opentext™

DATA SHEET

Exceed TurboX Security Features

Keeping all important IP related data in a central, well protected datacenter is the best practice for securing your IP. Secure remote access is key to protecting intellectual property.

- All data traffic is encrypted with latest standards encryption technology
- ETX integrates with a multitude of authentication systems
- ETX provides central management of users, sessions, and datacenter infrastructure
- Secure architecture that protects your IP

As many organizations look to consolidate data centers to reduce IT spending and increase central manageability, they also need to provide high performance, remote access to users of graphically demanding software on Linux®, Unix® and Microsoft® Windows®. This type of software, as well as other graphically demanding design and construction software, is what many organizations use to design their core products, such as semiconductors, engine parts or architecture. Organizations are looking for solutions that cover graphically demanding and standard business user desktops to enable the benefits of virtualization.

IP protection and security

A 2016 study showed that 60% of intellectual property leaks were perpetrated by negligent or malicious employees[1]. This is why many organizations in engineering, manufacturing, oil & gas exploration, scientific research, financial trading, medical imaging, architectural design, and other industries that deal with sensitive data have moved their data (and the applications that read and write that data) away from user workstations and into secure datacenters.

Remote Access Software (RAS) is a key part of the information security puzzle because it provides the sole entry point into the secure environment for users to view and edit information assets. RAS solutions must be extremely secure to ensure that data does not leave the datacenter. Exceed TurboX was developed in close partnership with customers who demand the highest possible security standards for protecting their sensitive data.

[1]https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

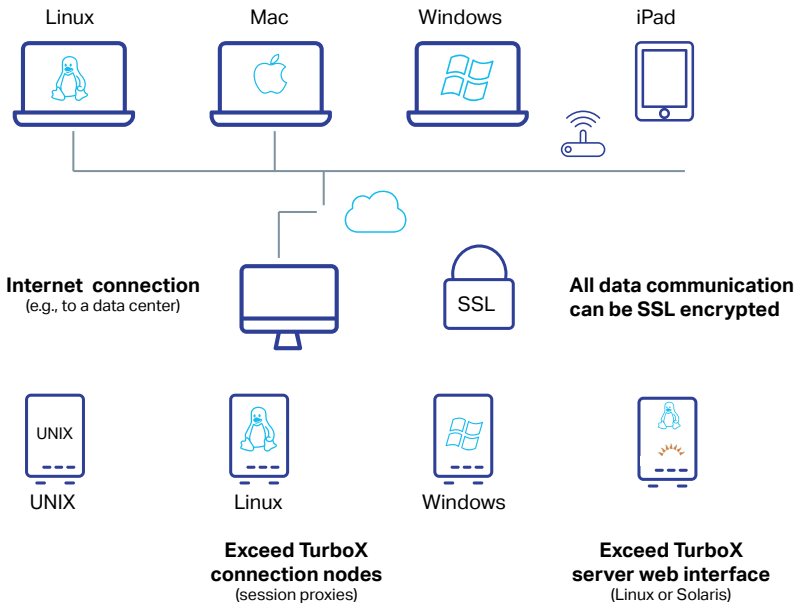
- File transfer, printing, and copy/paste features can be turned on or off based on application, user, user group, or user location (subnet).
- Clipboard contents for copy/paste operations between local and remote systems can be logged.
- File transfer and copy/paste operations can be enabled in either one or both directions.
- IT maintains complete control over user privileges, including which hosts can be accessed, which applications or scripts can be run on those hosts, and by which users or user groups.
- A single ETX Server can enforce enterprise-wide security across multiple datacenters in different geographic locations.
- With VPN or HTTP(S) proxy support, ETX provides secure access from external customer and contractor sites, eliminating the need to transfer data to third parties or transport sensitive data through airport security.
- Session windows can be blanked out in client-side screenshots, stopping users from capturing images of sensitive applications and data.

Encryption and identity verification

- All ETX connections are encrypted and server identities are verified to prevent network snooping and man-in-the-middle attacks.
- Data traffic between the client browser and the ETX web server is encrypted with TLS and supports HTTPS certificates.
- Remote sessions are encrypted with TLS 1.3; server identity is verified via certificate when sessions are established.
- Back-end connections between ETX nodes and application hosts may be encrypted with SSH.
- Back-end connections between ETX Servers, Nodes, and License Servers are TLS 1.3 encrypted.

Centralized management

- Exceed TurboX enables a small IT staff to manage thousands of application and desktop hosts across multiple regional datacenters, enabling IT to maintain control of complex computing environments.
- Email alerts notify administrators of problems with the environment, including memory or disk space issues, frozen or out of control user sessions, and other issues that may result in downtime.
- A full audit trail is provided for user logins, application and desktop launches, configuration changes, and permission changes.
- Application servers can be grouped into regions, and profiles targeting those server groups can be published to user groups in those regions, ensuring optimal network performance and creating logical separation between regions.
- Software updates installed to ETX Server are pushed out to all users and hosts, enabling quick patching of bugs and easy deployment of new security features.
- Detailed permissions can be set per-user or per-group for quick and easy management of privileges.



Authentication

ETX supports the following authentication methods:

- Lightweight Directory Access Protocol (LDAP)
- Microsoft® Active Directory® (AD)
- UNIX Pluggable Authentication Module (PAM)
- UNIX Native accounts
- OpenText Directory Services (OTDS) providing access to a multitude of authentication systems via OAuth2 and other 2FA providers
- Kerberos Single Sign On (SSO)

ETX provides Single Sign-On to Windows and UNIX hosts by securely forwarding ETX login credentials to back-end desktop and application servers. This includes forwarding Kerberos tickets from the browser to SSH hosts for end-to-end SSO support.

Other authentication features of ETX include:

- API keys for REST-based administration and launching of profiles.
- Permanent or temporary ETX account lockout to prevent password brute-force attacks, without locking domain accounts.
- Bulk-importing of users and assignment of privileges from the authentication directory.
- Detailed customization of user privileges
- The ability for new accounts to be created on successful login, or blocking of new accounts (requires manual creation by an ETX admin)

If you use a 3rd party solution for Single Sign-On or federated authentication, OpenText Directory Services (OTDS) is a free authentication server that supports 3rd party SSO, ADFS, SAML, OAuth2 and even custom authenticators. OTDS can authenticate against multiple systems simultaneously for companies that use a mix of directories and secure authentication solutions.

Secure architecture

The ETX client software does not require administrator privileges to install; any Mac, Linux, or Windows PC will be prompted to install a lightweight launcher when they log in or launch a session for the first time.

- ETX Server uses an embedded Eclipse Jetty web server, which has a small footprint and minimal surface area for potential attackers,
- ETX Server and Nodes can either be installed in a VPN, or for contractor and customer access, behind an HTTP(S) proxy or load balancer.
- The HTTP(S) proxy or load balancer can prevent direct connections to the ETX Server and Nodes by using private addresses on those hosts.
- HTTP(S) certificates and node certificates ensure that connections to back-end systems are secure.
- The ETX administration portal can be hosted on a private port which is only accessible from within the VPN or private network, ensuring that an attacker cannot gain administrative access.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: **opentext.com**.

Connect with us:

- **OpenText CEO Mark Barrenechea's blog**
- **Twitter** | **LinkedIn**

opentext.com/contact