Software applications have transformed enterprises of all sizes and across all industries — increasing efficiency, reducing redundancy, and driving innovation. However, these applications while streamlining organizational processes are also exposing enterprises to new risks. According to research conducted by several private and government agencies, more than half of all breaches are a result of an attack on the application layer. Yet, less than a tenth of all organizations verify the security of their business critical applications during development and in operation, and up to twenty-five percent of organizations don't have an accurate count of the applications in their ecosystem (source: SANS).

Modern enterprises need a new way of managing application security. One that encourages and promotes all the benefits that rapid investment in software can deliver to an organization, while ensuring a high measure of security and reliability. Such a framework should allow an organization to leverage all the processes available at its disposal to better monitor and evaluate software application security.

**Top 10 vulnerability categories and severity distribution**

**Key Risk Indicators**
- 86% of applications have weak security controls
- 74% of vulnerabilities are due to inadequate input validation
- 27% use no open source components
security within its ecosystem uniformly and continuously. It should provide a risk-first perspective to application development without hindering or slowing the pace of innovation. It should arm executives and security professionals with immediate visibility into the state of their virtual environment while empowering developers and risk professionals to achieve demonstrable improvement in the security posture of the enterprise. Brinqa Application Security Risk Management aims to deliver such a framework.

**Challenges**

While Application Security and Risk Management are firmly on the radar for most forward thinking security teams and executives, research by private and government agencies into the state of preparedness of most enterprises paints a stark picture. The gap between the current and desired states is not so much due to a lack of awareness or investment on part of organizations as it is due to the inherent complexity of the problem.

The spectrum of software applications in a typical medium or large sized organization is highly diverse. This is due to differences in development environments and methodologies, architecture (Web applications, Mobile applications, API only etc.), source (internally developed vs. externally provisioned) and business-criticality. Different development environments and frameworks may require distinct security controls to monitor and report the same type of risk information. Additionally, application security systems tend to evaluate a specific aspect of software applications (Static Code Analysis, Dynamic Code Analysis, Web Applications, Pen Testing, Open Source Vulnerabilities, etc.) and to cover every aspect, an organization will most likely have to acquire tools from different vendors, each with its own rating mechanism and terminology.

The security visibility into applications developed by third parties is often very different from that available for internally developed applications. Responsibility of application security programs also varies greatly among organizations with risk/compliance, software assurance groups, software development groups, IT and security roles all featuring as primary owners.

These challenges often result in a fragmented application security program with security and risk organizations typically managing a distinct initiative to monitor and evaluate risk while development organizations implement and integrate their own security measures into the development process. Procedures to manage the development process based on risk evaluation are rare and where they exist, they are often manual and disruptive. Often times very rudimentary or no security measures are in place for externally provisioned applications, exposing the organization to unknown risks acquired along with software.

**Brinqa Solution**

Brinqa Application Security Risk Management addresses the challenges to true Application Security and Governance by focusing on completeness, relevance and accuracy to promote secure applications. A single critical application left unevaluated can result in a catastrophic breach. To have true security, not only must all applications be accounted for and monitored, it is equally important to have a clear representation of the impact and relevance of each application to the organization.

At the core of the solution is a dynamic risk model pre-configured to ingest and represent risk information from most application security systems. By allowing program owners to select the most appropriate control monitoring system for any aspect of application security and by combining systems from different vendors into the same rating platform seamlessly, the solution ensures the most relevant and accurate risk representation. This mechanism also provides a ready template for which security controls are required to address every aspect of application security and highlights gaps in coverage of individual applications or the overall program. Advanced analytics provide detailed reporting and diagnostics. Comprehensive governance features provide risk-based lifecycle management for applications as well as any identified gaps and threats. By facilitating a risk based ‘gate-keeper’ approach to SDLC, the solution defines unambiguous risk and security goals for each step of the application development process, providing developers with clear directions about which gaps must be addressed to meet these goals, making ‘Application Development’ synonymous with ‘Secure Application Development’.

**Build an Authoritative Application Repository**

The most rudimentary step for any application security program is also often the most lacking and potentially harmful for most organizations. In a study conducted by SANS, 28% of the respondents did not know how many applications their organizations use and maintain. Enterprises struggle to maintain a complete and accurate repository of all applications in their environment. Applications are often developed by distinct teams with their own change and project management systems. Often, there is no structured, uniform process for on-boarding externally acquired applications. Mergers, acquisitions and subsidiaries further complicate the picture. The first step for establishing an effective Application Security and Governance program is to identify all sources within the organization — Engineering, Technology Relationships, Procurement, IT, etc. — that may identify a distinct application. Automated measures must then be set up to ensure that these disparate sources of application information are regularly polled and the results reflected into a
Leveraged using Brinqa data connectors to common asset management, CMDB or proprietary systems to populate the golden source. This ensures that an accurate application repository for risk evaluation is maintained at all times.

Establish the Business Context

Software applications form a wide range, from mission-critical applications central to the business to applications supporting trivial non-essential functions. An effective application risk management program factors this distinction into its risk evaluation methodology to ensure that risks and threats are rated based on business impact and not merely on security or technical requirements. Brinqa Application Security Risk Management solution promotes this by providing features in the application repository template to capture, maintain and represent this information. Alternatively, inherent risk assessments may be conducted to evaluate business relevance and impact if this information is not currently maintained or established in the organization.

Implement a Risk Evaluation Model

The driving engine of the Brinqa Application Security Risk Management solution is a risk model designed using the Brinqa Risk Analytics Platform. The model provides the mechanism to easily integrate, normalize, contextualize and evaluate security applications. It also highlights gaps in coverage, either in the form of missing controls or unevaluated applications.

Enforce SDLC Governance

Defects, bugs and logic flaws introduced during the application development process are consistently discovered to be the primary causes of exploited software vulnerabilities. There is substantial research that supports the idea that most vulnerabilities stem from a fairly small number of harmful development practices and programming errors. Equally substantial is technical literature focused on addressing the common errors and integrating secure coding practices into daily software development. Despite all this research and knowledge, most development organizations fail to introduce sufficient security checks and practices in the development process.

The main reason for this severe security lapse is the lack of a governance process and absence of risk based goals prescribed across the enterprise. Development organizations that follow some manner of security checks as part of their development process often report ad hoc measures that vary from team to team. This lapse often results in a significantly higher cost to fix issues during the deployment or maintenance phase. Research indicates that fixing software vulnerability during post-production as opposed to during testing incurs a cost multiplier of up to 7x.
Brinqa Application Security Risk Management solution allows organizations to put a uniform risk-based application development process in place without any detrimental impact to existing development processes. A risk-based ‘Gate-Keeper’ methodology ensures that relevant security inputs are evaluated at every step of the application development process and products are promoted in readiness only when the unambiguous, quantitative risk goals are met.

Development teams can continue to use their security and quality evaluation systems and configure them to deliver results to the application risk evaluation model automatically or manually. The solution enables development organizations to create and enforce consistent quality and security rules to be followed by disparate teams irrespective of their development frameworks and methodology.

Identify Issues and Plan for Remediation

Gaps and threats identified during any step of the application development or risk evaluation process may be converted into issues to be tracked for remediation. The integrated Brinqa Risk and Control Framework provides clear guidelines to developers or application owners about the actions that may be taken to remediate a problem. The controls framework also empowers program owners to demonstrate compliance with industry standards and regulations such as PCI, SOX, FISMA etc.

Brinqa Application Security Risk Management enables automatic issue creation and consolidation based on rules as well as manual issue creation on an ad hoc basis. Brinqa Risk Matrices enable predictive remediation planning by simulating granular remediation and analyzing the corresponding quantitative risk impact, providing a range of remediation strategies – from remediation of all identified issues to the minimum remediation effort required to meet SDLC or risk-monitoring goals.

Analyze and Communicate Risk

Brinqa Application Security Management Risk solution comes with a wide variety of application and business hierarchy based reports targeted for a diverse audience ranging from C-level executives to engineering managers. Reports based on products, line-of-business, organizational or reporting hierarchy provide a clear view into which parts of the organizations are most at risk. Threat and vulnerability based reports highlight the most critical and exploited issues and guide security and development teams towards remediation efforts that deliver most benefit to the organization. Risk trends across relevant risk areas promote understanding of the organization's software footprint and applications that impact it.

Advanced filtering and searching features make it easy for risk professionals and engineering managers to analyze and correlate application and risk data across their domains. Diagnostic analytics allow for in-depth investigation of the root-causes, patterns and impact associated with identified gaps and threats. Risk-model-graph exploration enables security professionals to identify at-risk applications and resources based on information flow and access patterns and help them implement effective precautionary measures and policies.

Conclusion

Brinqa Application Security Risk Management delivers a framework for comprehensive and continued security assurance of an organization's software ecosystem. By promoting secure application development through well-defined, risk-oriented SDLC governance, IT organizations can strengthen their application security posture from the inside out, building applications with a demonstrable focus on security during every step of the development process. Accurate and complete asset inventory, augmented by business context and supported by measures to integrate and evaluate third-party applications provide the most comprehensive picture of an organization's software footprint. Advanced remediation planning and detailed risk reporting ensure that risk and security professionals have access to real-time insights and definitive action plans to constantly improve the organization's security posture.

Visit www.brinqa.com or email sales@brinqa.com for more information.