Progress® OpenEdge®

Security Best Practices

The Importance of Securing Your Mission-Critical Applications

WHITEPAPER

According to IBM, “For 83% of companies, it’s not if a data breach will happen, but when. Usually more than once.” In today’s digital world, every organization faces threats to information and application security. It is critical to ensure you’ve taken the necessary precautions to secure your Progress OpenEdge application.

The Security of Your Applications Is Essential to Business Operations

As with any application, security is a critical concern, and organizations must ensure that their OpenEdge-based applications are secure. In this Whitepaper, we will explore the security considerations for OpenEdge-based systems and provide best practices for securing these systems.

What is Application Security?

The set of procedures, industry standards, and technological tools used to prevent unauthorized access to application data is known as business application security. The major areas where application data moves include disk storage, memory, operating systems, network connectivity, integration with other programs, and third-party technologies. As a result, it is important to carefully examine safeguarding the application data in each of these areas.

Have you ever read about or personally experienced a cybersecurity attack and seen chaos slowly unfold as tensions rise? Enterprise productivity gets bogged down if you lose access to important data, and unwanted negative attention comes your way should you not prevent the loss of sensitive data. According to security experts, outdated and unpatched systems are among companies’ leading causes of security vulnerabilities.

Enhancing Security of Your Existing Systems

When you are working to enhance the security of your existing system, there can be technical complexities that appear daunting. While you may then consider a different path, including starting over, there is little doubt that continuing to leverage your existing

OpenEdge system will be the cost-effective option. It is understandable that “rip and replace” is tempting, as it gives you free hand to define and implement an architecture with security in mind, but the time, effort, and cost to re-implement your currently working solution, not to mention the opportunity costs of a re-write, typically make this impractical. Security enhancements can be challenging, but Progress is here to help!

Risks of Not Upgrading Your OpenEdge Version

Suppose you are on an outdated OpenEdge version for your mission-critical application. Without access to the current security features and vulnerability mitigations that come with more current OpenEdge versions, you may be risking your organization’s security, ultimately impacting your customers and stakeholders.

- **You put your applications and their stakeholders at risk**
  Your risk of a security breach, ransomware attacks, and other threats grows if you are not upgrading. Mission-critical sensitive information can be immediately accessed by hackers through security breaches, who will then exploit that information against your company. Your consumers are now seriously at risk, as are your applications.

- **There are hidden costs of not upgrading**
  While doing nothing is simple, such as not updating your software, there are hidden expenses involved. Upgrading your applications is a small price to pay compared to the cost of dealing with a data breach and all the additional effects of a hack. To prevent customer distress and to safeguard other important stakeholders, there must be some amount of risk mitigation. If you continue to be under-protected, you will end up paying more in the long term.

- **The public perception and your company reputation may be tarnished**
  With ransomware attacks, many things can happen. IT gets locked out of critical applications, destroying a company’s ability to manage their internal systems. Data can be compromised, including sensitive customer/user information. This can result in a loss of services provided to customers, an inability to run your business, penalties/fines from governing agencies, a potential loss of customers, and even lawsuits.

Data Breach in Action

When companies or government agencies have a data breach, it is detrimental for many reasons. They must deal with the hidden costs of remediation, revenue loss, reputational harm, perhaps national security, and more. According to IBM and their Cost of a Data Breach 2022 Report, “Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022. This figure represents a 2.6% increase from last year, when the average cost of a breach was USD 4.24 million. The average cost has climbed 12.7% from USD 3.86 million in the 2020 report.

To Help Mitigate These Risks, Organizations Need to Make Sure They:

- **Make security part of their development and testing process**
  While OpenEdge provides a wide variety of capabilities in the security space, these are simply tools that you can choose to utilize. The security of your application depends in large part on the steps you take, including the use of OpenEdge capabilities, to secure your application. An overall understanding of the types of coding vulnerabilities that could be exploited is key, and many development organizations find it useful to use commercial security scanning tools to pinpoint areas in your application that may need attention.

- **Have a plan of action in case a security situation arises**
  Should your application come under attack, are you prepared? Should your data become unavailable due to a ransomware attack, or your system brought down, how will you continue to run your business operations? If sensitive data is compromised, what is your strategy for informing users or customers who may be impacted, and how do you recover? Similar to your disaster recovery plans, putting in place an action plan before a security breach takes place is an insurance policy that you cannot afford to ignore.

- **Staying up to date with the latest OpenEdge releases**
  For the current version of OpenEdge that you are operating with, be sure to apply Updates as they become available. Progress supplies both bug fixes and security patches in these Updates, and your security is only enhanced if you make use of them. In addition, as versions of OpenEdge age it becomes more difficult and at times not possible to address new security vulnerabilities. Moving to a more current release

greatly enhances your access to security patches, and provides you access to new security features that have been added to OpenEdge. You can see when OpenEdge versions will be retired by looking at the OpenEdge Life Cycle to assist you in planning the upgrade strategy for your OpenEdge applications to see new features and releases, stay current with What's New in OpenEdge.

Progress OpenEdge is Here to Help

Security should be top of mind for any business, as their data and mission critical applications need to be secure and protected from outside threats. With customer's concerns in mind, Progress OpenEdge continuously releases enhancements and updates (bug fixes and security patches) to support secure deployment across any platform, device type, and cloud. Customers not using the OpenEdge 12 series are missing out on the security, flexibility, scalability, performance, and agility necessary to stay ahead of market security demands.

By upgrading to OpenEdge 12, you can ensure that you are getting the latest and greatest for your application, ultimately protecting you from vulnerabilities that might be lurking.

OpenEdge Security Features and Services

In the OpenEdge 12.6 release, the Advanced Security package was launched. This new offering helps you to satisfy competitive demands, enhance application security, and meet regulatory compliance. This release includes hardware security module (HSM), JSON web encryption and transparent data encryption (TDE). These tools together are a superpower in application security for your mission critical apps.

Learn more

Progress OpenEdge also offers a health check service. The Progress OpenEdge Security Health Check is a Progress Professional Services engagement that enables you to assess and document the current state of your OpenEdge application so that you can implement any recommended improvements to minimize identified security vulnerabilities. The Health Check helps you have a more secure OpenEdge application and prepares you for future application extensibility, integration, and modernization.

Learn more

What are the next steps?

If you're on an older OpenEdge version, you may be taking unnecessary risk that is leaving your vulnerable to attack. By establishing a complete security strategy that includes user authentication, access controls, data encryption, network security, application security, and incident response, organizations may safeguard their OpenEdge-based systems from significant security issues.

To find out more about upgrading to the most recent version of OpenEdge, contact your Progress account executive.

Explore What's New in OpenEdge

About Progress

Worldwide Headquarters

Progress Software Corporation
15 Wayside Rd, Suite 400, Burlington, MA01803, USA
Tel: +1-800-477-6473

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software
progress_sw_

Progress®