Help protect data from theft with end-to-end application security.

Highlights

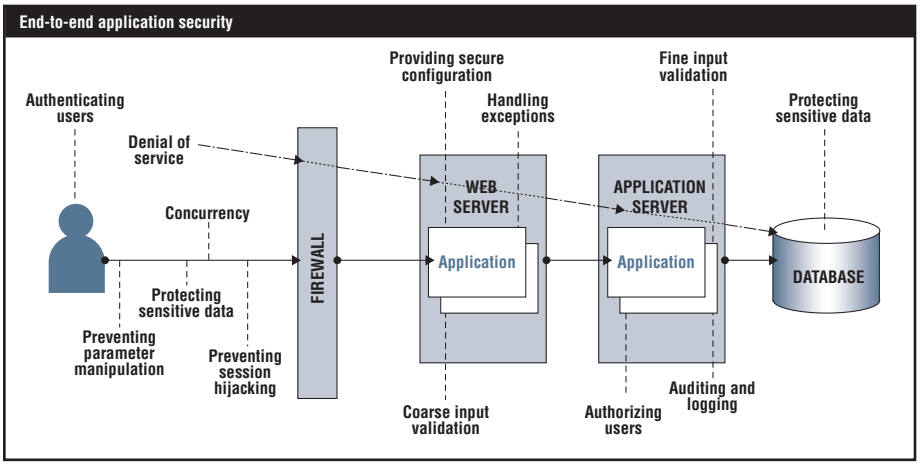
- Find application vulnerabilities using intelligently targeted security testing tools with reports that address specific industry standards
- Incorporate Web application testing and reporting into existing software development processes to help optimize vulnerability identification and remediation
- Leverage Web-based single sign-on capabilities for applications throughout your enterprise
- Allow only authorized users to access applications during run time
- Protect development assets from unauthorized access, change or deployment

In the past, IT resources for addressing security vulnerabilities nearly always focused on the network or operating system. But today, the robust Web applications used to conduct significant business transactions potentially can expose organizations to great risk. This is because of the Web applications' inherent lack of security and nearly endless number of entry points, from forms to query strings to cookies to header fields. If a malicious individual exploits a vulnerability in a Web application that is trusted by the database, other applications, the operating system and the network, then the entire system may be compromised. Furthermore, anytime, anywhere access to Web applications makes it more important than ever to help ensure that user access rights are accurate and up to date, to help protect sensitive content from inappropriate access and use. Additionally, the increase in Web services — leveraging heterogeneous applications — used to execute business transactions makes security more complex and difficult to maintain. These Web services often have a number of applications that share different security attributes and do not seamlessly integrate with one another.

Faced with these conditions, application security should be approached in an end-to-end life-cycle fashion, from the moment an application or Web service is designed to its continuous monitoring in production. To that end, software developers and IT operations

staff should collaborate. Increasingly, IT is turning to software developers to help address vulnerabilities as part of the quality management process, because if vulnerabilities remain unresolved, they can become much more difficult and costly to fix. IT operations staff require tools to help them understand and manage the aspects of application security they can handle, to keep development staff focused on innovative initiatives. As applications move into production, consistently enforcing who can gain access to the application can be costly, inefficient and sometimes ineffective if done individually for each application. Applications, especially when core to financial processes, also should be closely monitored and reports generated that summarize use and vulnerabilities for compliance purposes.

To address these requirements, IBM offers a broad portfolio of security solutions that help organizations manage application security throughout the life cycle of that application. These solutions can identify and quickly address vulnerabilities. Taking a preemptive approach to application security is one of several modular entry points into IBM security solutions, which help customers establish effective risk management strategies to manage and secure business information and technology assets,



anticipate vulnerabilities and risk, and maintain timely access to information. IBM security solutions help organizations align technology with business priorities — allowing you to redirect resources that might otherwise be dedicated to resolving security problems toward innovative initiatives that deliver substantial value to the business.

IBM offerings help your organization embed application security from design to production. Prior to deployment, applications are tested for unknown vulnerabilities to help ensure that at run time, only authorized users have the appropriate access to applications. Because IBM offerings help both developers and IT operations staff, they give you the flexibility to address application security in the ways that make the most sense for your enterprise. By building security into applications throughout the life cycle, you can proactively identify and rapidly resolve potential security problems before they significantly damage your business.

Test applications for unknown vulnerabilities

It is certainly important to look for known vulnerabilities and resolve them quickly. But usually, those vulnerabilities are in the supporting infrastructure. When thinking about application security, the pressing — and more difficult — challenge is to find *unknown* vulnerabilities. How does the code that your developers write introduce vulnerabilities that you had never considered before? Do you know if your packaged software applications that you have purchased and deployed have been properly secured?

Examples of the kinds of simulated hacker attacks that Rational AppScan software runs include the following:

- Cross-site scripting
- HTTP response splitting
- Parameter tampering
- Hidden-field manipulation
- Backdoor and debug options
- Stealth commanding
- Forceful browsing
- Application buffer overflow
- Cookie poisoning
- Third-party misconfiguration
- Known vulnerabilities
- HTTP attacks
- SQL injections
- Suspicious content
- XML/SOAP tests
- Content spoofing
- Lightweight Directory Access Protocol (LDAP) injection
- XPath injection
- Session fixation

IBM Web application security software, including IBM Rational® AppScan, specializes in giving software development teams — especially those with little application security expertise — tools to identify unknown vulnerabilities as part of the quality management process. Developers can use both automated and manual capabilities to explore applications and understand all their interfaces and inputs — all the potential "attack surfaces." Rational AppScan software features an adaptive test process that intelligently mimics human logic to adapt the testing phase to each application.

Once Rational AppScan software understands the specific parameters of the application and its attack surfaces, it can perform the relevant in-depth tests. In that way, the software's patented scan engine helps optimize the performance and accuracy of scanning.

To help your staff understand and respond to the information obtained from application testing, Rational AppScan software maps its tests and generates its reports using the Web Security Threat Classification developed by the Web Application Security Consortium (WASC) and other industry standards such as the Open Web Application Security Project (OWASP).* This helps your developers, IT operations staff and others share a common language when discussing application security issues. WASC identifies six major threat areas:

- Authentication
- Authorization
- Client-side attacks
- Command execution
- Information disclosure
- Logical attacks

In addition to performing intelligently targeted, in-depth testing, Rational AppScan software provides reports with information that your staff can act on — clear recommendations about how to fix vulnerabilities. The software seamlessly integrates with leading quality assurance tools, development environments and code-scanning devices from IBM and other leading vendors, such as IBM Rational Quality Management manual, functional and performance testing solutions; Mercury Quality Center; JBuilder; Microsoft® Visual Studio®; and Fortify. Consequently, security testing and remediation can easily become part of your existing software development processes.

Rational AppScan software is available in both practitioner and enterprise editions. For those that need to scale

their internal security teams or those with little or no security expertise in house, Rational software also offers — as a service — enterprise-class vulnerability assessment software for Web-based, multiuser applications.

To further help you protect the development environment, turn to IBM Rational Change and Release Management software. These offerings help you control access to and use of the valuable development assets that your organization creates. Rational Change and Release Management software helps you:

- Only allow authorized development personnel to access development assets.
- Track changes to development assets by authorized people so that you can audit development work.
- Only enable authorized development assets to be deployed, so that only those components that have been fully tested and meet your current requirements are available in production environments.

Control run time and federated access to applications with policy-based solutions

In conjunction with efforts to minimize the vulnerabilities within the application, an organization should also ensure that only authorized users are able to access the application. Traditionally, access control was coded into each individual application, but the result was a patchwork system of controls that introduced more vulnerabilities and became increasingly costly to manage.

IBM access management software, including IBM Tivoli® Access Manager for e-business and IBM Tivoli Federated Identity Manager, helps organizations centralize access management across their wide variety of applications and services.

To help you maximize application security, IBM access management software assists in two particular ways. First, the software enables Web-based single sign-on and centralized, auditable access control to all of your applications. Tivoli Access Manager for e-business offers single sign-on at the run-time level. By consolidating the multiple application-specific sign-ons required by individual applications (as well as IT infrastructure components), you can minimize the security exposures and the various combinations of passwords and user identities that frustrate users — and burden the administrators who manage them manually.

Tivoli access management software enables you to deliver application security to — and supports enterprise single sign-on for — applications such as:

- BroadVision One to One
- BusinessObjects
- Centric Product Innovation
- Citrix Presentation Server
- Documentum WebTop
- Documentum eRoom
- IBM Content Manager
- IBM FileNet P8
- IBM Host on Demand
- IBM Host Publisher
- IBM Lotus® Domino®
- IBM Lotus Notes®
- IBM Lotus Quickr™
- IBM Lotus Sametime®
- Intelliden R-Series
- Kintana (Mercury Interactive)
- Microsoft Exchange (OWA)
- Microsoft SharePoint® Portal
- Microsoft SharePoint Services
- OpenConnect WebConnect
- Oracle 10*g*
- Oracle Application Server
- PeopleSoft PeopleTools
- Rocksteady NSA
- SAP AS Java
- SAP AS ABAP
- SAP Netweaver Portal
- Secur-IT C-Man
- Secur-IT D-Man
- Siebel
- Sourcefire ISM
- Vasco Digipass (via C-Man)

Furthermore, Tivoli Federated Identity Manager helps you extend single sign-on across Web services. To realize the flexibility and stability benefits of a service oriented architecture (SOA), Web services should only contain business logic. Other infrastructure issues — including user identities and access management — should be handled by SOA middleware. Tivoli Federated Identity Manager establishes a trust management framework by passing user identities between domains according to your policies and the underlying technologies that you and your trusted partners share. As a result, end users can log on once using a Web browser and take advantage of federated single sign-on to connect seamlessly with services from other domains. Additionally, any heterogeneous applications utilized to deliver a Web service will leverage this trust management framework and help ensure that consistent security is maintained throughout.

The second way in which IBM access management software helps optimize application security is through authorization management capabilities. Tivoli Access Manager for e-business manages user entitlements in alignment with your corporate security policy. Because your staff does not need to code security into each application, you help minimize development, deployment and administration costs. Furthermore, since users can be assigned to groups and given specific access permissions, you will be in a position to enforce compliance. Both Tivoli Federated Identity Manager and Tivoli Access Manager for e-business can provide coarse-grained authorization. Federation also extends this authorization by managing user identities from outside your organization.

Tivoli Compliance Insight Manager enables you to monitor ongoing use of the application, compare it to acceptable use policy and report on it relative to key controls for compliance purposes. Dashboard and reporting capabilities of Tivoli Compliance Insight Manager translate log data to understandable language and perform privileged user monitoring across a wide variety of systems and applications.

For more information

IBM application security solutions help development and IT operations staff work together — efficiently and effectively — to build application security into software from its inception and to manage it consistently throughout its life cycle.

For more information about how your organization can use IBM security solutions to help optimize application security — or to find the IBM security solutions entry point that is right for your organization — contact your IBM representative or IBM Business Partner, or visit **ibm.com**/itsolutions/security

About IBM solutions for enabling IT governance and risk management

IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit **ibm.com**/itsolutions/governance

IBM Corporation
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
9-07

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

*Available online at webappsec.org/projects/threat

GMS10438-USEN-00