



Building a Unified Security Infrastructure



Agenda

- **Securant Technologies**
- **Customer Issues and Outcomes**
- **Evolution of eBusiness**
- **Access Management Solution Requirements**
- **ClearTrust Overview**
- **Customer Case Studies**

The Demand for AAA Security

- **The three A's will grow from \$2.8 billion in 2000 to \$7.7 billion, thanks to a CAGR of 28 percent. Authentication, a field that covers secure transactions, digital certificates, and PKI (public key infrastructure), will be a driving force in the growth of the market, with 2004 revenue ringing in at \$1.7 billion, Framingham, Mass.-based IDC said.**
- **Interestingly, the growth in the intrusion detection and vulnerability assessment market will not be driven by fears of security breaches but rather by a desire by corporate IT managers to control and be aware of the status of their networks, the study said. The three A's, on the other hand, will grow due to their importance in securing e-business transactions and partnerships.**



Securant Technologies

- ❖ Headquartered in San Francisco
- ❖ Six Years Providing Secure eBusiness Solutions to Fortune 500 Firms
- ❖ Global Capability - Offices in New York City, London, Chicago, Denver, Los Angeles, Toronto, Phoenix, Minneapolis, Dallas, Washington D.C., Philadelphia, Paris, Houston, Atlanta, Munich, Sydney, and Asia
- ❖ Fastest Growing Company in Web Access Control Space
- ❖ Winner of every major award and review given by the security industry



Customers

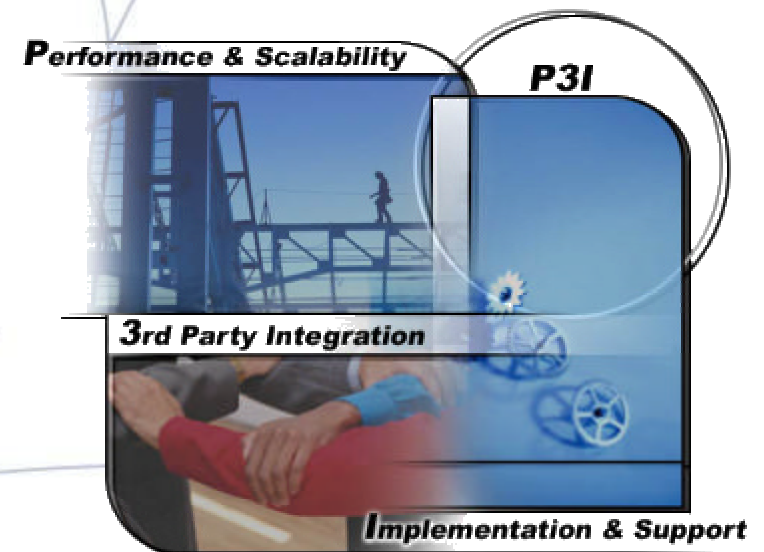


Business Issues

- ✓ **Defining a Unified Access Model**
- ✓ **Strong Authentication**
- ✓ **Flexible Authorization**
- ✓ **Access Control**
- ✓ **Single Account Store**
- ✓ **3rd Party Integration**
- ✓ **Personalization**
- ✓ **Single Sign-On**
- ✓ **Delegated Administration**
- ✓ **High Performance**
- ✓ **Registration Services**
- ✓ **Build vs. Buy**
- ✓ **High Value Transactions**
- ✓ **Maximizing Availability / Uptime**
- ✓ **Technical Support**
- ✓ **Professional Services Integration**
- ✓ **Rollout / Deployment**
- ✓ **Reporting and Auditing**
- ✓ **Leveraging Existing Infrastructure**
- ✓ **Privacy Issues**
- ✓ **Resistance to Change**
- ✓ **Organizational Philosophies**
- ✓ **Internal Politics**
- ✓ **Earnings Pressures**
- ✓ **Regulations**
- ✓ **Competition**

Business Outcomes

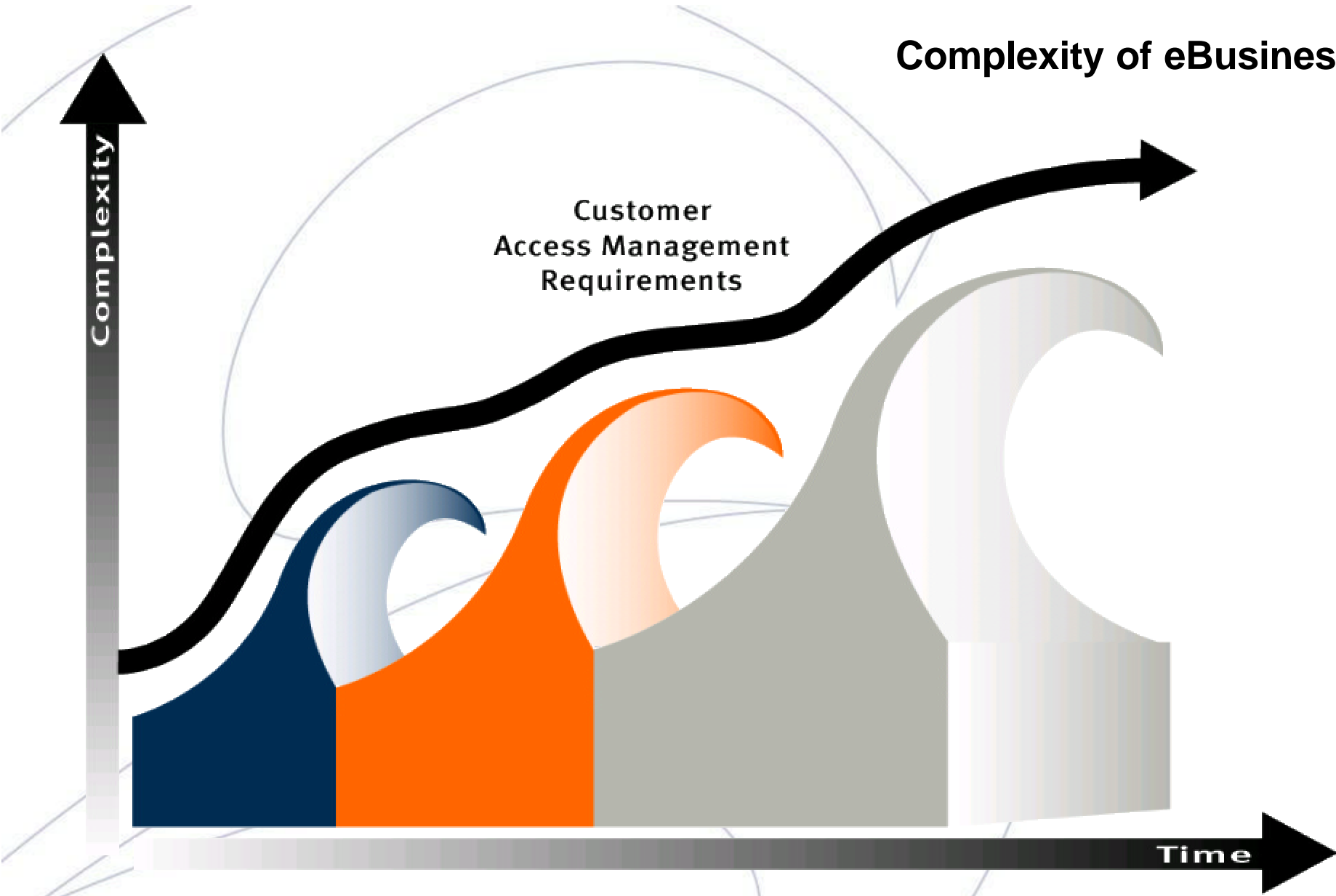
- ✓ Reduce Administration Overhead
- ✓ Provide Registration and Workflow
- ✓ Enable Higher Levels of Security
- ✓ Increase Usability
- ✓ Identify Revenue Opportunities
- ✓ Integrate Across All Technologies
- ✓ Enhance Business Continuity
- ✓ Scale for Global Deployment
- ✓ Provide Unparalleled Performance
- ✓ Create a Powerful Partnership
- ✓ Faster Time to Market
- ✓ Acquire Implementation Services
- ✓ Receive Platinum Technical Support



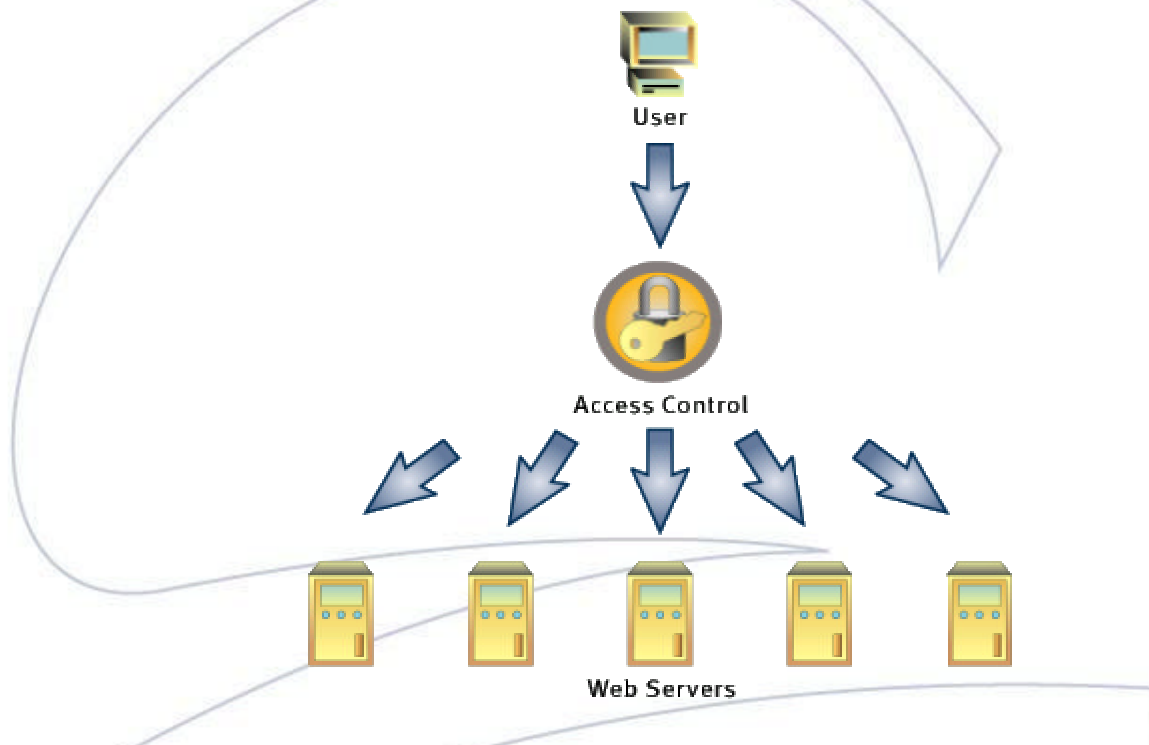
Evolution of eBusiness



Complexity of eBusiness



Wave I: Information Access



Major Trends:

- Emergence of the Intranet and Extranet as a cost-efficient and effective mechanism for disseminating information to employees, customers, and partners
- Risk of exposure of proprietary content

Wave I: Customer Requirements

Customer Needs

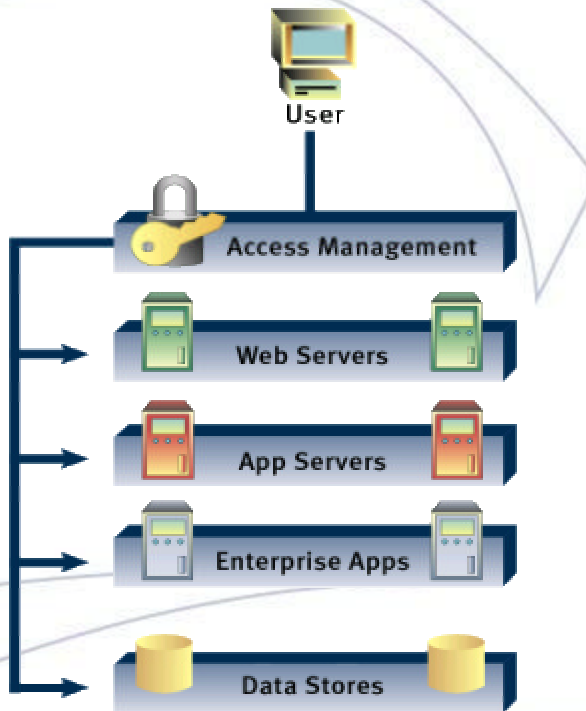
- Need to manage exponential growth of users
- Need to provide ease of use for users
- Increased risk by exposing proprietary content



Solution Requirements

- Delegated Administration
- Web Single-Sign On (SSO)
- Granular Access Control
- Integration to web servers

Wave II: Extended Enterprise Access



Major Trends:

- Demonstrated success with Wave I deployments
- Technology continues to innovate
- Companies extending internal business processes to the web
- Risk of exposure of proprietary content and transactions
- Self-service for employees, customers, and partners

Wave II: Customer Requirements

Customer Needs

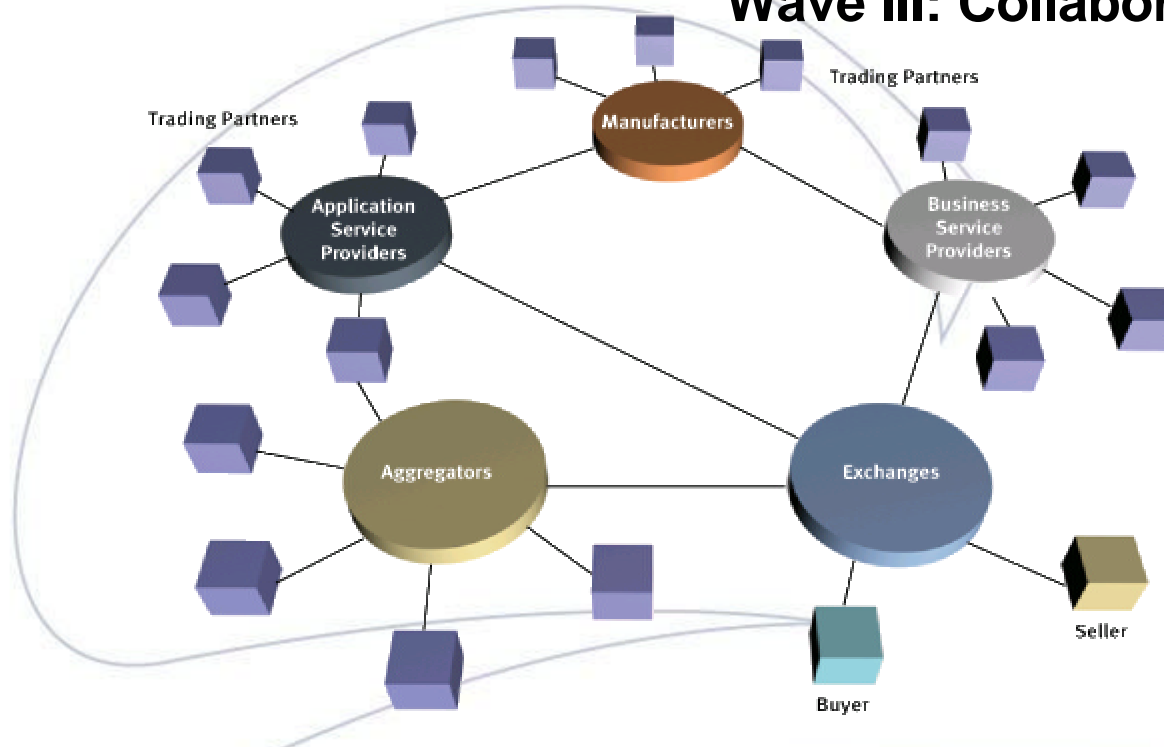
- Need to manage further growth of users
- Need to provide ease of use for users → Single Sign-On across the enterprise
- Further increased risk from exposure of business processes

Solution Requirements

- Delegated Administration
- Enterprise Single-Sign On
- Unified Access Management
- Granular Access Control
- 3rd Party Integration
- Auditing and Threat Detection



Wave III: Collaborative Commerce



Major Trends:

- Demonstrated success with Wave II deployments
- Emergence of networked business models
- Companies extending internal business processes across multiple organizations and service providers
- Risk of exposure of proprietary content and transactions between organizations

Wave III: Customer Requirements

Customer Needs

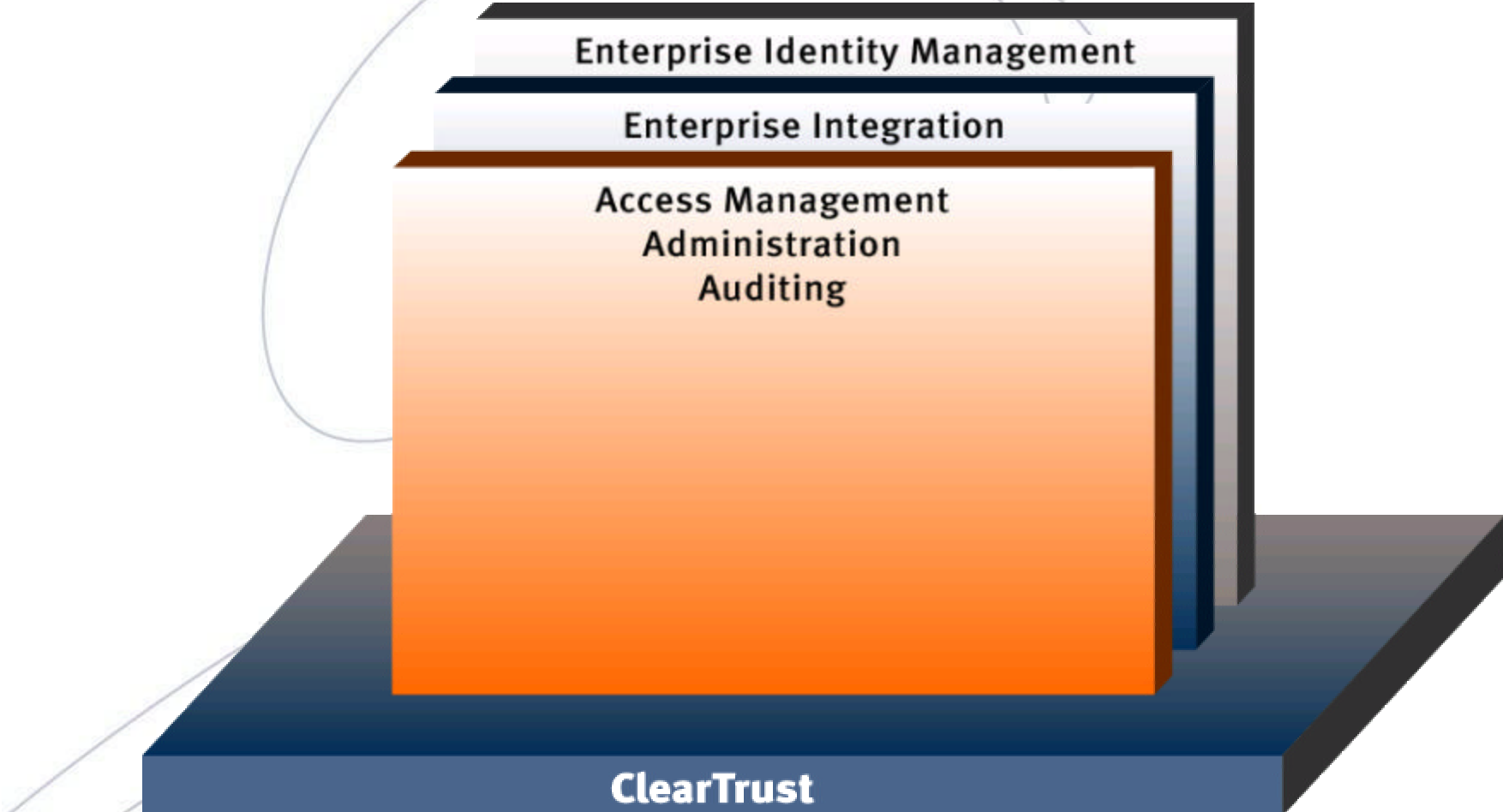
- Need for interoperability across sites and organizations
- Need to provide ease of use for users → Single Sign-On across multiple enterprises
- Further increased risk associated with transactions between organizations



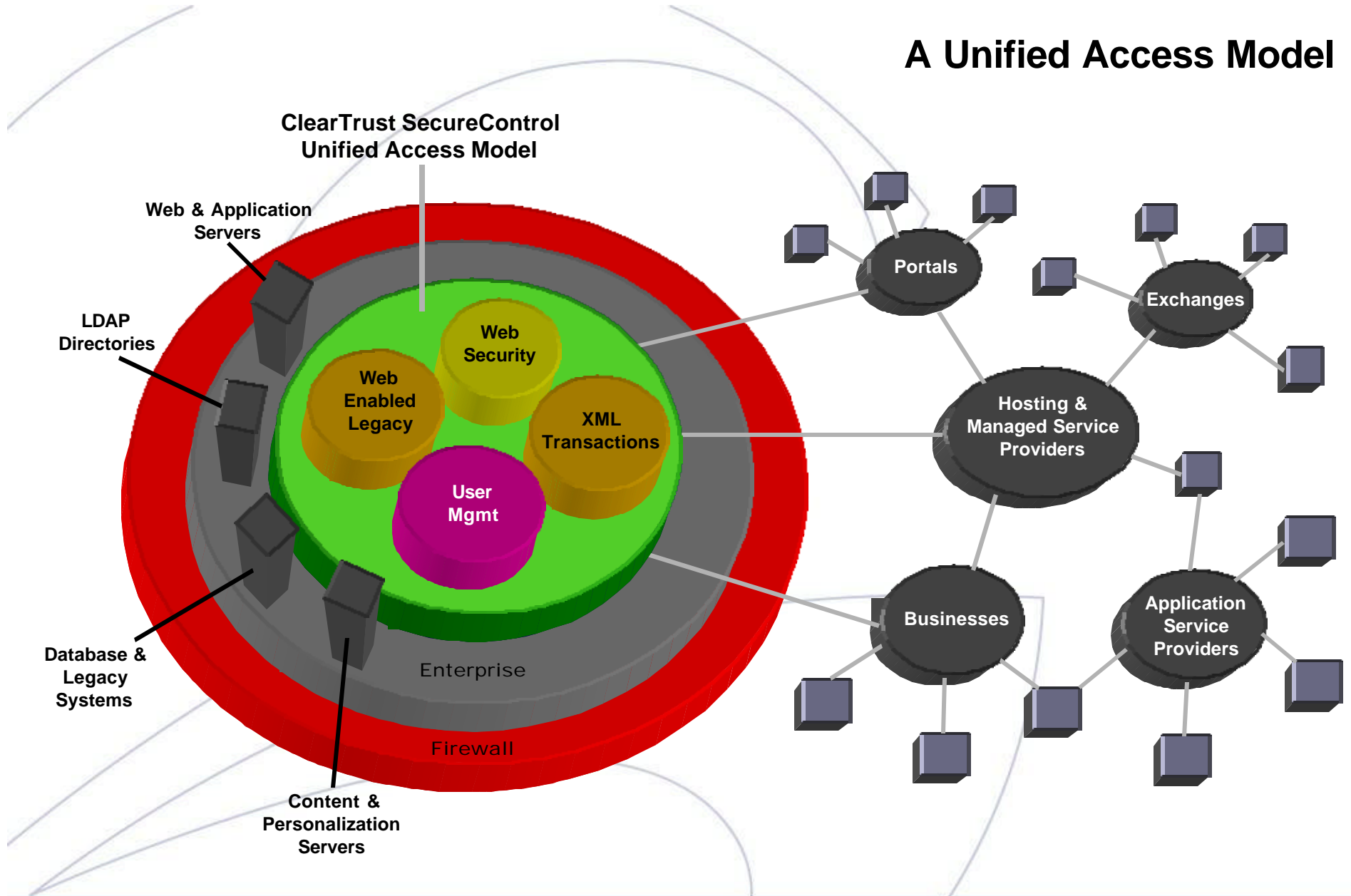
Solution Requirements

- Compliance and support for standards such as the Security Assertions Markup Language (SAML)
- Inter|Site Single Sign-On
- Secure transaction support
- XML support

Unified Access Management



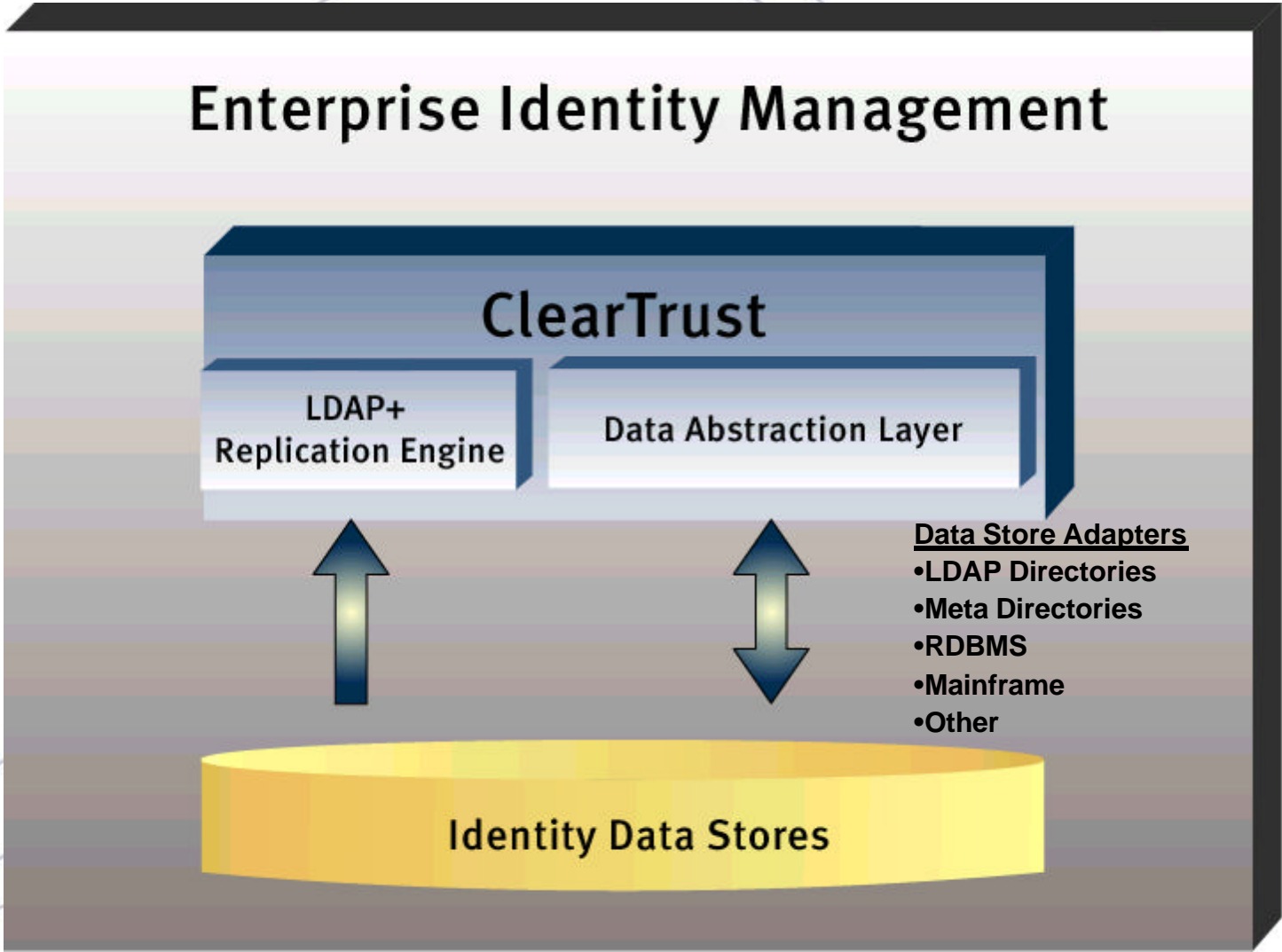
A Unified Access Model



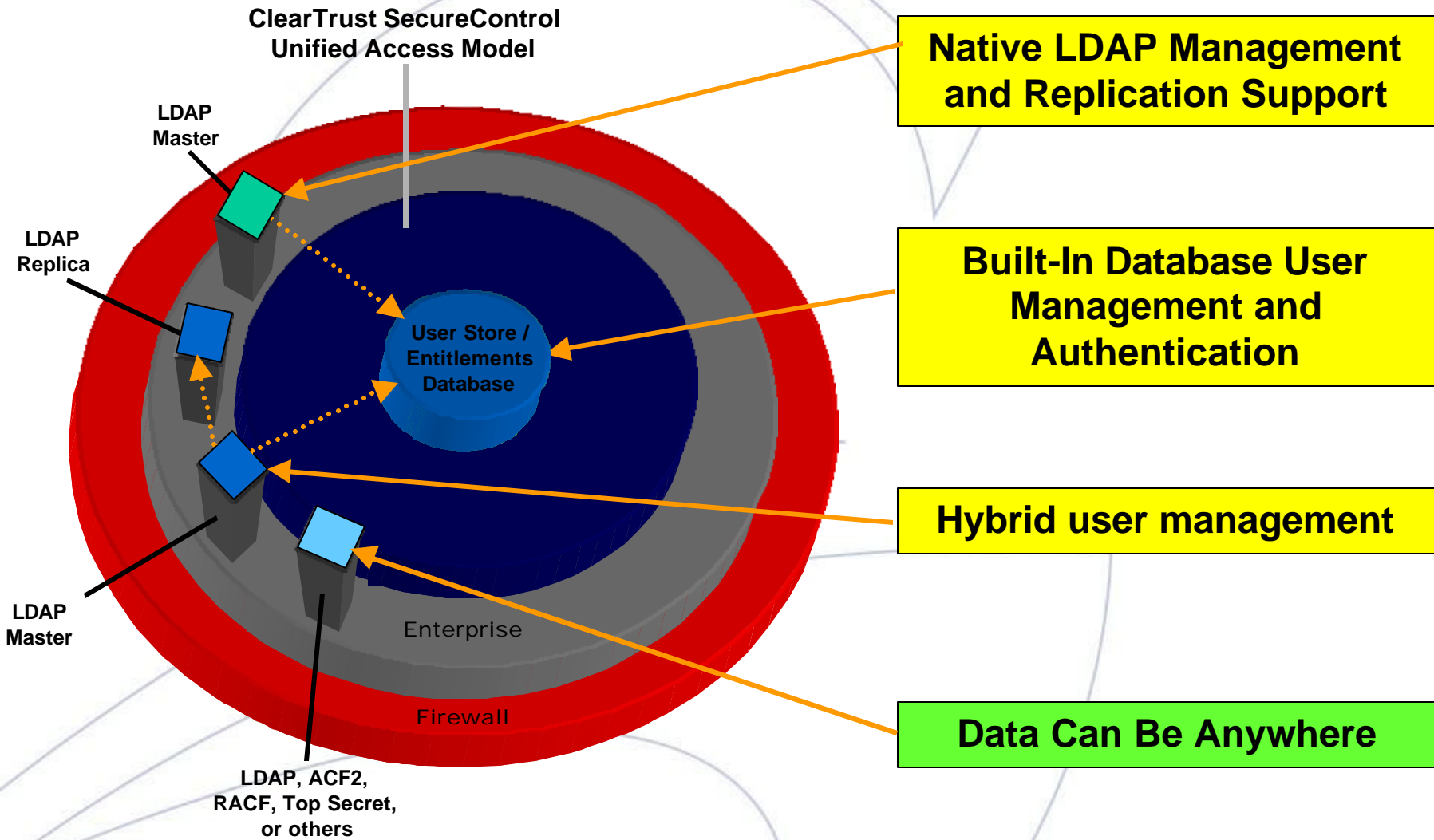
ClearTrust SecureControl serves as the framework for facilitating a Unified Access Model for web access control, authentication, authorization, auditing, and administration.



Enterprise Identity Management

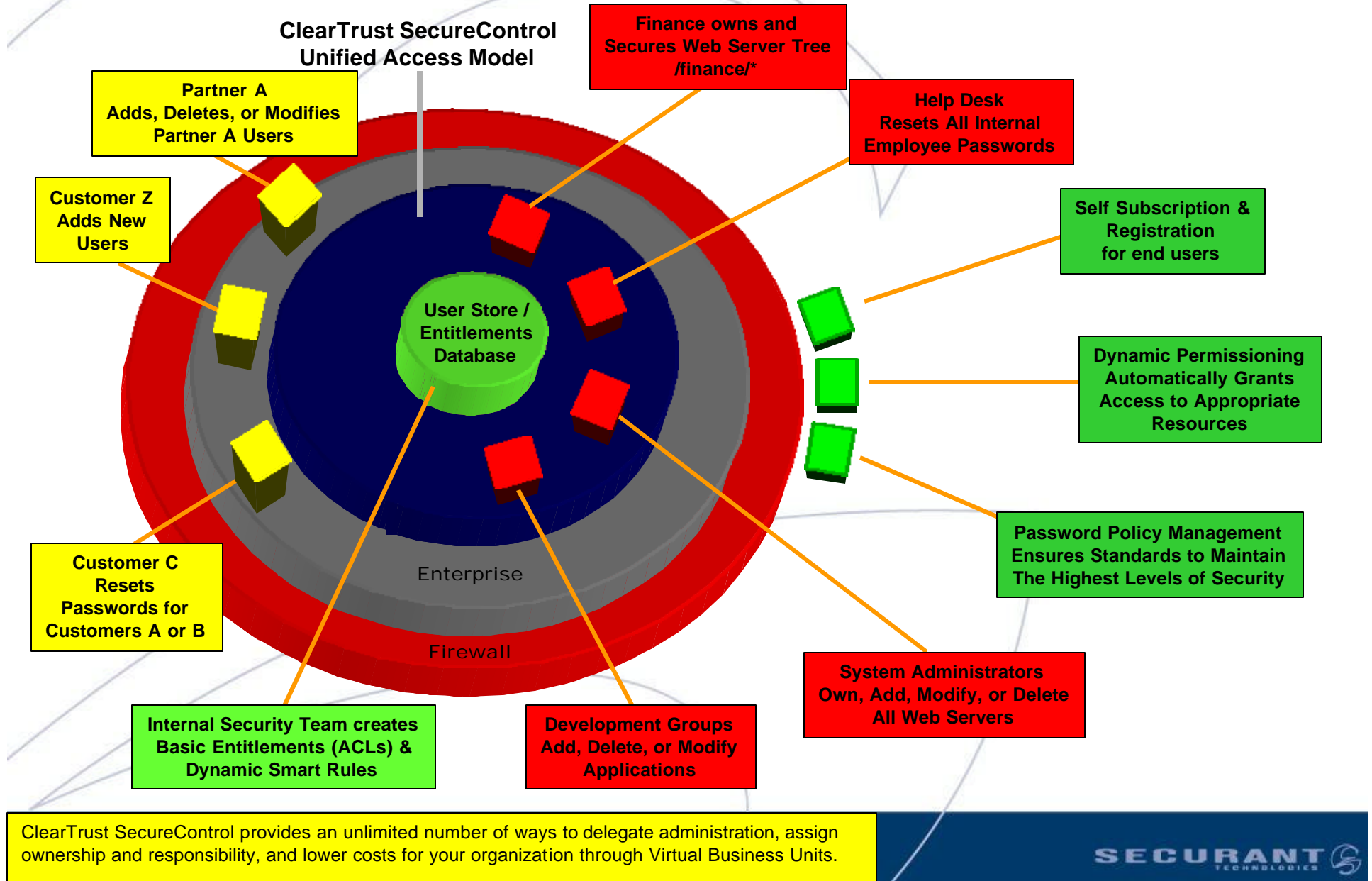


Delegated User Management

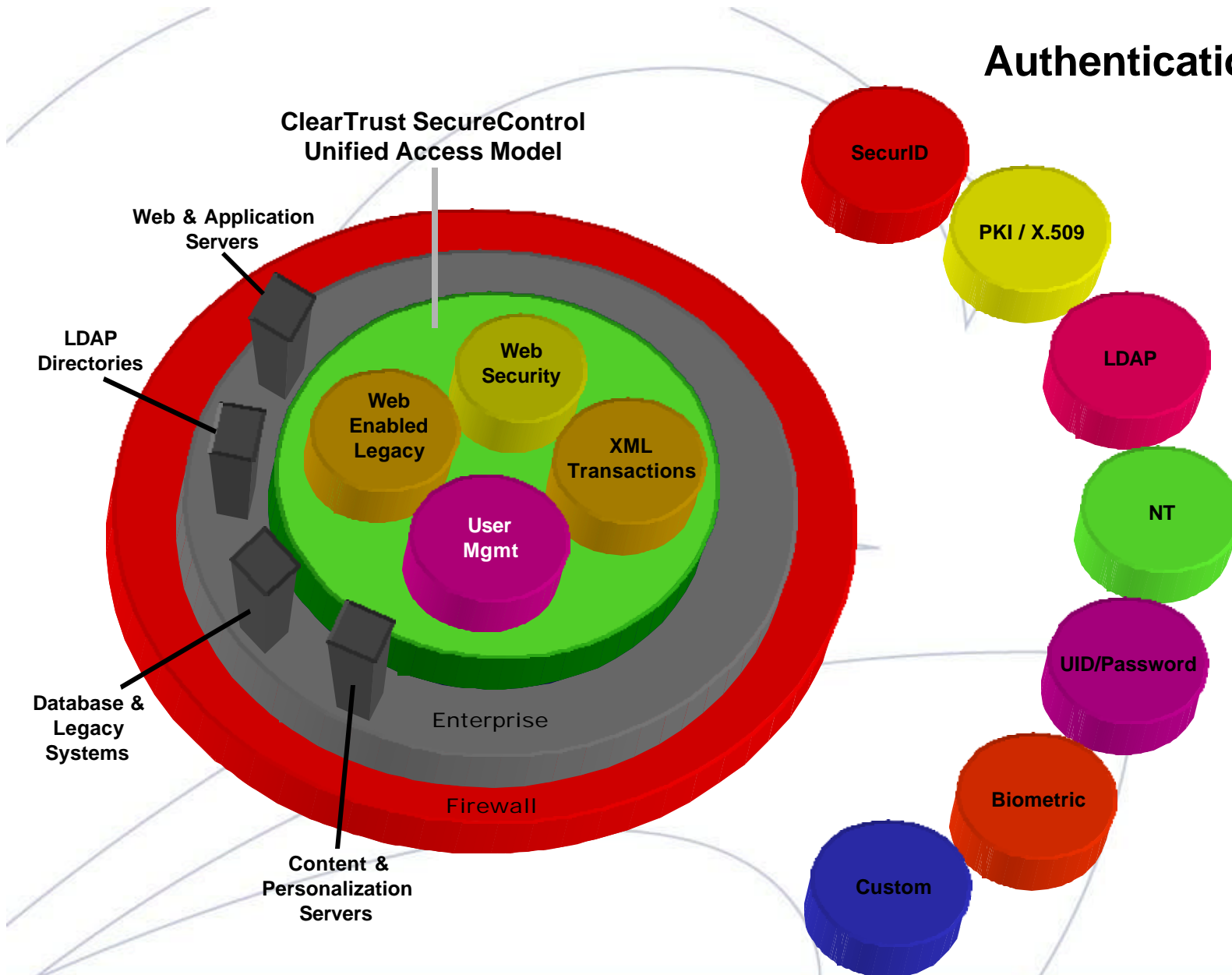


ClearTrust SecureControl provides built-in User Management and Authentication. SecureControl can also integrate natively with LDAP and other user data and security policy stores.

Delegated Resource Management



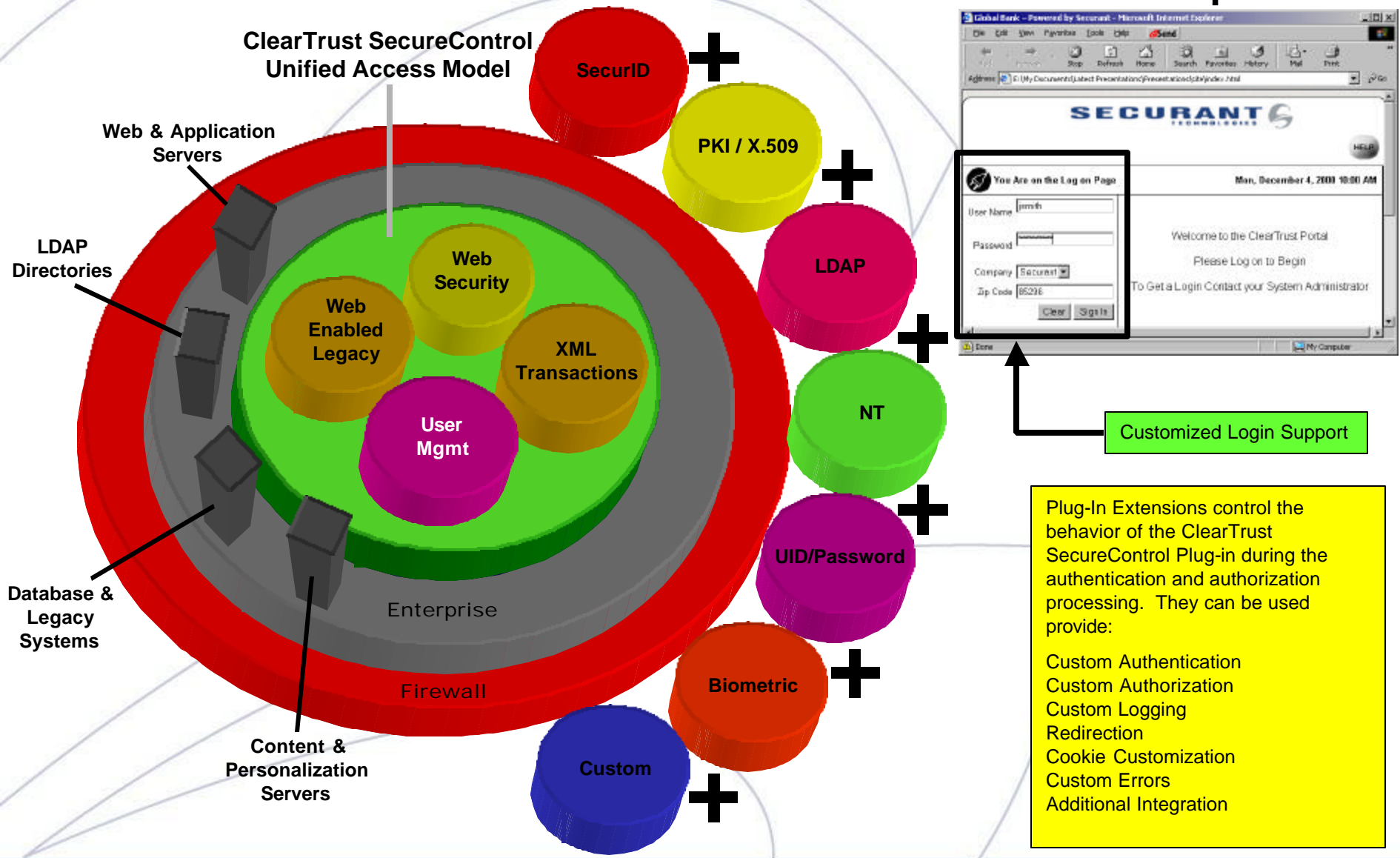
Authentication Services



Flex-Authentication provides the capability to select and combine different authentication types depending on the resources being accessed. All major authentication types are supported.

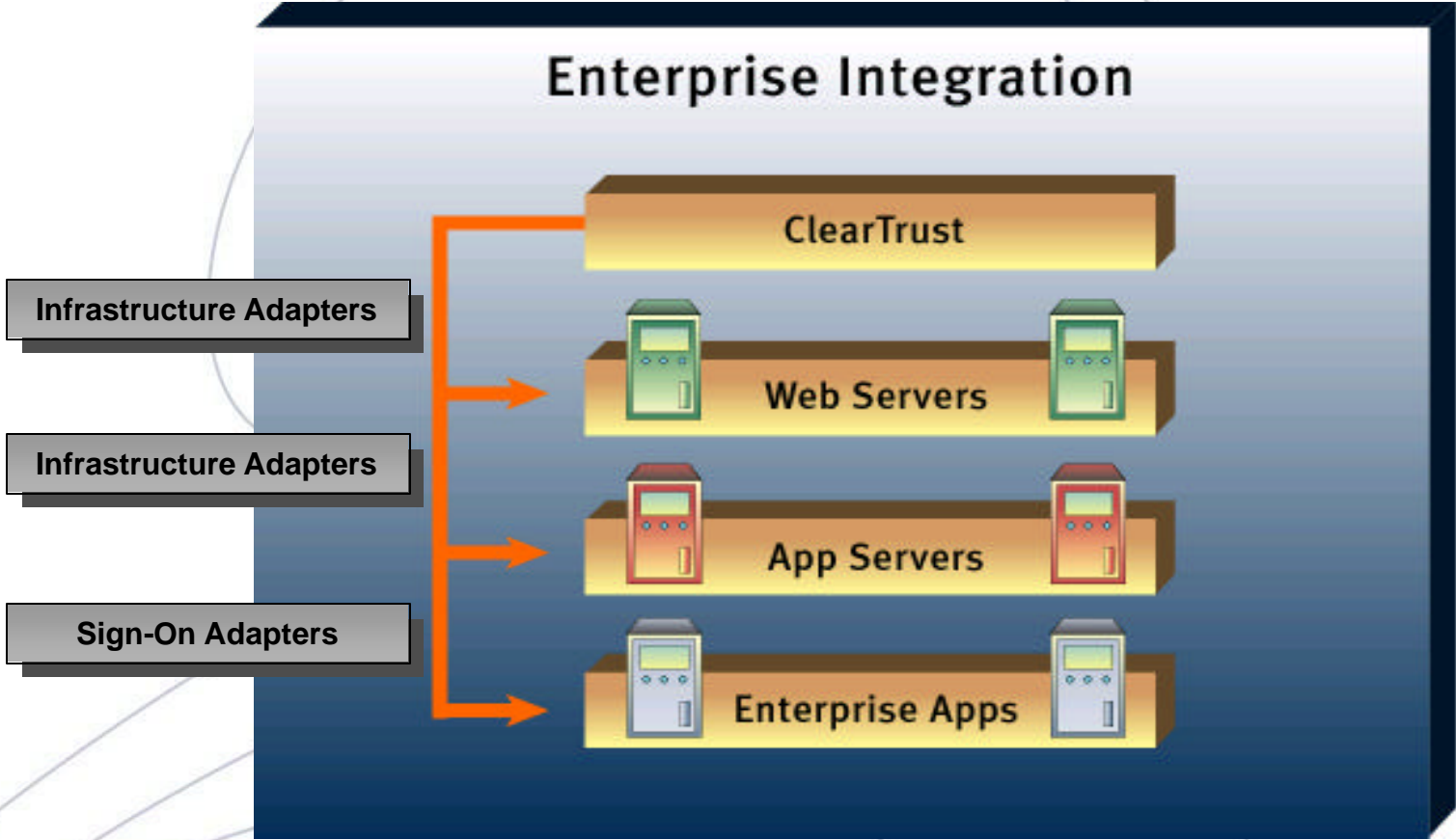


Flexible Authentication Capabilities



Authentication chaining plus support for custom authentication types provides maximum flexibility. Web Server Plug-In Extensions provide the ability to customize the authenticate process.

Enterprise Integration



The ClearTrust Suite

ClearTrust SecureControl

- Delegated User Management and Administration
- Flexible Authentication Capabilities
- Dynamic Granular Authorization
- Access Control
- Web & Inter-Site Single Sign-On
- Policy Assessment
- Auditing & Logging

ClearTrust SecureDetector

- Centralized monitoring of all activity
- Proactive response with automated actions
- Integration with network level security
- Identify revenue opportunity

ClearTrust Mainframe

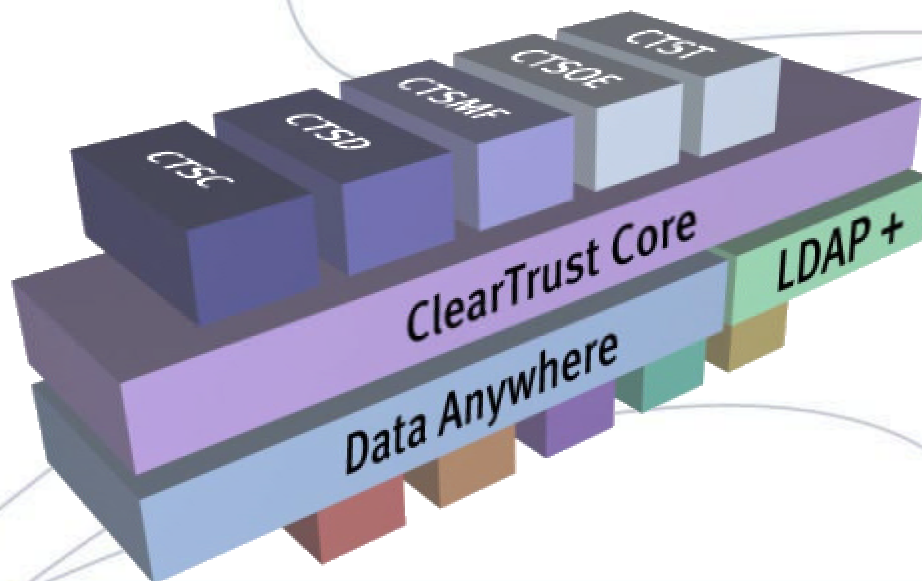
- Leverage existing mainframe security
- Extend Web security to mainframe
- Protect mainframe Web systems

ClearTrust 3rd Party Integration

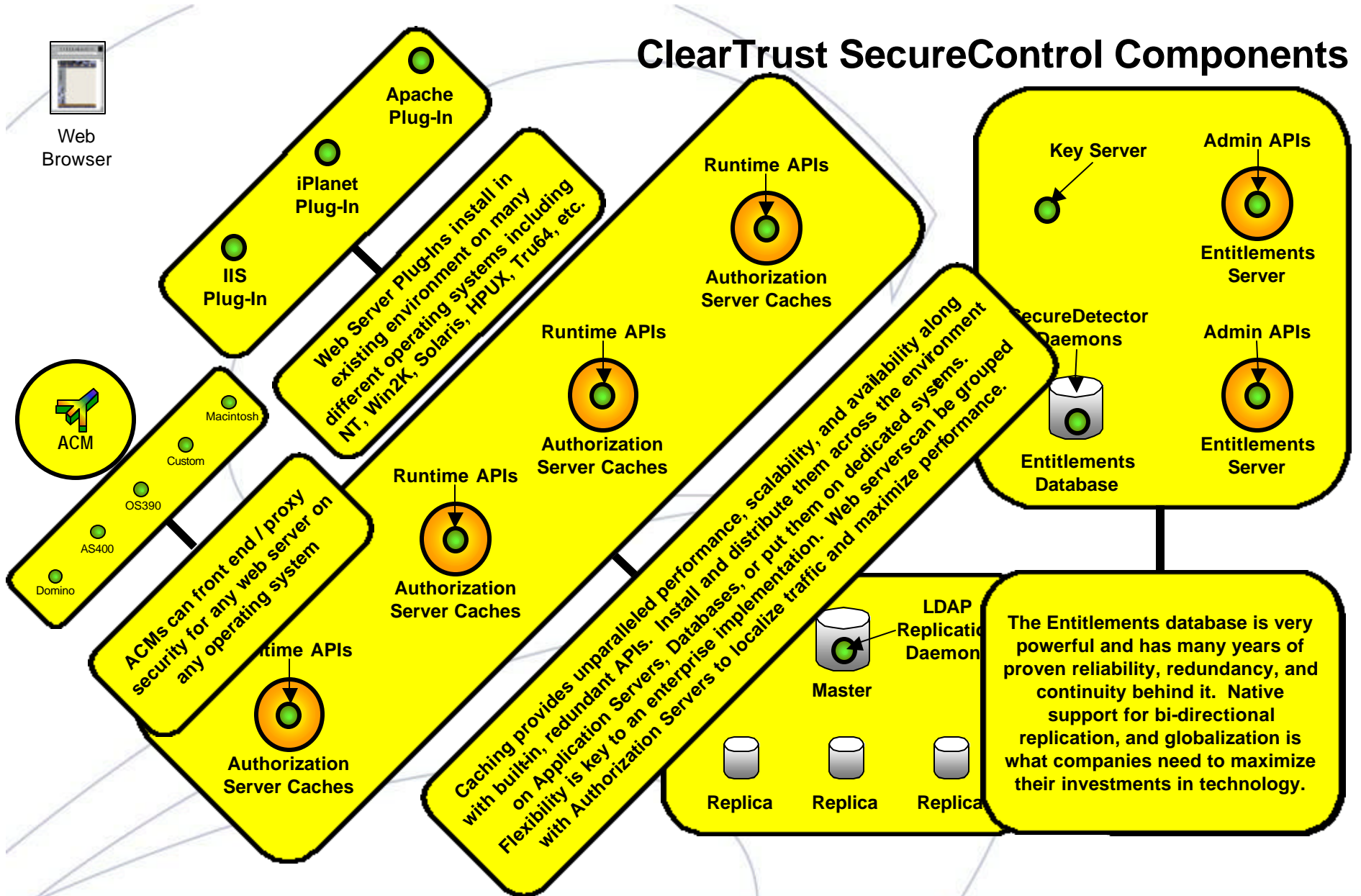
- Tight integration with 3rd party systems
- Rapid time to market and deployment
- Improve user experience across sites

ClearTrust Transaction Security

- AuthXML-SAML based interoperability
- Secure XML transactions
- Secure inter-party XML transactions



ClearTrust SecureControl Components



ClearTrust SecureControl plugs into your existing infrastructure. Components can be installed with existing application, database, web servers, etc. minimizing change to the environment.



The Management of Access

Web Single Sign-On (SSO)
InterSite Web SSO
Multiple Site Web SSO
UserID / Password
SecurID
Certificates
Flex-Authentication

Web Server authenticates and authorizes user

User Requests Page

Authentication
Logging
External Call-outs
Customization
Plug-In Extensions (PIX)

SSL



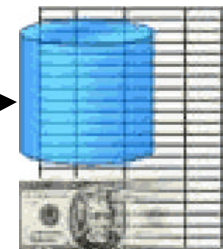
Web Browsers



Web Server Plug-Ins
iPlanet, Microsoft or Apache
provide secure web pages

Application Servers
Secure Applications with
Granular Method Level Security

Authorization
Assessment
Personalization
EJB Security
Logging
Monitoring
Reporting
Integration



Entitlements Database
Users and Security Policy in
Oracle, Sybase, or LDAP

SecureControl enables delegated administration, policy assessment, dynamic authorization, and logging while **SecureDetector** monitors, reports, and responds to any activity such as counting application accesses or bad password attempts over time.

Authorization Services

Basic Entitlements (ACL)s

Dynamic Smart Rules

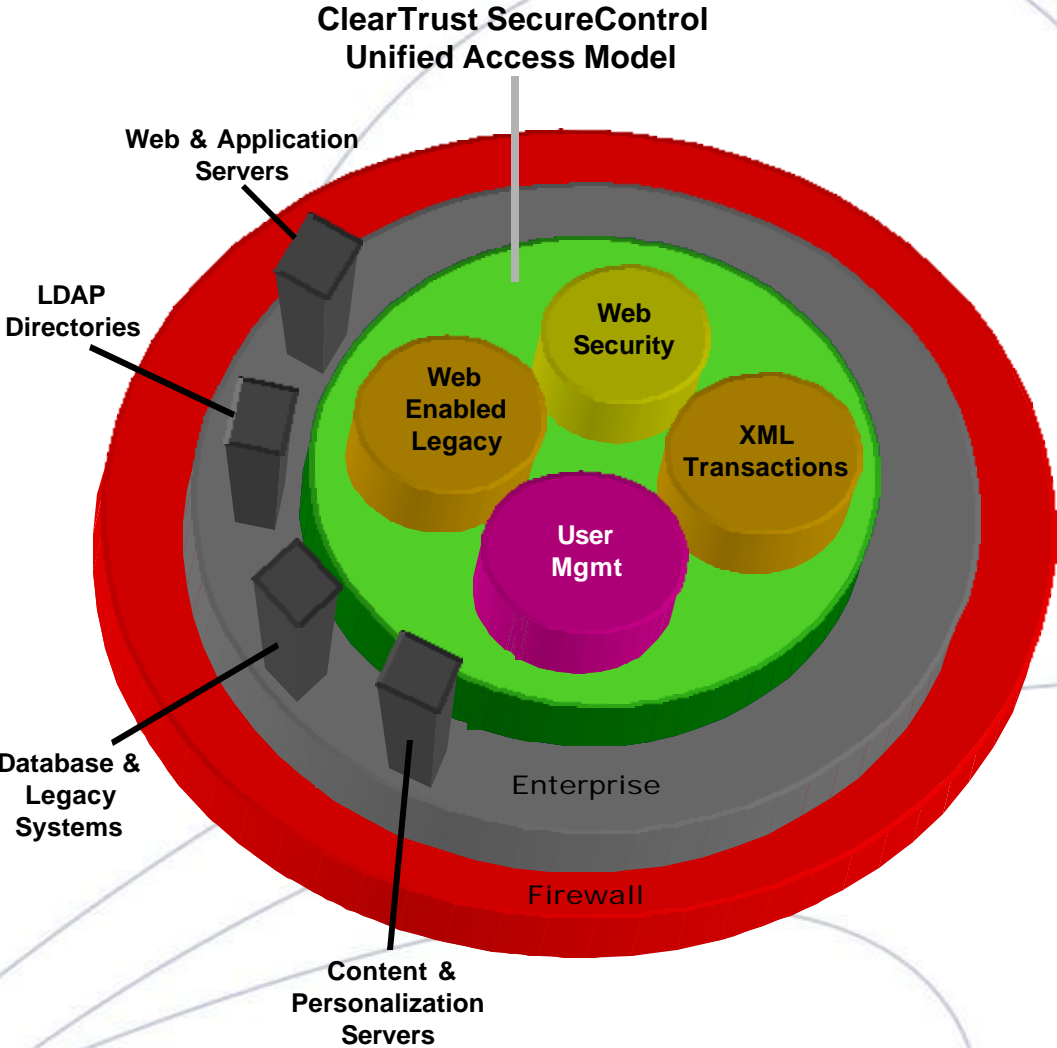
Allow

Deny

Require

Enterprise Web Security

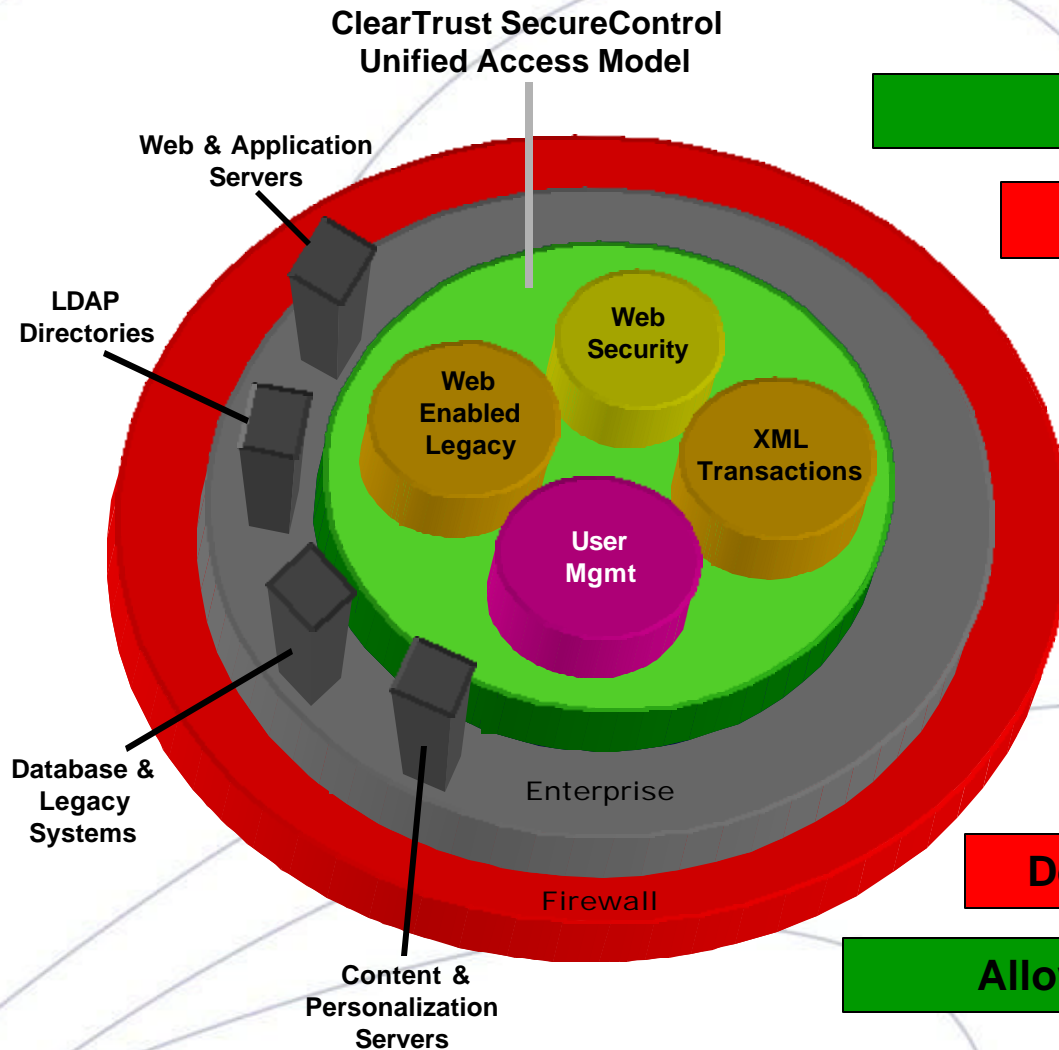
Granular Method Security



Basic Entitlements and Dynamic Smart Rules provide powerful capabilities for authorizing access to resources at any level.



Authorization Services



Allow if Group = HR

Deny if Location = Seattle

Allow if Time > 0800

Deny Access to Everyone

Allow Access to Buy Functions

Deny if Job Code < 16

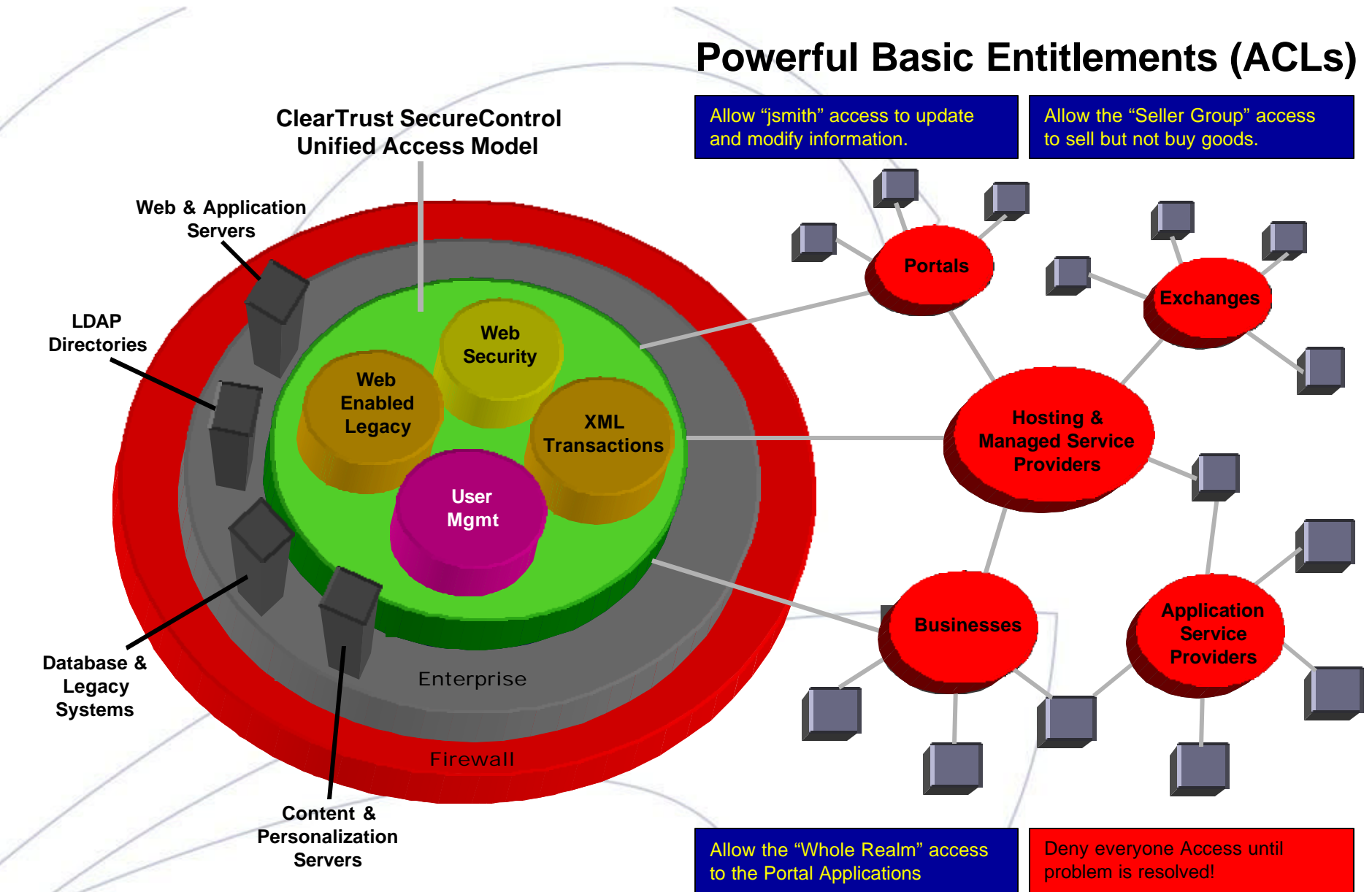
Allow Access to Everyone

Deny if Account.Standing != Current

Allow Access to Sell if Job = Seller

There are an unlimited number of access of people and processes to the resources.

Powerful Basic Entitlements (ACLs)

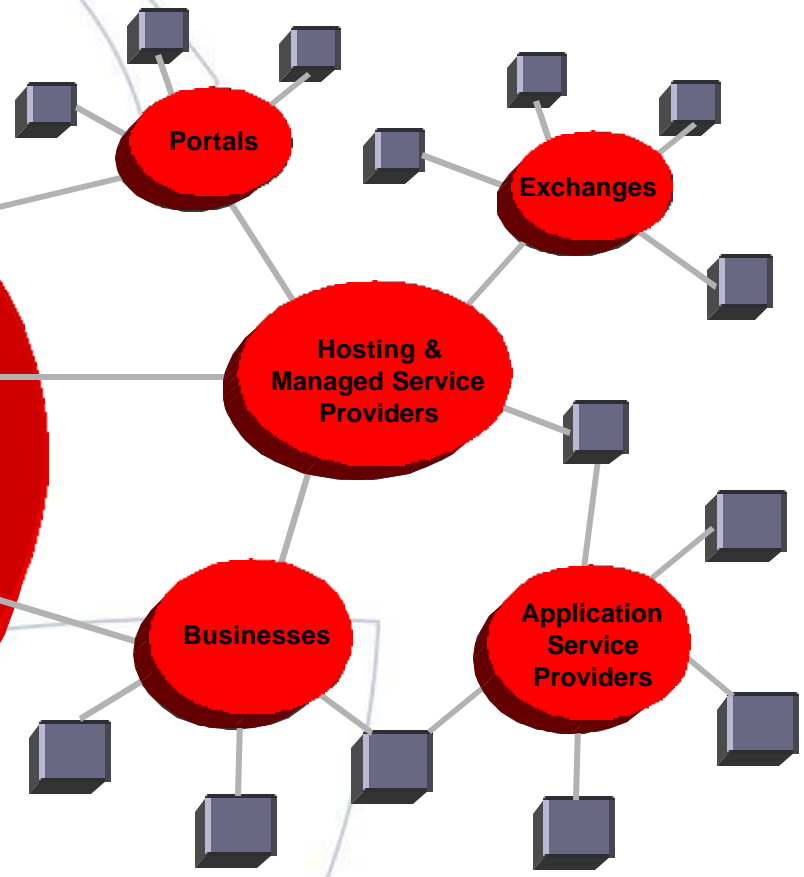
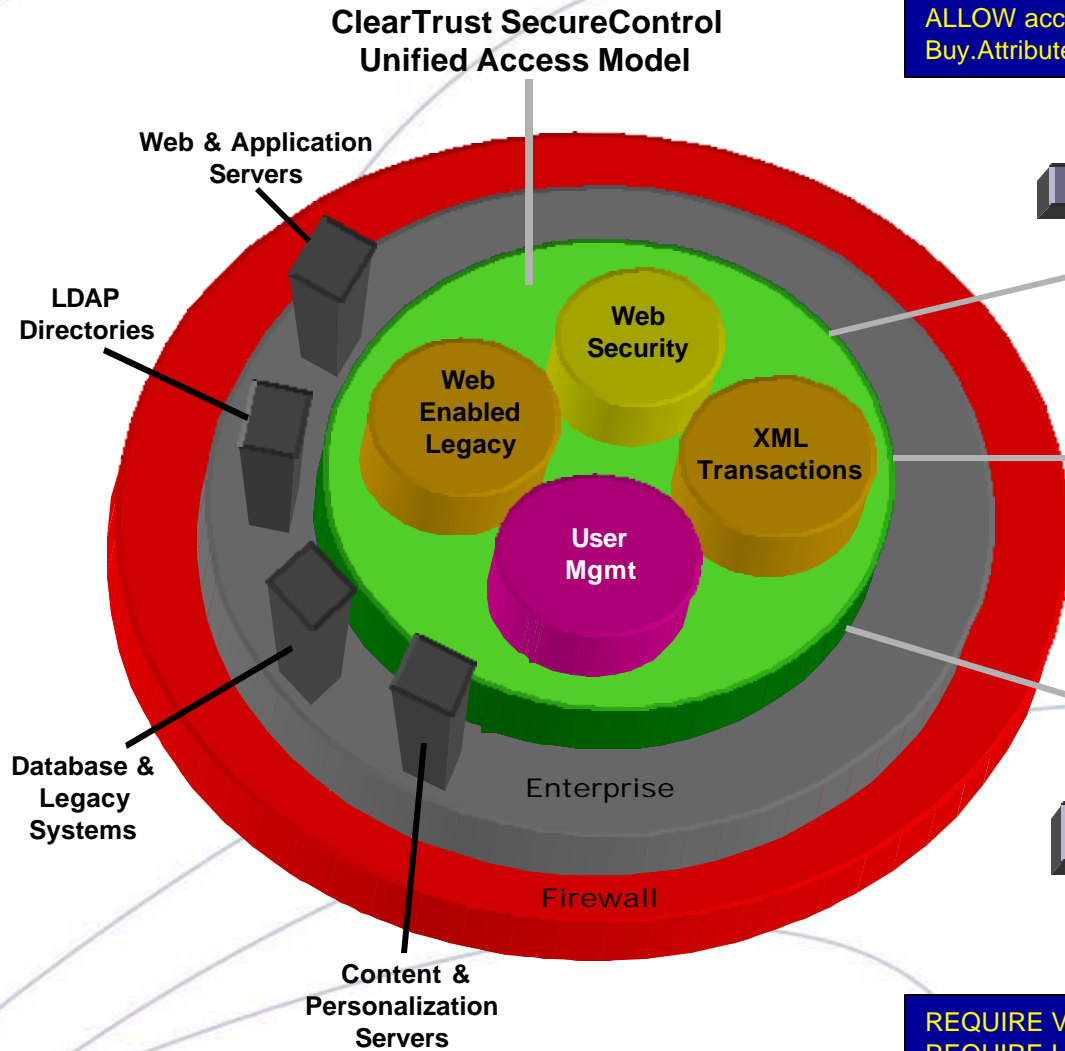


Basic Entitlements are ACLs that authorize users, groups, and realms to different resources. Resources can exist across any Web Server recursively, at a single page, or at a method level.

Flexible & Dynamic Smart Rules

ALLOW access to buy goods if
Buy.Attribute.Flag = TRUE

ALLOW access to sell goods if
Account.Status = CURRENT



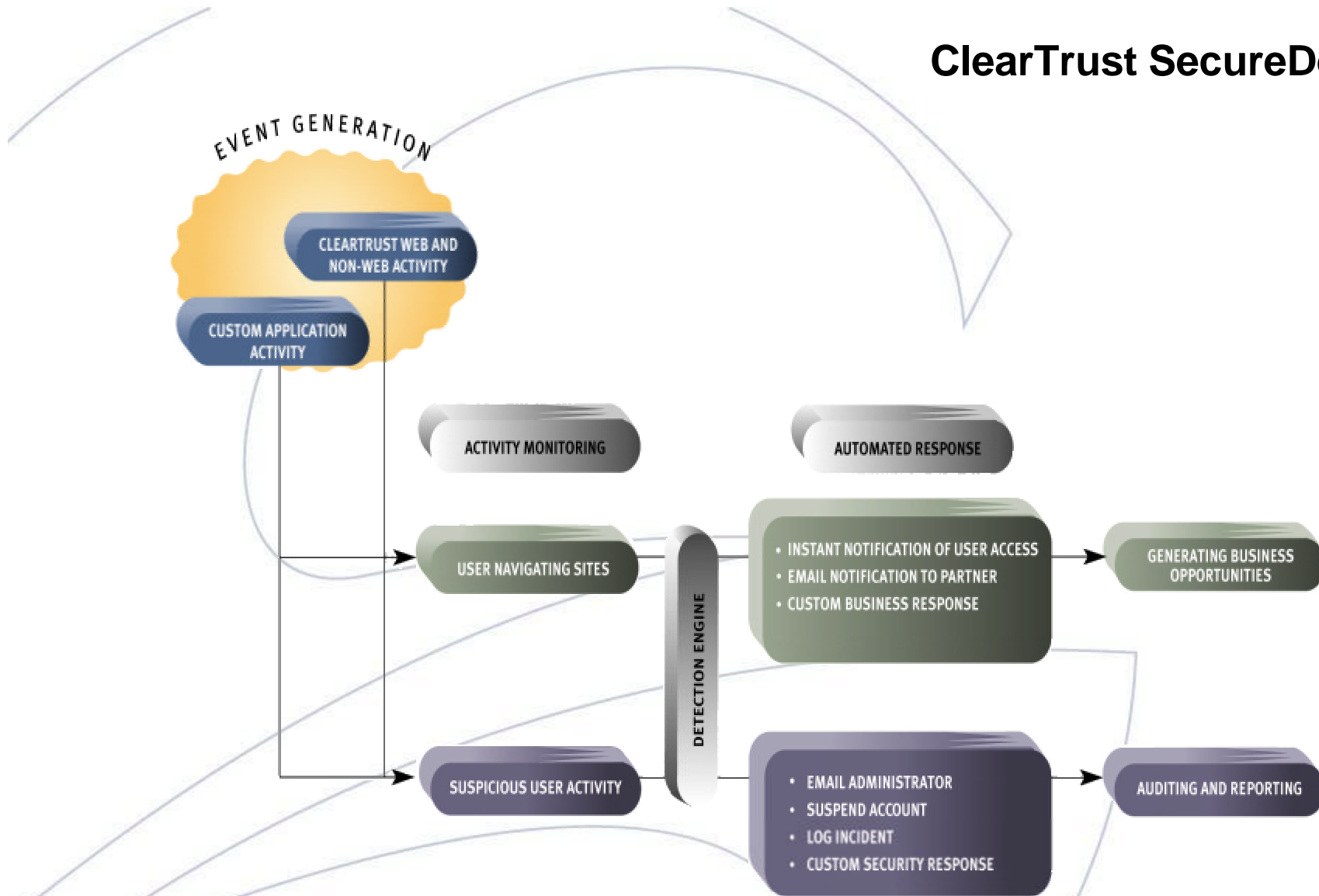
REQUIRE Vendor = 1A and
REQUIRE Location = US

Deny everyone Access until
problem is resolved!

Smart Rules dynamically evaluate attributes to authorize access to different resources. Attributes exist at the user level in the form of strings, dates, integers, floats, and Boolean values.

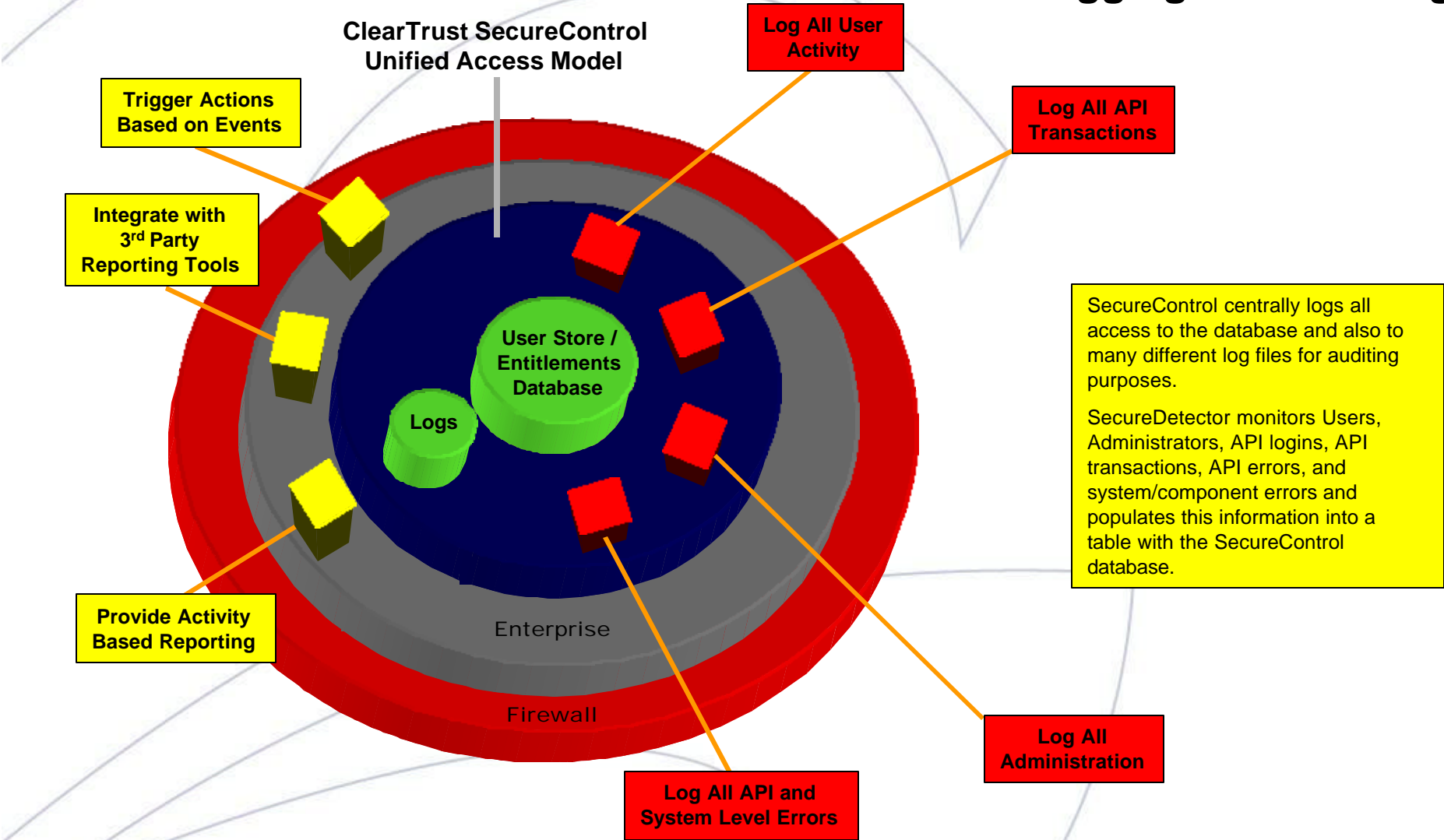


ClearTrust SecureDetector



THE COMPLETE RISK MANAGEMENT SOLUTION

Logging and Auditing



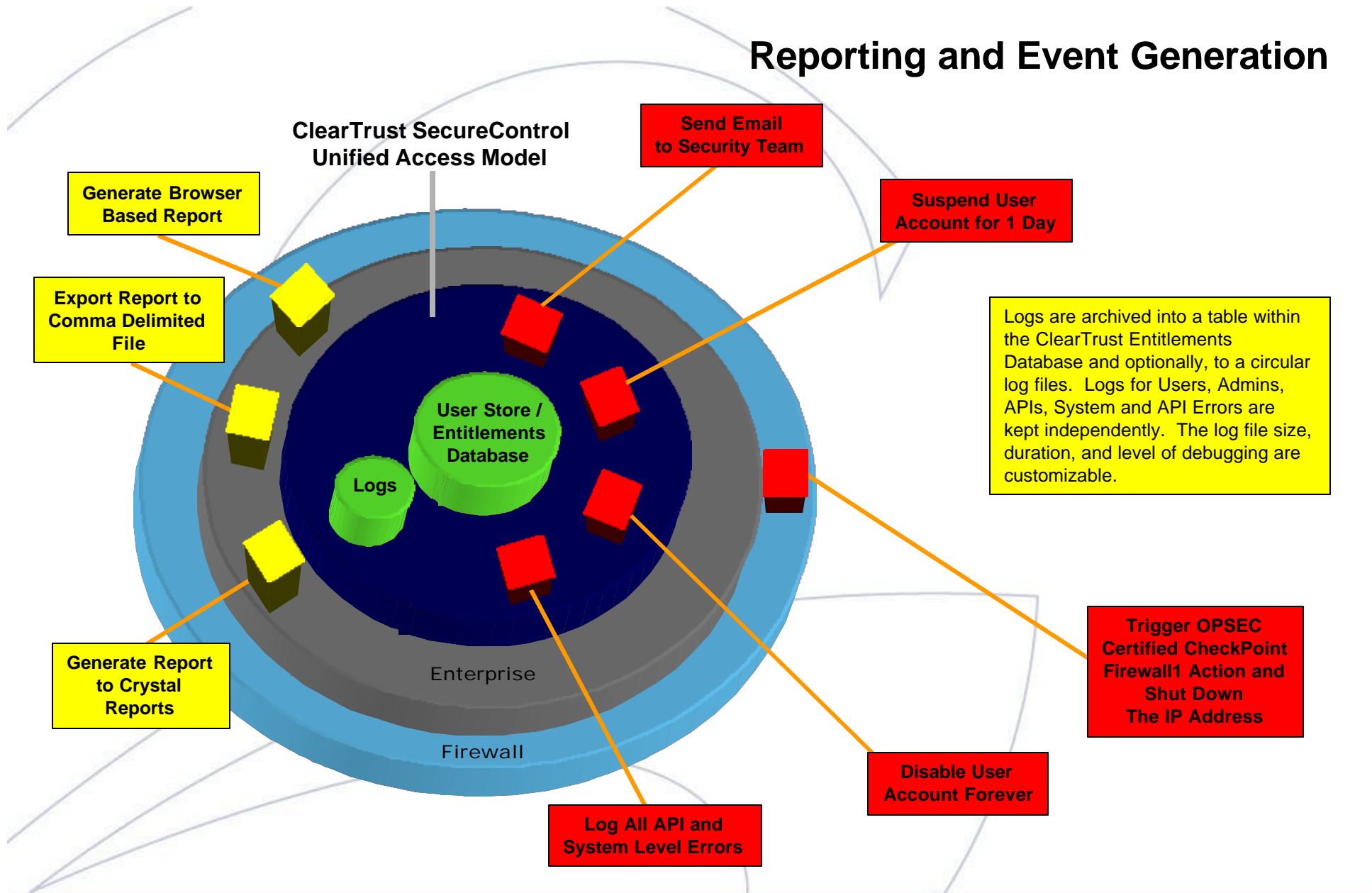
SecureControl centrally logs all access to the database and also to many different log files for auditing purposes.

SecureDetector monitors Users, Administrators, API logins, API transactions, API errors, and system/component errors and populates this information into a table with the SecureControl database.

SecureControl combined with SecureDetector enables intrusion detection, activity monitoring, logging, auditing, and reporting.

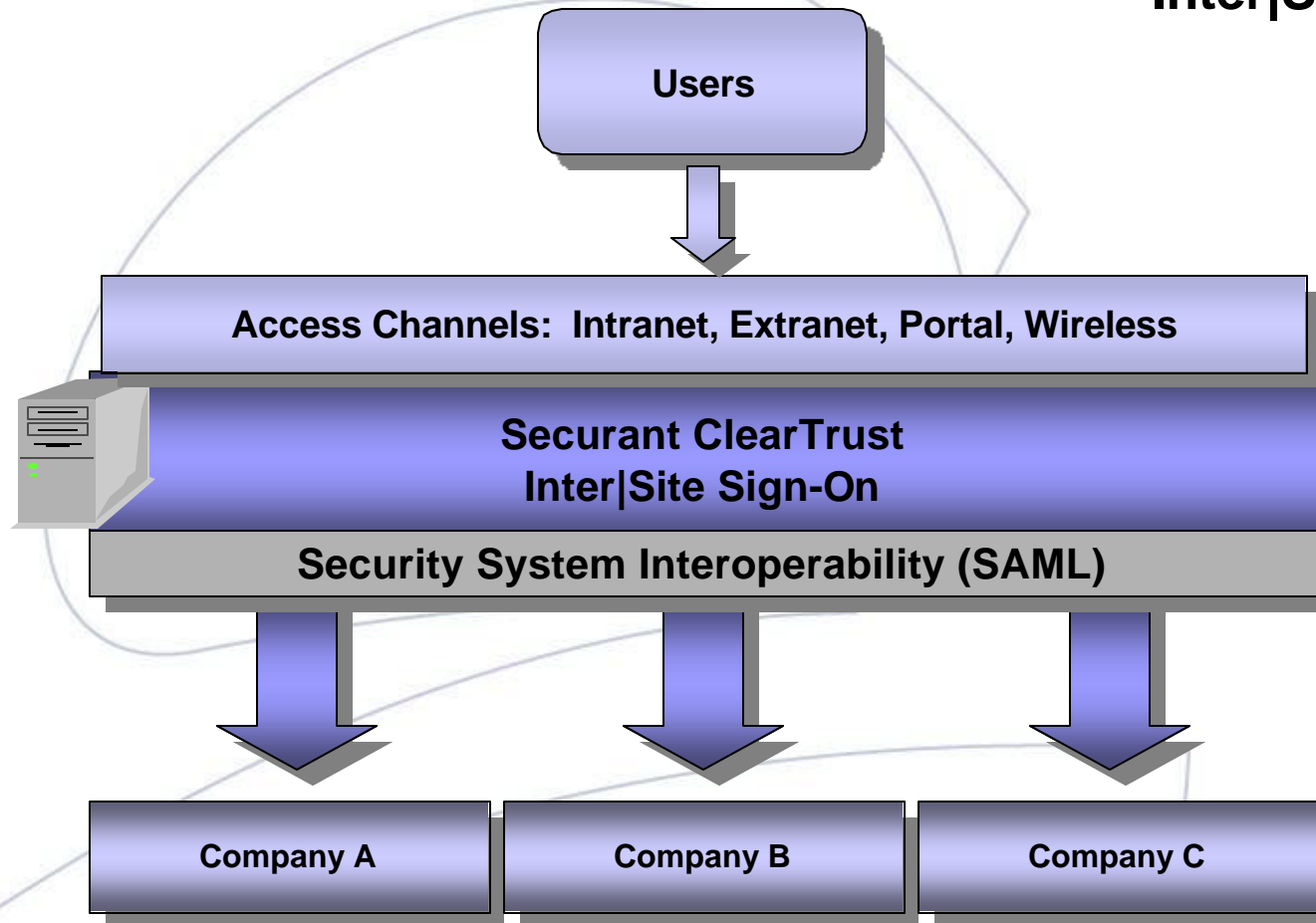


Reporting and Event Generation



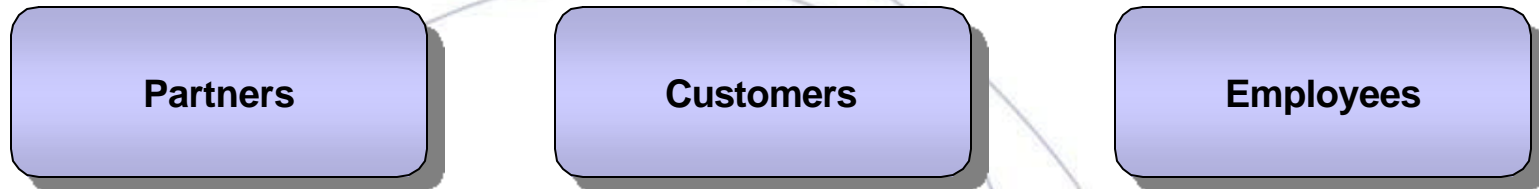
SecureDetector triggers actions based on patterns of good or bad activity. There are 16 default actions such as suspend or disable account, send email, or change user properties.

Inter|Site Sign-On



- Enhanced user experience across multiple sites and domains
- New revenue and co-marketing opportunities
- Standards-based solution means greater adoption and support by multiple partners
- Independence from specific Web security solutions allowing greater flexibility and partner selection

Unified Access Management Nirvana



Access Channels: Intranet, Extranet, Portal, Wireless

Network Security- Firewall, ISS, VPN

PKI

Securant ClearTrust

Web SSO

Access Management/Administration/Audit



Enterprise eBusiness Infrastructure
(Web Servers/Application Servers/Data Repositories/Etc.)

Enterprise eBusiness Applications

Retail
Banking

Commercial
Banking

Brokerage

Insurance

Customer
Care

SecureTransact (Security Assertions Markup Language)



- Future ClearTrust product providing security for business to business transactions
 - Authentication – authentication of end users performing transactions
 - Authorization – granular authorization of what transactions are allowed
 - Audit – centralized, secure audit logs with reports
 - Monitor and respond – fraud detection and response
 - Non-repudiation – digitally signed transactions and audit trails
 - Delegated User Management – definition of what users can perform what transactions
- Can be implemented as a transaction authority service (3rd party or in-house)
 - Authentication Service Bureau
 - User and Policy Management
 - Trusted Profile Management
 - Validation and Auditing Services

Unified Access Management across the enterprise(s) provides a positive impact on your bottom line!

Cost Savings

- User Administration Savings
 - Delegated administration savings
 - Help desk savings (password reset)
- Secure Self-Service
 - Improved productivity of employees
- Protection Against Security Breaches
 - Cost savings associated with damage to brand image and customer/partner relationships
- Out of the Box Third Party Integration
 - IT resources freed up to focus on core business
- Comprehensive Auditing and Reporting
 - Assists in compliance with all security audits and mandates

Revenue Impact

- Secure Access by Customer and Partners
 - Benefits of improved (and less expensive) customer acquisition and retention
 - Benefits of improved partner relationships

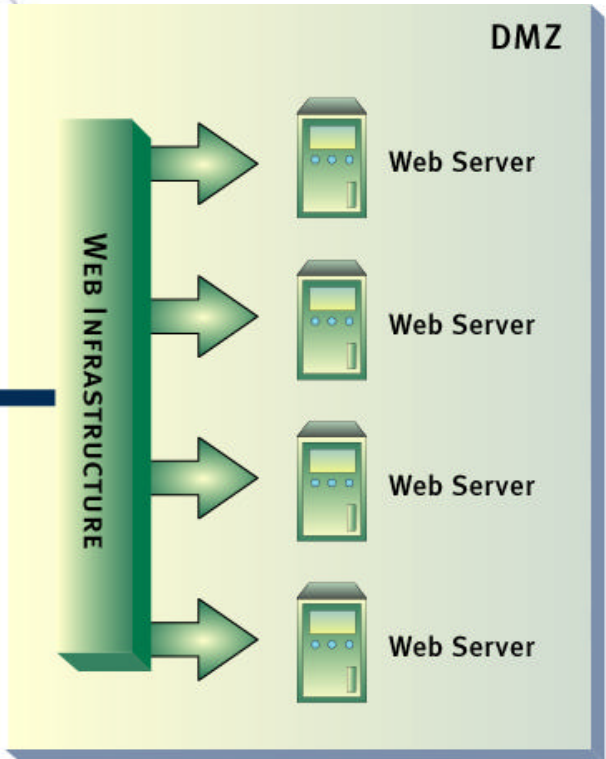
A large, abstract graphic composed of several thin, light blue lines that curve and sweep across the upper and middle portions of the page. The lines are fluid and organic, creating a sense of movement and flow. They start from the left side and curve towards the right, with some lines ending in sharp points or loops.

Customer Case Studies



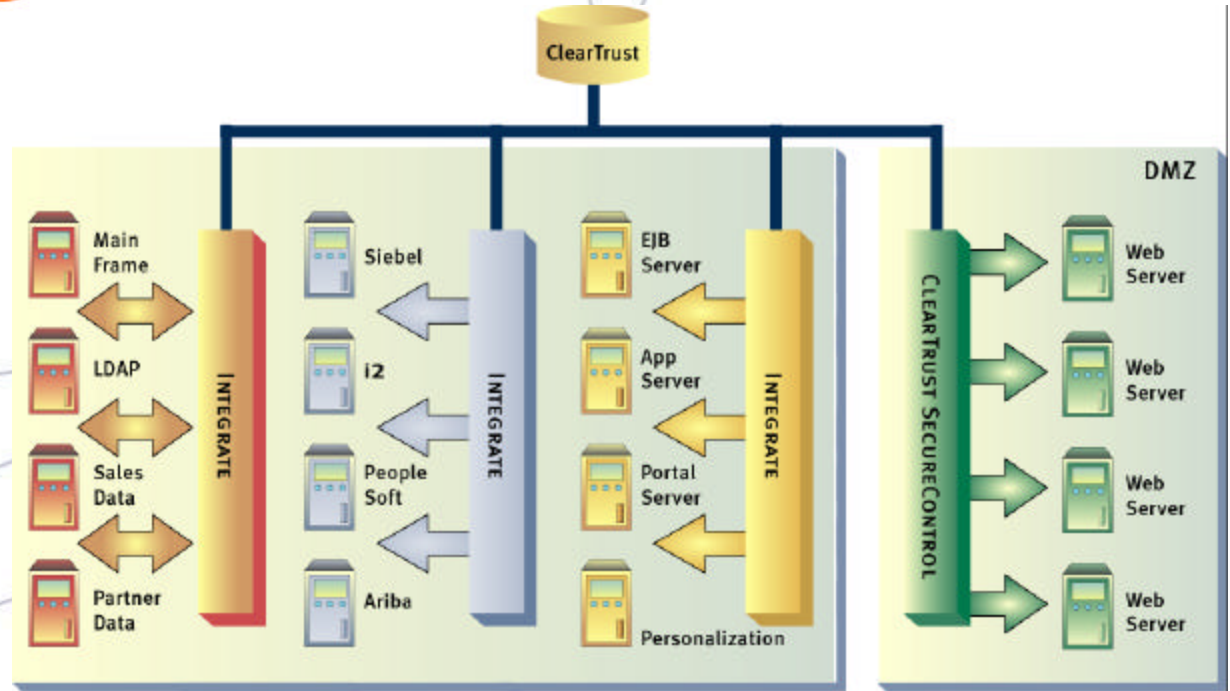
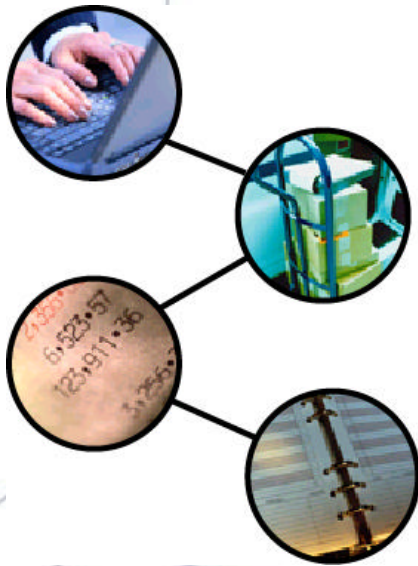
Customer Success: Major Pharmaceutical Firm

CUSTOMER SUCCESS →



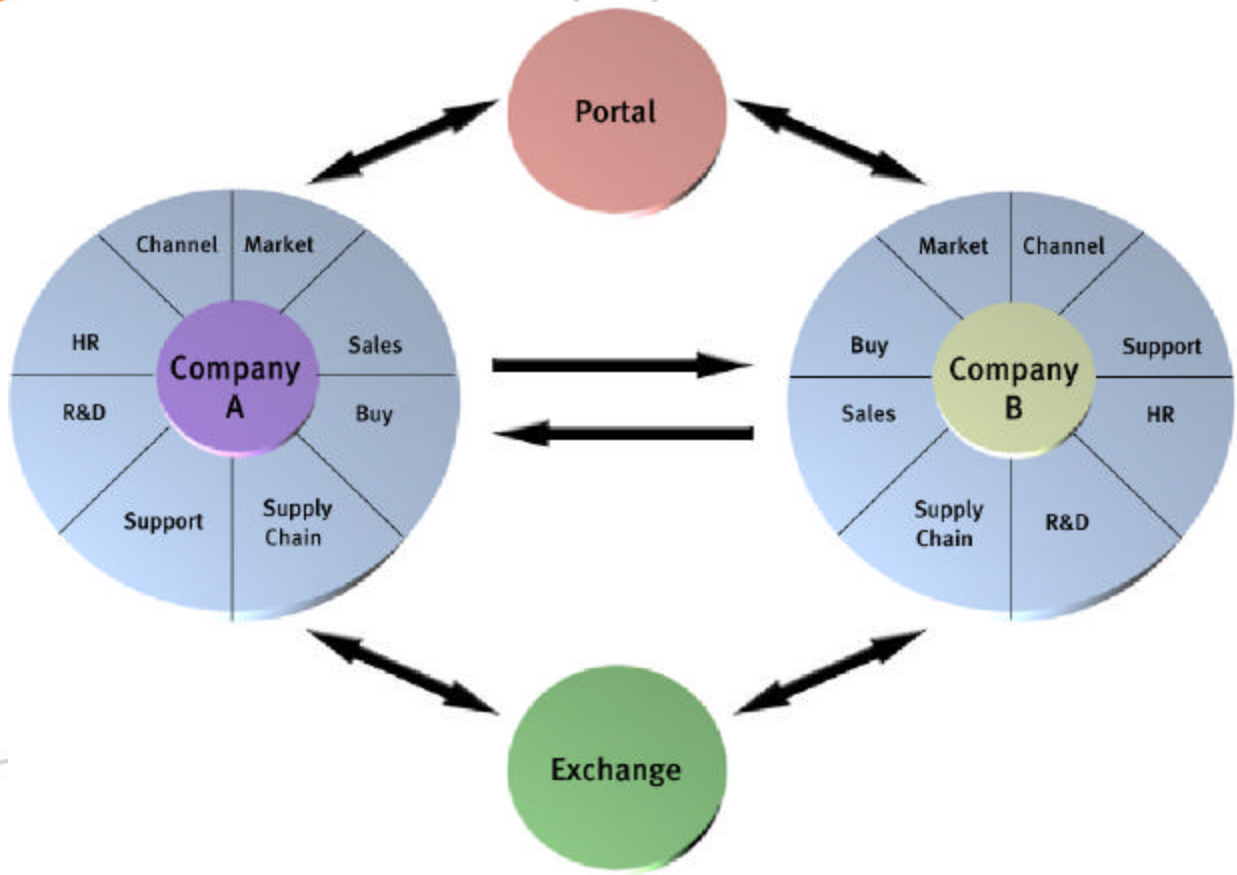
Customer Success: Trucking & Transport Firm

CUSTOMER SUCCESS



Customer Success: European Organizations

CUSTOMER SUCCESS →





SECURANT
TECHNOLOGIES

