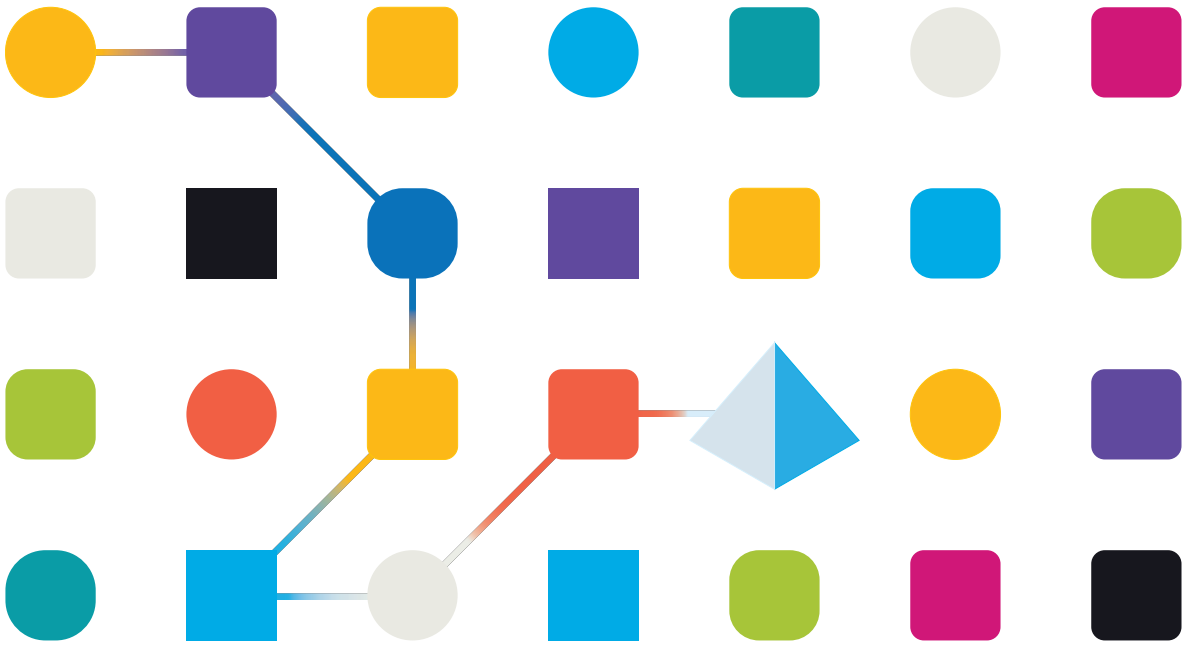
Blue Prism

Development Security

Document Revision: 1.0



Trademarks and Copyright

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.
Registered in England: Reg. No. 4260035. Tel: +44 370 879 3000. Web: www.blueprism.com

Contents

Introduction

Blue Prism® is the world's leading provider of Robotic Process Automation (RPA) software and methodologies for large scale enterprise deployments. We have customers utilizing our software to automate processes in several different vertical industries, across a large number of applications.

The company is dedicated to providing the world's best process automation software for the world's most demanding environments and has been recognized by the analyst and media community for our achievements.

Blue Prism RPA software was built in partnership with large enterprise corporations in regulated industries, specifically to address the critical requirements of scalability, flexibility, security, governance, auditability, and compliance.

This document gives an overview of our Secure Development Process (SDP). It describes the methodologies and best practices undertaken by Blue Prism during development and maintenance in order to underpin our customer's secure development requirements for software engineering.

Blue Prism ensures that its secure product developer process is fully understood by all relevant employees relating to the product development process, and that its procedures are implemented and maintained at all times. The secure product development process is periodically and systematically reviewed.

Comprehensive secure development process

Blue Prism's secure development process is a market-leading, embedded security culture, focused on delivering security excellence through four key principles:

- Education – Providing up-to-date knowledge, information, and training to the development team.
- Evaluation – Regular reviews of our products using industry standard frameworks and security tools.
- Elimination – Remove potential threats through the evaluation of standards, compliance, and performance.
- Evolution – Continued improvement of our security program, ensuring alignment with our product technologies and by reacting effectively to new and emerging threats.

Blue Prism secure development is based on OWASP ASVS, ISO 27034 and GDPR Article 25 standards and practices.

Education

Blue Prism recognizes the importance of providing high quality, engaging education to its development team, beginning during their induction and continuing regularly throughout their employment.

Interactive training and development for secure coding

Blue Prism partners with a world-leading educational platform that specializes in providing engaging and informative content. The platform assists organizations in achieving compliance requirement targets mandated by information security frameworks and standards such as:

- NIST
- PCI
- OWASP
- ISO 27001

All Blue Prism developers undergo initial and ongoing training and certification, which includes:

- A four-part interactive security training course included in their induction.
- Four tiers of ongoing security training, with every developer required to reach a minimum of level one.
- Bespoke courses designed to cover specific subjects of interest.
- Quarterly reviews, using the metrics taken from tournaments to address areas of low scoring.
- Education is further supplemented by:
  - Quarterly tournaments for all developers to take part in.
  - Micro learning modules that are automatically applied to development features.
  - Access to a guided offensive security testing lab to aid understanding of the exploitation of the OWASP top ten threats.

Evaluation

The evaluation principle contains components that have been put in place to review the effectiveness of the education principle, raise awareness, protect the business, and continually monitor performance.

Threat modelling

Blue Prism has adopted a subject matter-based threat modelling methodology, which provides a framework to understand and visualize threats that may apply to the product or the feature they are implementing. This enables them to:

- Use a combination of STRIDE and bespoke, in-house threat modelling techniques.
- Identify assets, threats, and controls.
- Raise awareness of potential issues earlier in the development process.
- Speed up software delivery and response times.
- Assess each individual software feature to create a threat model.

Dedicated application security team

A dedicated team of application security engineers are on hand to support the Blue Prism development teams in the following ways:

- Each Blue Prism development team has a dedicated primary and secondary security engineer.
- Engineers raise awareness and promote understanding of development security issues.
- Help identify and resolve security issues during refinement stage as part of the shift left initiative.
- Coupling engineers to development teams means experience and knowledge is fostered and specific to the team.
- Engineers keep up-to-date with relevant changes and developments in the security field and relay these to the development teams.

Static code analysis (SAST)

The source code of Blue Prism products is scanned using a variety of best-of-breed security tools to ensure compliance and code quality, and includes:

- Scans using multiple “best of breed” SAST tools.
- Over 450 different checks are applied to the entire codebase, with hundreds of scans being performed each month.
- Automated pipeline scans are performed overnight.
- Manual, on-demand scans are available when required.
- Control gates that prevent any issues from being committed to the code base.
- Complete SAST scanning coverage of the entire software portfolio.

- Scanning policy includes checks from the following security standards:
  - NIST
  - OWASP Top 10
  - SANS Top 25
  - PCI
  - HIPAA
  - FISMA
  - STIG
- Version-specific compliance reports that support our release procedures.

Software composition analysis (SCA)

All open-source dependencies are identified and evaluated using a market-leading dependency and license management tool, which provides:

- In-depth coverage dependency checking – direct and transitive software dependencies are analyzed.
- Overnight, automated pipeline and manual on-demand scans – performing more than 20,000 scans per month.
- Complete coverage of the entire software portfolio, including:
  - The implementation of open source components and license locks, preventing risks from entering our main codebases.
  - License detection and monitoring to ensure we are only using third-party dependencies that we are legally able to. A comprehensive list of third-party dependencies is provided with each release.
- Monitoring of current and previous releases of products for newly disclosed vulnerabilities. We monitor over 900 software projects and over 4000 software dependencies.

Automated dynamic security testing (DAST)

Web-based products are subjected to multiple dynamic security tests to ensure that the products operate in a secure and robust manner, which allows:

- Tests to be initiated on demand in the CI pipeline.
- A combination of frameworks, custom tools, and scripts to return targeted results.
- Validation of our secure development process.

Manual penetration testing

Manual penetration testing is performed as a final control against our SaaS products to ensure that our products are not vulnerable to complex exploitation techniques. This process includes:

- Rigorous testing of web-based products prior to release.
- Utilization of multiple consultants to ensure varied approaches and results.
- Targeted testing of security-specific features carried out on all on-premises products.

Elimination

The elimination principle underpins our vulnerability approach by applying the outcomes of evaluations to allow us to aim for:

- The removal of all reported high, medium and low severity threats that have not been mitigated prior to release.
- The removal of all exploitable third-party threats that have not been mitigated prior to release.

Evolution

Blue Prism is committed to a security program that evolves in line with our product technologies and new and emerging threats meaning:

- Our process tools and policies are under constant review to ensure we continue to deliver Security Excellence.
- We have a multi-vendor approach, allowing us to select the most appropriate tools from the market-leading vendors.

Information and platform security

Corporate information security

Blue Prism has a comprehensive information security strategy and documented policies across several areas, such as employee vetting, physical asset management, logical security, and access control to electronic devices, use of personal equipment (for example, mobile devices), etc.

Blue Prism takes network security very seriously and adds further controls to mitigate the risk of viruses or malware breaching any aspect of the network. There are several policies and controls in place to assure this that govern corporate security, physical site access, logical and remote network access, antivirus software, and email scanning processes.

Security and vulnerability assessments are carried out periodically, which validate the appropriateness of the controls that are in place. These include input validation and sanitization; authentication and access control; audit; and management of sensitive information. Blue Prism is ISO 27001 compliant throughout the organization. Blue Prism corporate information security is led and overseen by our IT Services organization.

Development platform security

Development on physical devices

Each physical development machine is secured by centrally enforced operating system controls, which administer high-quality security measures, including full disk encryption, anti-virus software, and network firewalls.

Provision and maintenance of centralized development and test environments

Centralized development and test systems are managed through central access control policy. Security patches are validated and applied to the operating systems. Microsoft patches are made available to Blue Prism through the Microsoft Insider program.

Access controls of centralized test environments

Direct or native access to the centralized test environments is not typically permitted. Access is instead offered through a VPN or secured web socket proxy provided only over HTTPS (TLS), with individual user accounts managed within the support system's version control repository and a multi-factor authentication process. Direct access is only permitted and available to a small number of authorized administrators for diagnostics and troubleshooting purposes.

All test environments are protected by file system permissions and operating system access controls, which are managed centrally via a configuration management system.

Software data security and code integrity

How do we ensure anonymized test data?

Our test data is refreshed to baseline test data each night before test automations take place. There is both physical and logic separation between production and test environments. No customer production data is held at Blue Prism. Any data from customers required for testing purposes is sanitized and anonymized to ensure all content is non-sensitive.

How do we store code safely?

Blue Prism uses GIT, which is the industry-standard source code repository. Individual development team members are provided access to development/test systems according to their role. Role-based access control is realized with a combination of systems, including GitLab, HTTPS, and SSH authentication.

Specific access to Blue Prism source code is further secured through 2048-bit RSA-based SSH key pairs.

How do we ensure release integrity and validation?

All software releases are built and verified in an automated, secure, clean room environment and signed with a code signing certificate within that same environment. All servers run up-to-date anti-virus software.

Following this, automated and manual verification takes place alongside automated testing across a wide range of platforms and configurations. When a release is approved, secure publication to the Blue Prism customer and partner portal is again automatically handled, leaving an audit trail of the entire release life cycle.

The source code and build scripts can only be obtained over an SSH connection, with ECDSA keys verifying the remote server to ensure the integrity of the transferred code.

Blue Prism use a code signing certificate to protect against accidental or malicious alteration of the application files. The code signing certificate is secured with the source code and is not available outside that environment, assuring the integrity of the source and any installer signed with it.