New Rowley

TC: CO1018

December 2006
Version 1.0

The Challenge of Securing SOA

Organizations continue to invest in service-oriented architecture (SOA), including the adoption of the Extensible Markup Language (XML) and Web service technology, as a cornerstone of their modern computing infrastructure. Why? Because the benefits of adopting SOA include:

- **Increased business agility.** SOA solutions enable an organization to quickly develop the underlying technology needed to support new business initiatives.
- **Enterprisewide software reuse.** SOA solutions allow IT to leverage the software and components that they have paid for, developed, and tested.
- **Incremental rollouts.** SOA solutions don't require a massive upfront, multiyear commitment to see a reasonable return on investment (ROI).
- **Vendor-neutral standards.** SOA technology relies on a variety of open standards that organizations can use and enhance.

However, many of these benefits, such as the relatively easy reuse of software assets, create new security challenges. The good news for organizations is that IT departments can invest and roll out SOA security processes and solutions incrementally – like SOA solutions themselves – based on organizational priorities. This ensures that SOA benefits will not be overwhelmed by the effort and cost of implementing the related security initiatives.

Critical aspects of SOA security

1. **SOA creates new security challenges**
   IT will need to invest in new SOA-centric security initiatives
2. **Security efforts shouldn't swamp benefits**
   IT will need to prioritize risks and incrementally roll out SOA security
3. **IT can choose from security best practices**
   Organizations can implement a variety of best practices that match security priorities

The goal of this report is to: 1) discuss how the adoption of SOA solutions creates specific new security challenges for organizations; 2) emphasize that SOA security efforts should not overwhelm SOA ROI; and 3) highlight a series of SOA security best practices. The final section discusses IBM offerings that organizations can use to support SOA security best practices.

SOA ADOTPION CREATES NEW SECURITY CHALLENGES

Organizations – private, public, and government – are increasingly rolling out SOA-based solutions, despite the absence of a coherent or feasible security strategy. But to begin the process of creating and implementing an organizationwide strategy, IT must first recognize that SOA solutions create new security challenges. SOA, for all of its benefits, changes the rules of the security game. Its very success entails exposing a vast amount of data and systems to a new set of internal and external users.

The root of security issues: Evolving standards and software reuse

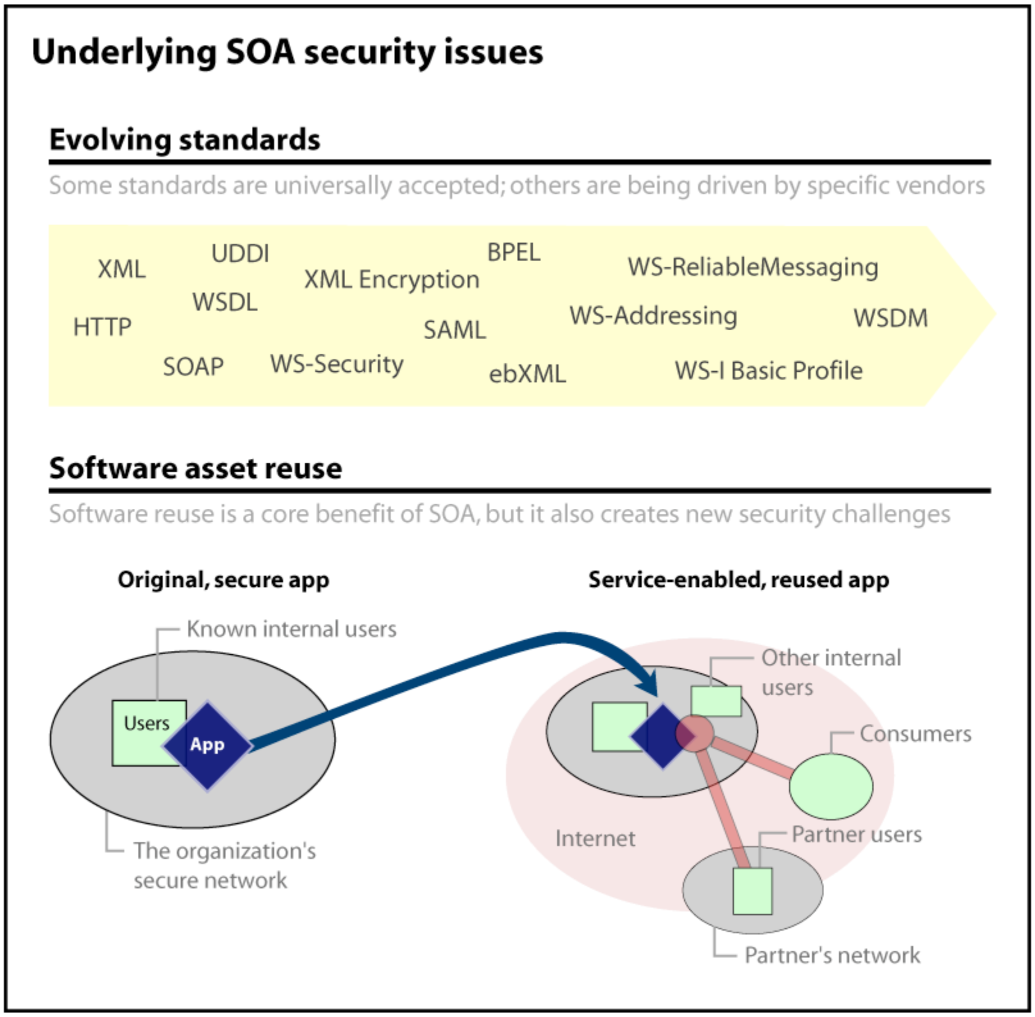
While SOA, in many ways, is simply an evolution of various distributed computing concepts and technologies, the architecture does create new security risks based on two core issues.

- **Evolving standards for data access and transmission.** Web and Web service standards, such as HTTP, XML, and SOAP, were not originally designed with security in mind. In fact, in many cases, they were designed to avoid existing security systems, such as firewalls, with the goal of making data exchange seamless across private and public networks.

  What's changed: As organizations begin to rely on SOA solutions for accessing and transporting vital data and conducting critical transactions, the lack of mature security standards becomes an increasingly important issue. IT, vendors, and standards organizations are aggressively improving baked-in or add-on security for core SOA technologies, but the pace of developing, approving, and building standards-compliant solutions, particularly in the more complex SOA technologies, can be frustratingly slower than vendor marketing or IT enthusiasm for deploying services.

- **The reuse of software assets inside and outside of the organization.** Historically, IT developed software with the assumption that the resulting systems would have a limited and defined set of users and that the system would be contained within a controlled private or secure public network. Application security, including user authentication and authorization, was hard-coded into the application logic, related database, or both. Any use of third-party data or interaction with external software or users was defined and controlled manually.

  What's changed: In an SOA world, software systems or components designed for a limited set of known users and controlled environment can be easily service-enabled and reused as part of a multi-organization composite application. The business agility that SOA solutions enable through the quick reuse of existing software assets creates a multitude of unintended consequences, such as security, privacy, and other compliance-related risks and exposures. With each successful SOA rollout, the potential security challenges grow.



Underlying SOA security issues

Evolving standards

Some standards are universally accepted; others are being driven by specific vendors

Software asset reuse

Software reuse is a core benefit of SOA, but it also creates new security challenges

The price of SOA admittance: Specific security challenges

What types of security challenges will organizations face as they adopt SOA solutions? Important challenges include:

- **Managing security across borders.** SOA implementations will expand from initial, contained deployments to instances in which service-enabled systems cross internal and external boundaries, exposing data to unauthorized and malicious third parties. Trying to manage security manually in this scenario will add tremendous cost and slow down deployments and use of the system.

  Example: A branch IT group service-enables an application for the local sales department. Later, an IT group for another business unit finds and reuses the service, exposing the data to a new set of users and networks within the organization. The initial branch IT group and application owner may not be aware of the reuse of the application and its ramifications. The situation becomes more serious from a security perspective when this formerly contained department app is later incorporated into a composite app used by partners and customers.

- **Managing security in multiservice composite applications.** As organizations gain more experience with Web services, they will create composite applications by combining multiple services, including those from inside the organization, partners, and other third parties. As with the border issue, a manual solution will explode security management costs and delay the introduction and enhancements of more complex SOA solutions.

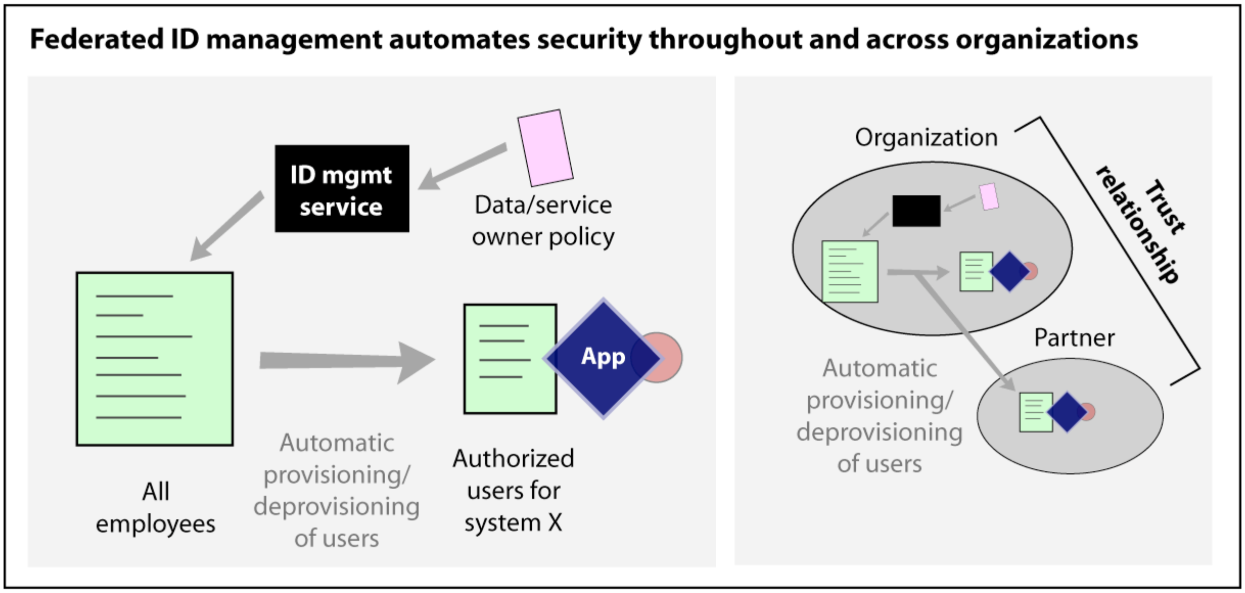
  Example: IT creates a composite app that combines two internal services as well as three services from external sources. In addition, the app is made available for customers. To secure the composite app, IT will have to understand and manage the security of each component and the security related to the new system. In addition, IT will need to automatically link its ID management solution with external systems to ensure that only authorized customers can have access.

- **Ensuring security during frequent data transformation.** At the heart of each service and composite application is an XML document with a message envelope. The various SOA components – from XML firewalls at the border to enterprise service buses (ESBs) routing traffic according to security policies and composite app logic – will interact with the various messages, often requiring data validation, message protection, and transformation. IT will need to prioritize and invest in ways to secure, validate, and keep performance levels appropriate during many of these transformations.

  Example: A user asking for a rate quote triggers a service-enabled mainframe to generate an appropriate message. The XML document is encrypted, de-encrypted, and validated a variety of times as it passes through various ESB control points and firewalls with a final transformation before arriving at the customer's PC.

- **Securing data, system access, and transactions to meet compliance and governance demands.** Organizations increasingly need to show that not only can they control access to data but that they also can track and report on any data access or transaction activities. In a pre-SOA environment, IT knew which systems to manage, monitor, and audit. But in a world of composite apps that straddle organizational boundaries, IT will need to enable granular SOA-auditing capabilities that can track and analyze services, composite apps, and other SOA components.

  Example: Material financial information is made public before earnings, and IT needs to find out how the information was accessed. Using its auditing tools, IT will check logs and records to find out whether internal or external users accessed the back-end systems that contained the data in question.


Federated ID management automates security throughout and across organizations
ID mgmt service
Data/service owner policy
All employees
Automatic provisioning/ deprovisioning of users
App
Authorized users for system X
Organization
Trust relationship
Partner
Automatic provisioning/ deprovisioning of users

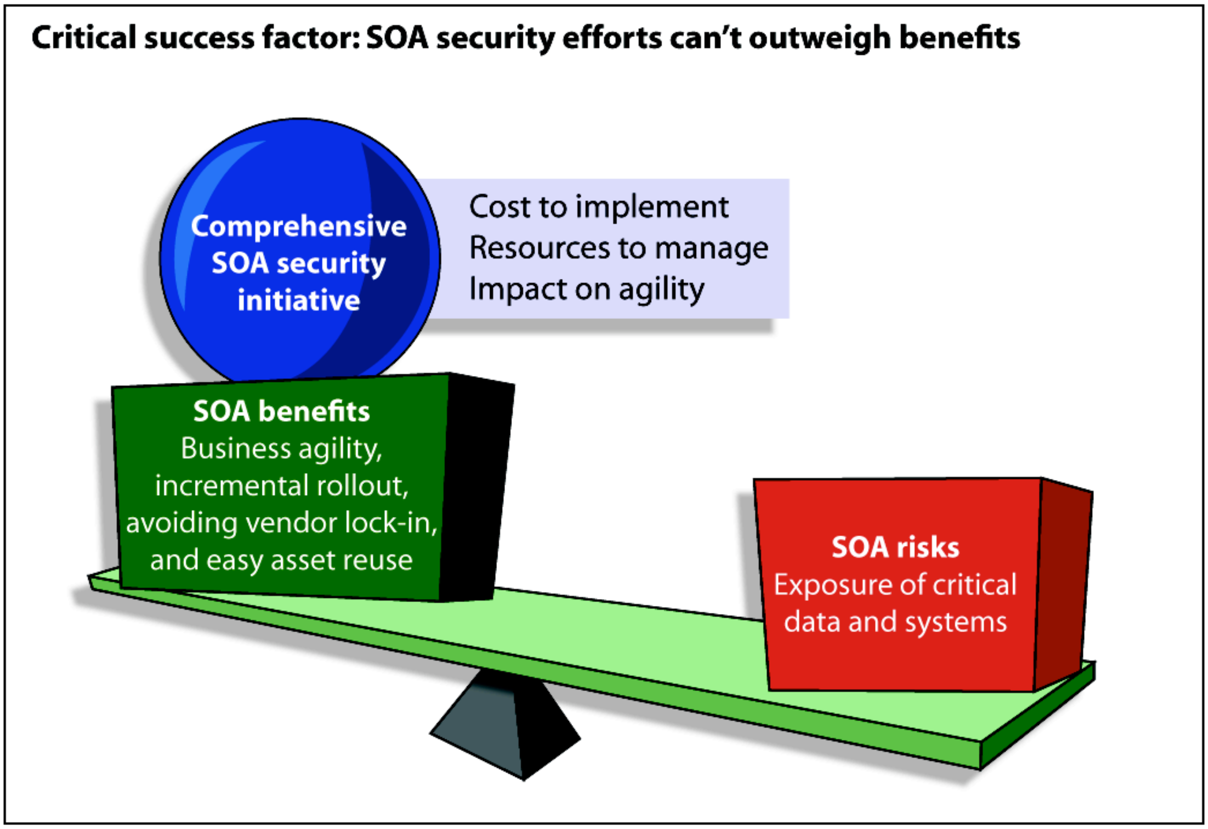
SECURITY SHOULDN'T SWAMP SOA BENEFITS

To succeed in the long term, IT needs to match its enthusiasm for adopting SOA with a pragmatic yet comprehensive security initiative that can be rolled out incrementally and that does not overwhelm the inherent benefits of adopting SOA. Balancing SOA security risks versus the cost to secure the SOA will be the key to success. To start, IT should:

- **Develop enterprisewide SOA security guidelines.** SOA security efforts will affect all existing and future SOA rollouts. All of the related technology investments – from SOA-specific software, such as an ESB or a composite app developer tool, to broader technologies, such as an identity management solution – must be included in a security guideline. The guideline should be based on security best practices, such as those outlined in the next section.

- **Publish the guidelines for all relevant users.** In most organizations, a centralized IT team will develop and publish the guidelines for use by all relevant users, including internal, third-party, and partner developer groups. However, in many cases, the actual security policies will be created and managed by non-IT personnel, such as compliance officers. This split responsibility will enable an organization to adhere to a single policy yet distribute data management and security polices across the organization.

- **Ensure that SOA solutions adhere to the best practices guidelines.** SOA solutions will be developed on many levels, from individual departments to the enterprise. CIOs and top IT executives need to ensure that all SOA rollouts follow the SOA security best practice guidelines. Otherwise, IT will be forced to eventually deal with a series of short-term, one-off security solutions that don't meet established security standards. Adherence can be achieved through a combination of technology (e.g., locking down software assets) and processes (e.g., requiring new services can only go live after passing an approval checklist).



Critical success factor: SOA security efforts can't outweigh benefits

Comprehensive SOA security initiative
Cost to implement
Resources to manage
Impact on agility
SOA benefits
Business agility, incremental rollout, avoiding vendor lock-in, and easy asset reuse
SOA risks
Exposure of critical data and systems

SOA SECURITY BEST PRACTICES

In building an enterprisewide, comprehensive SOA security guideline, IT should examine a variety of best practices. This paper breaks down the best practices into groups based upon the way to think about and plan security initiatives, the best practices related to SOA-relevant processes, and best practices around specific technology implementations.

New thinking: Planning and conceptual best practices

IT needs to promote certain SOA security best practices as being overarching and applicable in every situation. These conceptual best practices don't involve specific changes to process or require investments in technology; instead, they are about adopting a new way of thinking around SOA security. They include the need to:

- **Plan for incremental security adoption.** SOA security is a major undertaking that will affect many existing and future systems, processes, and technology. The SOA security guideline authors need to make sure that the developers and business leaders understand that security will not – and cannot – require one massive round of investment and effort. The concept of incremental adoption should be prevalent in every discussion and document.

- **Build security capabilities and rules as services.** It is a waste of IT resources to reinvent the security wheel with each project. In addition, embedding security into specific services or composite apps will reduce the organization's ability to enhance or modify security policies in the future. In a security as a service model, policy owners will update security policies in central locations, and those changes will automatically propagate out to the relevant SOA infrastructure components that enforce security policies.

- **Assume public exposure.** Individual services and composite apps have no boundaries, and their underlying technology has no built-in security and is capable of innocuously crossing firewalls. A critical best practice will be for each and every service creator – whether a development team is simply enabling an existing application or building a greenfield, service-ready system – to assume that its service and the data that it transports will be exposed to the public. This assumption, and the subsequent security applied in each instance, will also ensure that internal security threats – the most common source of organizational espionage – will also be thwarted.

New behaviors: Process best practices

While all of those involved in SOA creation and use should internalize the conceptual best practices outlined above, they must also change how they define, create, roll out, and reuse SOA solutions. The organization should:

- **Assess SOA risks and prioritize security implementations.** Organizations will need to understand their entire services portfolio, including the dependencies of services, the existing security of the underlying apps, and the exposure of these services. Once an organization understands the scope of its current situation, it will need to prioritize the security efforts to minimize risk and exposure. Moving forward, new service and composite app developers must scrutinize their projects and determine how to embed security before deployment – or at the very least, design the solution so that it can adhere to SOA security guidelines at a later date.

- **Design in auditing capabilities.** Just as developers should assume that a service or composite app will eventually be exposed on public networks, they should also assume that their project will require an auditing capability. With compliance and auditing demands expanding, SOA projects should be designed to ensure that data is kept confidential, information cannot be altered, and systems can document these capabilities.

- **Create a security-savvy service life cycle.** Successful services will undoubtedly be reused, so IT needs to create a service life-cycle policy that manages services from cradle to the grave, including events like service planning and development, deployment, modification (version control and migration), deprecation, and removal. A service must be able to function appropriately throughout its entire useful life, even as message protection policies for data privacy, access, and encryption are continually updated.

New investments: Technology best practices

Certain best practices require integrating with existing security components or licensing software with security capabilities. From a technology standpoint, IT should look to:

- **Message protection solutions.** Protecting messages and the data they carry is a basic SOA requirement, but the reality is that most organizations will only be able to selectively protect their data in the short term. Once an organization has prioritized and identified data and services that must be secure, IT can invest in a variety of plug-in components to fulfill the level of protection that they – or their partners and customers – feel is required. If performance is an issue, vendors offer a variety of hardware-based acceleration products for speeding up secure message processing, such as encryption and validation.

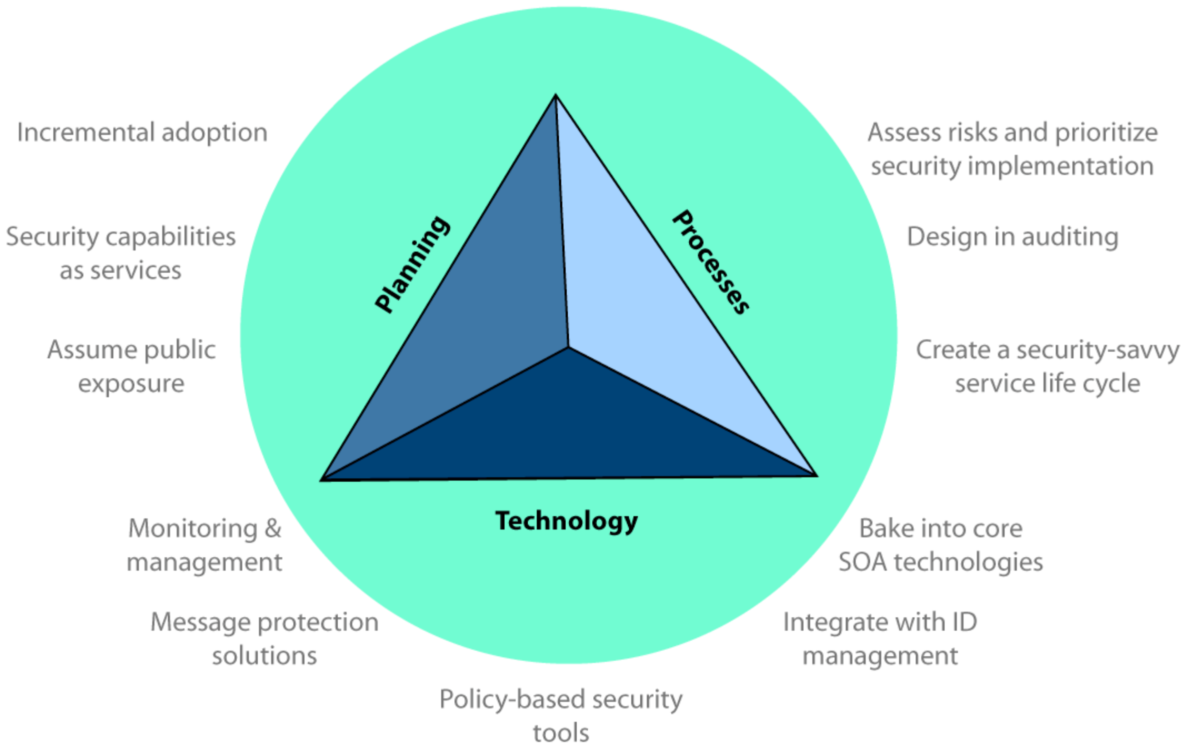
- **Policy-based security software.** The concept of security as a service will at some point require an investment in a security policy solution designed for SOA. These products must be able to support distributed creation and modification of security polices throughout the organization but ensure enterprisewide enforcement of the policies across all relevant SOA instances.

- **Federated ID management solutions.** In a secure SOA implementation, organizations need to be able to control who or what can access a system and under what circumstances. If it doesn't rely on one already, IT will need to invest in a federated ID management solution. This type of solution enables seamless single sign-on to services and composite applications that include services outside of the enterprise for both internal and external users. Without such an automated solution, SOA security management costs will skyrocket.

- **Service monitoring and management.** While SOA technology allows IT to relatively quickly assemble services and composite apps to meet changing business needs, this high-level capability comes at a price in terms of the complex interrelationships between services, polices, SOA components, and traditional IT assets, such as applications and databases. IT will need to be able to both proactively and reactively monitor, analyze, and fine-tune the various SOA components and their relationships. If IT can't monitor its systems, understanding – let alone prioritizing and addressing – the security issues will be impossible.

- **Core standards-compliant SOA technologies.** As the SOA matures from a few projects to a large and critical portion of the organization's computing infrastructure, SOA-specific technologies, such as ESBs and service registries/repositories, must be tied into the security framework as they are developed and rolled out. IT will need to ensure that existing and future solutions adhere to the evolving SOA-related standards identified as critical in its guidelines, such as SOAP, BPEL, WS-Security, and SAML.

SOA security best practices: Embedding security in every facet of the SOA


Planning
Processes
Technology
Incremental adoption
Security capabilities as services
Assume public exposure
Monitoring & management
Message protection solutions
Policy-based security tools
Integrate with ID management
Bake into core SOA technologies
Create a security-savvy service life cycle
Design in auditing
Assess risks and prioritize security implementation

IBM OFFERINGS FOR SOA SECURITY BEST PRACTICES

IBM offers a variety of products and services to help organizations meet the goals developed in their SOA security best practices guideline. These offerings can be broken down into two categories. The first category covers the IBM resources – some in the form of free material and research tools – that can help organizations as they develop successful SOA security guidelines. The second category encompasses the available IBM software and services for developing and implementing a secure SOA. In many cases, large organizations will use a mixture of the available resources, software, and services to develop and incrementally implement their SOA security initiative.

Resources for laying the foundation

Even before selecting a software package or writing a line of integration code, organizations need to lay the groundwork for SOA security through self-education, focused learning, and sometimes direct help from external service providers. IBM offers a variety of resources to help organizations set the foundation for adopting SOA security best practices, including:

- **Lots of free IBM and third-party content.** The vendor offers a large cache of internally authored, SOA-centric whitepapers, developer-oriented documents and tools, research notes, and extensive topic primers (called Redbooks). IBM also makes available a variety of third-party material related to various SOA aspects and products from analyst firms and business partners.

- **A services arm to help craft the security guidelines.** For those who need firsthand help or access to people who have actually implemented SOA and security practices in large organizations, IBM's comprehensive service offerings are available. The personnel are knowledgeable in IBM solutions and partner offerings and in integrating existing legacy systems and other third-party software.

Software and services for implementing SOA security

With a basic foundation and road map in place, organizations can look to extending and enhancing the technology of their existing infrastructure as well as adding new SOA security-specific components, such as federated ID management integration packages, message protection tools, and composite application development software. IBM offers a variety of solutions, including:

- **SOA core technology solutions.** IBM software offerings that can form the foundation for a secure SOA include Rational Web Developer for WebSphere Software; IBM Rational Software Architect; IBM WebSphere Integration Developer; and WebSphere DataPower SOA Appliances. IBM is a major supporter of open source solutions, so these solutions can be deployed on a variety of platforms. And since SOA is built on industry standards, IBM products can be deployed and integrated with other vendors' offerings.

- **Related core technology.** Solutions that are key to deploying SOA security best practices include IBM Tivoli Access Manager for e-business, IBM Tivoli Access Manager for Business Integration, IBM Tivoli Composite Application Manager for SOA, and IBM Tivoli Composite Application Manager for Response Time Tracking. IBM can leverage its years of experience with large organizations, legacy systems, massive databases, and systems integration to help deliver a complete solution or stitch together the various components required to help secure the SOA.

- **SOA security enablement offerings.** One of the key software components of an enterprisewide security solution is a federated ID management tool. IBM's entry in this field is the IBM Tivoli Federated Identity Manager, which can be rolled out with other IBM or third-party solutions to create the automated, trust-based security framework needed to secure borderless services and multi-organization composite applications.

- **Services for implementation, deployment, and secure SOA management.** As mentioned above, IBM Global Services can help plan *and* build the SOA security infrastructure using IBM or third-party products and services. How much real-world knowledge and experience does the company have? IBM reports that its services arm has experience with more than 3,000 SOA engagements and works with more than 2,500 SOA-related partners.