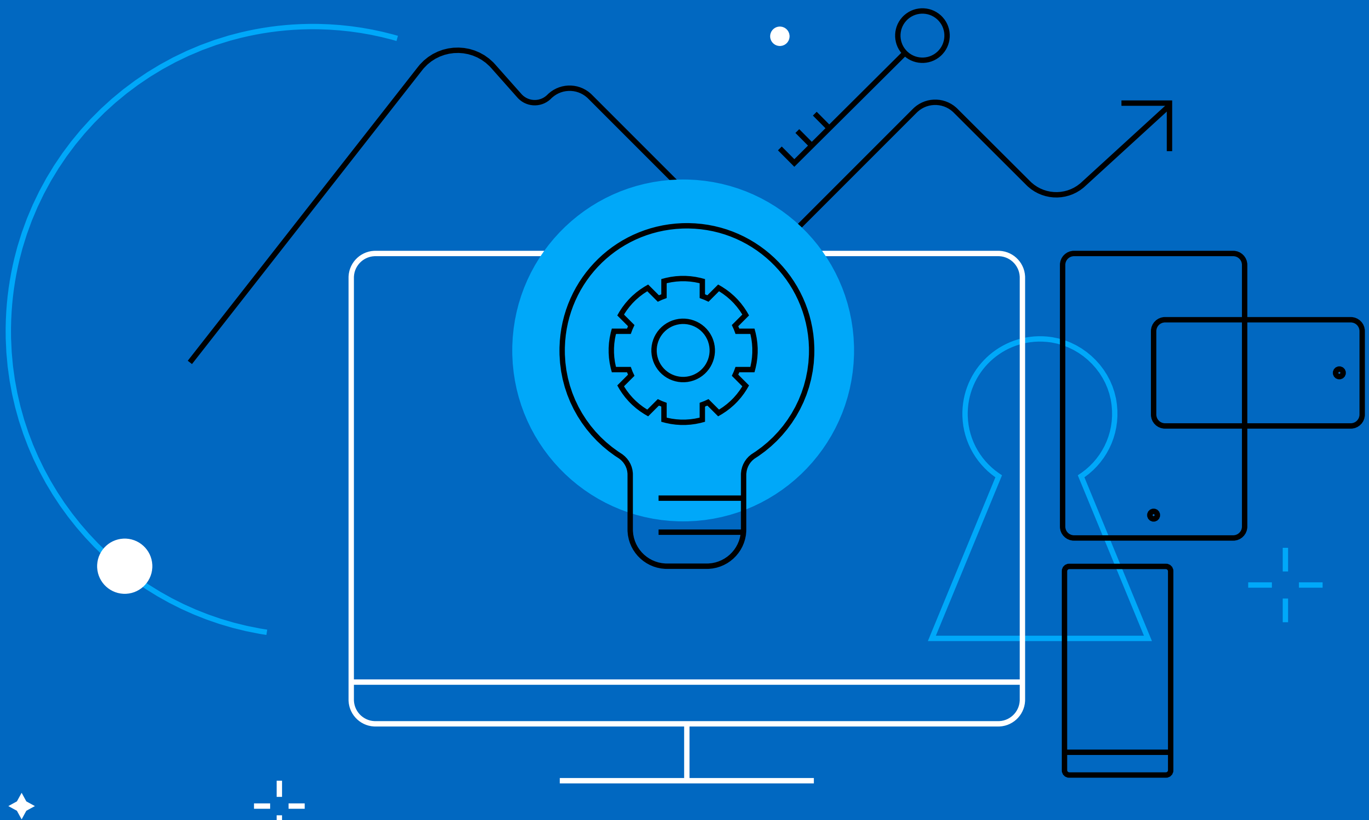
Progress



Progress OpenEdge

Protecting Applications in a Challenging Environment

WHITEPAPER

Effectively securing applications has been a matter of concern for organizations large and small for over 15 years. As the recent Gartner report, TechInsights: State of Application Security conveys, the challenge continues to escalate as hackers become increasingly savvy. From Home Depot to Sony to the 2016 US presidential campaign, the media has been amplifying the attention received by data and privacy breaches, frightening consumers, causing stringent and costly government regulations and placing security at the top of every CIO's priority list.

State of Application Security — By the Numbers

15 Year+	47%	up to 55%
knowledge of vulnerabilities such as XSS and SQLi in web applications	of web applications tested by Veracode in 2015 had XSS vulnerabilities	of web applications tested by Whitehat Security in 2015 were "always vulnerable"

Application security is still mostly improvization

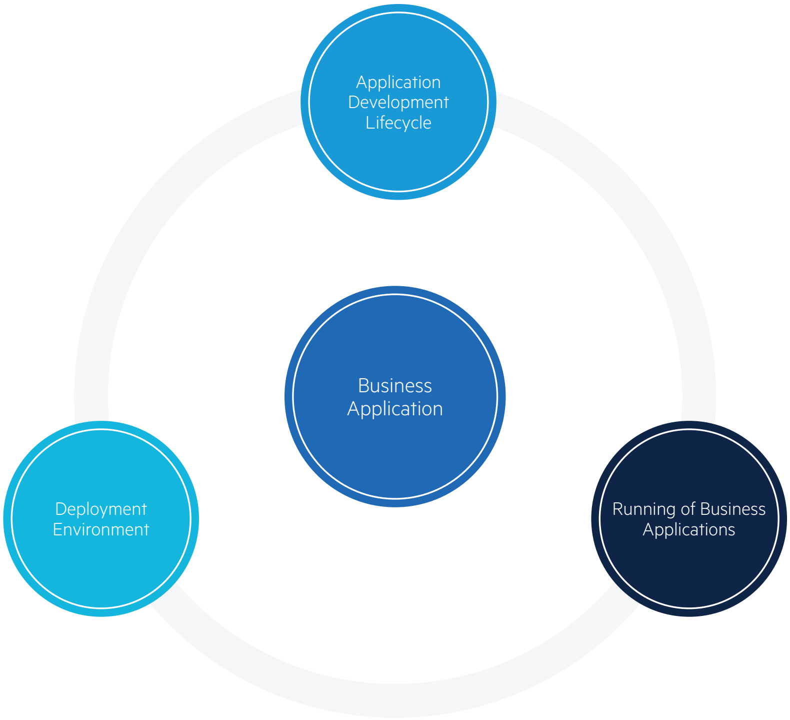
Source: TechInsights: State of Application Security, Gartner

Security challenges today are escalated due to the need to manage massive volumes of data, while ensuring high availability, anytime access and accurate information intelligence. Recent global legislation concerning sharing and transferring data, though not unfounded, promises to add to the anxiety of operating and protecting vital systems that are the basis for a competitive business advantage in today's digital economy.

Strategies and tools are available that companies should employ to help secure their applications. Some of these include setting reasonable security standards, to utilizing tools that help assess vulnerabilities throughout your environment, to training programs that help developers truly understand the ramifications of the coding decisions they make and the importance of adhering to security standards. As you continue to develop or evolve a holistic security strategy, understanding how to enhance the security of your Progress® OpenEdge® application is a fundamental factor.

Securing OpenEdge Business Applications

Going back to basics, one could define business application security as processes, best practices and technologies used to prevent unauthorized access to application data. Data security includes securing data-at-rest, as well as data-in-motion. Running business applications, operating environments, network connectivity and integration with other applications and third-party technologies are the broad categories where application data flows; thus, it is warranted to carefully consider not only securing the application data, but all of these aspects:


Application Development Lifecycle
Business Application
Deployment Environment
Running of Business Applications

Secure Application Development Lifecycle

Securing business applications requires good development practices, processes and technologies throughout the software lifecycle to prevent and detect security vulnerabilities during design and coding so applications are built in a manner that minimize risk.

Secure Running Business Applications

The primary focus of securing running business applications should be placed on the application data, i.e. CRUD (Create, Update, Read, Delete) activities within the application. In other words, it's about the who, what, when and how of the application data. Best practices such as authentication, authorization, auditing and data security via configuration are keys to making sure that application content is secure at runtime, while application network connections are extremely important to the security of data in-motion.

✓ **Tip:**

The OWASP Top Ten represents a broad consensus concerning the most critical web application security flaws. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. OWASP Top 10 vulnerabilities is a good place to start exploring best practices, and there are many tools available to scan application code for known vulnerabilities.

Many business applications interface with other business applications and integrate with third-party technologies. Properly securing business applications means considering third-party technology integration as this will have a huge impact on potential access to your application.

Secure Deployment Environment

Securing deployed business applications requires security of the deployment environment, including the Operating Systems (OS) and any other infrastructure such as the cloud. There are many tools and best practices available from multiple sources, such as the Microsoft Baseline Security Analyzer, to identify any missing security updates and common configurations.

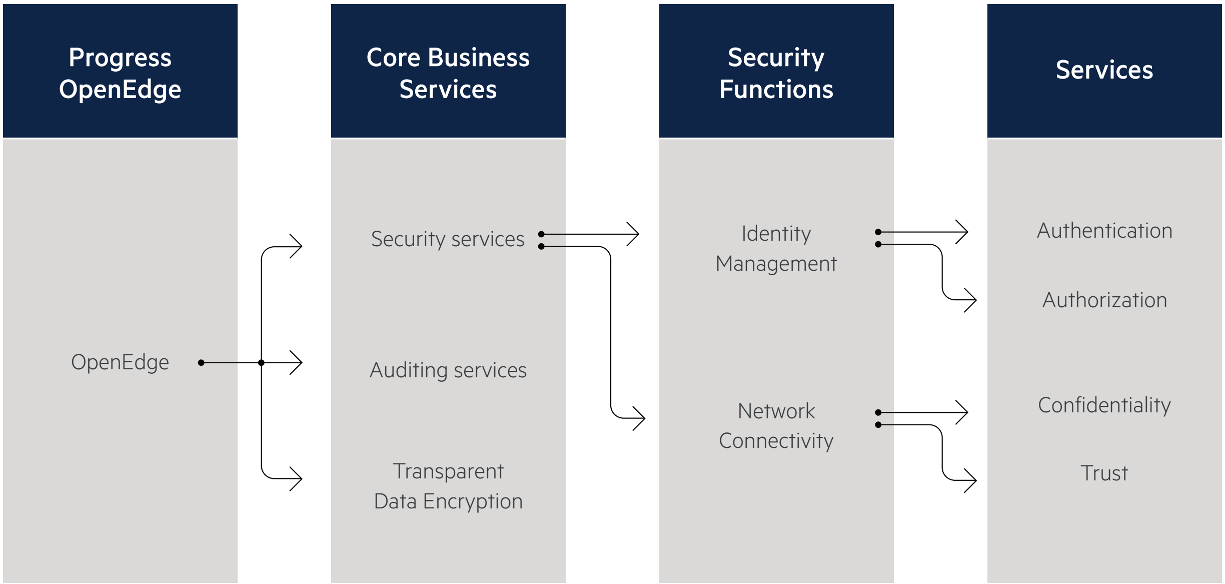
Although addressing these three elements is crucial, the focus of this whitepaper will predominantly cover technologies and aspects related to securing running application data.

> Theft of intellectual property, unlike other kinds of data breaches, often goes years without being detected, as it did in nearly a third of the cases studied by the Wall Street Journal. This same study indicated that in 97% of these cases the breaches were avoidable, but proper measures had not been taken.

Securing Running Business Applications

Securing running business applications includes securing the data generated and maintained, and the application's connectivity to the network. It requires consideration of the following basic elements:

- **Authentication of Users:** Who is allowed to get in either via a User Interface (UI) or directly to API's?
- **Authorization:** Once a user logs into your application, what data are they allowed to access?
- **Auditing:** What did the user change?
- **Data-at-rest:** Is the data secure when it's stored in the application?
- **Data-in-motion:** Is the data secure when it's flowing through various architectural components of your application?
- **Network connectivity:** How do you make sure that the various ways in which a user can access your application are safe, both inside and outside the application boundaries?



OpenEdge provides security services for each of these:

Identity Management (IdM)

Identity Management allows the right individuals to access the right resources for the right reasons. This is achieved through Authentication and Authorization. Until a decade ago, business applications were protected behind firewalls, making it far easier to limit access. Today, the first barrier to keeping intruders out is Authentication, or understanding who the user is. Not every customer, network configuration or market you are in will want or accept a single authentication system that you may choose to support. You may be required to use their existing systems, while Authentication systems provide ease in integration with third-party systems.

Once the right individual gains access to the system, it is paramount to restrict that access to information they are entitled to operate. Ultimately, authorization to data/functions and auditing will only be as good as the authentication of the real user throughout the application's distributed services and components.

The goal is to make it easier to determine proper accessibility through single sign-on or federated authentication through integration with third-party authentication systems. The weakness in an application's IdM most often comes from a developer's written authentication and authorization systems. These systems are typically designed and implemented by general application development and testing standards, and not by security service development and testing standards.

Therefore, OpenEdge will migrate its IdM services to industry recognized authentication and authorization services that are designed and tested according to higher standards and integrate them into the application developer's friendly OpenEdge environment.

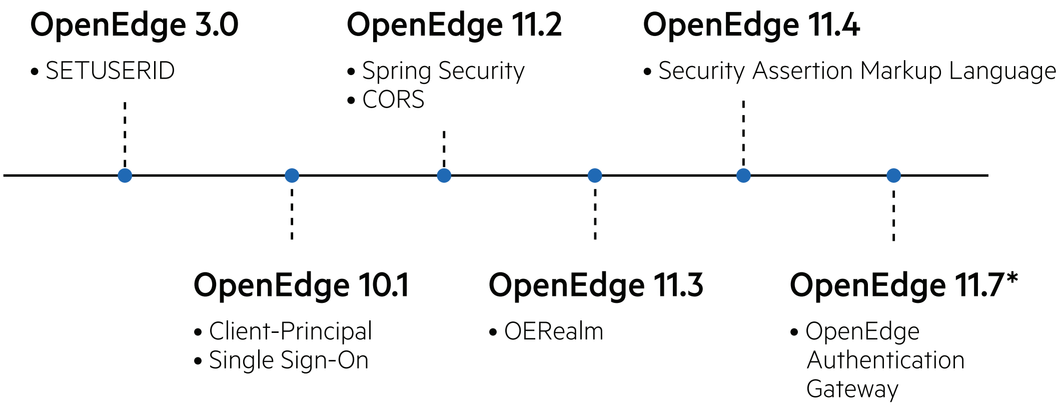
IdM was first deployed in OpenEdge Version 3.0 via setuserid function. Introduction of client-principal, a decade ago, has enabled developers to seal login credentials, thus preventing anyone from tampering with the credentials and enabling single sign-on. A client-principal is a handle-based object that functions as the security token in an ABL application, holding the login information of a user. It's a secure, time sensitive token with an expiration date that is sealed, verified and protected. Once validated and accepted by OpenEdge, the client-principal's user-id can be used for the purposes of establishing the user-id in auditing records or for ABL run-time checking of database table and field permissions. The user can now login once and pass the access token to other Progress sessions, including OpenEdge AppServer to Progress WebSpeed agents, and between WebSpeed and AppServers themselves.

Progress Application Server for OpenEdge is a modern, sophisticated, highly scalable application server requiring fewer system resources and easing installation, configuration and management. This innovative technology helps you bring your application into the future by modernizing experiences and limiting security vulnerabilities using the Spring Security framework.

With the introduction of REST and mobile, Spring Security, a powerful and highly customizable authentication and access control framework, was integrated into OpenEdge, providing a comprehensive solution for authentication and authorization for enterprise applications. This capability was also extended to support OpenEdge AppServer-based authentication mechanisms through OERealm as well as other industry standard authentication models like Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML).

Security is not a onetime undertaking. It needs to evolve as hackers find new ways to invade mission-critical business applications. Progress is now developing a new security server known as Progress OpenEdge Authentication Gateway, available in the upcoming release of OpenEdge.

Progress OpenEdge: Security Technologies Release Cycles



OpenEdge 3.0
- SETUSERID

OpenEdge 10.1
- Client-Principal
- Single Sign-On

OpenEdge 11.2
- Spring Security
- CORS

OpenEdge 11.3
- OERealm

OpenEdge 11.4
- Security Assertion Markup Language

OpenEdge 11.7*
- OpenEdge Authentication Gateway

*Progress OpenEdge 11.7 is due for release in the Spring of 2017.

Network Connectivity (Data-in-Motion)

Data-in-motion is exactly as the name implies—the process of transferring data between all versions of the original file, especially when data may be in transit on the Internet. It is data that is exiting the network via email, web, or other Internet protocols and has three major considerations:

- **Trust** is about maintaining trust-worthy relationships in a networking environment. Trust, using well-defined patterns, is used when peers establish a trusted connection over which data can be safely transported based on a strong source of identity and granted permissions. This trust is generally established through a process of registration and issuance of certificates at and by a certificate authority (CA).

Example: Peer authenticated TLS connections—one of the well-known key-exchange mechanisms is based on something exchanged and something both peers know.

- **Integrity** prevents sensitive information being communicated between two or more entities from being altered, intentionally or unintentionally, throughout its journey. While cyclic redundancy check (CRC), an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data, exists to protect data from accidental change, OpenEdge provides additional means to protect data from intentional changes by intruders.

- **Confidentiality** prevents sensitive information communicated between any two or more entities from being read by anyone beyond those entities. Confidentiality extends from raw storage (in all its locations and forms) through one or more 'trusted connections' until it reaches its strongly authenticated and authorized consumer. The strength of Confidentiality is based on the IdM employed to establish those 'trusted connections' and the data hiding implementation of the components involved, which is achieved through data encryption and security tokens.

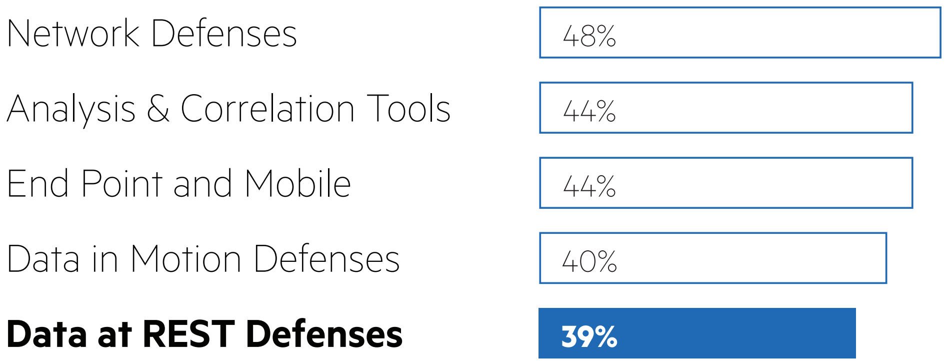
To ensure **Confidentiality**, **Integrity** and **Trust**, Progress OpenEdge provides many tools along with support for third-party tools to secure data.

Secure Sockets Layer (SSL) and Transport Security Layer (TSL) act as a base technology to ensure secure communication between systems. OpenEdge employs, and with each release, upgrades TLS technologies into the platform. OpenEdge now communicates over TLS 1.2 by default. A user can change the default to other supported protocols, ciphers or certificates. OpenEdge policy is to balance between backwards compatibility and eliminate well-known vulnerable protocols (SSLv3) and cryptography hashes and encryption.

Other ways of providing high levels of confidentiality include file system storage encryption, backup file encryption, data obfuscation of application variables, digital certificates, message digests, cryptographically sealed security tokens and more.

Transparent Data Encryption (Data-at-Rest) provides protection against intruders that attempt to access your private data while "at rest." Data-at-rest is a description for information that is stored on disk inside your database. Although companies today have placed an emphasis on minimizing security risk, many underestimate the value of data protection.

Increases in IT Security Spending Plans by Category



Source: Global Edition of the 2016 Vormetric Data Threat Report, by 451 Research and Vormetric

IT security budget allocation has increased in the areas of network or mobile by almost 50%, while encryption of data-at-rest planned spending increases were under 40%, despite proving to be far more effective in minimizing vulnerabilities because it creates a barrier to the most valuable asset—corporate data.

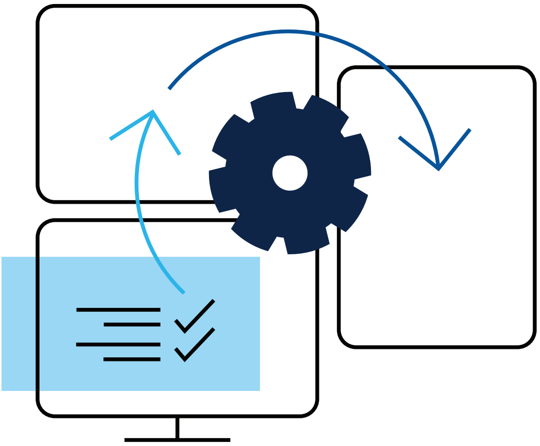
To support data-at-rest protection, Progress OpenEdge offers an add-on product known as Progress OpenEdge TDE. It is a complete "in the box" solution that requires no changes to your application, user procedures or database administrator (DBA) management processes. Data is read into memory and stored unencrypted. This means the application is able to execute at full speed with less than 2% performance degradation while encrypting/decrypting. Support for TDE is embedded within the OpenEdge RDBMS and all language clients. OpenEdge combines various cipher algorithms and encryption key lengths, secure storage of encryption keys and user access controls to your encryption keys to ensure that data encryption cannot be reversed by anyone other than those granted access. No language client can query the Encryption Policy Area.

Additional aspects include encrypted backups, temporary notes files (aka logs) and data transfer from database to database. One of the early distinguishers of OpenEdge TDE is that other products suffer from decreased index lookups, where OpenEdge TDE has full indexing capabilities.

Auditing allows an organization to see who did what, where, when and how. The focus is on detection and forensics: recording of event information that cannot be compromised, evaluating events for abnormal patterns and using the recorded event information to identify who and how, so that process changes can be made to block the behavior.

OpenEdge uses a consistent auditing mechanism across its components that helps to comply with regulations. Users can audit database events such as create, update and delete or internal events such as login, schema changes, database utilities and security administration and for application defined events. The level of auditing depends on the applications to be audited. OpenEdge has defined a set of best practices for auditing that can be found in the documentation.

Third-Party Technology Integration—Many business applications include multiple technologies for integration to address other business needs, necessitating the highlighting of an Application Programming Interface (API) based strategy.



Many applications use third-party libraries like Java that are packaged with the application. Due to tighter release schedules, it is not always possible to upgrade third-party libraries to the latest versions. Not being on the latest version poses a greater risk of exposing business applications to security vulnerabilities. This is also true for operating systems that OpenEdge applications are designed to run on. Many open source and commercial tools are available to help you scan for security vulnerabilities in operating systems, AppServers, Webservers and other third-party integration tools, and should be a fundamental process in your security strategy and application development lifecycle. Of course, these should be complemented by developer-focused security programs, clear security standards and frequent training sessions to drive security-focused behavior among developers.

Progress strives to certify OpenEdge on the latest versions and operating systems. If your application is architected on a version of OpenEdge prior to the 11.4, you are not utilizing the latest security features OpenEdge has to offer. Each new OpenEdge release takes significant strides to proactively secure your applications against emerging threats. The next release of OpenEdge — OpenEdge 11.7 due for release in 2017—will help customers and partners to strengthen security of their business applications. With new security issues evolving all the time, staying current is one of the most effective ways to avoid putting yourself at risk for hidden vulnerabilities. Please refer to OpenEdge documentation for more details.

"Mitigation costs grow exponentially the longer it takes a development team to identify and fix a security issue during the development process. Defining a solid app security architecture during the design phase and coupling it with accurate development against that design are critical components of the secure code delivery process."

App Security Can't Happen Without Developers: Use A Combination Of People And Tools To Deliver Secure Apps
John M. Wargo
May 26, 2016

Conclusion

Progress is committed to providing technology that helps you improve the security of your OpenEdge applications. The current release of OpenEdge employs the latest TLS security, helping you meet security standards such as PCI. OpenEdge also uses Spring Security as the foundation of our next generation Progress Application Server for OpenEdge. Other recent enhancements in OpenEdge 11 address identity management, authorization and access controls and data encryption. Your ability to safeguard intellectual property for your company and your customers minimizes the disruptive and destructive impact a security breach brings. Upgrading legacy technology is one necessary precaution that also distinguishes your company from your competition. In a recent survey, only 34% of IT professionals felt at least somewhat vulnerable to attacks, but 90% of businesses were attacked on some level in 2015. It is not a risk worth taking.

We've long been devoted to helping our customers with everything from making sense of regulatory issues, connecting to their data and modernizing their applications. We're dedicated to providing you the support you need to succeed in a rapidly changing security environment.

Contact Us

To learn more about the offerings available by members of the OpenEdge community, please visit and register for our forum dedicated to driving networking, sharing and learning opportunities: Progress Community
If you have questions or would like more information,
please Contact Us

Worldwide Headquarters

Progress, 14 Oak Park, Bedford, MA 01730 USA
Tel: +1 781 280-4000 Fax: +1 781 280-4095
On the Web at: www.progress.com
Find us on facebook.com/progresssw twitter.com/progresssw youtube.com/progresssw
For regional international office locations and contact information,
please go to www.progress.com/worldwide

Progress®