SERENA™

Centralized Secure Vault with Serena Dimensions CM

A single artifact repository for development, quality and operations

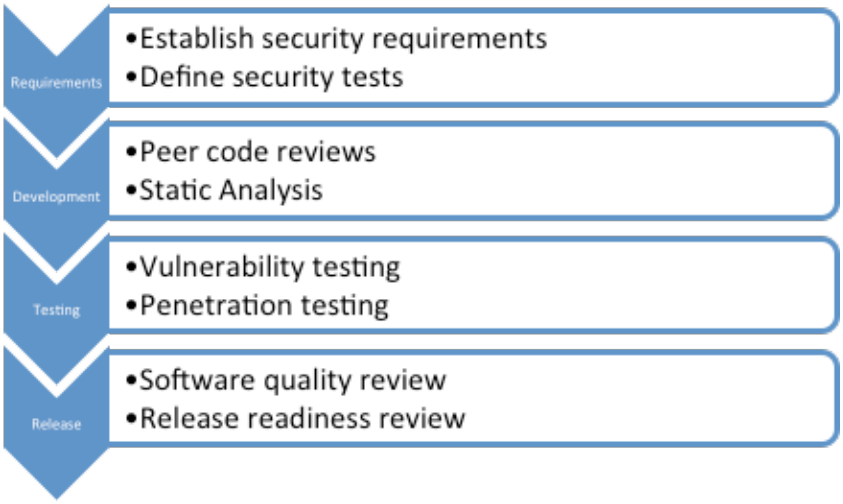
SOLUTION BRIEF

> *We're a bank not a startup, and we need to be using appropriate tools to ensure the integrity and security of change, not tools that add to a developers resume. We don't want to be the next big headline!*
>
> *SVP, QA at Large Financial Services firm*

Why Security and Software engineering

Most application development teams align to the software engineering principles that follow a standardized SDLC (Software Development Lifecycle), but rarely consider or adopt a disciplined approach to security within the SDLC. With the increasing volume and velocity of application development, the broadening security concerns surrounding distributed version control (DVCS), and the increasing security attacks at the application layer have made organizations realize the critical importance of security in the definition, development and delivery of software applications.

Security as a process must be incorporated into the SDLC phases, with the goal of identifying and remediating security risks well before deployment into production. For example:



The reality of today's SDLC

While many organizations have historically documented their SDLC policies and practices within a series of stages, the push to speed up the pace of delivery is increasing the focus on agile and DevOps practices.

Key disciplines of an SDLC include:

- Software requirements definition and management
- Software change and configuration management
- Software project planning, with an increasing focus on agile planning
- Work item management
- Quality management, including defect management
- Release management

Additional capabilities have included reporting, workflow, collaboration and integration.

Not surprisingly, current regulatory standards and requirements have increasingly identified the need for application security. Specifically, organizations need to determine whether application security has to be considered at the pre or post code/development phase or throughout the SDLC process of application development and delivery.

Evolution of the SDLC

Agile and DevOps is having a profound impact on the SLDC and specifically the policies and practices of planning, development, testing and releasing software applications.

As the pressure to release applications at greater velocity grows, so has the freedom and empowerment experienced by development teams. At a consequence, there is a growing risk of unauthorized, unexpected or insecure changes or access to internal systems, customer facing apps and perhaps more worryingly, sensitive IP data. In addition, the rush to explore the value of containers has to be balanced by security considerations and safeguards.

However, the fact that many tools are open source, including Distributed Version Control Systems (DVCS) has led to a proliferation of software repositories in use without any coordination or wider considerations for management, visibility and security.

Centralized management practices, evolved from a leading SCCM tool such as Dimensions CM, are needed to match the freedom of DVCS practice to the discipline required for enterprise scalability, performance, security and integration in supporting large-scale secure and safe enterprise deployments.

Managing risk is an increasingly important role of CIOs and IT executives. While risk management includes securing corporate systems, networks, and data, ensuring availability of systems and services, planning for disaster recovery and business continuity, complying with regulations and license agreements, and protecting the organization against an array of threats - this must now include critical business and custom applications.

Centralized Secure Vault

Within any enterprise, there may be small teams with good process discipline and limited requirements for security and immutable audit history that may be using DVCS.

Larger teams are more concerned with coordinating the evolution of downstream test and release processes and often need support for sophisticated change and release management.

The enterprise's needs for quality, visibility, security and consistency are critical for highly regulated companies, and for those with with a complex software applications portfolio.

Enterprise groups, particularly those with DVCS, are increasingly uncomfortable at the possibility for loss of IP through misappropriation of source code.

For many years, there has been a concept in the SDLC of a "gold" vault, a secure and highly inspected and validated repository of application code that is being built, tested and prepared for release. Given the number of disparate source code repositories and 3rd party software that comprises today's applications, and the growing complexity surrounding release preparation and readiness, this is now a MUST HAVE.

A secure vault represents the "single version of the truth". Development can be challenged when consuming software components and deliveries from different teams and source code repositories. Operations has long been concerned with the innumerable changes entering the production environment from too many different paths. Quality, reliability and transparency need to be the same irrespective the size, complexity or origin of the changes. A single secure vault is the essential first step. Development teams check their code into

the common vault where builds are assembled and a battery of automated tests are applied, ensuring both rapid feedback to development, and aggregated KPI Metrics that indicate the software quality index and release readiness. This ensures a common minimum standard of quality is always maintained, so essential for successful deployment automation.

Providing enterprise wide visibility, security and governance, Dimensions CM has long been prized by change and release management teams and often implemented as a secure vault for both development and operations teams.

Software risks impacting quality are currently at the heart of the DevOps Shift-Left practice and Dimensions CM with its secure vault provides a framework for incorporating security into all phases of the SDLC.

Security attributes of Serena Dimensions CM/Vault

Security Attribute	Description	Dimensions CM
Confidentiality	Limiting information access and disclosure to authorized users, and preventing access by or disclosure to unauthorized users.	Granular role-based permissions model enables or restricts access to, and visibility of software components or code, ensuring separation of concerns.
Integrity	Trustworthiness of information resources. Specifically the concept of data integrity ensuring that data has not been changed inappropriately, whether by accident or corrupt activity. Also the concept of origin or source integrity ensuring the authorized user is not an imposter.	Dimensions CM maintains the integrity of history and every change, recording the “who, what, when and why” in a comprehensive and tamper proof audit trail.
Availability	Information system that is not available when you need it is almost as bad as none at all.	Dimensions CM supports both on-line and off-line working, and supports atomic commit operations. Dimensions CM is architected to support a variety of Enterprise needs, supporting high scalability and availability.
Possession	Ownership or control of information, as distinct from confidentiality.	Dimensions CM maintains strict ownership and does not allow impersonation.
Coding standards	Recommended coding styles, practices and methods.	Dimensions CM Automates on Check-in via Continuous Inspection tool chain.
Peer Code Review	Examination of source code.	Dimensions CM automates collaborative Peer Code Review on Check-in or Delivery.
Static Analysis	Analyzes code reporting findings.	Dimensions CM Automates on Check-in via Continuous Inspection tool chain.
Web Vulnerability	Analyzes code reporting security vulnerabilities.	Dimensions CM automates vulnerability checks on Check-in or Delivery.

Summary

Serena Dimensions CM is a highly scalable and secure SCCM solution supporting the needs of development, and a critical centralized secure vault supporting the key DevOps practices of version everything, continuous inspection and automation.

Serena Dimensions CM provides an optimized development experience for both traditional and agile teams, and co-exists with popular open source versioning tools such as SVN and Git. It's secure vault integrates a centralized continuous inspection toolchain, assuring a high degree of release readiness for successful deployments while ensuring confidentiality, security and integrity.

Leveraging Dimensions CM's integrated continuous inspection toolchain dramatically improves code quality and development productivity while reducing costs of re-work.

A secure vault removes the headache associated with repository sprawl and maintains a unified repository of application code streamlining release preparation and continuous inspection and enabling safe and secure deployment automation.

SERENA™

Website: www.serena.com | Phone: 1-800-457-3736 | Email: info@serena.com

Serena Software is the largest independent Application Lifecycle Management (ALM) vendor with more than 2,500 enterprise customers. Serena helps the highly regulated large enterprise move fast without breaking things – increasing velocity of the software development lifecycle while enhancing security, compliance, and performance. More information is available at www.serena.com.