



# Secure SDLC

Early Security Matters



# Table of Contents

**01**

Introduction

**02**

Why Start Security Early

**03**

Late Security Risks

**04**

Best Practices

**05**

Role of Managed Security Services

**06**

Cypress Data Defense

**07**

Conclusion

# Introduction

In today's fast-paced development world, security often gets overlooked. Teams are pressured to deliver apps quickly, but neglecting security can lead to costly vulnerabilities and breaches.

It's time to shift gears and embrace a proactive approach to security. Securing apps early in the development process helps identify and fix vulnerabilities before they become serious problems.

This e-book explores the benefits of early security, the risks of waiting until later, and practical strategies for integrating security seamlessly into your development workflow.

# Why Security Should Start Early in the SDLC

Securing applications early in the SDLC ensures that vulnerabilities are identified and mitigated before they become major risks.

## Reality of Application Security Today



### Vulnerabilities in the code

80% of vulnerabilities are introduced during development (Source: OWASP).



### Cost of fixing vulnerabilities

The cost of fixing vulnerabilities post-production is up to 30x higher than fixing them during development.



### Compliance Risks

Failure to comply with security regulations can result in fines and penalties.





## Late-Stage Security Implementation

### Costly and Risky

Implementing security measures after a breach is expensive and time-consuming. Financial Impact: IBM reports that the average cost of a data breach is \$4.45 million

It can also lead to loss of customer trust, data recovery challenges, and legal liabilities.

Responding to security incidents can also be very disruptive to business operations, potentially leading to downtime and lost productivity.

Operational Delays: Security issues discovered post-development can lead to release delays.



## Embed Security Early

Building security into your application development from the start is more efficient and effective.

## Best Practices



### Shift Left Security

Implement security testing from the planning phase.



### Automated Security Scanning

Integrate security tools into CI/CD pipelines.



### Developer Training

Ensure teams follow secure coding best practices.



## Role of Managed Security Services

**Expert-Led Security Testing:** Get continuous security oversight without hiring an in-house team.

**Reduced False Positives:** Avoid alert fatigue and focus on real threats.



**Scalability:** Ensure security keeps up with agile development cycles.

Business benefits can include cost savings, faster development cycles, improved customer trust, and a much stronger security posture.

# Cypress Data Defense

Cypress Data Defense provides a fully managed Secure SDLC solution that integrates seamlessly with your development process. Our EASy managed service ensures security is embedded in your SDLC from day one, reducing vulnerabilities, minimizing false positives, and helping you meet compliance requirements effortlessly.

## Why Choose Cypress Data Defense?



### Proactive Vulnerability Detection and Remediation

Tailored, proactive, managed security services to help your organization build, deploy, and maintain secure software.



### Compliance-ready Security Controls

Our experts will help you to ensure compliance with standards like PCI-DSS, HIPAA, and GDPR



### Real-time Vulnerability Detection and Remediation

We do all the work. Your team can monitor vulnerabilities real-time and remediate based on our recommendations.

Want to learn more? Schedule a free security assessment today!

Contact us - <https://cypressdefense.com/contact/>

# Conclusion

Securing your applications early in the SDLC is not optional, it's essential for your business success. It reduces development costs, accelerates time-to-market, and safeguards your reputation.

By adopting a proactive approach and investing in security from the start, you can build secure, reliable applications that protect your business and your customers.