99.95%" (https://aws.amazon.com/ec2/sla). More detailed availability statistics can be found at https://cloudharmony.com/status-1year where all services met the 99.99+ availability metric.

eBLVD operates in multiple availability zones and uses load balancing across availability zones to increase performance and availability. In case of a component failure, load balancers route traffic to other availability zones.

Monitoring
All eBLVD platform components are continuously monitored 24/7. Communication among all monitoring components is encrypted.

CONTACT US care@eBLVD.com | 877.438.3258

Customer Privacy Policy

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.

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.

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.

Digitally Signed Applications

Software is installed by visiting eBLVD's Web site and launching a signed browser 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.

CONTACT US care@eBLVD.com | 877.438.3258

Firewall Compatibility

eBLVD is firewall friendly. It generates only outbound 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.

eBLVD is compatible with:

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

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).

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

CONTACT US care@eBLVD.com | 877.438.3258

with end-to-end SSL encryption.

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

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.

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”

CONTACT US care@eBLVD.com | 877.438.3258

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.

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.

Certifications & Compliance

eBLVD, via inheritance of the Amazon AWS platform complies with the most demanding certifications, namely:

- Sarbanes-Oxley (SOX) compliance
- ISO 27001 Certification
- PCI DSS Level I Certification
- HIPAA compliant architecture
- SOC1 Audit, SOC2, SOC3
- FISMA MediumATO

For full up-to-date list of certifications and compliance audit reports see https://aws.amazon.com/compliance/.

CONTACT US care@eBLVD.com | 877.438.3258