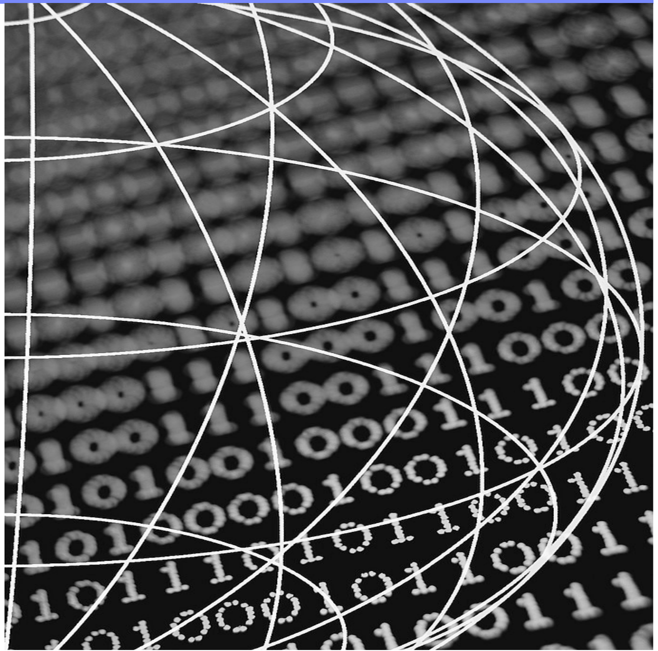
Securing the Enterprise Leveraging System z™



Tivoli software

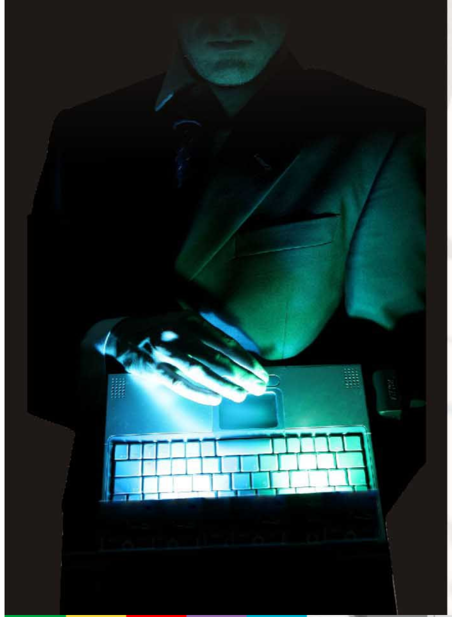
ON DEMAND BUSINESS

A Security Perspective

- Companies are seeking comprehensive security approaches to protect the **extended** enterprise
- **Regulatory** compliance requirements raise security visibility to the executive suite
- Every new technology generation unveils new vulnerabilities- you **cannot just protect the perimeter**
- Attackers revise their tactics. To ward off new threats, security must be **integrated** into the infrastructure stack
- The **global** workplace introduces additional risks; main processing hubs must be especially resilient
- Organizations that innovate with **SOA applications** need supporting security services

Security Threats are Pervasive

Breaches demonstrate the spread of security threats



Data theft affects 88 million-plus Americans
SearchSecurity.com, June 21, 2006

Phishing attacks against over two dozen European banks were detected by security firm Websense last weekend
The Register, September 20, 2005

MasterCard says 40 million files are put at risk.
New York Times, May 18, 2005

Government agencies and companies in the U.K. are under attack by a concerted series of Trojan horses out to steal information.
TechWebNews, June 16, 2005

New Trojan Hits Symbian Smartphones
Information Week, July 5, 2005

The number of bank accounts accessed illegally by a New Jersey cybercrime ring has grown to 676,000, according to police investigators.
ComputerWorld, May 20, 2005

At least a million machines are under the control of hackers worldwide.
ZDNET March 16, 2005

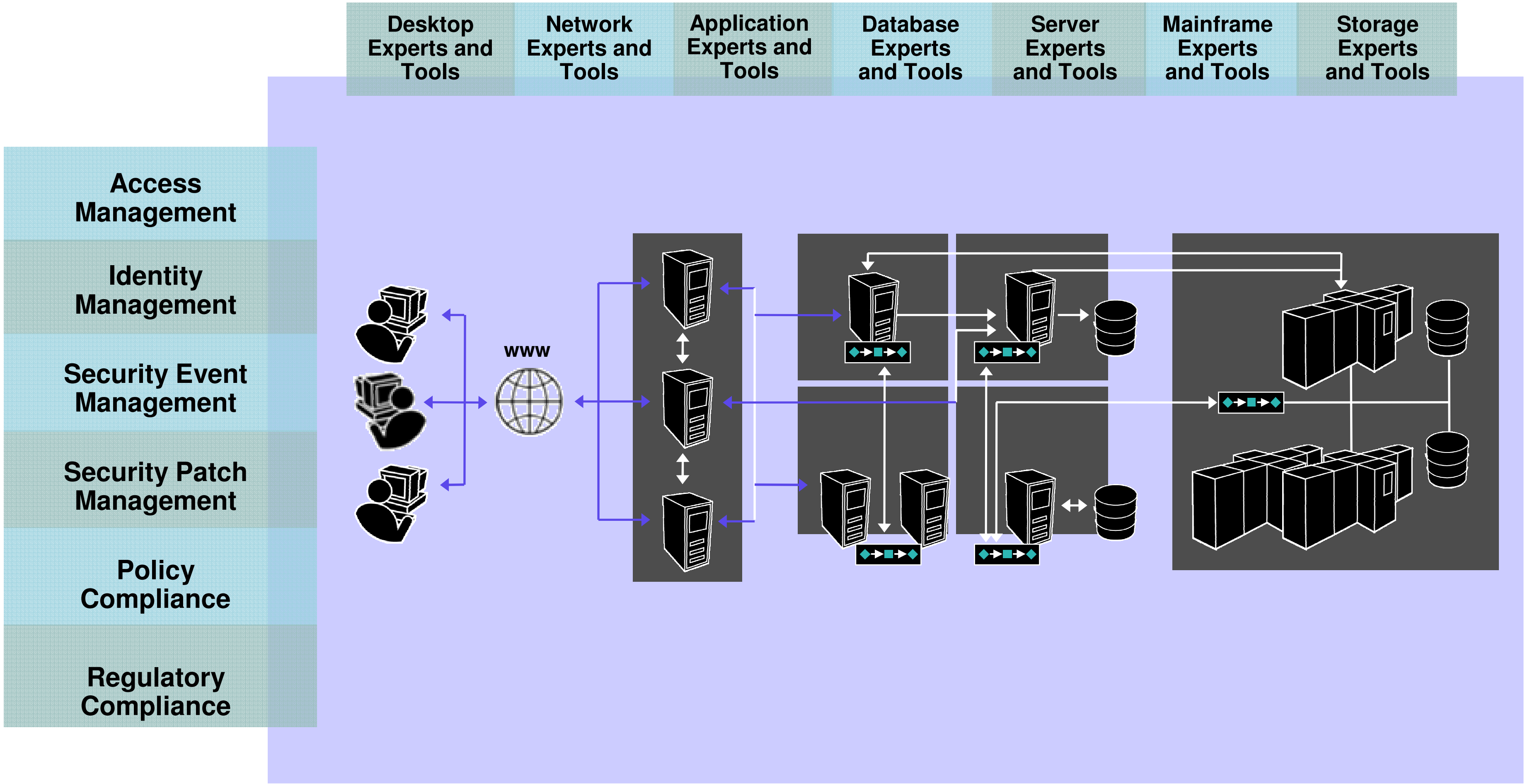
System z Architecture: Security Built In By Design

Proven secure by 40 years of secured operations!

- Enforced Workload Isolation
  - Each user in a separate address space
  - LPAR separation ensures integrity
  - Supervisor state & system programs protection
- Authorized program facility (APF)
  - Executables only accessible to authorized users
- Storage Protection Keys
  - Controls access to protected storage
  - Cross memory services prevent unauthorized data access
- Access Control Environment Element (ACEE)
  - z/OS security control block itself is protected
- Common Criteria program certifies IBM software at the highest levels
  - z/OS and RACF at a high level of certification (EAL4+)
  - LPAR at EAL 5

End to End Security

Multiple security-related events and workloads, leads to increased likelihood of error, vulnerability, non-compliance, and business loss.

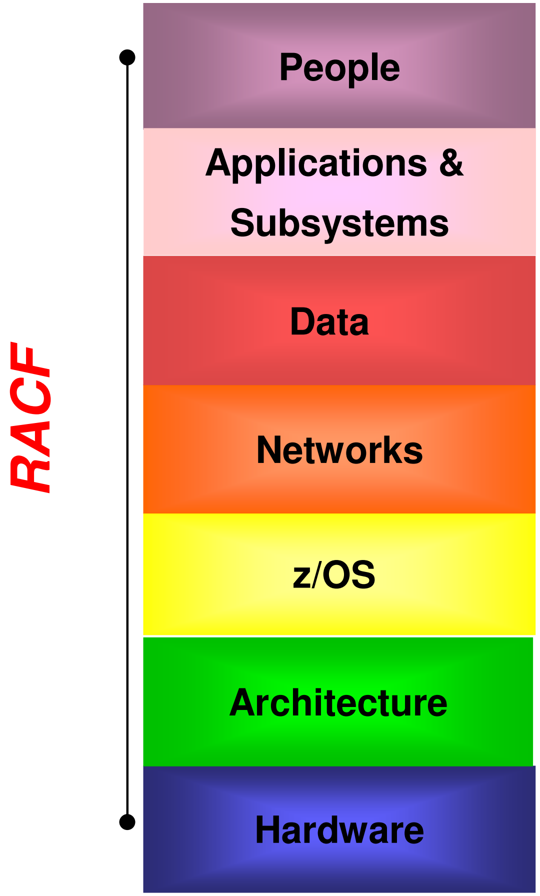


Desktop Experts and Tools
Network Experts and Tools
Application Experts and Tools
Database Experts and Tools
Server Experts and Tools
Mainframe Experts and Tools
Storage Experts and Tools
Access Management
Identity Management
Security Event Management
Security Patch Management
Policy Compliance
Regulatory Compliance
www

Integrated Security Throughout the Stack Uses System z

Includes identity management and privacy management	Users	RACF Administration	Privacy	Vanguard
Applications, OLTP and other subsystems maintain integrity	Applications-Subsystems	Integrated Subsystem Security	RACF	Logging and auditing
Information protected against unauthorized access	Data	Data Life Cycle Encryption	Multilevel Security	Tape encryption
Internetworked SOA applications require integrated security	Networks	Secured communication	Network resource protection	Intrusion Detection
RACF built into architecture, ensures consistent security	z/OS	RACF Enforcement	Authorized System Programs	Common criteria evaluation
Secured operating system designed to prevent viruses and malware	Architecture	Storage Protect Keys	Workload Isolation	No Buffer overflow
Hardware has built in security protection, encryption, and resiliency	Hardware	Tamper proof cards	Tape Encryption	Hardware crypto processor

The Backbone of System z Security



RACF

People

Applications & Subsystems

Data

Networks

z/OS

Architecture

Hardware

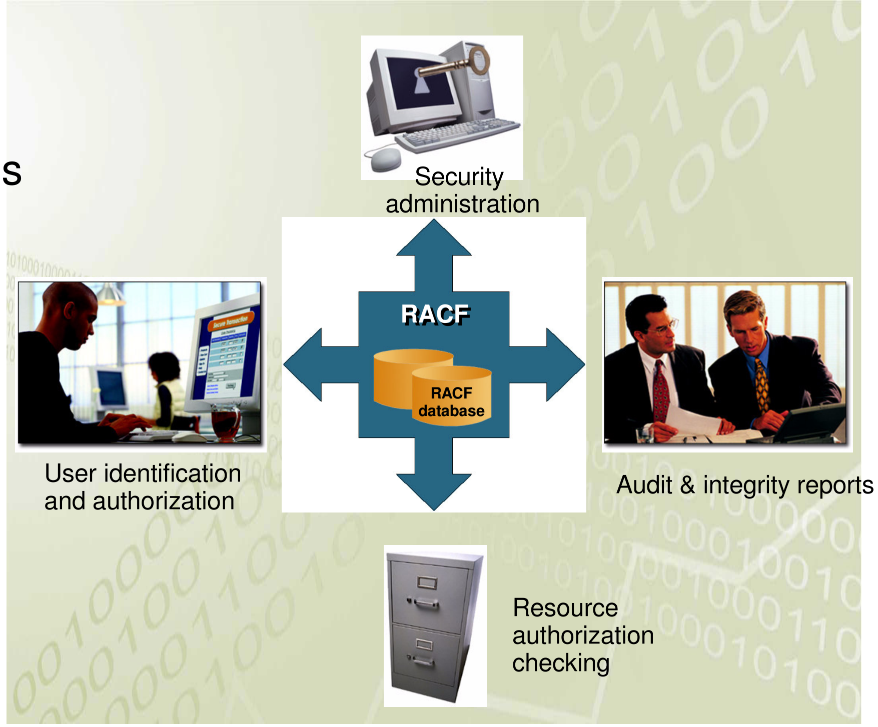
Resources protected by RACF:

- Programs
- WebSphere
- CICS
- DB2
- SNA/VTAM
- Console
- VSAM
- Print
- DASD

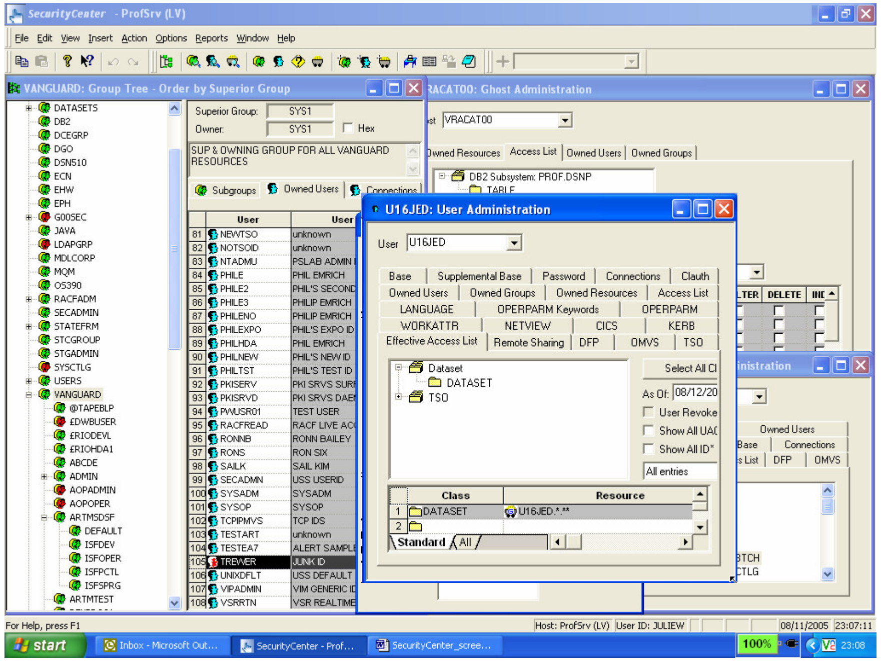
- Utilities
- MQ
- IMS
- ISO
- SDSF
- JES2/JES3
- DFSMS
- Ports
- Tape

RACF Provides Comprehensive Security for System z and the Extended Enterprise

- Resource Access Control Facility (RACF) part of the Security Server for z/OS
- RACF controls access to all System z resources
- What does RACF do?
  - Identifies and authenticates users
  - Matches security classification of users and resources to authorize access
  - Identifies users optionally via digital certificates
  - Logs and reports access attempts
  - With remote sharing, allows administrators to manage several systems centrally
- It is impossible to bypass RACF


Security administration
RACF
RACF database
User identification and authorization
Audit & integrity reports
Resource authorization checking

Simplifying z/OS administration and audit
Vanguard Security Solutions to simplify administration



Superior Group: SYS1
Owner: SYS1 □ Hex

SUP & OWNING GROUP FOR ALL VANGUARD RESOURCES

	User	User
81	NEWTSO	unknown
82	NOTSOID	unknown
83	NTADMU	PSLAB ADMIN I
84	PHILE	PHIL EMRICH
85	PHILE2	PHIL'S SECOND
86	PHILE3	PHILIP EMRICH
87	PHILENO	PHILIP EMRICH
88	PHILEXPO	PHIL'S EXPO ID
89	PHILHDA	PHIL EMRICH
90	PHILNEW	PHIL'S NEW ID
91	PHILTST	PHIL'S TEST ID
92	PKISERV	PKI SRVS SURI
93	PKISRVD	PKI SRVS DAEI
94	PWUSR01	TEST USER
95	RACFREAD	RACF LIVE ACC
96	RONNB	RONN BAILEY
97	RONS	RON SIX
98	SAILK	SAIL KIM
99	SECADMN	USS USERID
100	SYSADM	SYSADM
101	SYSOP	SYSOP
102	TCPIPMVS	TCP IDS
103	TESTART	unknown
104	TESTEA7	ALERT SAMPLE
105	TREWER	JUNK ID
106	UNIXDFLT	USS DEFAULT
107	VIPADMIN	VIM GENERIC ID
108	VSRRTN	VSR REALTIME

...st VRACAT00

DB2 Subsystem: PROF.DSNP
TABLE

User U16JED

Dataset
DATASET
TSO

As Of: 08/12/20
□ User Revoke
□ Show All UAC
□ Show All ID*
All entries

	Class	Resource
1	DATASET	U16JED.*.**
2		

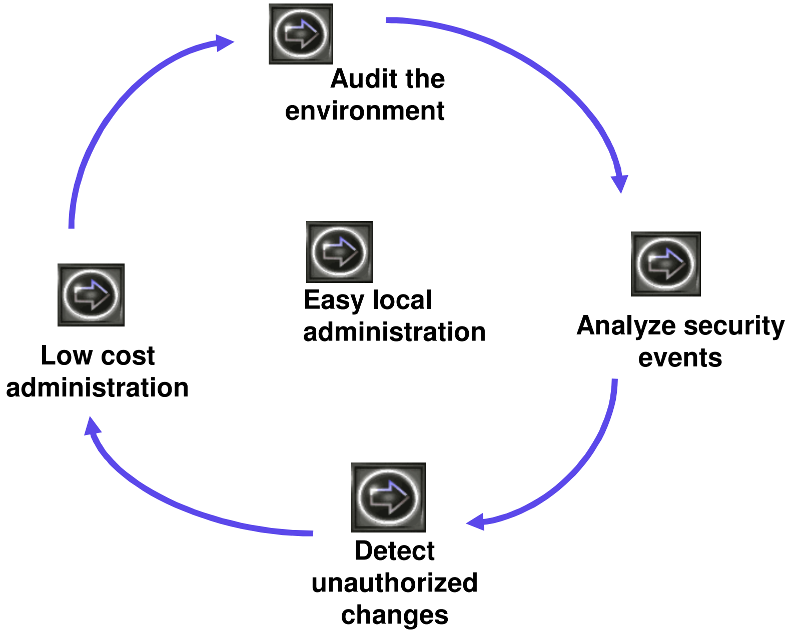
Host: ProfSrv (LV) User ID: JULIEW 08/11/2005 23:07:11

- IBM & Vanguard Security Solutions
  - **Vanguard Security Center** offers ease-to-use graphical user interface for RACF and DB2 security administration on z/OS
  - **Vanguard Administrator** provides advanced security server management and analysis with automation and power utilities
  - **Vanguard Analyzer** assists with security system snapshots or full-scale System z9 security audits
  - **Vanguard Enforcer** manages and enforces security policy in z/OS and RACF
  - **Vanguard Advisor** provides event detection, analysis and reporting capabilities for the z/OS and RACF

Vanguard Provides a Modern User Interface for RACF

Security Management Solutions:

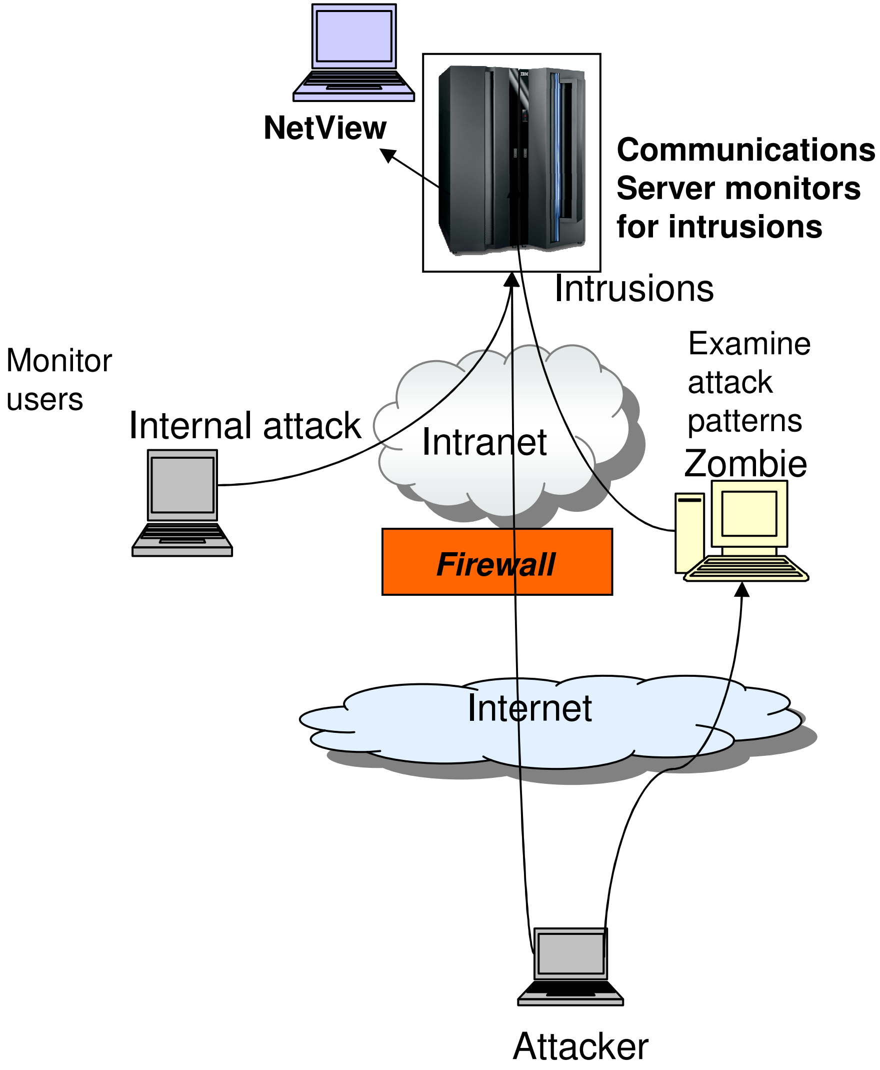
- Security administration, integrity auditing, and management
- Address stringent security rules and regulations
- Simplify RACF security administration and enforce best practices



Vanguard Tools
Simplifies Administration and helps with Auditing

Network Security Enabled by System z Communciation Server

- Information Spying
  - Network and system topology
  - Data content and location
- Impersonation/Theft
  - Initial attack launches further attacks on others
- Denial of Service
  - Attack on availability
  - Floods systems
  - Can be run from a zombie machine
- Attacks can occur from Internet or intranet
  - Firewall provides some protection
  - Perimeter Security may not be sufficient
  - Requires trust of intranet
- Considerations:
  - Access permitted from Internet
  - Internal attacks
  - Errors



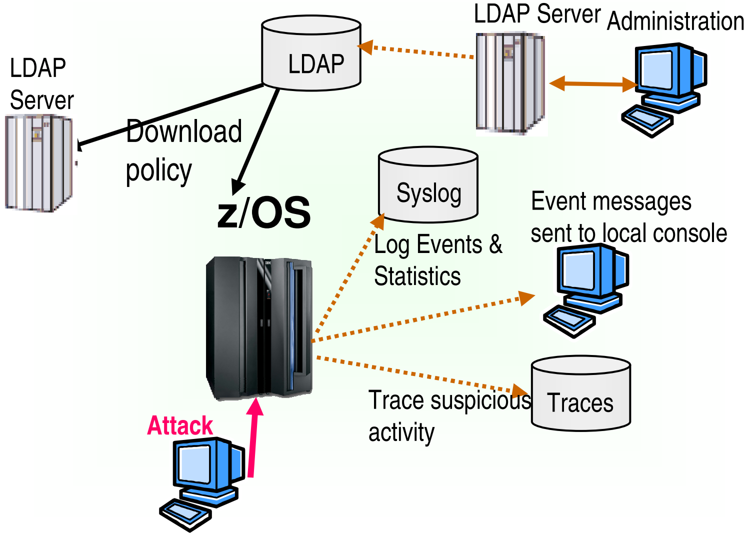
Network Security

Security features of System z Communications Server

- Intrusion Detection Services
  - Detects, records, and defends against scans, stack attacks, flooding
- Protect system integrity
  - Protects against Denial of Service
  - IP packet filtering eliminates malicious traffic
  - Intruders can't access system log
- Protect network resources
  - Protect users from sending to certain TCP/IP addresses, ports, FTP, network commands, socket options
- Protects network data
  - Encryption with Triple DES
  - Uses crypto hardware assist
- Transparent Application Security
  - Enable stronger network security without changing application code
- Network security protocols supported
  - Secure Sockets Layer SSL
  - Kerberos support
  - Secure Domain Name Server
  - SNMPv3

Communications Server: More than Intrusion *Detection*- Intrusion *Defense*

- Defines profiles of suspected IP traffic
- Monitors incoming packets
- Built in alternative to firewalls
- Can evaluate encrypted data *after* decryption
- Defends against malicious attacks real time:
  - Scans, Attacks, Flooding
- Filters inbound and outbound packets according to rules:
  - Packet information, IP address, port, protocol, time
- Proactive– active defense against intrusions
  - Packet discard, Limits number of connections
  - Logs errors
- Reporting:
  - Logs to NetView



ISS Acquisition- Extend Network Security Services to the endpoints

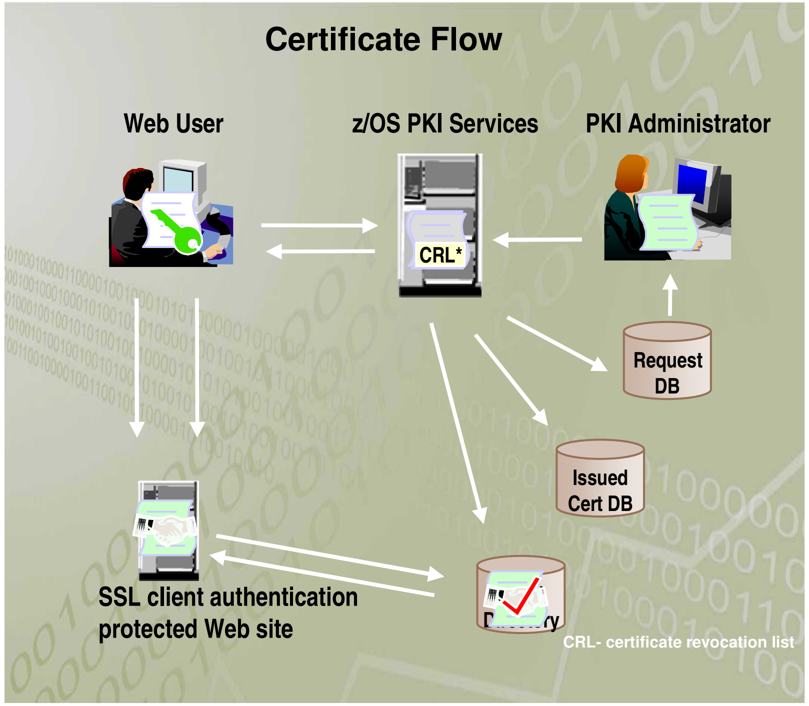
- ISS products are targeted in specialized security infrastructure and operational layer
  - intrusion detection and prevention, vulnerability assessments and remediation.
  - ISS' security products add another layer of protection as SOA is extended throughout the organization
- ISS Solutions include
  - Proventia Intrusion Detection and Prevention products prevent multiple forms of attack
  - Vulnerability Scanning technologies
  - Proventia Desktop for a multi-layered approach to securing endpoints within the network
  - Proventia portfolio of server protection platforms
  - X-Force threat analysis
  - ISS Managed Security Services -system monitoring, emergency response and 24/7 protection.

A recent IBM study of 3000 CIOs revealed that 84% of IT executives believe that organized criminal groups possessing technical sophistication are replacing lone hackers in cyber -crime.

NEW!

Digital Certificates for Secured Transactions

- A PKI infrastructure is the standard for public-key cryptographic security that ensures the security of digital certificates.
- PKI Services is part of RACF
  - Customers can issue their own certificates
  - Customers can be their own CA
  - No need for extra infrastructure
- IdenTrust^{TM} compliant certification
  - standard used by over 60 banks
- Leverages System z capabilities:
  - Secures private keys with cryptography
  - Provides digital certificate life cycle management
  - Administer certificates via RACF
  - Dynamically checks for expired certificates
  - Support smart cards



CRL- certificate revocation list

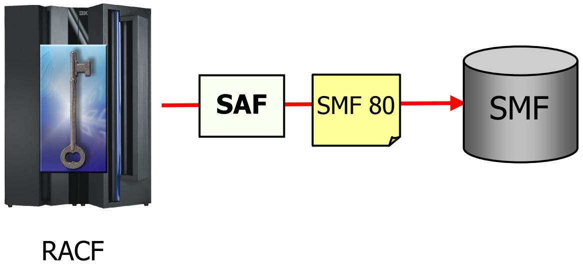
Reduce Risk of Inadvertent Errors as Well

IBM Health Checker identifies potential configuration problems such as changes in configuration values that occur over the life of an IPL before they cause damage

- Health checker consists of:
  - A framework to manage registration, scheduling, processing, reporting of health checks
  - Checking mechanism that evaluates settings
  - Extensible- authored by IBM, ISVs, or users.
- Health Checker Framework improvements:
  - Support for defining checks in parmlib
- More health checks:
  - GRS
  - Communications Server
  - DFSMS
  - others
- z/OS Communications Server GUI improvements:
  - Support for QoS and IDS policy configuration
  - Configure IPSec, AT - TLS, QoS, and IDS policy via a consistent user interface

Common Logging and Auditing

- All subsystems log RACF records system events from multiple subsystems
- Consistent and consolidated auditing to address compliance needs.
- Data Security Monitor Reports – 13 static reports that monitor system security and integrity
- Report access to protected resources, security violations, unauthorized actions
- Monitor user activities:
  - Write SMF records
  - Report Writer and XML reporting interfaces
- SMF Data Unload Utility

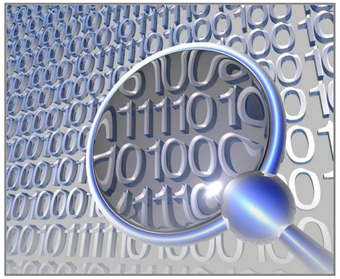


> "On a typical day, the security team logs 38,000 attempts – by unauthorized individuals or automated probes – to access the state's networks.
> **That's about one every 2.3 seconds.**"
>
> *Defending Data: a Never-Ending Vigil-Dan Lohrman, CSO , State of Michigan Baseline, 2004*

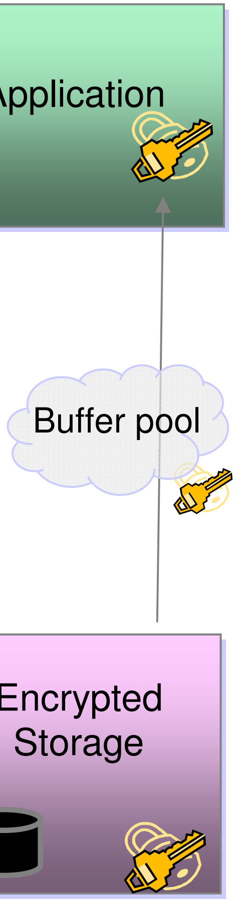
Additional Information Protection for Data and DB2

- IT shops must conform with privacy regulations, but resources and skills are scarce. Encryption solutions must be efficient and easy to implement.
- DB v8 also offers encryption options:
  - Column level encryption
    - Enabled by the application
  - Row level encryption
    - IBM Encryption Tool for DB2
- Encrypt DB2 System Resources helps prevent unauthorized access and use
  - Table and Index encryption
  - Image copies encrypted
  - Logs/archives encrypted
- Exploit System z Crypto Express2 hardware

Encrypt using the application or utilities



Encrypted on storage media



For Column and row level encryption

Data in channel, or in buffer pools is encrypted

Encrypted data stored on disk, in dump files, or on archival files

Data Protection Throughout the Life Cycle

Protection of data at rest

Encryption of Data with Key Management

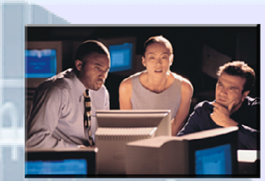
- Encrypt data on output, leverage z/OS key mgt.

Protection of data in transit

Encryption Services

- Secure data transfers across the Internet

Protection of data exchange



Java Client

- Provides secure data transfer with partners

- Provides long-term key management

Protection of archived data

DFSMSdss

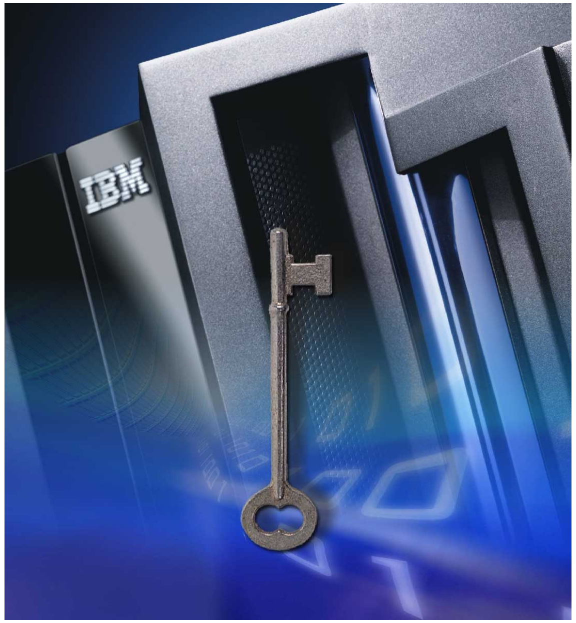
- Encryption for removable media

Over 90% Of Companies Regularly Expose Employee And Customer Data

System z Hardware Accelerates Encryption of Data

Cryptography for System z

- CP Assist for Cryptographic Functions (CPACF)
  - One CPACF chip per processor, scales out
  - Supports DES/TDES and SHA-256
  - Provides AES support in hardware
- Crypto Express2 (CEX2)
  - Tamper evident packaging
  - Configurable either as a Coprocessor or Accelerator
  - Very fast SSL processing
  - Available with System z9 EC, z9 BC, z990 and z890
- Optional TKE Workstation
  - Provides a secure, auditable, and remote method of key entry over a TCP/IP network
  - Runs on embedded operating system
  - Smart Card reader.



IBM Encryption Facility for z/OS

IBM Encryption Facility for z/OS
ICSF integrated key management
Cryptographic & Compression capabilities

Protected Data at Rest & in Transit
Encryption Services Feature

- Supports encrypting & decrypting data files
- Leverages z/OS centralized key management
- Uses mainframe cryptography & compression
- Can use Public Key/Private keys or passwords to create secure data exchange

Protected Data Exchange
Encryption Facility Client Web Download

- Java download code that allows client systems to decrypt and encrypt tapes for exchange with z/OS systems
- A decryption-only z/OS client. Can process encrypted and compressed data from z/OS Encryption Facility

Protected Data Archive
DFSMSdss Encryption Feature

- Allows encryption and compression of dump data sets created by DFSMSdss
- Supports decryption and decompression during RESTORE process
- Leverages z/OS centralized key management and IBM mainframe cryptographic and compression

Leverages z/OS centralized key management and IBM mainframe cryptographic and compression capabilities

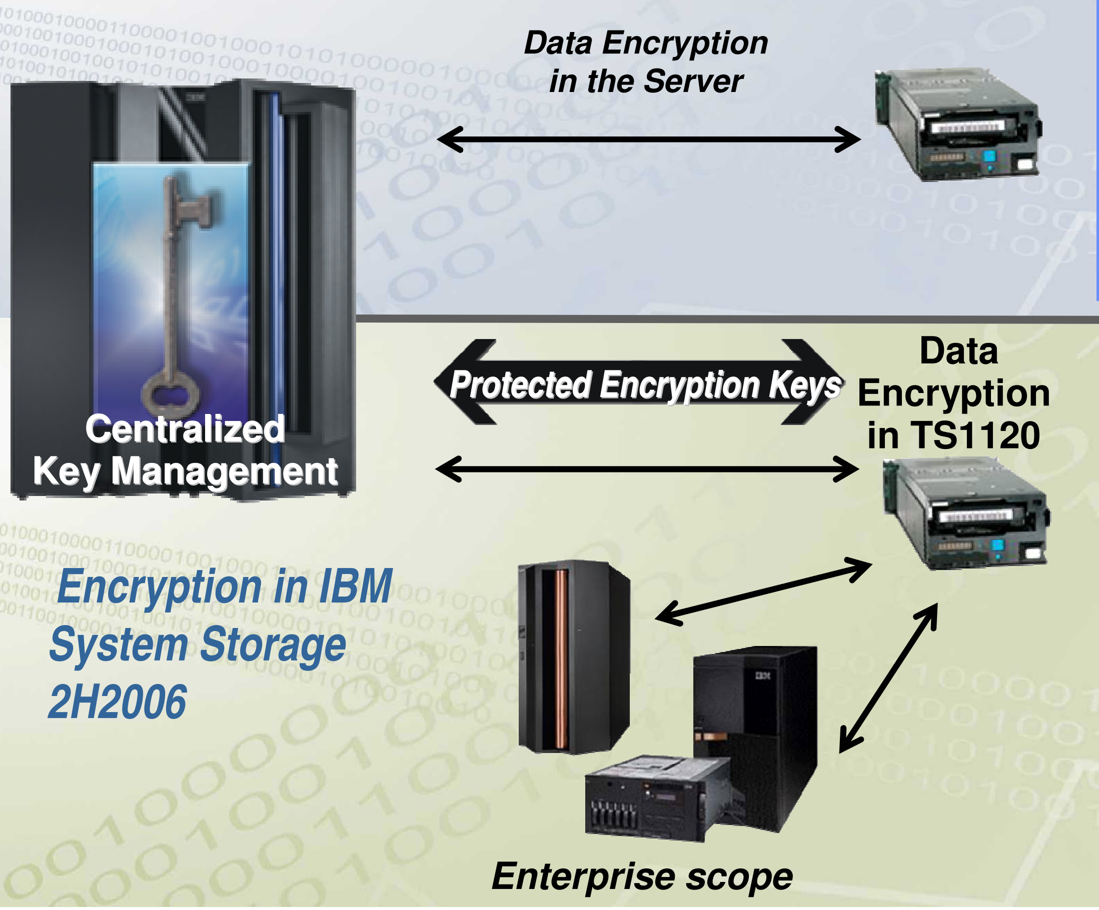
New Tape Encryption

z/OS centralized key management

- **Helps to protect and manage keys**
  - **Highly secure and available key data store**
  - **Long term key management**
  - **Key recovery**
  - **Single point of control**

Encryption Facility for z/OS, V1.1

- **Flexible options for business partner exchange**
- **Partners can encrypt and decrypt using no-charge JAVA client**
- **Supports public key or password based exchange**



Data Encryption in the Server
Centralized Key Management
Protected Encryption Keys
Data Encryption in TS1120
Enterprise scope

Encryption in IBM System Storage 2H2006

- **Highly secure tape library**
- **High performance archive encryption**
- **Transparent to existing applications**
- **Can help with audit compliance**

System z Certifications and Recent Tivoli evaluations

The Common Criteria program from NIST and NSA establishes a framework to evaluate the trustworthiness of IT products

IBM Tivoli Directory Server Version 6.0- evaluated under Common Criteria at Evaluated Assurance Level 4- March 2006.

IBM Tivoli Access Manager for e-business V 5.1 evaluated under the Common Criteria at EAL3.July 2005.

Tivoli Access Manager for Operating Systems V 5.1 was evaluated under the Common Criteria at EAL3- March 2006.

Tivoli Identity Manager Version 4.6 was evaluated under the Common Criteria at EAL3 - February 2006.

z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.7 + RACF
- **IdenTrust™** certification for z/OS PKI Services

System z EC and other System z servers

- **Common Criteria** EAL5 with specific Target of Evaluation
  - **Logical partitions (LPARs) thank**
- **FIPS 140-2 level 4**
  - Crypto Express 2

- **Common Criteria** EAL3+ with CAPP and LSPP
  - **z/VM 5.1 + RACF**

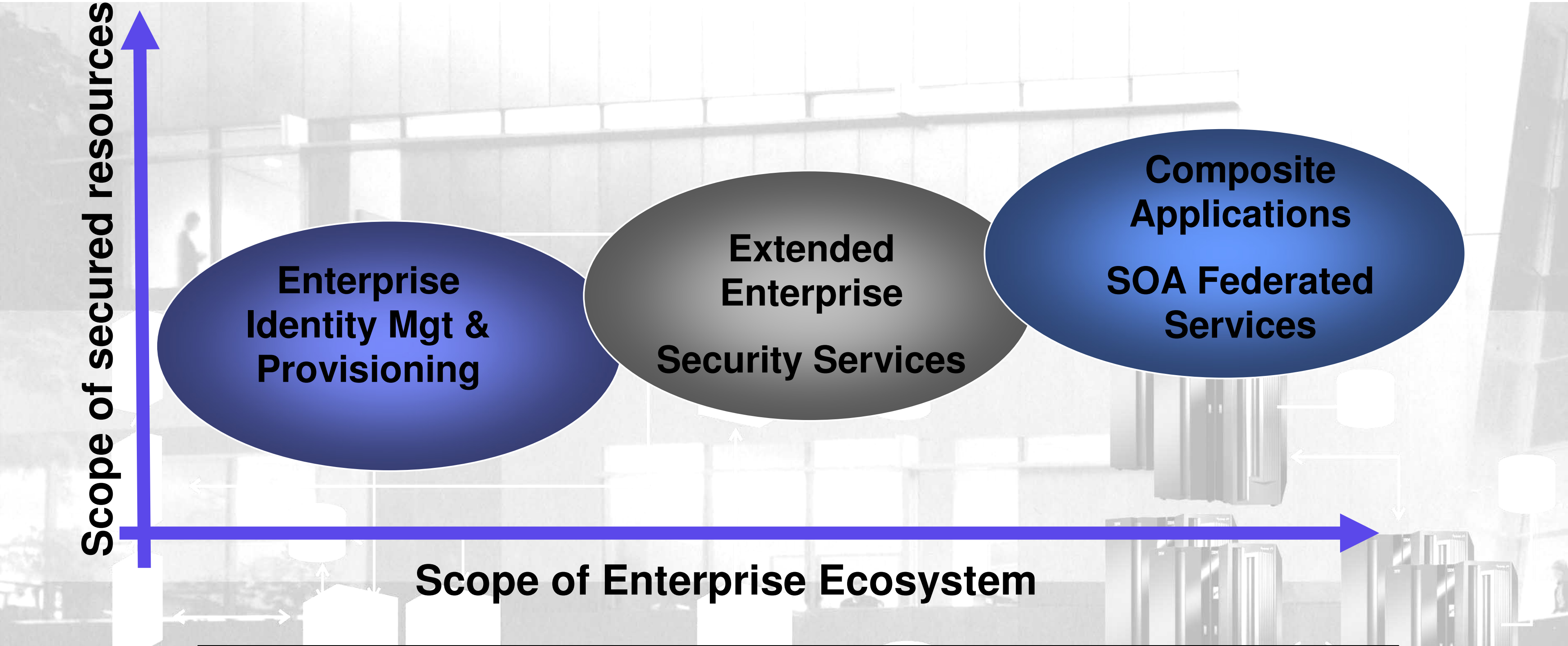
Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **SUSE LES9 certified**
- **Common Criteria** EAL3+ with CAPP and LSPP
  - **Red Hat EL3 certified at EAL3+**
  - **Red Hat EL4 EAL4+ in progress**

Tivoli Security Enhancements

- Tivoli security products increase the value of System z:
  - Enable System z customers to participate in a secured end to end security strategy
    - Provide a standards based approach to security
    - Provide seamless provisioning across platforms
    - Authenticate users with more precision
  - Provide audit and compliance to:
    - Report on security events
    - Analyze security logs
  - Provide a seamless approach to leveraging System z security capabilities outbound from the host
    - Leverage System z authentication
    - Leverage System z resource authorization
  - Begin to develop secured SOA applications
    - Leverage Tivoli and RACF
    - Authenticate more seamlessly

Securing identities across the Enterprise


Scope of secured resources
Enterprise Identity Mgt & Provisioning
Extended Enterprise
Security Services
Composite Applications
SOA Federated Services
Scope of Enterprise Ecosystem

New models of security and identity services will be required to integrate federated web services transactions. Current approaches will not scale to meet the emerging needs of complex company environments. Security can be rendered as a service that supports granular business processes spanning the extended enterprise and ecosystem.

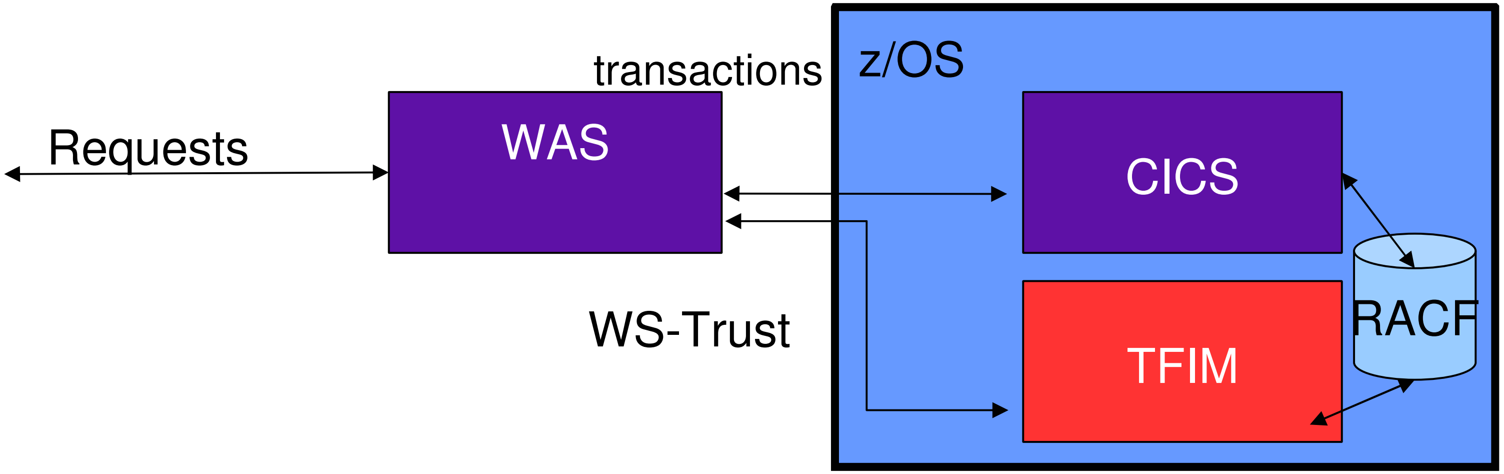
Federation at a glance

IBM Tivoli Federated Identity Manager V6.1 provides:

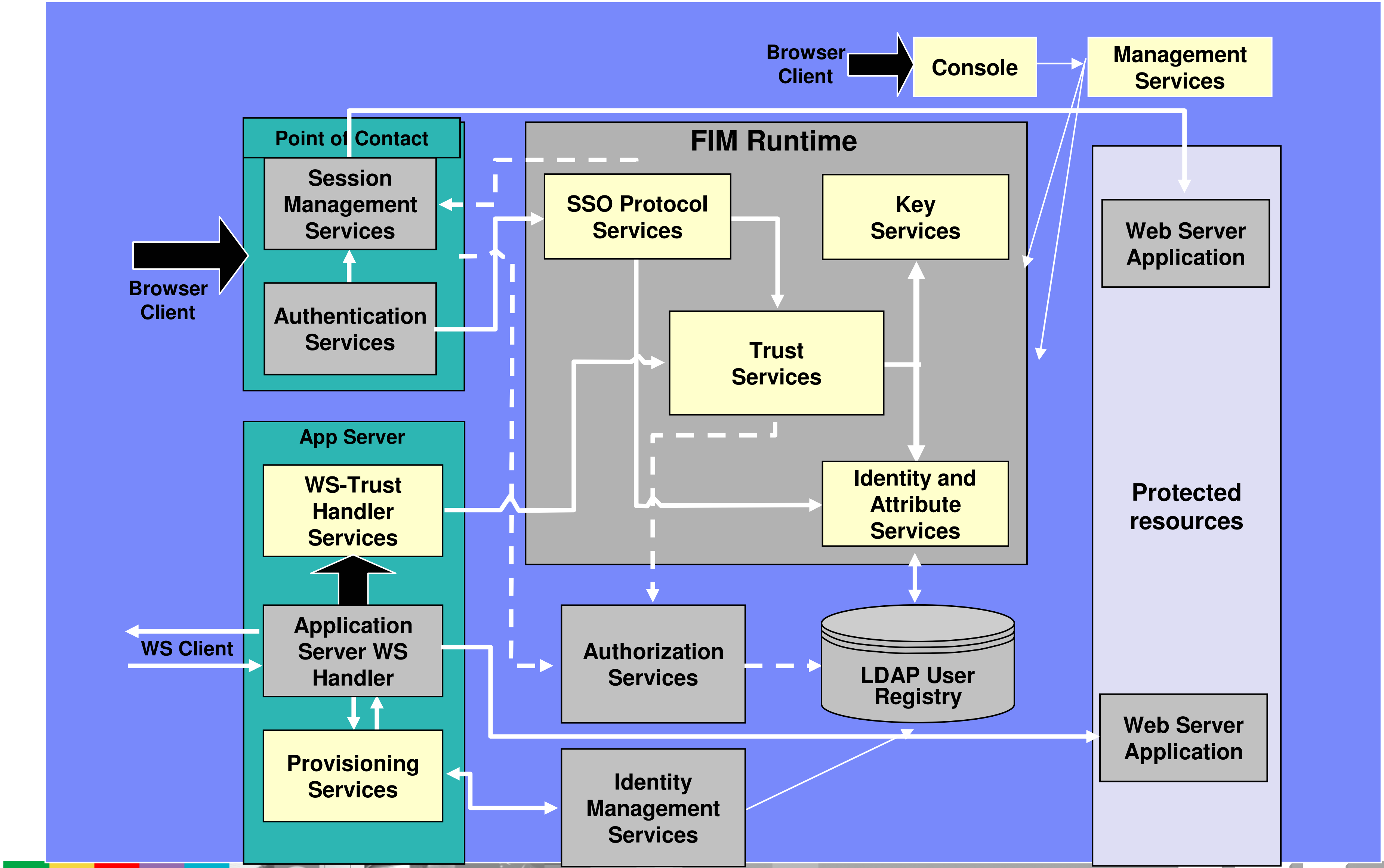
- Managed identity flow across services to help realize SOA benefits.
- Concurrent support for leading federated single sign-on protocols to allow collaboration with a partner organizations.
- Support for open standards and specifications including Liberty, SAML, WS-Federation, WS-Security and WS-Trust.
- Integrated audit data collection and reporting.
- Provides Security Token Services (STS) for identity mediation leveraged from WAS (WebSphere Application Server).
- Using the Tivoli reverse proxy, WebSeal, companies can integrate Web applications via a a web HTTP/HTTPS connection
  - Allows Web applications to connect into a federated environment without requiring application changes

Tivoli Federated Identity Manager on z/OS

- Allows web services, backed by z/OS-based subsystems, to be secured with z/OS Security Services
  - Preserve identity at granularity of original requesting user
  - Reduce operational cost, improve integration and user experience
  - Provide authentication processing across a heterogeneous environment and support transformations among credential formats
  - Supports SAML, Liberty, and WS-Federation
- Use z/OS Auditing (SMF) to improve regulatory compliance
- Use RACF passtickets in applications connecting to z/OS



FIM service architecture – The full picture



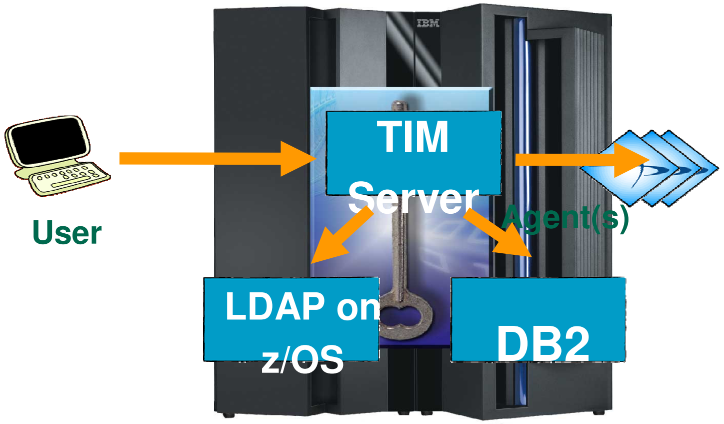
Uses of Tivoli Federated Identity Manager

- Supports SSO with emerging protocols
  - Use TFIM's Web Services Security Management and TAM for e-Business for single sign on
  - HTTP requests are handled by TAM for e-Business
  - Complex authentication and Single Sign-on flows are handled by TFIM
- Securing access to web services invocations
  - Use TFIM's Web Services Security Management, Web Services Gateway, and TAM for e-Business
  - Web Services requests are handled by the Web Services Gateway
  - Access control checks are handled by TAM access control engine
- Cross-organization user and group management
  - Use TFIM's WS-Provisioning support, TDI assembly lines, and Tivoli Identity Manager
  - WS-Provisioning web services requests are accepted by TFIM
  - TFIM uses TDI assembly lines to effect the changes requested and optionally invoke TIM APIs to effect the changes

Tivoli Identity Manager on z/OS (4Q06)

Helps centralize the definition of users and the provisioning of user services across your enterprise.

- Tivoli Identity Manager provides a:
  - Single point for managing users
  - Automated provisioning of resources
  - Self-care account and password resets
  - Web delegated administration
  - Simulation nd preview of provisioning policy
  - Auditing & Reporting Mechanisms



- It leverages automation tools which off-load administrative tasks
  - Self administer via A Web self-service interface and embedded workflow engine
  - Automate submission and approval of user administration requests

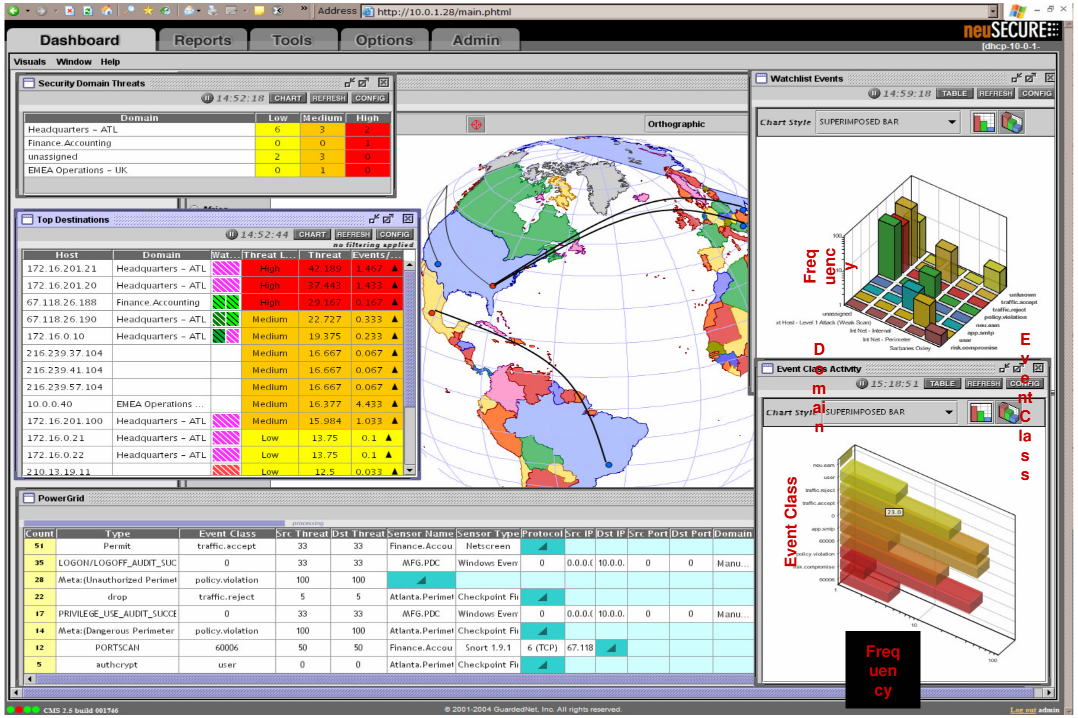
- Provides account discovery support and searches for out-of-policy changes made directly on a managed resource

- Centralizes the management of identity and account data
  - LDAP stores personal and account information
  - Database stores audit information
  - Agents perform operations on the target system

75-80% of Help desk calls are for password reset or other trivial items. Average per Call cost is about 20 Euros.

Tivoli’s Security Operations Manager 3.1

- Intelligent dashboard to manage complex security environments
- Real-time, cross-device event correlation to improve incident recognition
- Communicates critical security information throughout IT
- Integrated asset weighting to assist with prioritization
- Automated remediation
- Customizable reporting for audit and compliance



Security Domain Threats

14:52:18 CHART REFRESH CONFIG

Domain	Low	Medium	High
Headquarters – ATL	6	3	2
Finance.Accounting	0	0	1
unassigned	2	3	0
EMEA Operations – UK	0	1	0

Top Destinations

14:52:44 CHART REFRESH CONFIG

no filtering applied

Host	Domain	Wat...	Threat L...	Threat	Events/...
172.16.201.21	Headquarters – ATL	▨	High	42.189	1.467 ▲
172.16.201.20	Headquarters – ATL	▨	High	37.443	1.433 ▲
67.118.26.188	Finance.Accounting	▨▨	High	29.167	0.167 ▲
67.118.26.190	Headquarters – ATL	▨▨	Medium	22.727	0.333 ▲
172.16.0.10	Headquarters – ATL	▨▨	Medium	19.375	0.233 ▲
216.239.37.104			Medium	16.667	0.067 ▲
216.239.41.104			Medium	16.667	0.067 ▲
216.239.57.104			Medium	16.667	0.067 ▲
10.0.0.40	EMEA Operations ...		Medium	16.377	4.433 ▲
172.16.201.100	Headquarters – ATL	▨	Medium	15.984	1.033 ▲
172.16.0.21	Headquarters – ATL	▨	Low	13.75	0.1 ▲
172.16.0.22	Headquarters – ATL	▨	Low	13.75	0.1 ▲
210.13.19.11		▨	Low	12.5	0.033 ▲

PowerGrid

processing

Count	Type	Event Class	Src Threat	Dst Threat	Sensor Name	Sensor Type	Protocol	Src IP	Dst IP	Src Port	Dst Port	Domain
51	Permit	traffic.accept	33	33	Finance.Accou	Netscreen	◢					
35	LOGON/LOGOFF_AUDIT_SUC	0	33	33	MFG.PDC	Windows Even	0	0.0.0.(	10.0.0.	0	0	Manu...
28	Meta:(Unauthorized Perimet	policy.violation	100	100	◢							
22	drop	traffic.reject	5	5	Atlanta.Perimet	Checkpoint Fi	◢					
17	PRIVILEGE_USE_AUDIT_SUCCE	0	33	33	MFG.PDC	Windows Even	0	0.0.0.(	10.0.0.	0	0	Manu...
14	Meta:(Dangerous Perimeter	policy.violation	100	100	Atlanta.Perimet	Checkpoint Fi	◢					
12	PORTSCAN	60006	50	50	Finance.Accou	Snort 1.9.1	6 (TCP)	67.118	◢			
5	authcrypt	user	0	0	Atlanta.Perimet	Checkpoint Fi	◢					

CMS 2.5 build 001746

© 2001-2004 GuardedNet, Inc. All rights reserved.

Tivoli Directory Integrator for Consistent Identities

Maintain data consistency across multiple identity repositories to synchronize user information quickly and efficiently

- Cost-effective way to synchronize heterogeneous identity data sources in heterogeneous directories, databases, systems and applications
- Deploys a meta-directory that synchronizes data from disparate sources
- Provides a single access point to multiple data systems.
- Uses multidirectional data flows called Assembly lines.
  - links data residing across IBM and non-IBM directories, databases, password stores, and applications.
  - provides a front end to back-end data repositories.
  - clients can access TDI through LDAP, HTTP, Java™ Message Service (JMS), Web services and Java API.
- Automatically detects changes and pushes modifications out to databases & applications
- Triggers include e-mails, database or directory updates, HTML pages, SOAP messages

Family of Tivoli Access Manager Products

TAM for Business Integration

- Protects access to MQSeries queues; Protects messages sent over MQSeries queues

TAM for Operating Systems

- Enhances access control checks performed by Linux or AIX

TAM for e- business

- Authenticates users accessing information via the web
- Protects access to information based on URL
- Supports single sign on to multiple web-accessible applications

TAM for Enterprise Single Sign On

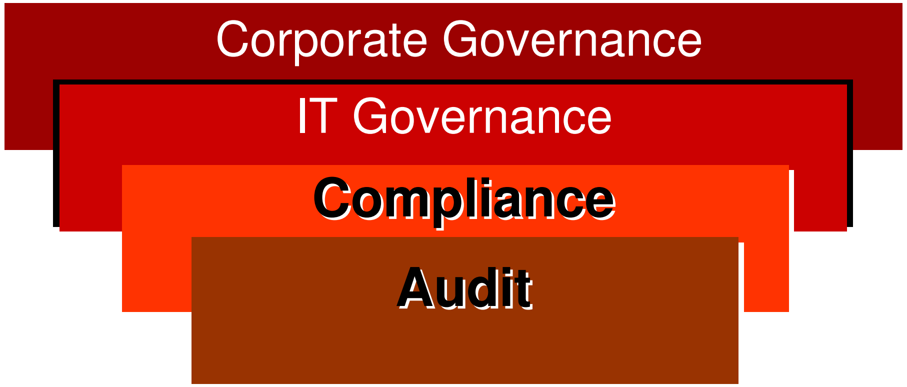
- Simplifies logon every application
- Random passwords can be set up so the user need not remember

Further Integration with System Z

Tivoli Access Manager for e-business

- A centralized approach to authenticating and authorizing access to Web applications - at the HTTP/HTTPS level
- A single sign-on for Web, Microsoft, telnet and mainframe environments
- Support for mainframe applications and support for Java 2 and Java Authentication and Authorization (JAAS) APIs on z/OS ;WebSphere on z/OS
- Offers a flexible and scalable proxy architecture & Web server plug-ins
- Provides role-based access control, support for user registries and platforms
- Use web-based SSO spanning multiple sites, exploiting cross-domain technology or protocols (e.g. SAML)
- Uses Common Auditing and Reporting Service for out-of-the-box reporting
- Supports many user-authentication mechanisms
  - user IDs, passwords,   certificates, tokens.

SOA, Governance and Compliance



Corporate Governance

IT Governance

Compliance

Audit

The current regulatory environment is driving adoption of control systems such as COSO or COBIT.

This is leading to the implementation of IT control systems such as ITIL.

This is taking place in the midst of business process reengineering via SOA-based models

A Compliance Perspective

Business Policy Compliance

Comply with policies governing business transactions between business partners, suppliers and customers

Security and IT Compliance

Comply with policies governing resource access, authentication, auditing and administration

Privacy & Regulatory Compliance

Comply with policies governing controls, segregation of duties, access to sensitive information

License & Asset Compliance

Comply with policies governing resource access, authentication, auditing and administration

Reduce Costs and Mitigate Risks

Compliance Risk Reduction

- Software vendor license compliance audits
- Compliance with business rules
- Impact of Sarbanes-Oxley Section 404

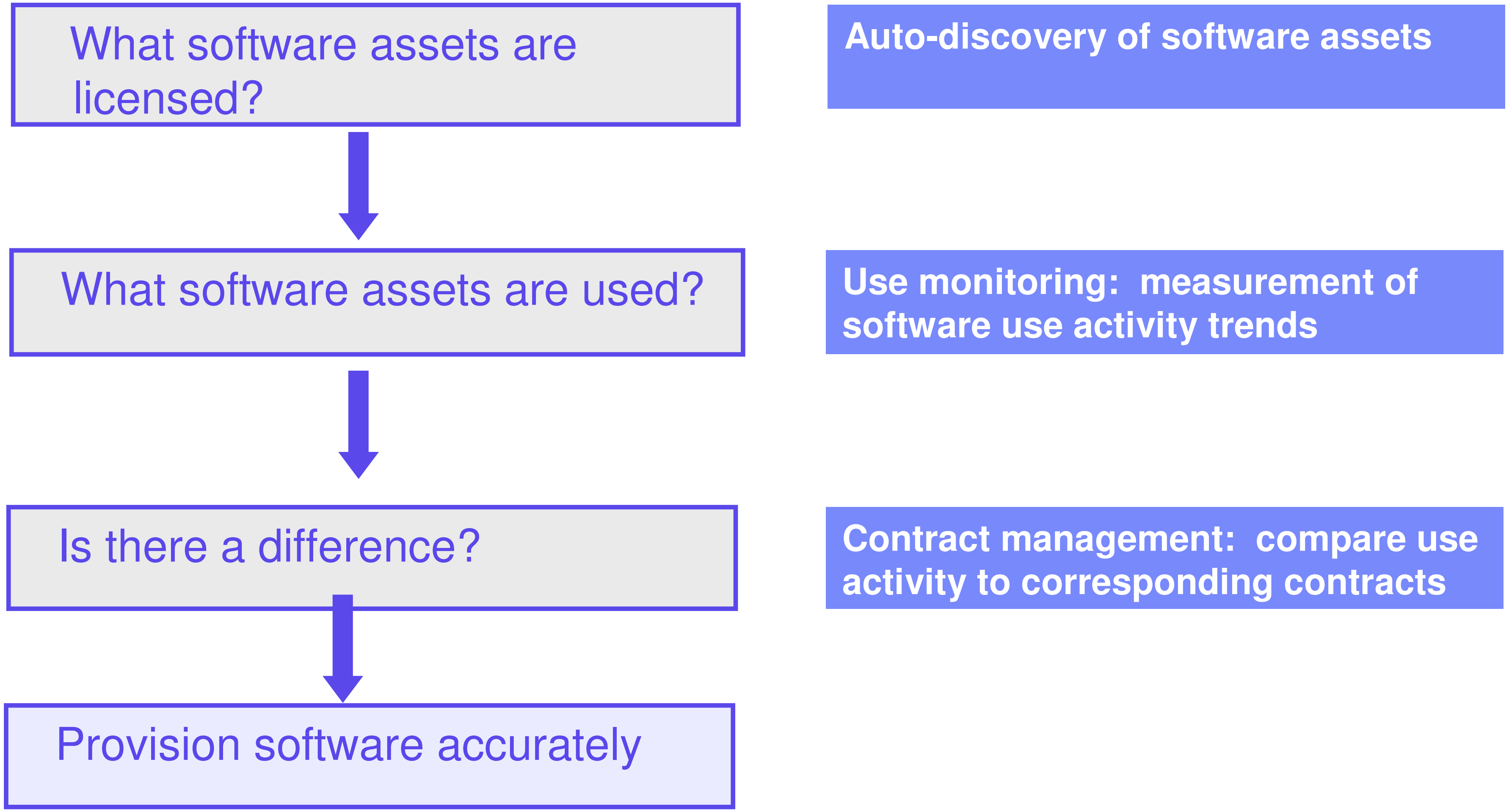
Software Cost Management

- Identification and reduction of underutilized software
- Efficient server consolidations
- Optimize software and hardware capacity upgrades
- Vendor contract negotiation leverage
- Reduced software fees through competitive replacement
- Invoice validation and charge-back
- Business continuity software licenses

"Enterprises that begin an asset management program experience up to a 30% reduction in costs the first year.. and continue savings of 5-10% for the next 5 years" – Gartner

Aligning IT Spend with Business Policy

Align IT Software Spending_with Business Priorities



What software assets are licensed?

Auto-discovery of software assets

What software assets are used?

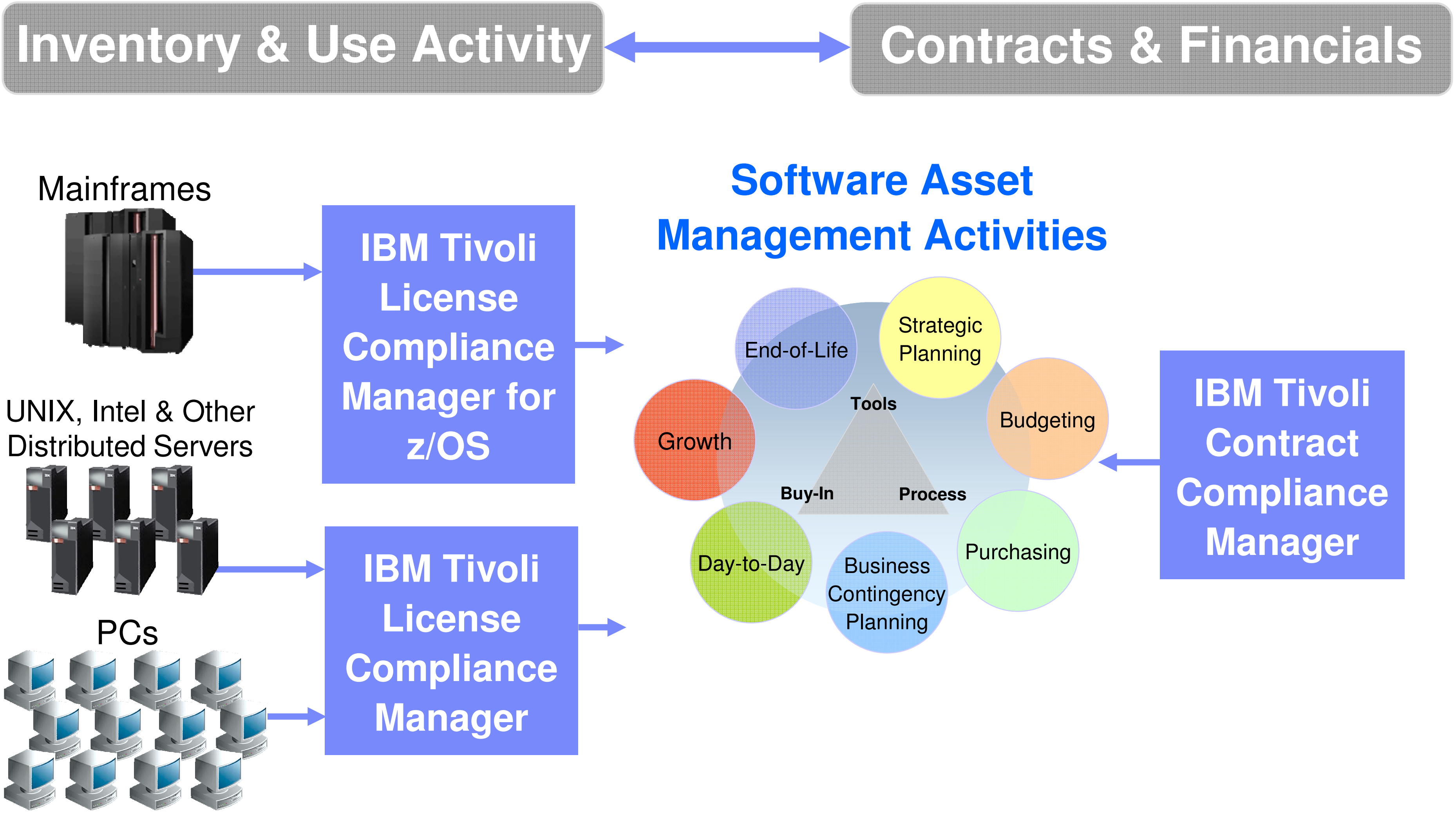
Use monitoring: measurement of software use activity trends

Is there a difference?

Contract management: compare use activity to corresponding contracts

Provision software accurately

Comply with Contractual & Business Policies


Inventory & Use Activity
Contracts & Financials
Mainframes
UNIX, Intel & Other Distributed Servers
PCs
IBM Tivoli License Compliance Manager for z/OS
IBM Tivoli License Compliance Manager
Software Asset Management Activities
End-of-Life
Strategic Planning
Budgeting
Growth
Tools
Buy-In
Process
Day-to-Day
Business Contingency Planning
Purchasing
IBM Tivoli Contract Compliance Manager

Summary: Comprehensive Security Capabilities

- Integrated throughout the stack
- Network security
- Compliance and audit support
- Data lifecycle protection
- Excellent cryptography
- Risk reduction
- Meets stringent standards
- Leveraged beyond System z

Rock Solid Security

Innovate securely

Leverage the synergy between Tivoli and System z to secure the federated enterprise

System z

B. Sannerud sannerud@us.ibm.com
SWG System z Competitive Project Office
https://w3-03.ibm.com/sales/competition/compdlib.nsf/pages/swgcpo

- EXTRA SLIDES DO NOT SHOW

Directional View of System z Security

Cryptography

- Improved autonomics around cryptography
- Extended cryptography support and improved authentication
- Management and maintenance of key information spanning multiple key stores
- Crypto enablement of new SOA applications
- Continued support for industry standards

Secured Enterprise

- TAM reverse proxy server on z/OS to further exploit System z security
- Map z/OS interface points to TFIM leveraging WS-* standards
- Improved authentication, authorization and access leveraging System z security hub
- Improved transparency of end to end security solutions

Compliance

- Improved depth and breadth of audit capabilities
- Improved support for multiple data types
- z/OS specific SMF event data extracted for security reporting spanning platform boundaries
- Analysis of policy and reporting to validate access rules
- Enhanced reporting and autonomics around processing of security events

Security as a Service

- Integration points with DB2, CICS, WAS, for credential validation and transformation
- TFIM evolution as the SOA credential transformation agent
- Improve cross-platform integration to provide security as a service
- Extended resource and process security capabilities

*All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.