IBM/Tivoli Systems Security Update

David Hemsath, Chief Technologist, IBM Global Security Solutions, dhemsath@us.ibm.com

07 March 2002

SHARE 98, Session 1745

Related sessions this week at SHARE

- 1711 – Security Management - Trends and Directions
- 1732 – IBM Policy Director Authorization Services for OS/390 and z/OS
- 1766 – Web Application Server - Part 1 of 2
- 1767 – Web Application Server - Part 2 of 2

Disclaimer

The information contained in this document is distributed on an “as is” basis without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM’s licensed programs may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

Trademarks

- IBM, SecureWay, AIX, MQSeries (IBM)
- DCE, OSF, Open Software Foundation, UNIX (The Open Software Foundation)
- Microsoft, Windows, Windows NT, Windows 2000 (Microsoft Corporation)
- Java and all Java-based trademarks and logos (Sun Microsystems)
- Other company, product, and service names may be trademarks or service marks of others.

Abstract

IBM/Tivoli Systems provides a comprehensive set of security components embedded by other IBM offerings and used directly by customers. This presentation will give an overview of these security components and how they fit into customers' overall IT Security deployments. Areas to be covered include:

- Authorization management
- Identity management
- Risk management
- Privacy

Agenda

- Overview of the Tivoli Security portfolio
  - Including recent news
- Growing exploitation of Tivoli Security technology by other IBM offerings
- Use of Tivoli Security technology by third parties

How Security Management Can Enable e-business

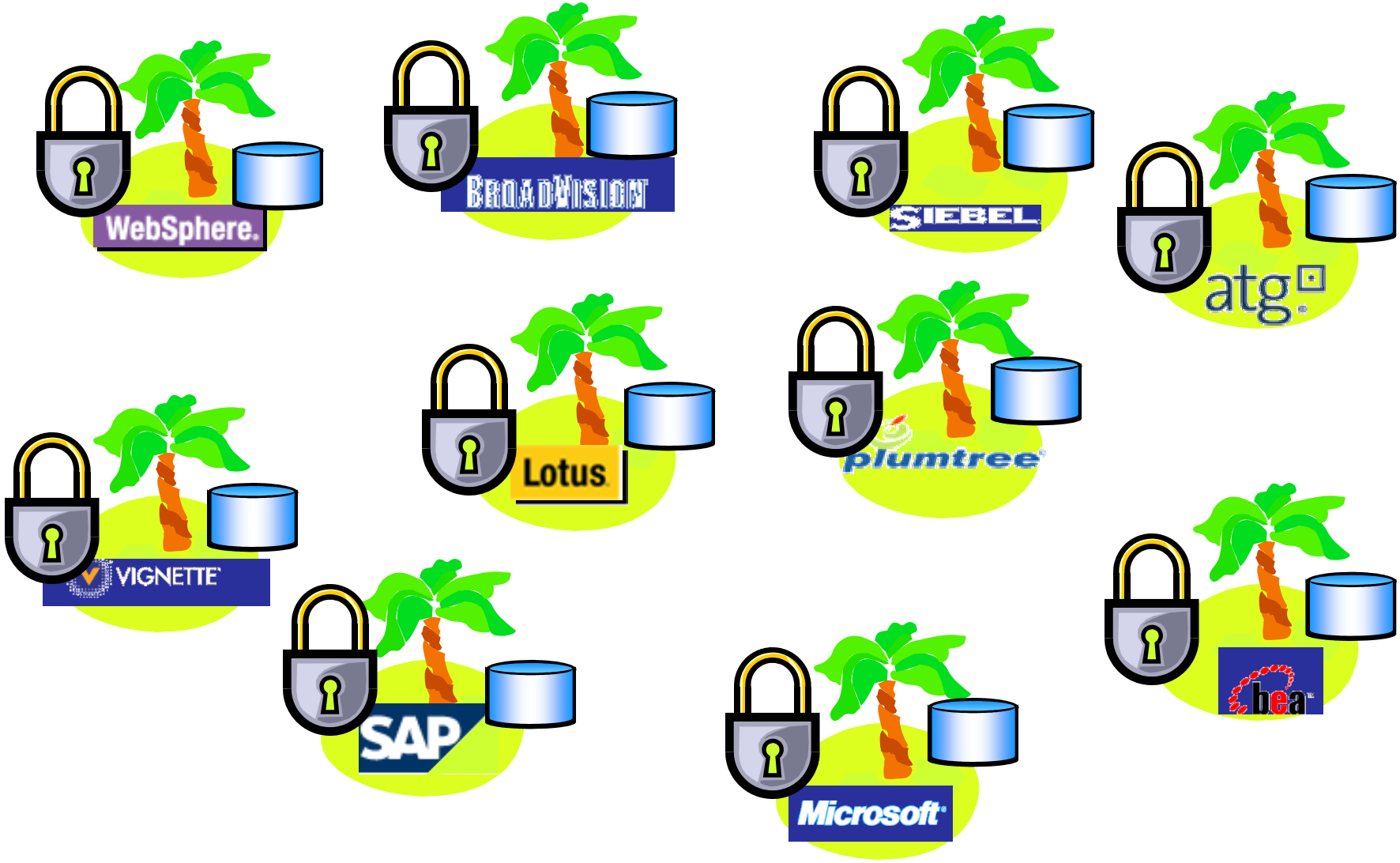
- Deploy e-business initiatives faster
  - Instead of implementing customized security with each application/environment
- Get users on-line and productive faster
  - Instead of manual, varied, help desk-intensive processes for registering users and provisioning their resources
- Enable quick reaction to security compromises
  - Instead of having multiple administrators manually monitoring security alerts and logs (or ignoring them, due to their volume)

Tivoli Security Portfolio

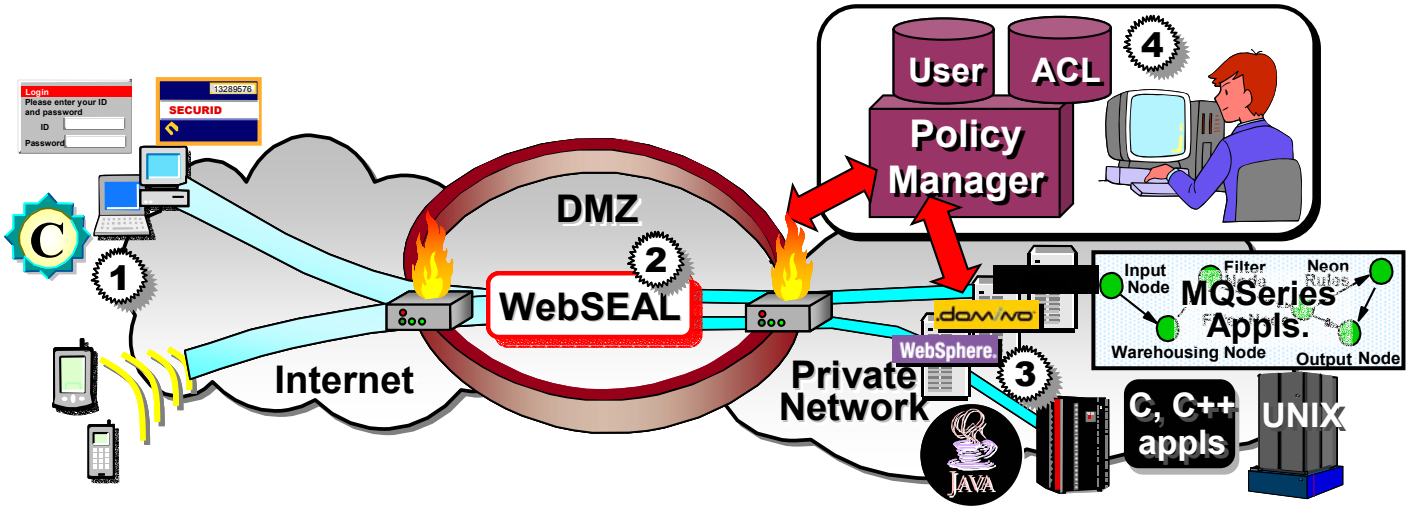
- Access Management
  - Authorization for e-business (Policy Director family)
- Identity Management
  - ID/authorization management for the enterprise (Identity Director and predecessor products)
- Risk Management
  - Correlation of security alerts/events in a proactive risk management scheme (Risk Manager, Intrusion Manager)

Access Management

Instead of This . . .

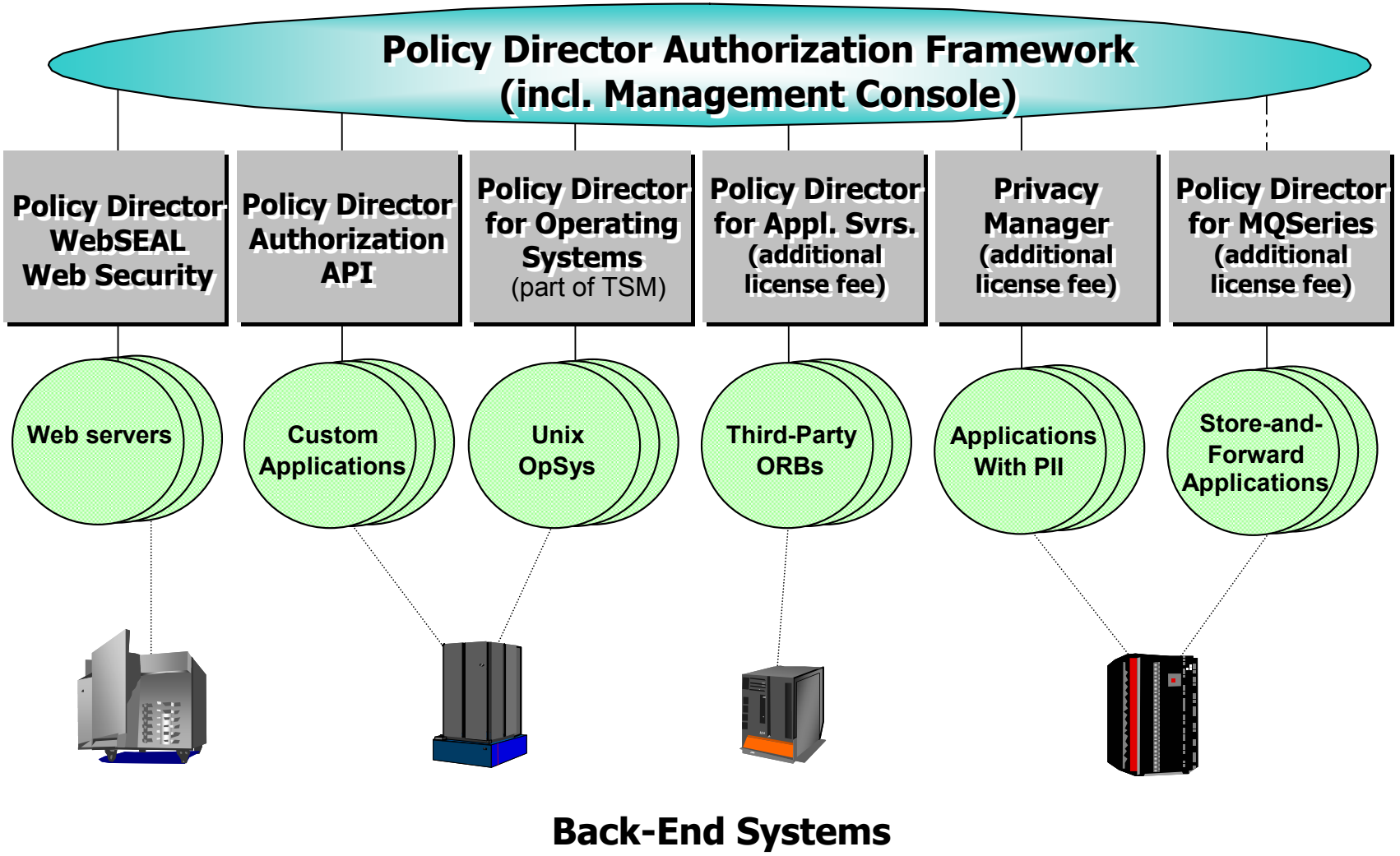


A Policy-Based and Comprehensive Security Approach

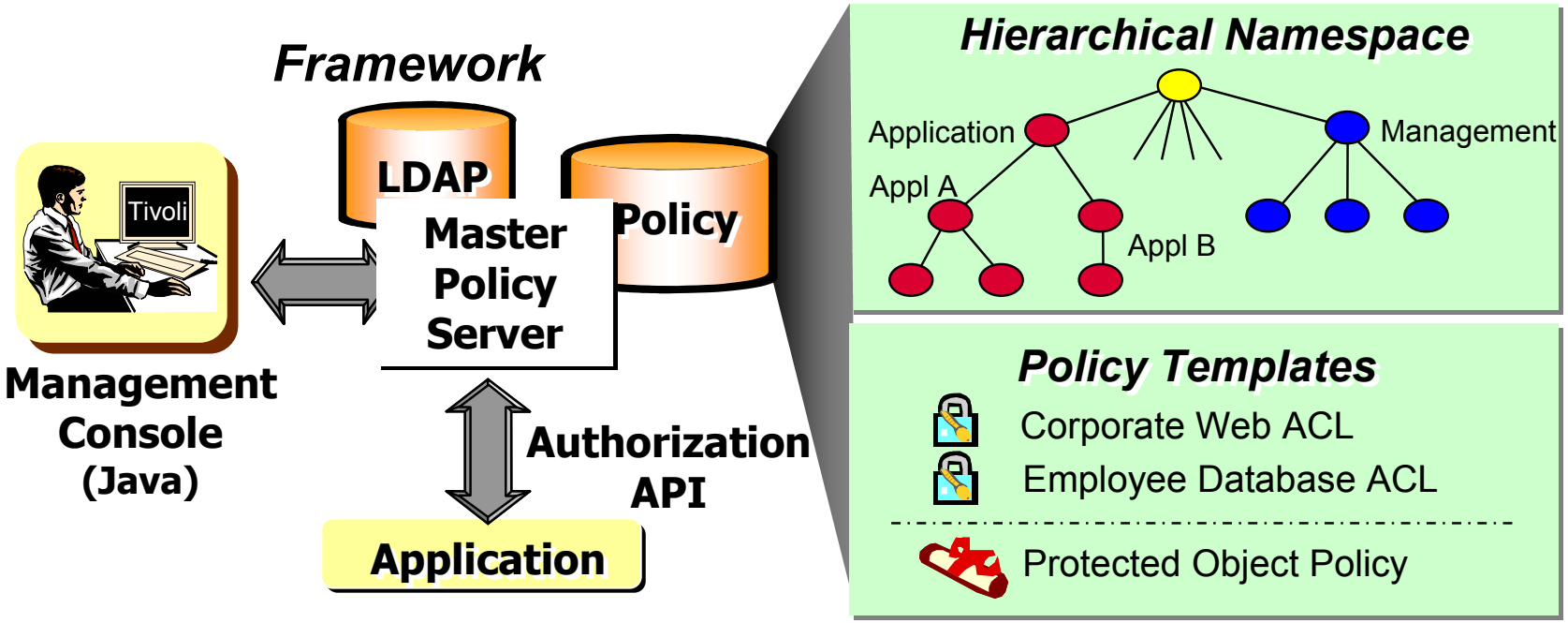


1. **Supports multiple means of identity** (User ID/PW, certificates from many PKI vendors, wireless device identities, SecurID card, and others via customization)
2. **Provides Web authorization services** (Policy Director's WebSEAL server authenticates users, ensures high availability, provides Web SSO and manages access to URLs, CGI programs, HTML files, servlets, …)
3. **Provides application authorization services**, with integrated security for Domino, WebSphere, Siebel, … and can extend to cover MQSeries/UNIX
4. **Provides robust Web security administration** (Centralized, browser-based, delegatable administration, rich registry support, single protected object namespace, comprehensive, policy-based audit)

Policy Director Components and Related Products

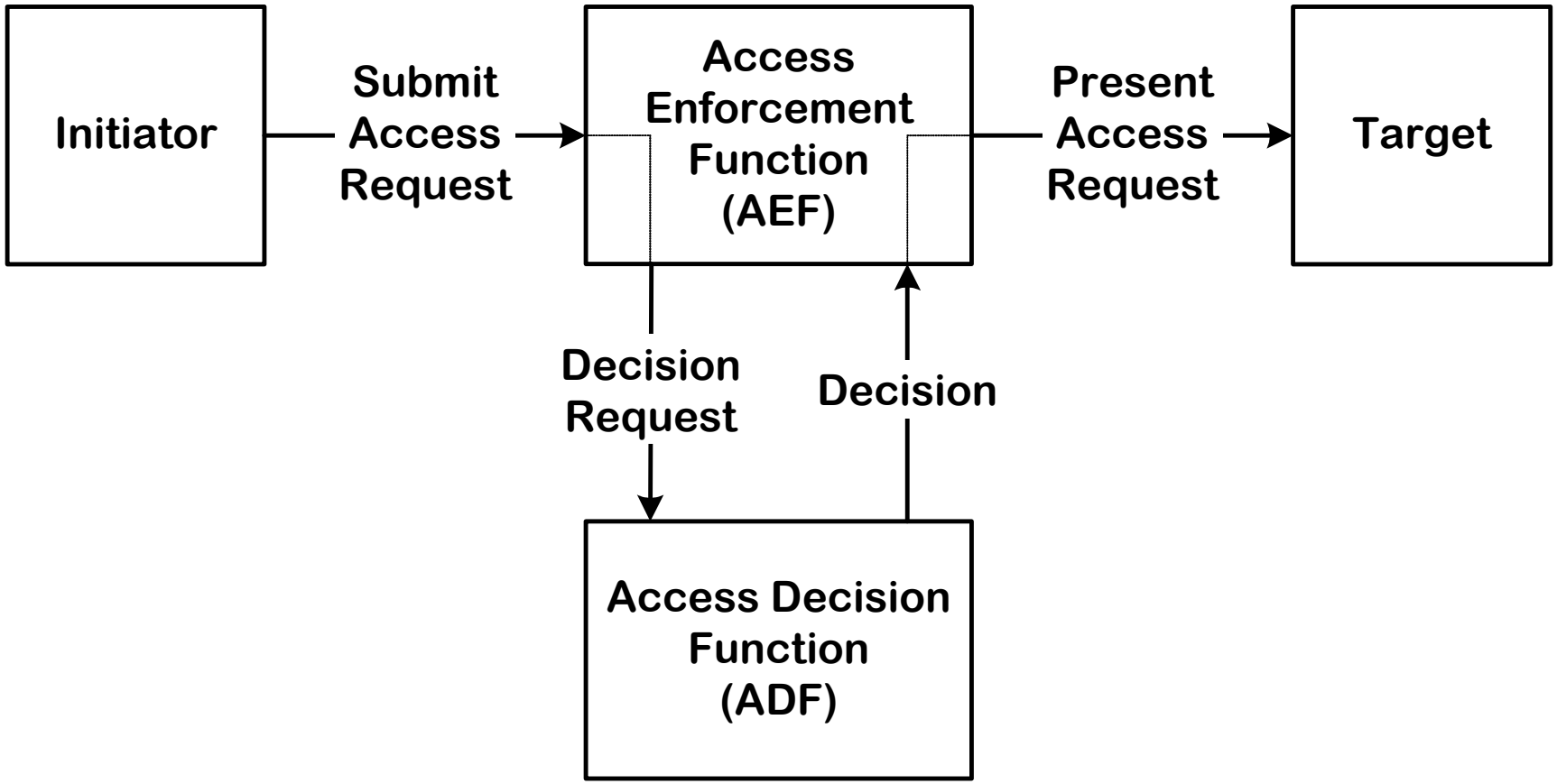


Authorization Framework/Concepts

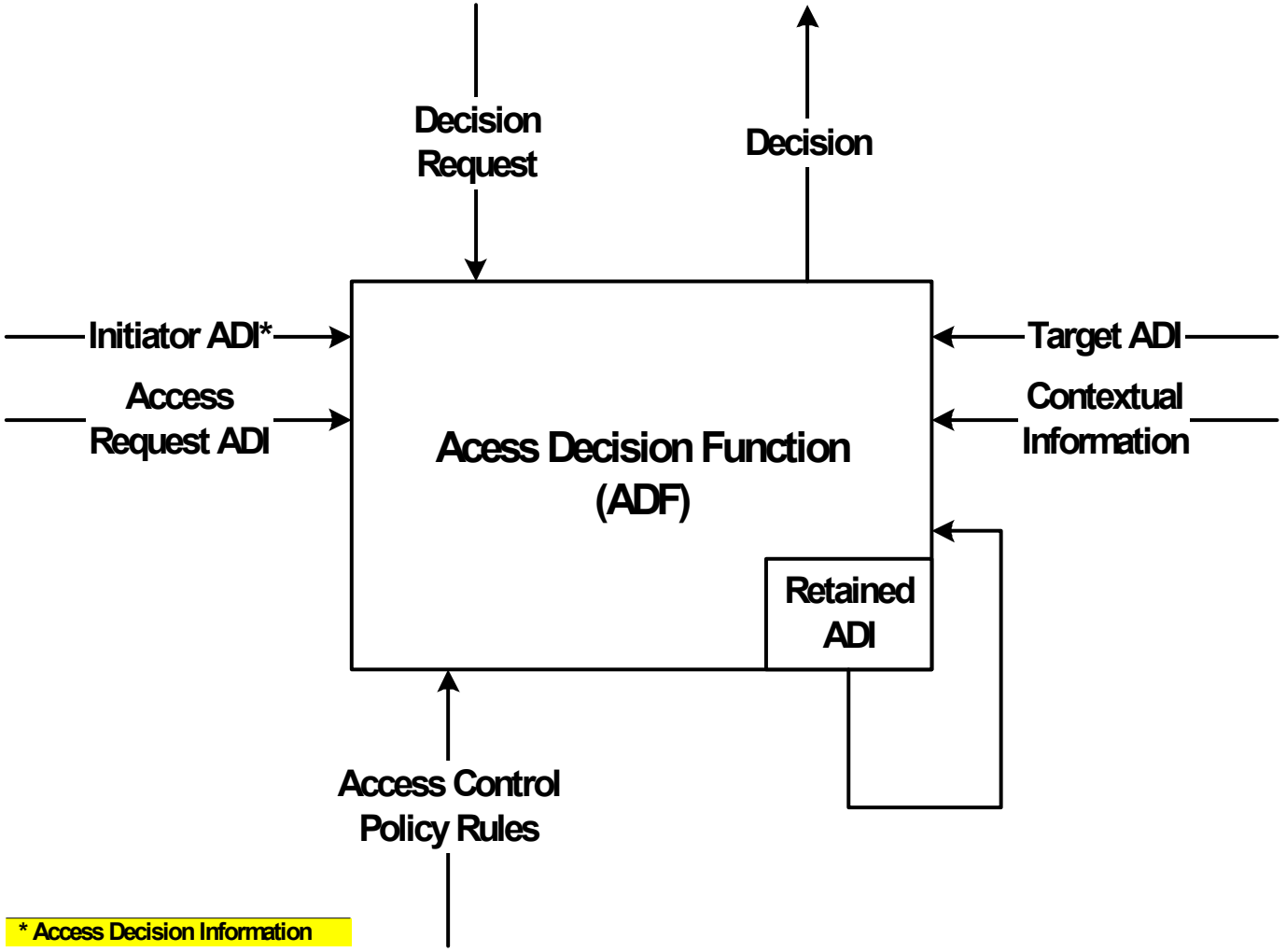


- Master framework avoids the need for authorization code in each application
- Management console
  - Define users/groups
  - Define access control policy (ACLs = users with permissions re: objects or resources)
  - Define Protected Object Policies (POPs = object or resource characteristics)
  - Associate ACL and POP templates with objects in the hierarchical namespace

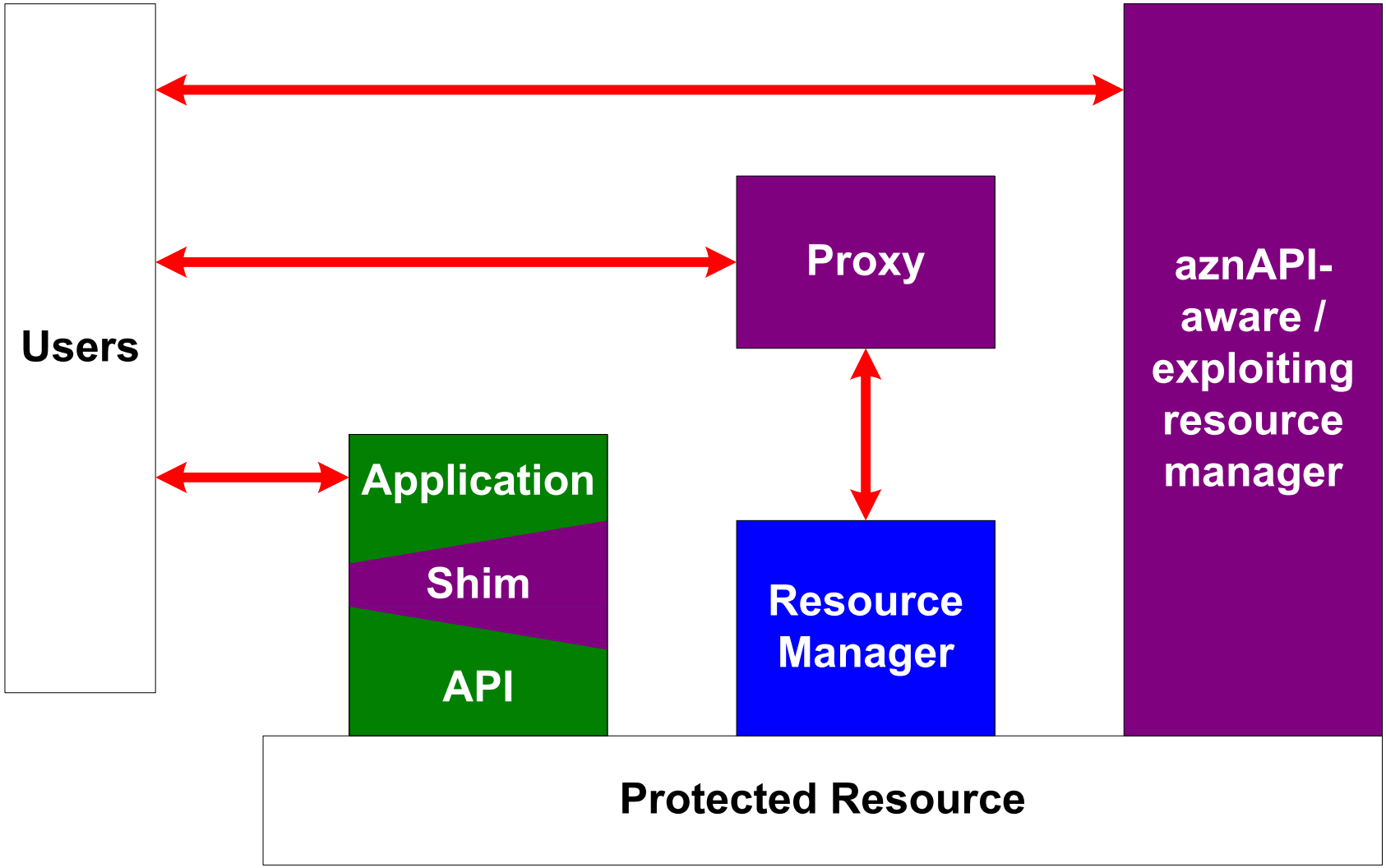
ISO 10181-3 Access Control Model



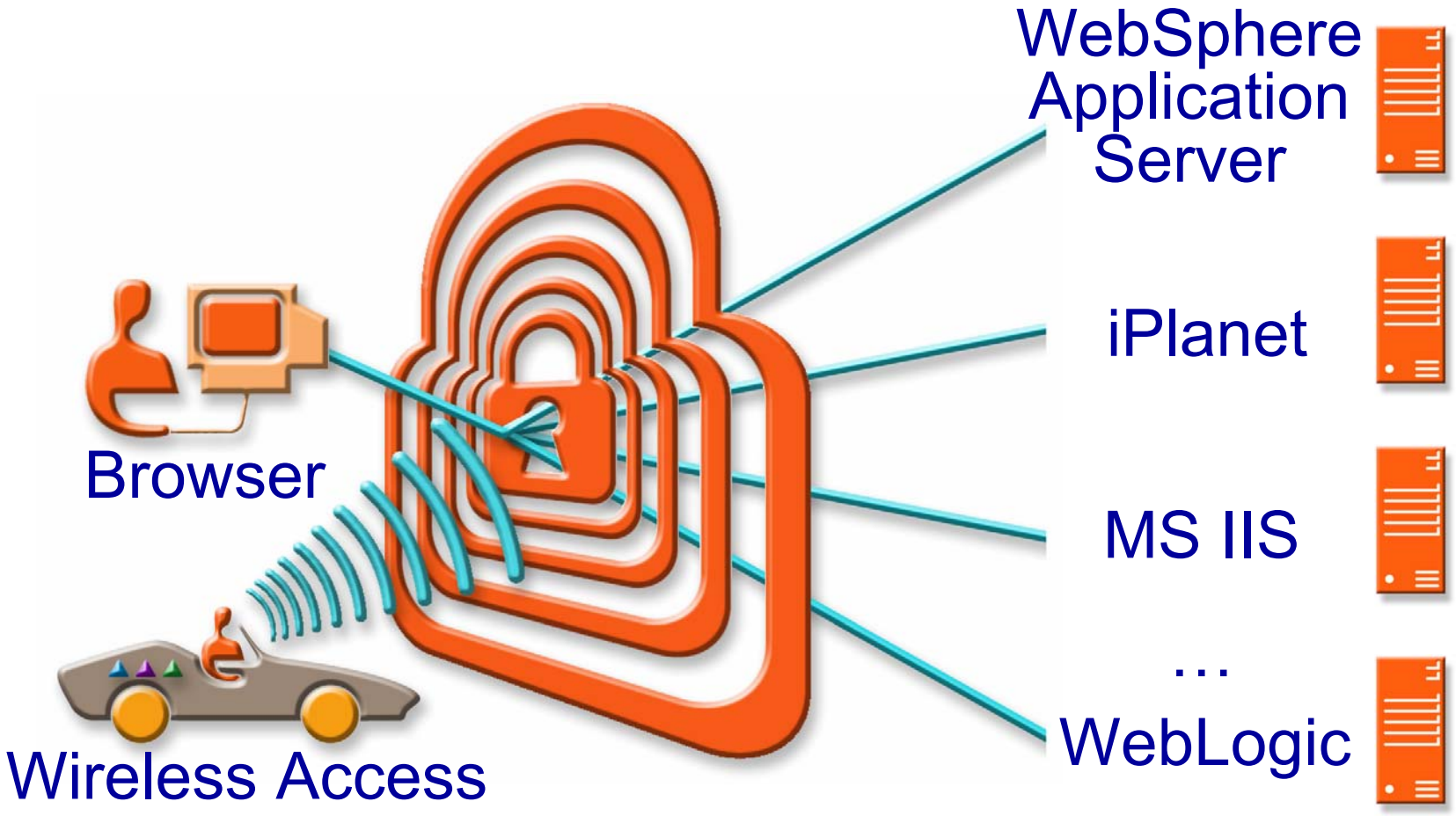
The Access Decision Function



AEFs and the aznAPI



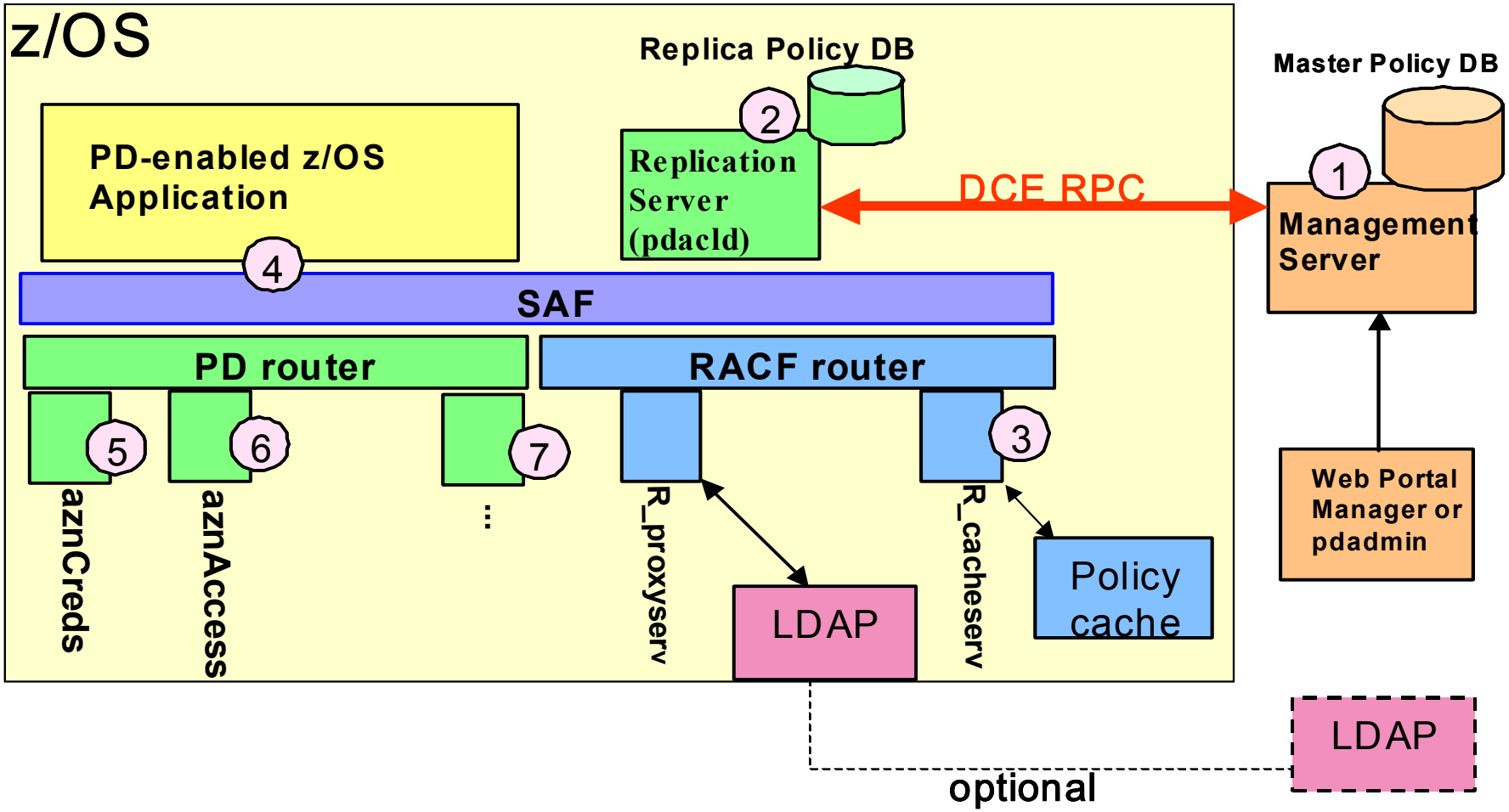
Securing the web with WebSEAL, WebSphere Edge Server and/or WebSphere Everyplace Suite



Policy Director 3.8 & Directions

- Policy Director 3.8
  - DCE-free
  - Performance and RAS improvements
  - Web-based, delegatable administration
    - Still have console, CLI and API management options
  - More/concurrent NLS
  - Functional enhancements
  - Platform coverage
- Directions
  - HTTPD plug-ins
  - Support for Additional User Registries
  - Application Server Integration, incl. JSR 115
  - Additional/enhanced authentication
  - Platform coverage
  - Hardware-based SSL acceleration
  - Improved Java API support (admin & ops)

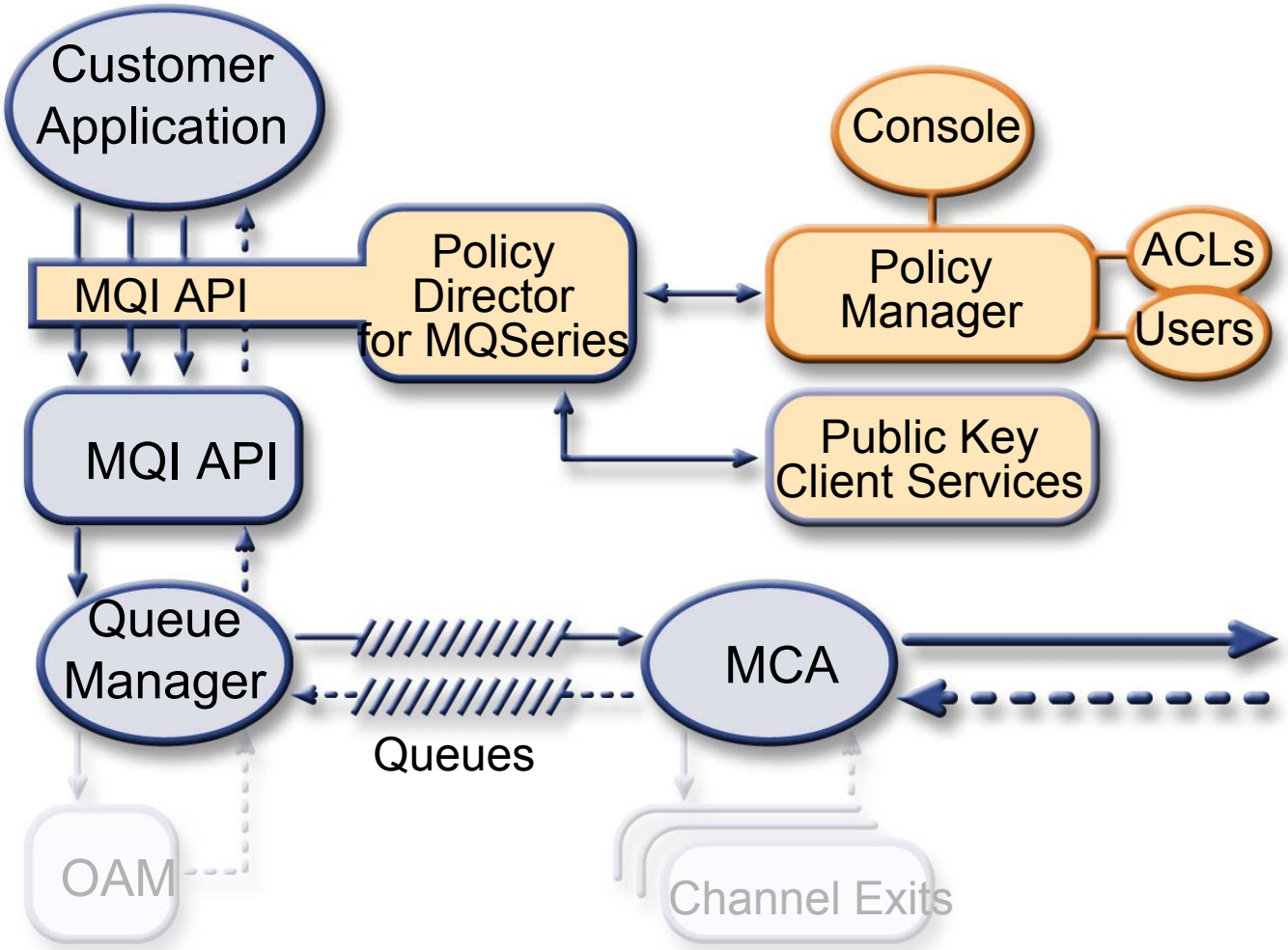
2001.11.30 – Policy Director Authorization Services for z/OS and OS/390 V1R1M0



Additional mainframe news

- z/OS and OS/390 V2R10 LDAP Servers now supported as a User Registry for Policy Director 3.7.1 and 3.8
- SAF-based WebSEAL authentication through the LDAP server's *Native Authentication* support
- z/OS and OS/390 V2R10 LDAP Servers successfully tested with next generation of Tivoli Identity Director

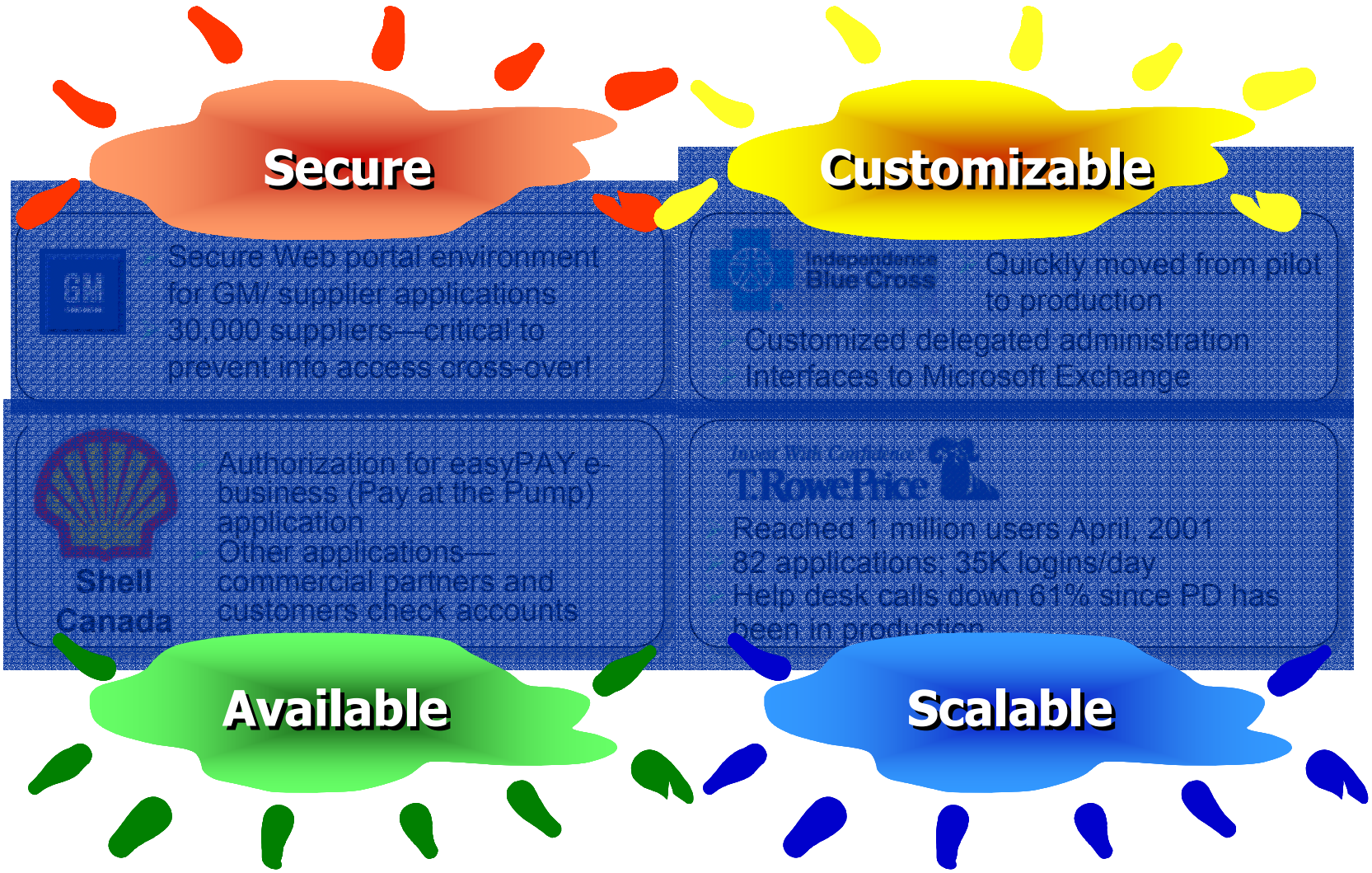
Policy Director for MQSeries



Policy Director for MQSeries Version 3.8 for z/OS and OS/390 V2R10

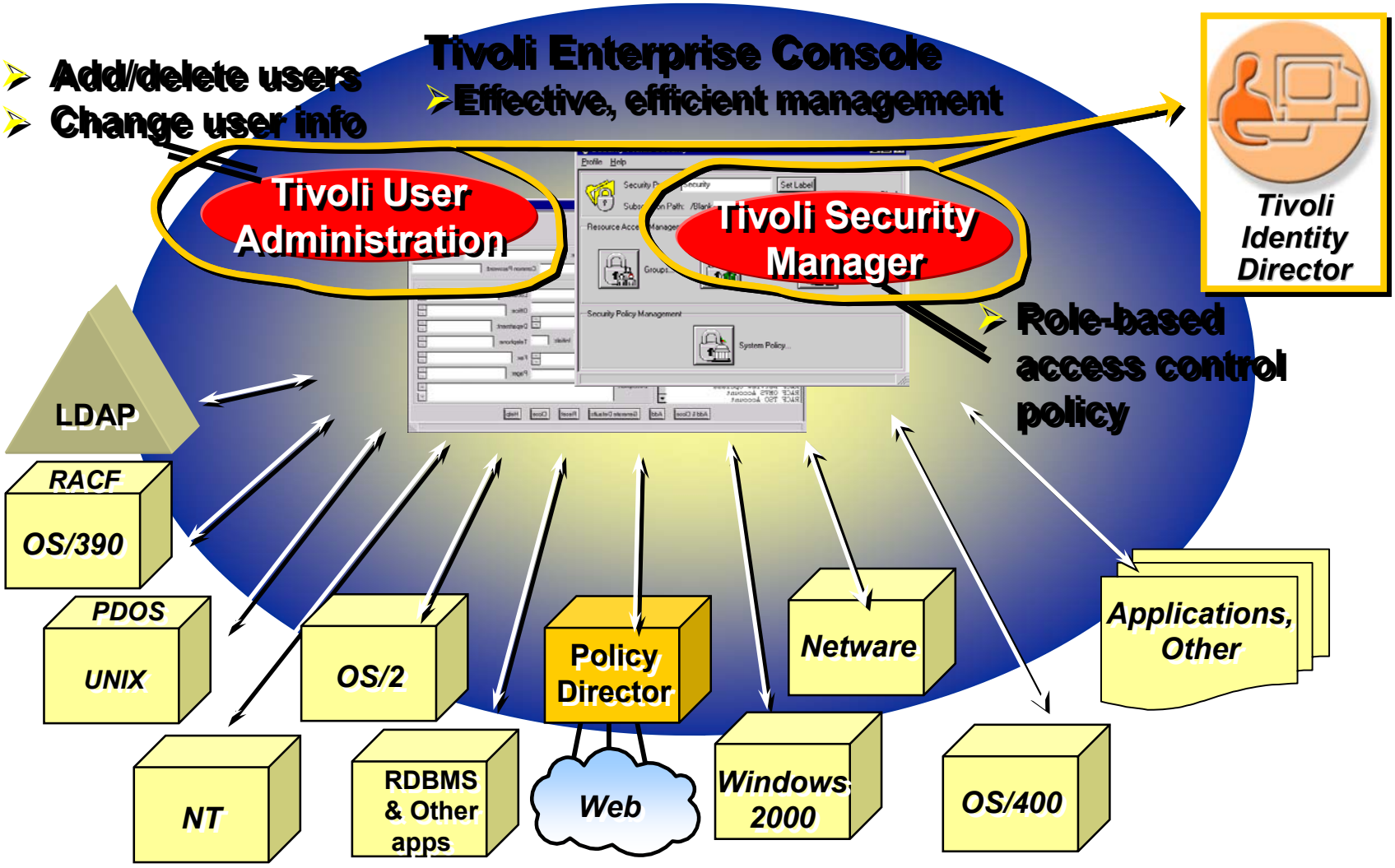
- Access control of queues, data encryption, data signing, auditing, rogue message identification
- Support for CICS/Batch/Open Edition subsystems
- PKI support - Tivoli, Netscape, Entrust, others
- S/390 Hardware Crypto support
- Supports MQSeries V5.2 only
- Requires OS/390 V2R10 and z/OS V1R1 or higher
- Requires IBM Policy Director authorization services for OS/390 and z/OS which is PD V3.7.1 based
  - As with “PDAS,” this is a PL/X-based reimplementation of the distributed “PD/MQ” code for maximum performance, scalability, RAS, integration, etc.
- Requires System SSL V1.1 or V2.1

Policy Director Usage Examples

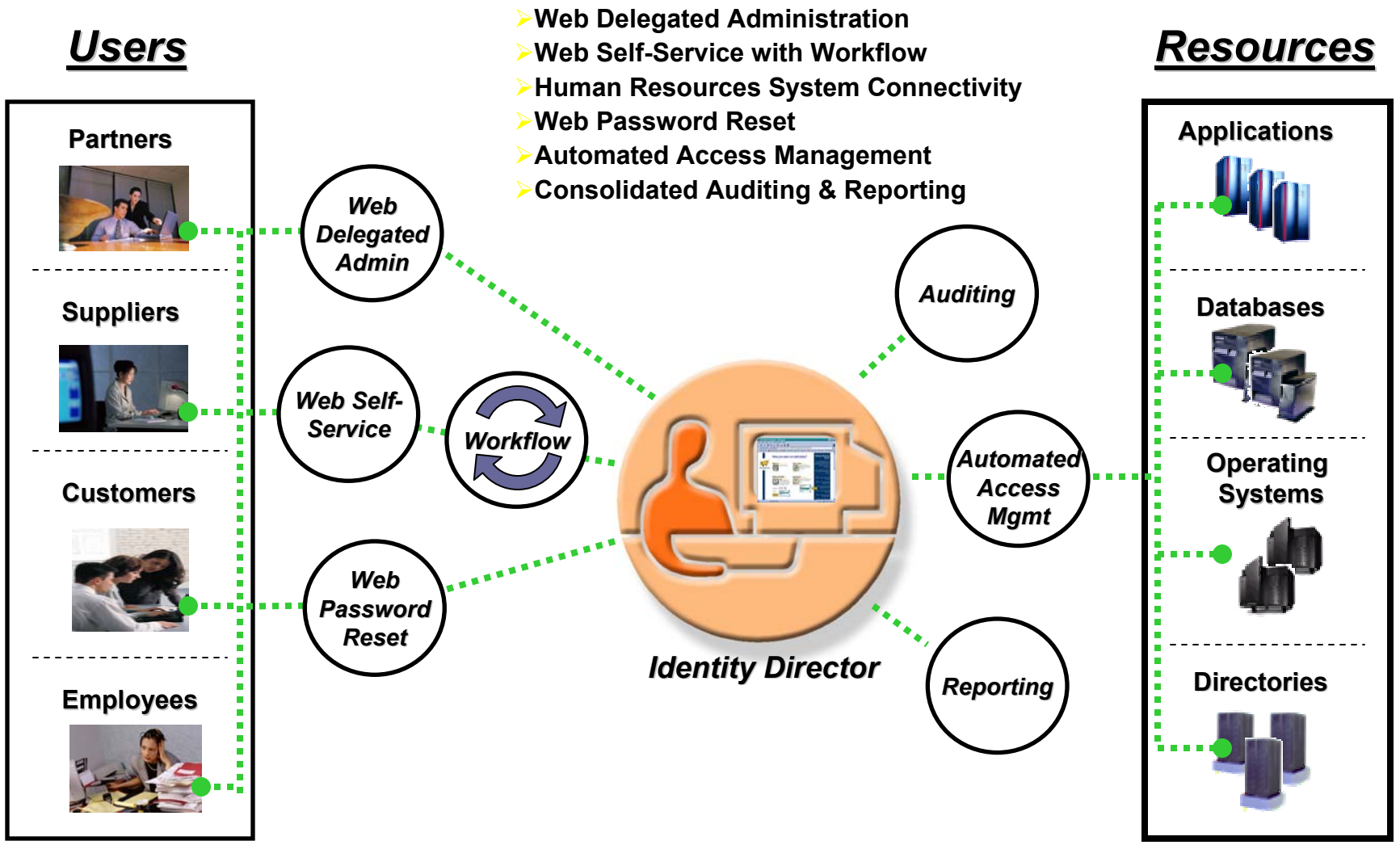


Identity Management

Tivoli Enterprise Security Management



Tivoli Identity Director



- Web Delegated Administration
- Web Self-Service with Workflow
- Human Resources System Connectivity
- Web Password Reset
- Automated Access Management
- Consolidated Auditing & Reporting

Tivoli Identity Director—Business Value

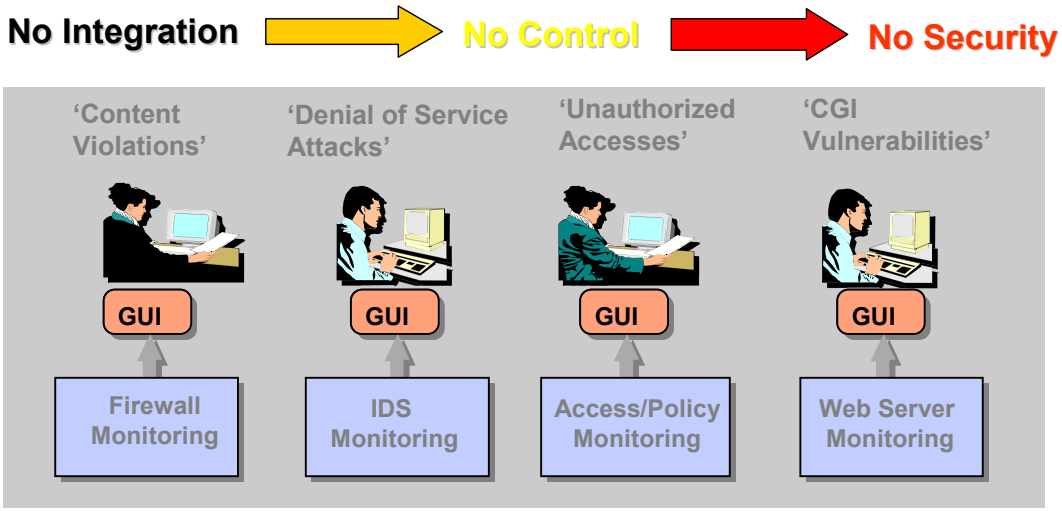
Feature	Value
Web Administration Interfaces (centralized control)	**Eliminate the education and training costs** of managing from multiple interfaces.
Role-Based Delegated Admin (across organizational/geographical boundaries)	Easily **accommodate distributed management** needs.
Web Self-Service Interfaces (register for services, perform password resets, modify personal info, . . .)	**Reduce help-desk costs** and **ease the burden of day-to-day administration** on IT and help-desk staff.
Embedded Workflow Engine (automates submission/approval process for access requests & user info changes)	**Establish SLAs** and clear **security audit trails**. **Decrease errors and inconsistency** in manual business processes.
Embedded User Provisioning Engine (automated implementation of admin requests)	**Meet SLAs**. **Increase productivity** and reduce administrative overhead.
Application Management Toolkit (extends management to new/custom application environments)	**Assimilate changing business environments** and company growth more easily.
Directory Connectivity Architecture (consolidates user information)	**Leverage data** for security audits, organizational charts, company directory, applications, etc.

Risk Management

Customer Value—Risk Management Solution

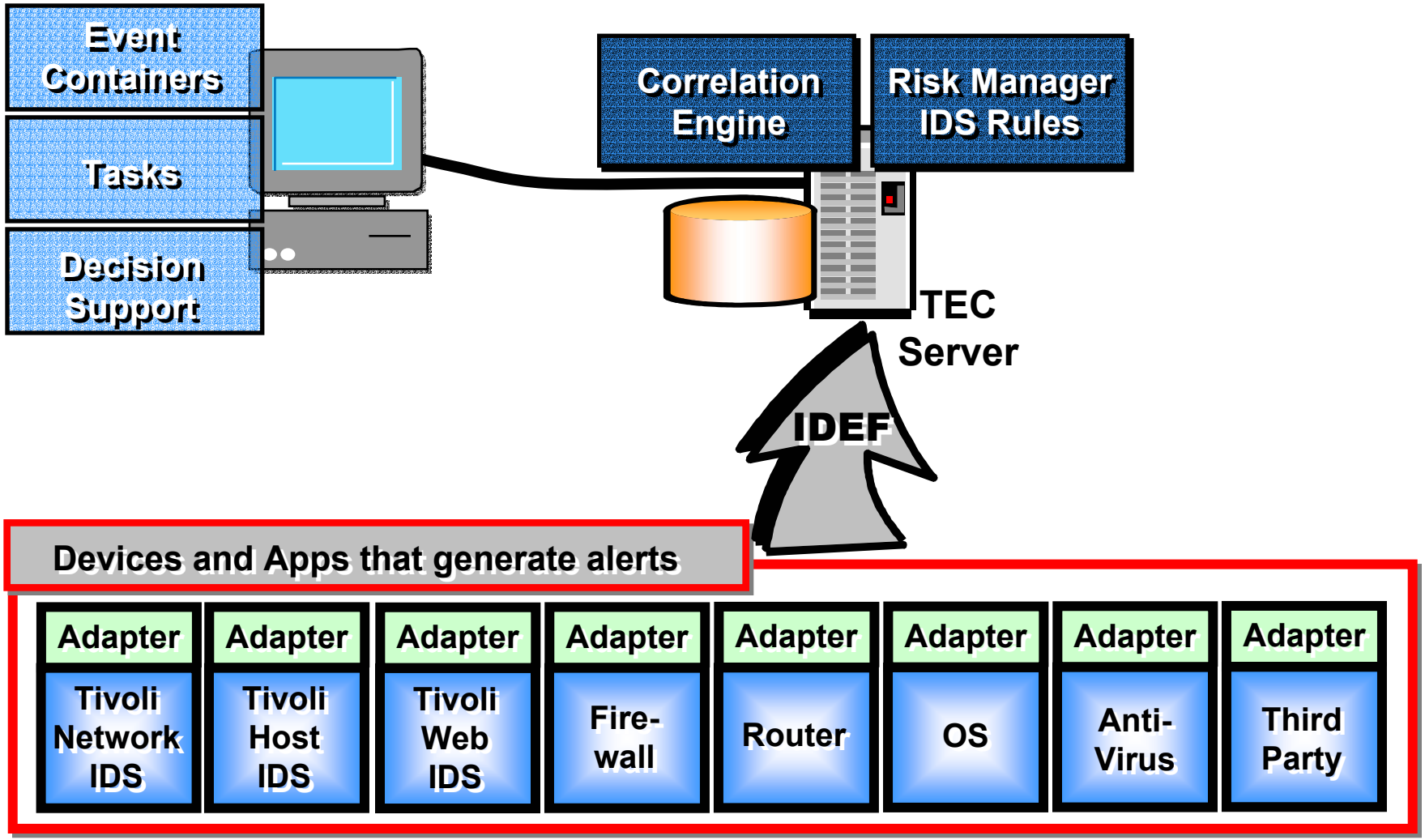
- Proactive, real-time analysis of valuable security alert/event information
- Quick reaction to breaches/compromises
  - Hacker penetration
  - Virus outbreak
  - Denial of service
- Reduction in cost and complexity of managing/ operating a secure e-business by centralizing management of:
  - Firewalls and other DMZ hosts
  - Web Servers and Application Servers
  - Antivirus programs/information
  - Intrusion Detection (host, network, hybrid)

The Problem: Multiple Point Products; No Consolidation

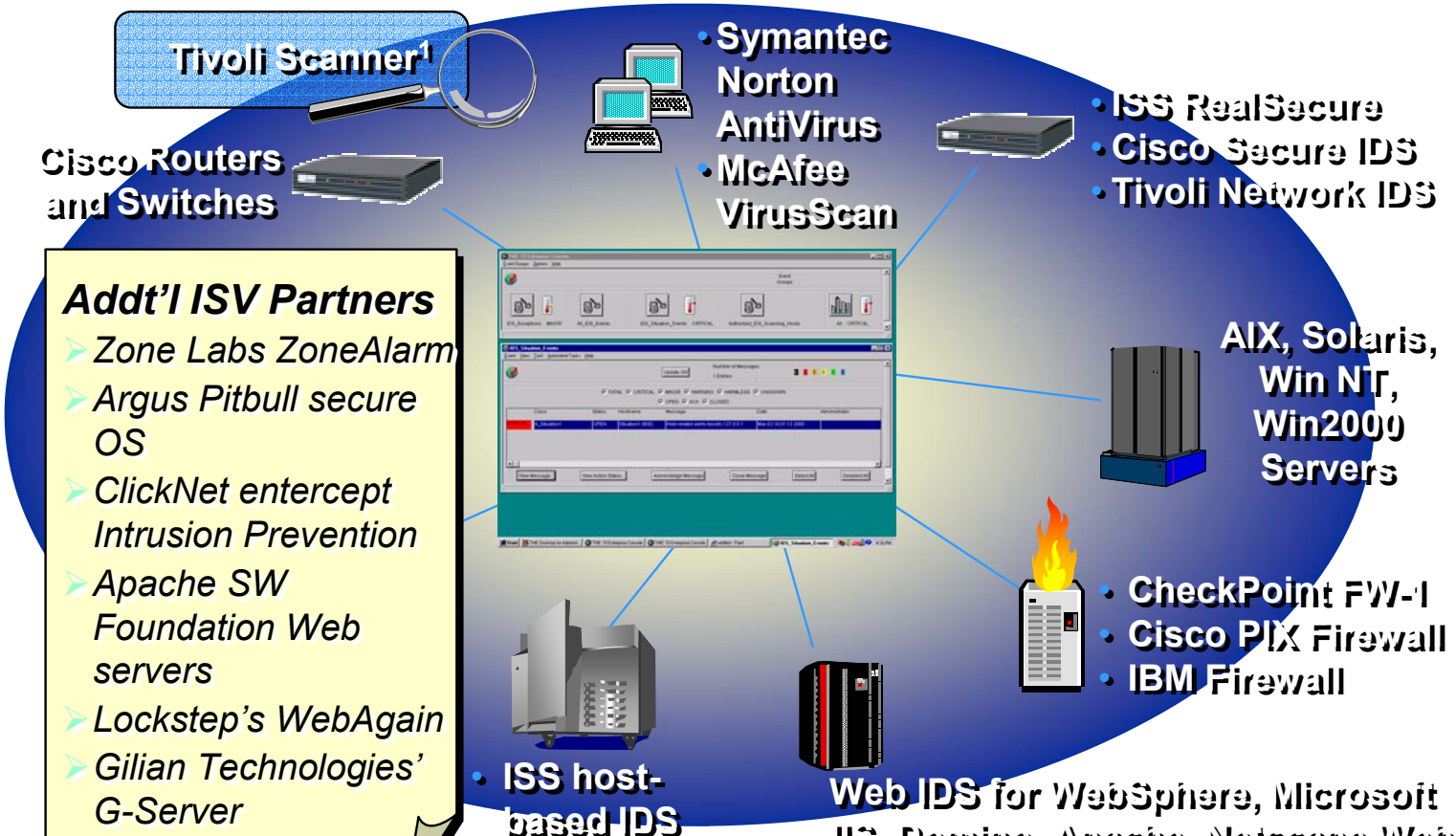


- Many sources of alarms, alerts
- Single problem can generate hundreds of events
- Poor operator productivity because of multiple consoles
- Staff can't zero in on the critical, relevant problems

Tivoli Risk Manager Architecture



Tivoli Risk Manager Integration



[1] Technology Preview

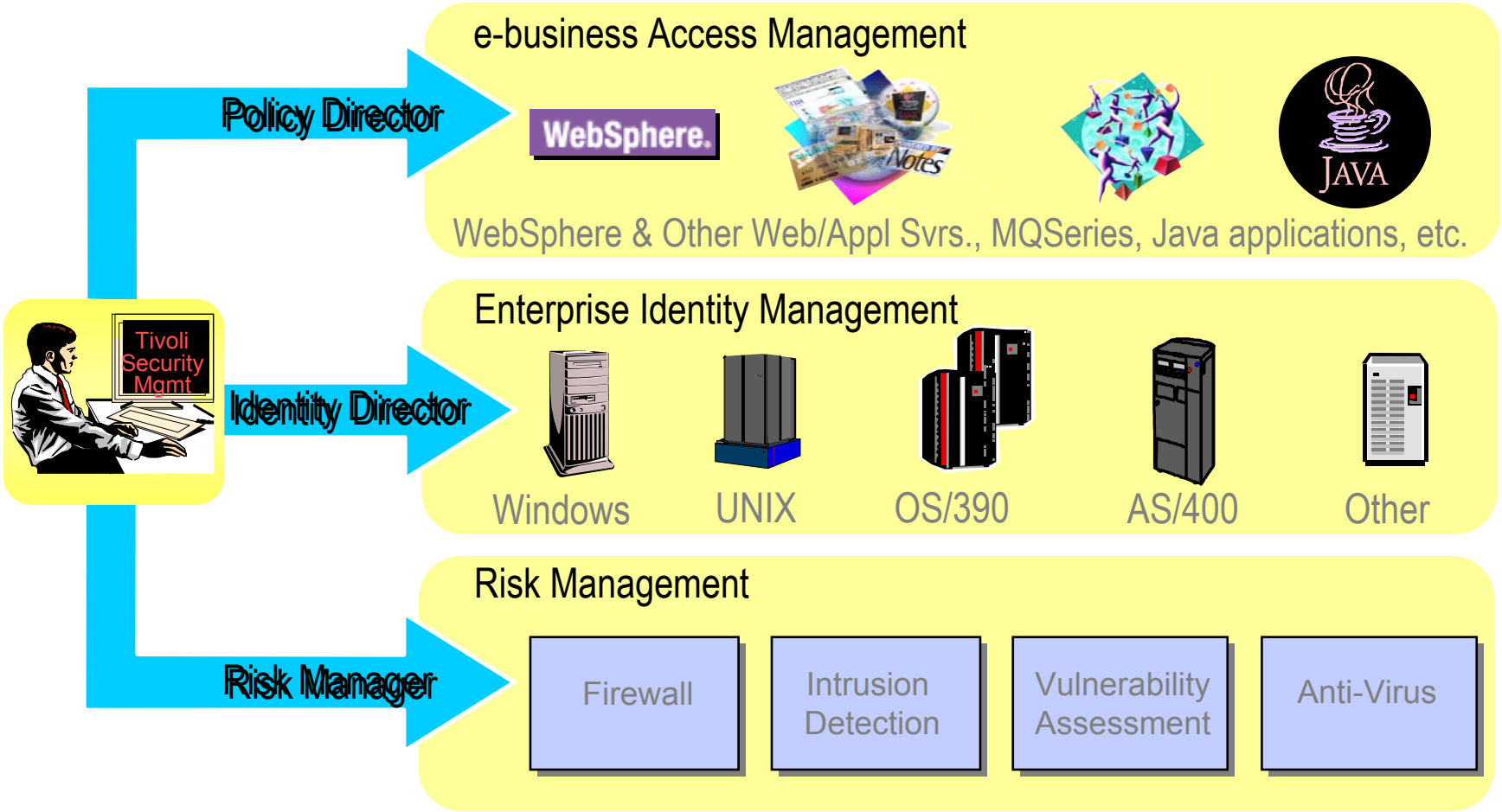
Intrusion Manager

- Intrusion Manager is a subset of Risk Manager, specifically designed for mid-sized e-businesses to mitigate risks and reduce security vulnerabilities. The software enables organizations to monitor attacks, threats and exposures across third-party applications, servers, network devices and operating systems, from a centralized management console.
- Intrusion Manager serves as an entry security management tool for mid-sized companies that need to identify real security threats in the network and Web servers by reducing security event clutter and false positives.
- Components:
  - Event correlation engine
  - Web intrusion detection system (IDS)
  - Network IDS
  - DB2 Universal Database

Other Tivoli Security Offerings and Infrastructure

- Tivoli PKI
- Tivoli Global Sign-On (GSO)
- Tivoli Policy Director for Application Servers
- SecureWay Firewall
- GSKit – Imbedded S/MIME CMS, SSL and Crypto toolkit
  - AdTech investigation – OpenSSL's SSL & its imbedded libcrypt
- Java security
  - JCE, JSSE, JGSS (Kerberos mechanism), JPKI, JAAS, etc.
    - Major contributions back to Sun
  - Participating in JCP, W3C XML DSig, Crypto, XKMS, XACML, OASIS SAML, Web Services security, etc.

Recap of Tivoli Security Portfolio



Privacy

TOYSRUS.COM Pays $50K to Settle Privacy Case

- Toysrus.com no longer faces privacy violation charges in New Jersey after agreeing to pay the state $50,000 to develop educational programs on Internet privacy issues. The settlement was announced last week in Newark by the state Division of Consumer Affairs. The privately held subsidiary of Toys R Us Inc. had been sued for allegedly sharing customers' personal information gleaned from tracking Internet users' movements on the retailer's Web sites. As part of the agreement, Fort Lee, N.J.-based Toysrus.com admits no wrongdoing. The company also says it now prominently displays its privacy policy on its Web sites. Other lawsuits have been lumped together in a class-action suit to be heard in a San Francisco federal court.

Eli Lilly Settles FTC Charges of Web Privacy Violation

- January 22, 2002

  On January 18, the Federal Trade Commission (FTC) announced that Eli Lilly has agreed to settle charges related to the unauthorized disclosure of personal information received from consumers through the company's Web site, Prozac.com. At the site, over 600 consumers signed up to receive messages reminding them to take the company's anti-depressant drug Prozac. Last June, while notifying these consumers that the service was to be discontinued, the company disclosed the email addresses of everyone who had signed up for this service.

  See also: 2002.02.27's episode of *Law and Order*.

SNAFU Leaves Thousands of Medical Records Exposed

- February 8, 1999

  Medical Records Exposed by James Glave, Wired News

  A Web-server administration snafu at the University of Michigan Health System left thousands of patient medical records open to the world until late Monday morning.

Current and Future Tivoli Privacy Manager Mission

- "Privacy Manager provides an enterprise-wide system that enables a company to use the *Personally Identifiable Information* (PII) it collects according to the principles of Fair Information Practices and monitor and enforce its compliance to those principles."
- Direction: Privacy Manager's dynamic roles support will be subsumed by Policy Director over time.
- Direction: Particpating in P3P's next-generation *Enterprise Privacy Markup Language* (EPML) definition and implementation.

The Five Steps of Privacy Management

1. Define the privacy policy.
2. Deploy the privacy policy.
3. Record user consent to policy.
4. Monitor/Enforce access according to the policy user consented to.
5. Create audit trail reports.

Revised Mission Statement

- "Privacy Manager will add the best practices of privacy management to your e-business applications and will manage the data these applications collect according to the OECD* Guidelines on the Protection of Privacy."

  Note: OECD Guidelines have replaced the FTC's "Fair Information Practices" because the OECD Guidelines are more "global."

* Organization for Economic Cooperation and Development, http://www.oecd.org

Exploitation of Tivoli Security Infrastructure

Exploitation of Tivoli Security by other IBM offerings

- Infrastructure: 50+ products
- Policy Director
  - WebSphere Edge Server
  - WebSphere Everyplace Suite
  - IBM Global Service's Policy Director Practice
  - Direction: Increased support for WebSphere Application Server and other J2EE-conformant web application servers
- Identity Director
  - Direction: Use by WebSphere Application Servers for user self-registration/care

January 2002 IBM-VeriSign (non-exclusive) announcements

- IBM will offer Tivoli Policy Director as a managed service, hosted by VeriSign and called the "VeriSign Managed Entitlement Service." Both Tivoli software and VeriSign will offer this.
  - Note that Tivoli Policy Director, WebSEAL, PD/MQ, etc. will continue to support other IETF PKIX-conformant PKIs.
- IBM and VeriSign will continue to develop standards and Web Services technologies to provide trusted services, (e.g., XKMS and SAML).
- IBM Global Services (IGS) will offer Public Key Infrastructure (PKI) as a managed service, hosted by VeriSign. IGS and VeriSign have announced a new global partnership, which includes IGS' new integration services for VeriSign's existing managed PKI service.
  - Note that Tivoli PKI continues to be offered and fully-supported within the Tivoli Security software portfolio.

Back Matter

Acknowledgements

- Mike Campbell
- Calvin Powers

For More Information

- http://www.tivoli.com/security
- http://www.ibm.com/security