The Data Protection Benefits of Modern Apps

Exploited software vulnerabilities are one of the most common pathways for cybersecurity breaches. In May (2020), Colonial Pipeline shut down its entire fuel distribution pipeline along the U.S east coast because of ransomware and paid almost $5 million in ransom.

In the most recent attack, at Miami-based software provider Kasaya Ltd., hackers exploited vulnerabilities in the company's virtual system administrator software to infect not only the company's corporate system but several of Kaseya's customers. The Russian hackers responsible demanded $70 million in ransom payments. With increased ransomware attacks on high-level organizations, application security and data protection are front of mind.

Modern applications are built with security in mind from the ground up and offer several data protection benefits over traditional applications that make them more resilient to global security threats. The modern application development process provides several data protection advantages. Let's look at some of them.

Security From The Ground Up

In modern application development, security issues are addressed as early as possible, resulting in more resilient and secure applications. This methodology is known as DevSecOps, which incorporates IT Security into the DevOps model. In a DevSecOps environment, security is a shared responsibility for the development, operations, and security teams.

Security and compliance objectives of the project are defined from the planning stage, rather than as an afterthought. Automation is used to integrate security into every phase of the software development process from the initial design through development, integration, testing, and delivery to ensure the application's compliance with the security standards and requirements for the project.

Using DevSecOps practices, application development teams address security issues as they occur, vastly reducing the chances of vulnerabilities in the released product.

More Secure Code

Bugs and vulnerabilities are the doorways hackers most often employ to infect an application. Modern applications use security tools, processes, and frameworks to automate and enforce security procedures in code.

Continuous integration and testing during modern application development reduce the risk of bugs and errors that cause code vulnerabilities. Continuous testing implemented throughout the

entire development process ensures that bugs and vulnerabilities are caught early and fixed as they are discovered.

In the Continuous Integration process, each code check-in triggers a build that runs unit and integration tests. Failed tests must be resolved before the code is moved to the next stage ensuring that faulty code does not make it through the other stages of development to production.

Code analytics tools and vulnerability assessments are also used to find vulnerabilities in functions, APIs, open-source libraries, and modules that could lead to data loss or improper use of data.

Integrated Security Testing

Modern application development integrates security testing into the entire software development process to ensure that the software is thoroughly tested for vulnerabilities and that the code meets security and data protection standards. Several security tests are carried out including vulnerability assessments, acceptance tests, and dynamic and penetration testing.

Vulnerability scans confirm that no security loopholes are being pushed to production and acceptance tests ensure that authentication and login features are working as they should. Dynamic testing using both automated tools and manual reviews tests the functionality of running code to analyze how the software behaves with different user permissions and during critical security failures.

Penetration testing is carried out before the software is released to find, exploit and detect vulnerabilities. The results of the security tests are analyzed and used to make the software more robust.

Continuous Monitoring

Continuous monitoring is an automated process that gives developers and operations teams visibility of security threats and compliance issues at every phase of the development process. Once the software is released, continuous monitoring processes will alert team members of any issue that arises in the production environment. It provides early warnings and feedback on the issue and alerts the relevant persons so that the issues can be fixed as soon as possible.

Continuous monitoring provides real-time data and metrics on past and current issues that teams can use to prevent potential risks and vulnerabilities and is particularly helpful for implementing security measures like incident response, threat assessment, root cause analysis, and database forensics, all of which play an important part in data protection.

Cloud-based Environments

Modern applications are built on cloud architecture, which provides several benefits for keeping data secure. With cloud-based environments, it's easier for companies to maintain complete visibility across multiple environments, whether public, private or hybrid cloud.

Application development teams can proactively monitor the environment to identify security threats, malware, or suspicious user behavior and file activity. Disaster recovery tasks such as replication, recovery, and reliable data backups are easier while encryption and data reduction services ensure sensitive data remains secure.

Cloud-based environments make it easier to define and automate security controls to define policies and govern access to aid the prevention and detection of data loss.

Modern Applications Require Modern [redacted]

Switch to data infrastructure designed for the modern era. [redacted] delivers Rapid Restore for development, test, and production workloads with up to 270TB/hr of data-recovery performance. You can rely on [redacted] solutions to meet your data protection needs with:

- Ransomware protection and built-in data replication
- Fast, relatable data backup and recovery with [redacted]
- [redacted] for true built-in active-active cluster with support for Ethernet and Fibre Channel

Leverage the benefits of modern data protection and disaster recovery solutions from [redacted].