



# Enhance Your Enterprise Security with Progress OpenEdge 12.8

# The Security of Your Applications Is Essential to Business Operations

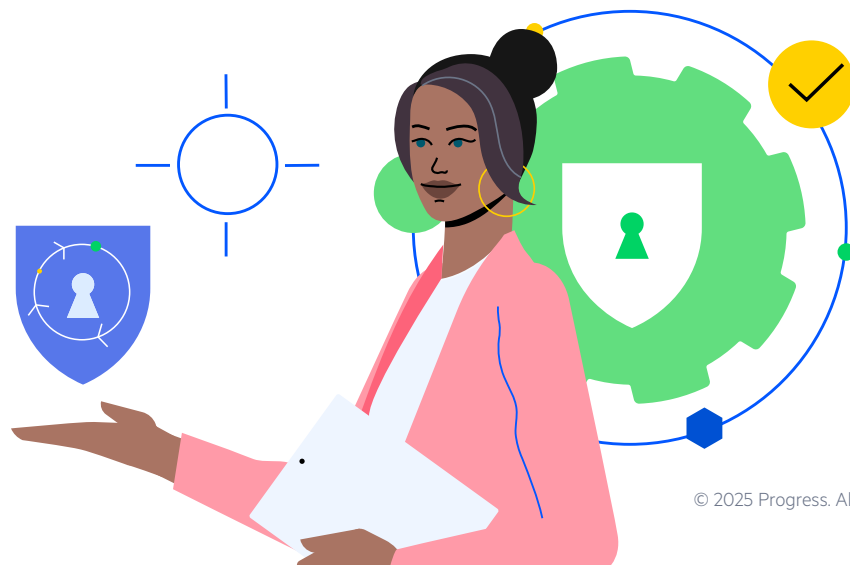
Security should be top of mind for any business, especially with the technology available to hackers and bad actors today. Because of these growing and persistent threats, an organization's mission-critical applications need to be secure and up-to-date for better protection from outside threats.

Progress® OpenEdge® 12.8 introduces a variety of advanced security features designed to supplement operating system and filesystem security, helping organizations protect themselves against breaches and strengthen robust data protection. This whitepaper highlights the key security features and enhancements in OpenEdge 12.8 and explains why upgrading from older versions is crucial for maintaining enterprise security.

## The Growing Threat Landscape

Cyberattacks are becoming increasingly frequent and sophisticated. Hackers exploit known vulnerabilities in outdated software to gain unauthorized access, steal sensitive data and disrupt business operations. The financial and reputational damage from a data breach can be catastrophic, potentially costing millions of dollars and irreparably harming your brand's reputation.

Because of these risks, regulatory bodies worldwide are imposing stricter data protection laws. Compliance with regulations such as GDPR, LGPD and HIPAA is not optional. Failure to comply can result in hefty fines and legal repercussions. By not upgrading your OpenEdge applications to fully supported versions, you may lack the necessary security features to meet these stringent requirements, putting your organization at risk of non-compliance.





\* \* \* \*

## Key Security Features in OpenEdge 12.8

OpenEdge 12.8 has features, tools and capabilities built to strengthen the security within your mission-critical business applications. The top features include:

- Dynamic Data Masking
- Transparent Data Encryption
- Hardware Security Module
- OpenSSL and TLS 1.3
- Enhanced Application Server
- Protected Compile
- Code Signing
- External Security Administration Manager
- OpenEdge Authentication Gateway
- And more!

## Dynamic Data Masking (DDM)

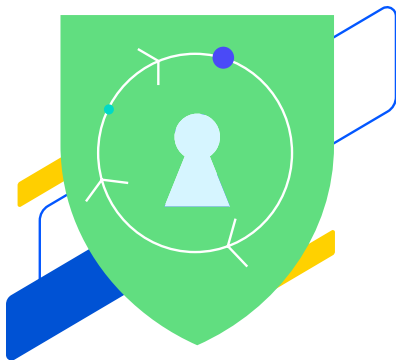
Dynamic Data Masking (DDM) dynamically obfuscates sensitive data so it can't be viewed by unauthorized users. For example, HR personnel with DDM privileges can view employee salaries, while others see a masked version. The underlying data remains unmasked in the database. Queries using DDM-configured columns see the unmasked value, but unauthorized users receive masked results. Allowing users to mask fields from unauthorized users helps administrators support data privacy and protection, meet regulatory requirements and safeguard sensitive information.

Enhance data security and governance with Dynamic Data Masking (DDM) capabilities, including:

- Track DDM activities, changes and rule management
- Control sensitive data access using authorization tags
- Alert database clients about DDM schema changes

A DDM administrator configures masks for table fields and controls access privileges. DDM affects database clients like ABL, Progress Application Server (PAS) for OpenEdge and SQL Server, but not utilities like binary dump or load.

DDM applies to Change Data Capture (CDC) tables and all data types except CLOB and BLOB. CDC change tables inherit mask configurations from their parent tables, which can be modified later. Data from CDC tables is masked for users without unmasking privileges.



DDM can be configured for user-defined multi-tenant tables, applying settings to all tenants. It affects commands, clauses and database objects like triggers, functions and procedures based on user privileges.

An executive should care about implementing Dynamic Data Masking (DDM) in their OpenEdge applications for several important reasons:

- **Data Security:** DDM helps protect sensitive data by masking it from unauthorized users while keeping the data unchanged in the database. This reduces the risk of data breaches and unauthorized access.
- **Regulatory Compliance:** DDM assists in meeting regulatory requirements such as GDPR and HIPAA by keeping sensitive information from being exposed to unauthorized users.
- **Operational Flexibility:** DDM allows for different levels of data visibility based on user roles and permissions. This means that sensitive data can be masked for most users while remaining accessible to those with the necessary authorization.
- **Risk Management:** By masking sensitive data, DDM minimizes the risk of data exposure during activities like software testing, sales demos or user training.
- **User Trust and Confidence:** Implementing DDM demonstrates a commitment to data security, which can enhance trust and confidence among customers, partners and stakeholders.

OpenEdge 12.8 provides tools to easily enable, disable and manage DDM, making it straightforward to integrate into existing systems without significant disruption.

[Learn more about Dynamic Data Masking.](#)



## Transparent Data Encryption (TDE)

OpenEdge Transparent Data Encryption (TDE) balances both security and performance needs using industry-approved encryption technologies and encryption key management processes for secure, encrypted data. Controlling access to stored private data, or “data at rest,” is at the core of the OpenEdge TDE solution. This is accomplished by combining cryptography technologies and processes to give security administrators or database administrators control over who can access the private data within the database.

TDE allows for execution at full speed with less than 2% performance degradation while encrypting and decrypting data. It includes both policy tools and a secure encryption key store separate from the database. By leveraging the authentication, authorization and auditing functionality inherent in the Progress OpenEdge platform and the additional Advanced Business Language (ABL) security features, OpenEdge TDE helps protect data on disk, in backups and in binary dump files—supporting leading encryption ciphers.

Each encrypted database has a single, unique Database Master Key (DMK). The DMK is created and managed by your Database Administrator and stored in your database key store, which is separate from your database. This key store is an independent entity that provides secure storage of data encryption keys and controls access through user accounts.

Encryption of your database objects is managed through encryption policies. You define which objects are encrypted and the encryption cipher for each object. Policies are stored in your database in a designated Encryption Policy Area. Object policies use virtual data encryption keys derived from your DMK and the specified cipher, so the encryption key for each encrypted database object is unique.

By implementing Transparent Data Encryption (TDE) in their OpenEdge applications, executives can support:

- **Data Security:** TDE keeps sensitive data encrypted while at rest, helping protect it from unauthorized access and breaches. This is crucial for maintaining the confidentiality and integrity of the data.
- **Compliance:** Many industries are subject to strict regulatory requirements regarding data protection (e.g., GDPR, HIPAA). TDE helps organizations meet these compliance standards by providing a robust encryption solution.
- **Risk Management:** By encrypting data at rest, TDE minimizes the risk of data theft or loss, which can have severe financial and reputational consequences for the organization.
- **Customer Trust:** Demonstrating a commitment to data security can enhance customer trust and confidence in the organization, potentially leading to increased customer loyalty and business opportunities.

- **Operational Efficiency:** TDE is designed to be transparent to applications, meaning it does not require significant changes to existing systems or workflows. This allows for seamless integration and minimal disruption to business operations.
- **Competitive Advantage:** In a market where data breaches are increasingly common, having strong data encryption measures in place can differentiate an organization from its competitors, showcasing a proactive approach to data security.

[Learn more about Transparent Data Encryption.](#)

## Hardware Security Module (HSM)

Numerous industries, including the public, financial and insurance sectors, require the highest level of security when storing and using cryptographic keys. Hardware Security Module (HSM) supports compliance with stringent security standards and provides an additional layer of protection for cryptographic keys. It accomplishes this by:

- Utilizing tamper-resistant physical data storage and data-in-transit transfers
- Storing and protecting keys, making them available only to authorized users
- Eliminating the need for supporting keys to be loaded into the web/application server memory

An HSM is an enterprise-scale security solution that helps safeguard and manage digital keys, performs encryption and decryption functions for digital signatures and provides strong authentication and other cryptographic functions. It can be hardware, firmware, software or a network device. To strengthen OpenEdge key store security, you can add an external enterprise-managed HSM component to the OpenEdge TDE encryption key storage security. This HSM storage, which can be a local, network or cloud service, provides client access using the PKCS #11 standard API and is designed to comply with FIPS 140-2 Level 2 or Level 3 certification requirements.

An executive should care about implementing an HSM in their OpenEdge applications for several reasons:

- **Enhanced Security:** HSMs provide a highly secure environment for managing cryptographic keys, which are crucial for encryption, decryption and digital signatures. These devices are tamper-resistant and designed to protect against physical and logical attacks.
- **Regulatory Compliance:** Many industries have stringent regulatory requirements for data protection (e.g., GDPR, PCI DSS, HIPAA). HSMs help organizations meet these standards by supporting secure key management and encryption processes.
- **Risk Mitigation:** By securely storing and managing cryptographic keys, HSMs reduce the risk of key compromise, which can lead to data breaches and significant financial and reputational damage.

- **Operational Efficiency:** HSMs offload cryptographic operations from general-purpose servers, improving overall system performance and reliability. This can be particularly beneficial for applications that require high volumes of cryptographic processing.
- **Trust and Confidence:** Implementing HSMs demonstrates a strong commitment to data security, which can enhance trust and confidence among customers, partners and stakeholders.
- **Future Readiness:** As cyberthreats evolve, having robust security measures like HSMs in place better prepares organizations to handle emerging threats and maintain a strong security posture.

[Learn more about Hardware Security Module \(HSM\).](#)

## OpenSSL, Java JSSE TLS and TLS 1.3

The OpenEdge platform supports TLS client and server connections over the Internet (using HTTPS and appropriate middleware) or on an intranet (OpenEdge embeds and uses TLS). This offers stronger encryption algorithms and improved performance, reducing the risk of data interception and man-in-the-middle attacks.

An executive should care about implementing OpenSSL TLS 1.3 in their OpenEdge applications for several important reasons:

- **Enhanced Security:** TLS 1.3 offers significant security improvements over previous versions by eliminating outdated cryptographic algorithms and providing stronger encryption methods. This helps reduce vulnerabilities and protect against various cyberthreats.
- **Performance Improvements:** TLS 1.3 is designed to be faster, with a more efficient handshake process that reduces latency. This can lead to better application performance and a smoother user experience.





- **Regulatory Compliance:** Adopting TLS 1.3 can help enhance security for Personally Identifiable Information (PII) or Protected Health Information (PHI) in transit, aligning with GDPR's and/or HIPAA's stringent requirements for the protection of sensitive information.
- **Future Readiness:** Adopting the latest versions of security protocols like TLS 1.3 enables organizations to be prepared for future security challenges and to integrate new security features as they become available.
- **Customer Trust:** Demonstrating a commitment to using the latest and most secure technologies can enhance customer trust and confidence in the organization's ability to protect their data.
- **Operational Efficiency:** OpenSSL 3.1 includes various improvements and optimizations that can enhance the overall efficiency and reliability of cryptographic operations within applications.

[Learn more about TLS.](#)

## Enhanced Application Server (JWE, OAuth2, HTTPS & SAML2)

PAS for OpenEdge supports OAuth2 authorization, allowing your ABL business application or data service to accept an OAuth2 access token (in JWT format) or a simple JWT token. PAS for OpenEdge validates the OAuth2 token and exchanges it for an OpenEdge Client-Principal object, which is the standard mechanism for securely passing user identity across OpenEdge products. This Client-Principal object is then passed to your ABL application, where it can be used to manage user access to OpenEdge database connections and other secured resources.

The use of enterprise-controlled OAuth2/JWT tokens enhances the security of web applications, supporting secure web application access and data exchange.

If there are concerns about exposing OAuth2 tokens over network connections at a deployment site, security can be further enhanced by implementing best practices, such as:

- Transmitting every HTTP message containing an OAuth2/JWT token over HTTPS
- Securely storing and sharing cryptographic keys between authorization and resource servers
- Using JSON Web Encryption (JWE) to transport an OAuth2/JWT token



JWE enables secure, end-to-end communication of JSON-formatted data within a tamper-proof, confidential container. PAS for OpenEdge provides an option to use JWE for transporting OAuth2/JWT tokens. By using JWE, organizations can:

- Establish confidentiality of the OAuth2/JWT token between the token's producer and the PAS for OpenEdge server, regardless of the network architecture
- Eliminate the requirement for HTTPS when transporting public application data

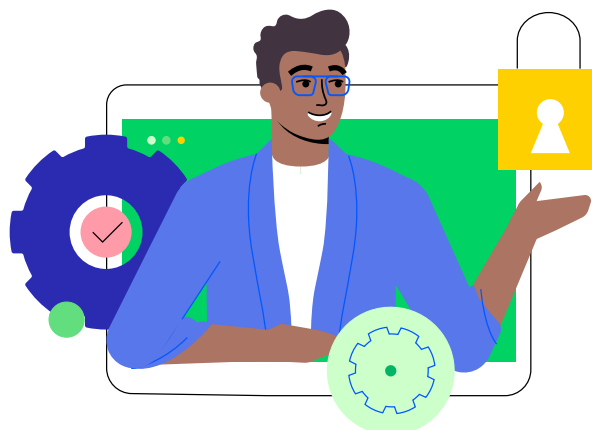
As an alternative to OAuth2/JWT tokens, PAS for OpenEdge supports enterprise-controlled Single Sign-On (SSO) using SAML tokens. SAML 2.0 is an open standard that allows users to access multiple applications with a single SSO token. PAS for OpenEdge can fully integrate with the enterprise's Identity Provider to facilitate login and logout processes for web applications. The contents of a validated SAML token are used to generate and deliver a Client-Principal token, which can then be leveraged by the business application to control access to its databases.

PAS for OpenEdge support for OAuth2, JWT and SAML tokens conforms to established standards, helping to safeguard user identification in business applications. These measures are used by organizations to:

- Confirm who is who when trying to access and use various business applications
- Make sure that information is only visible to those who are permitted to view it
- Protect sensitive information in transit, reducing the risk of data breaches

An executive should care about implementing an Enhanced Application Server with JWE (JSON Web Encryption) and OAuth2 in their OpenEdge applications for several key reasons:

- **Advanced Security:** JWE provides robust encryption for data transmitted between clients and servers to keep sensitive information confidential and protected from interception or tampering. OAuth2 offers secure authorization, allowing applications to access resources on behalf of users without exposing their credentials.
- **Compliance:** Using JWE and OAuth2 supports stringent regulatory requirements for data protection and privacy, such as GDPR and HIPAA. These protocols promote secure handling of data and properly controlled access.



- **User Trust and Confidence:** Implementing these advanced security measures demonstrates a strong commitment to protecting user data, which can enhance trust and confidence among customers, partners and stakeholders.
- **Operational Efficiency:** OAuth2 simplifies the process of managing user permissions and access control, reducing the administrative burden and improving operational efficiency. This can lead to smoother user experiences and more streamlined application management.
- **Future Readiness:** Adopting modern security standards like JWE and OAuth2 helps prepare the organization for future security challenges and enables them to easily integrate new security features as they become available.
- **Interoperability:** OAuth2 is widely adopted and supported by many platforms and services, facilitating easier integration with other systems and enhancing the overall functionality of OpenEdge applications.

[Learn more about JWE and OAuth2.](#)

## Protected Compile

This capability helps secure the compilation process so only authorized users can compile and execute ABL code. It helps prevent unauthorized code modifications and enhances the integrity of the application development process. During deployment, you can protect your compiled OpenEdge application code by using OpenEdge tools to:

- Package r-code and image files into an archive file (.apl)
- Digitally sign the archive file

An executive should care about implementing Protected Compile in their OpenEdge applications for several important reasons:

- **Code Security:** Protected Compile encrypts the source code, preventing unauthorized access or modification. This helps safeguard the intellectual property and business logic embedded in the code against tampering and reverse engineering.
- **Compliance:** Many industries require stringent security measures to protect sensitive information. Using Protected Compile helps organizations meet regulatory requirements and industry standards for data protection and software security.
- **Intellectual Property Protection:** Protecting the source code helps maintain the competitive advantage by keeping proprietary algorithms and processes from being exposed to competitors or malicious actors.
- **Operational Integrity:** Executing only authorized and verified code helps maintain the integrity and reliability of the application. This reduces the risk of introducing vulnerabilities through unauthorized code changes.

- **Customer Trust:** Demonstrating a commitment to robust security practices, including code protection, can enhance customer trust and confidence in the organization's software solutions.
- **Ease of Implementation:** OpenEdge 12.8 provides tools to easily enable and manage Protected Compile, making it straightforward to integrate into existing development workflows without significant disruption.
- **Database Security:** Protected Compile enables only authorized users to compile source ABL code and execute it at run-time in a connected OpenEdge Database. The runtime compilation will apply the OpenEdge Database's table and field permission settings at execution time.

[Learn more about Protected Compile.](#)

## Code Signing

You can organize and store r-code in an ABL archive (.apl file), a library that supports code signing. Archives allow you to manage and execute r-code more efficiently while helping prevent the execution of tampered or malicious code, enhancing overall application security.

An archive contains r-code that executes in local memory, streamlining operations. You create archives using the PROPACK utility. It is important to note that using PROPACK alone does not provide added security. PROSIGN, however, is a crucial tool for enhancing the security of your OpenEdge applications. With PROSIGN's code signing capabilities for ABL archives:

- The integrity of the r-code within the .apl files is validated
- The authorship of the archive is authenticated
- Tampered or malicious code can be prevented from executing

As part of code signing, OpenEdge products support integrity and authorship validation for Windows OS executables, libraries and scripts. This is particularly significant for customers, as it aligns with corporate security requirements and is essential for maintaining a secure application environment.

Using signed ABL archive libraries provides an alternative to loading, storing and executing r-code from individual operating system files for each ABL session. With an ABL archive library, r-code is loaded once into the OS process and shared across all ABL sessions.

When you execute r-code from an archive, you gain several advantages:

- Faster access to r-code (for non-signed archives)
- Fewer file open and close operations

During deployment, you can protect your compiled OpenEdge application code by using OpenEdge tools to:

- Package r-code and image files into an archive file (.apl)
- Digitally sign the archive file

A signed archive file confirms that compiled OpenEdge application code has not been corrupted or tampered with. Business leaders should care about implementing Code Signing in their OpenEdge applications for several key reasons:

- **Integrity and Authenticity:** Code signing confirms the code has not been altered or tampered with since it was signed. This promotes the integrity and authenticity of the software, verifying that it comes from a trusted source.
- **Security:** By verifying the identity of the software publisher and confirming the code has not been modified, code signing helps protect against malicious software and unauthorized changes. This is crucial for maintaining a secure application environment.
- **Compliance:** Many regulatory frameworks and industry standards require the use of code signing to support software integrity and authenticity. Implementing code signing helps organizations meet these compliance requirements.
- **User Trust:** Digitally signed code provides users with confidence that the software they are installing is legitimate and safe. This can enhance user trust and reduce the likelihood of security warnings or installation issues.
- **Reputation Management:** Executing only verified and trusted code helps protect the organization's reputation by preventing the distribution of compromised or malicious software.
- **Operational Efficiency:** Code signing can streamline the deployment process by reducing the need for manual verification and increasing the reliability of automated systems.

[Learn more about Code Signing.](#)

# External Security Administration Manager (ESAM)

ESAM equips OpenEdge System Administrators with the ability to centralize and strengthen the governance and security of OpenEdge installation environments and the applications they support.

- **Centralized Security Management:** ESAM enables administrators to manage security policies across multiple OpenEdge environments in a consistent and centralized manner, reducing complexity and potential gaps in security.
- **Seamless Integration:** By operating independently of OpenEdge code and configurations, ESAM provides governance without requiring changes to existing applications or environments, minimizing disruption and deployment effort.
- **Proactive Risk Mitigation:** The default always-on policy enforcement supports consistent application of security policies, helping prevent vulnerabilities from arising due to misconfigurations or oversight.
- **Compliance with Enterprise Standards:** ESAM policies are designed to align application runtime practices with corporate and security requirements, helping organizations meet regulatory and internal compliance standards.
- **Adaptability Across Modern Infrastructures:** ESAM is compatible with OpenEdge 12.6 and later, providing governance for applications running in diverse environments, including traditional systems, virtual machines (VMs) and containers.
- **Enhanced Operational Efficiency:** By enabling real-time validation of installations and providing logging for troubleshooting, ESAM helps administrators quickly identify and resolve issues, improving operational reliability and efficiency.
- **Future-Ready Security:** As a flexible and external manager, ESAM supports evolving security needs and can scale with an organization's infrastructure, allowing for longevity and relevance.

In summary, ESAM offers a powerful combination of streamlined security management, operational efficiency and compliance support, providing critical value to organizations that rely on the OpenEdge platform for their mission-critical applications.

[Learn more about ESAM.](#)

# Application Quality and Security Management (QSM)

As OpenEdge applications mature, codebases can accumulate technical debt and security risks that threaten agility, maintainability and compliance with security regulations. To address these challenges, organizations can leverage the [Application Quality and Security Management](#) (QSM) service.

QSM provides a fact-based, data-driven approach to measure the structural and security health of OpenEdge applications. Powered by the Sigrid® software assurance platform from Software Improvement Group (SIG), the service benchmarks application code against one of the industry's largest databases, helping organizations proactively identify maintainability issues, technical debt and security vulnerabilities. The assessment includes maintainability scoring, targeted improvement recommendations and security risk analysis with visualization of architecture and code hotspots for efficient remediation. Recommendations are prioritized based on business risk and potential impact, allowing for remediation to align with your most important objectives.

Key benefits include:

- **Objective Maintainability Scoring:** Gain clear, benchmarked ratings of the quality of your codebase, empowering teams to set realistic improvement goals and track progress over time.
- **Automated Security Insight:** Identify vulnerabilities and weak points before they potentially impact compliance or business operations, with prioritized remediation guidance.
- **Transparency and Alignment:** Visualize technical debt, architectural issues and risk areas in formats suited for development teams and executive stakeholders alike, supporting data-driven decisions on anything from daily improvements to modernization strategy.
- **Support for Incremental Improvement:** Progress Professional Services experts partner with your team for practical, sustainable enhancements, emphasizing targeted actions in high-impact areas and continuous improvement, rather than requiring large, disruptive overhauls.

By integrating quality and security management into the OpenEdge application lifecycle, organizations can future-ready their business systems, reduce cost and foster ongoing innovation.

To learn more about Application and Quality Security Management, [request a consultation](#) with the Progress Professional Services team.

# Additional Security Features

## AES-GCM Encryption support in ABL

This encryption mechanism promotes data confidentiality for ABL applications.

For more information, see our [What's New documentation](#).

## OESECTOOL for testing

Security administrators and application developers can use the OESECTOOL command line utility to test security configurations before configuring their production systems to connect to external authentication systems.

With this tool you can:

- Manage key stores
- Test OAuth2 configurations
- Test SAML configurations

For more information see the [PAS for OpenEdge documentation](#).

# Why Upgrade to OpenEdge 12.8?

Upgrading to OpenEdge 12.8 is essential for enterprises to stay on top of evolving security threats. Older versions may lack the advanced security features necessary to protect against modern attack vectors. By upgrading, organizations can benefit from:

- **Enhanced Data Protection:** Advanced encryption and masking techniques help protect sensitive data both at rest and in transit.
- **Improved Compliance:** Meet regulatory requirements with robust security features that support data privacy and integrity.
- **Stronger Authentication and Authorization:** Modern authentication protocols and secure key management enhance overall security.
- **Simplified Security Management:** Centralized security administration streamlines the management of security policies and configurations.



## Operational Efficiency and Reliability

Newer OpenEdge versions are optimized for performance and reliability. They include features that streamline operations, reduce downtime and enhance the overall user experience. This not only improves productivity but also equips your applications to handle increasing workloads and user demands.

## Future-Readying Your Business

Technology is constantly evolving, and staying on outdated software versions can leave your business behind. Migrating to the latest OpenEdge version keeps your applications compatible with modern technologies and frameworks, making it easier to integrate with other systems and adapt to future changes.

[Learn more about migration to OpenEdge 12.8.](#)

# The Cost of Inaction

## Financial Implications

The cost of a data breach can be staggering. According to recent studies, the average cost of a data breach in 2023 was \$4.45 million. This includes direct costs such as legal fees, fines and remediation efforts—plus indirect costs like lost business and reputational damage. Investing in a migration to the latest OpenEdge version is a fraction of this cost and can help prevent these devastating financial losses.

## Reputational Damage

A data breach can severely damage your organization's reputation. Customers and partners expect their data to be protected, and a breach can erode trust and confidence. Rebuilding a tarnished reputation can take years and significant resources. By proactively migrating to a more secure OpenEdge version, you demonstrate a commitment to data security and help uphold your brand's integrity.



# What's Next?

Progress OpenEdge 12.8 offers a comprehensive suite of security features designed to protect enterprise applications and data. This includes our [Advanced Security Package](#), which features Dynamic Data Masking, Transparent Data Encryption, Hardware Security Module and JSON Web Encryption. Additionally, Transparent Data Encryption (TDE) is included as part of the [OpenEdge RDBMS Advanced Enterprise Edition](#).

The security of your business applications is not something to be taken lightly. The risks associated with outdated software are too great to ignore. Migrating your OpenEdge applications to the latest version is not just a technical upgrade—it is a strategic imperative that helps protect your organization from cyberthreats, supports regulatory compliance and helps future-ready your business.

Don't wait for a breach to happen. Act now to secure your applications and safeguard your organization's future.



**Learn more about the security features in Progress OpenEdge 12.8**






## About Progress

Progress (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and digital experiences with agility and ease. Customers get a trusted provider in Progress, with the products, expertise and vision they need to succeed. Over 4 million developers and technologists at hundreds of thousands of enterprises depend on Progress. Learn more at [www.progress.com](http://www.progress.com)

© 2025 Progress Software Corporation and/or its subsidiaries or affiliates.  
All rights reserved. Rev 2025/10 | RITM0325094

## Worldwide Headquarters

Progress Software Corporation  
15 Wayside Rd, Suite 400, Burlington, MA 01803, USA  
Tel: +1-800-477-6473

 [facebook.com/progresssw](https://facebook.com/progresssw)  
 [twitter.com/progresssw](https://twitter.com/progresssw)  
 [youtube.com/progresssw](https://youtube.com/progresssw)  
 [linkedin.com/company/progress-software](https://linkedin.com/company/progress-software)  
 [progress\\_sw\\_](https://instagram.com/progress_sw_)