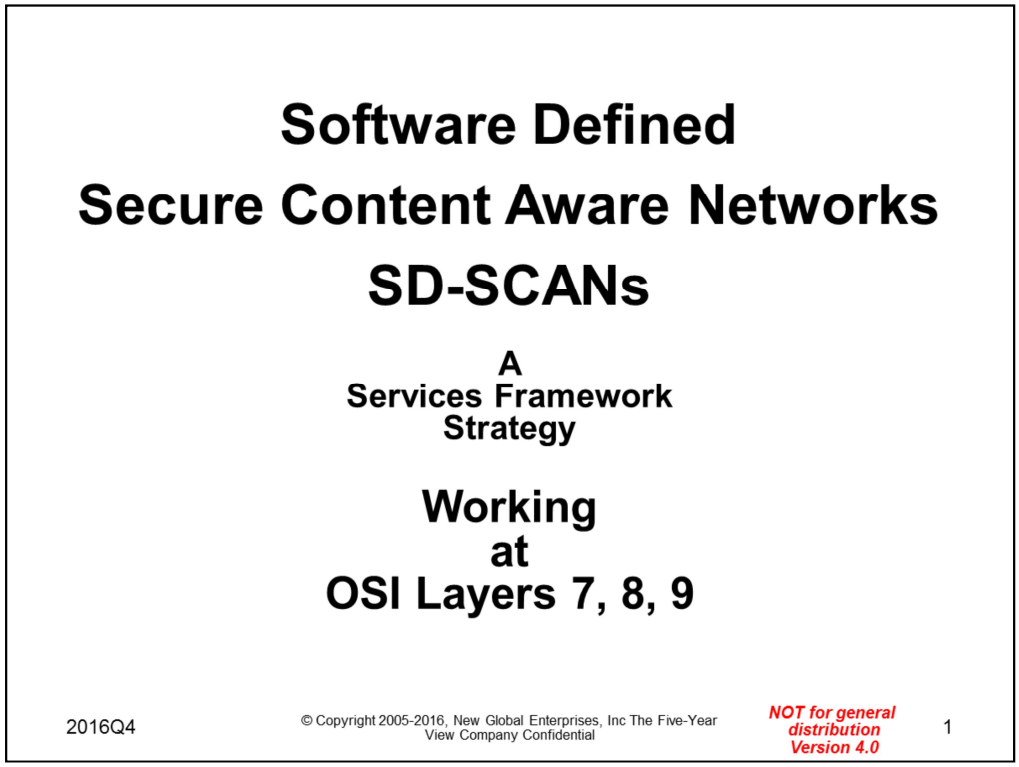


Updated to 2016: Added Software Defined to SCAN, SD-SCAN

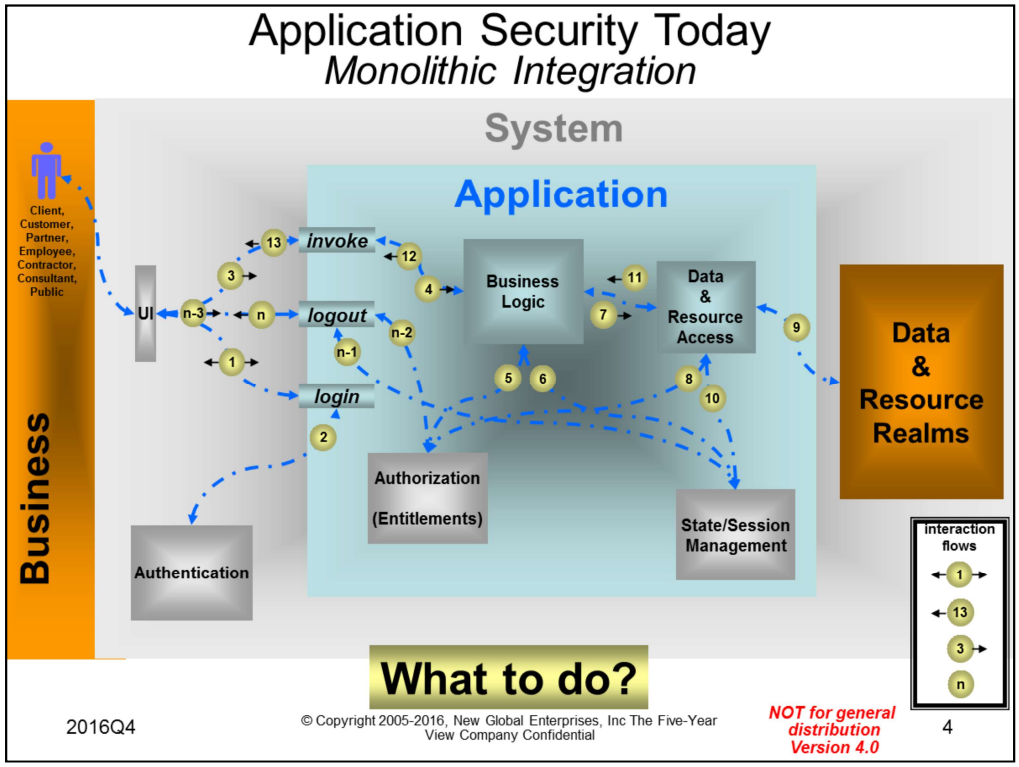
And Added Predictive Analytics Engine to augment Rules Engine

SOA,
you wanta' change?

Need to factor
current applications, processes,
organizations
and
redeploy in controllable
private, trusted settings

For example

Look at Application Security



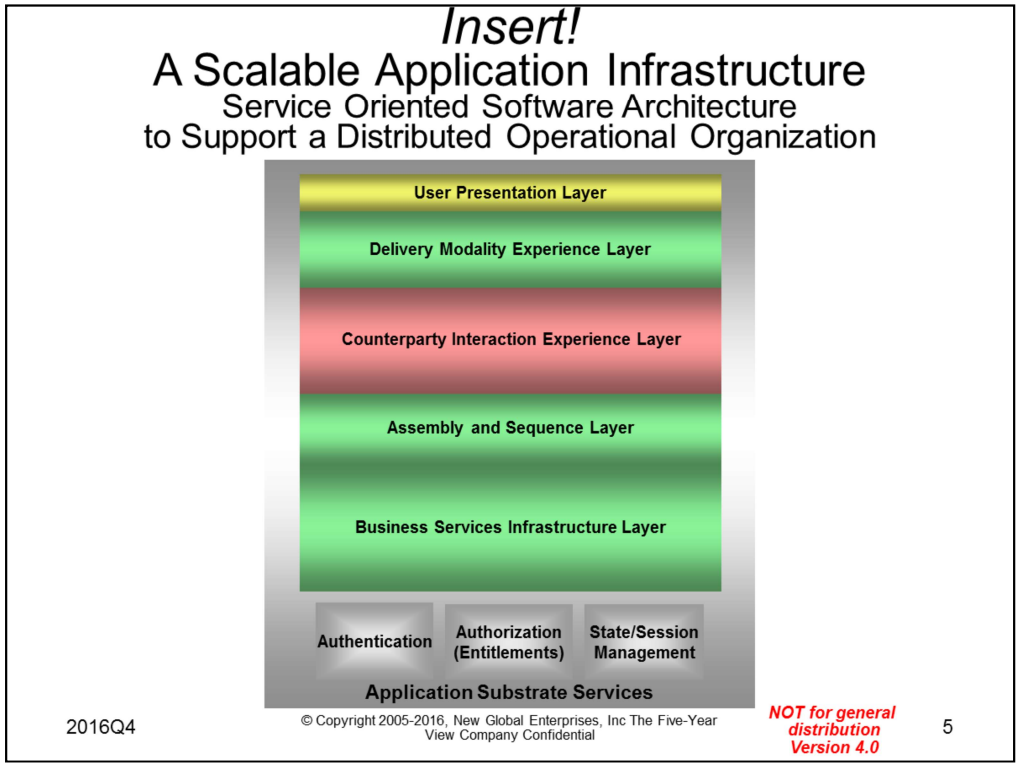
Example sequence and flow

1. Credential presentation protocol (https put ***login*** form + password factor and role resolution sequence: rich client?), ends with a Navigation Window
2. Verification Protocol, produces a Certificate which expires if not used within a variable but fixed period of time and always in a variable but fixed period of time
3. Selection protocol in navigation Window (https put ***invoke*** form)
4. Method invocation in app server of a Java Process: Application Function object
5. Verify credential for use in function (method invocation to Authorization Enterprise Java Bean)
6. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
7. Request object profile from Data Manager (method invocation to Data Realm Enterprise Java Bean)
8. Verify credential for access to data (method invocation to Authorization Enterprise Java Bean)
9. Send SQL statement to Data Base (e.g., Oracle PS SQL)
10. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
11. Return Protocol for Result Set
12. Formatting protocol for User View (JSP dhtml)
13. Presentation protocol for User (Browser)
14. Yada yada yada

-
-
-

n-3. Logout protocol
n-2. Destruction Protocol for Certificate
n-1. Destruction Protocol for State/Session
n. User Notification of exit from Application

Etc., etc., etc.



Business Investment Focus:

Creating Capabilities (Processes that produce significant results) known as Service Point Suites in the SOA World.

•Products
Targets basic Business Entity services like Customer, Product, Partner, Employee, etc, and the capabilities to orchestrate and integrate because this is the Product customization feature

•Channels
Targets Channel and User Presentation Experiences which are the modalities that the Customer/Clients Segments deal with the Services/Products of the Firm

•Segments
Targets the Client Services Experience with Firm Business Processes

•All three Firm Business Units invest in the Application Substrate Services as these are common infrastructure for Applications

Service Layers

•**User Presentation Experience**—the look and feel of the Client and Provider interaction.

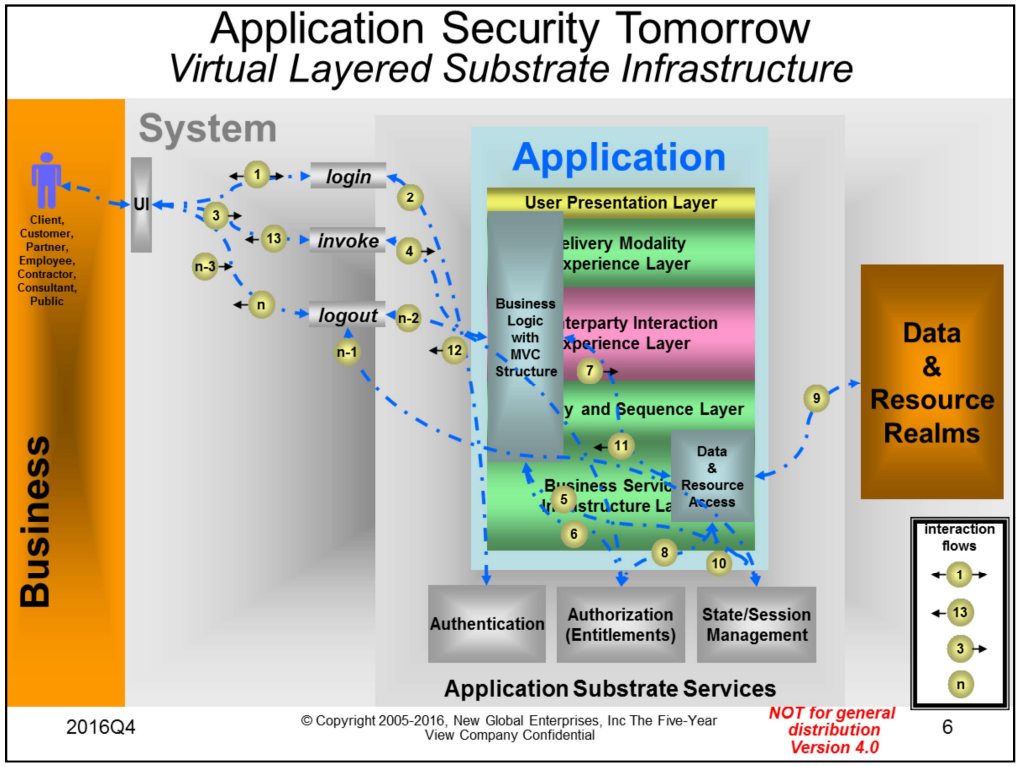
•**Delivery Modality Experience**—which is how a device/delivery mechanism mediates the Client Experience: a cell phone is different from a Blackberry is different from a mouse, keyboard and monitor which differ through direct-connect served by an agent as opposed to through the Web.

•**Counterparty Interaction Experience**—which is how the Client and Provider discover and deliver the Value in those services: this is, after all, the Business point of it all.

•**Assembly and Sequence**—which composes those basic and other composite services: the subject of current W3C working group debate.

•**Business Services Infrastructure**—which form the basic component substrate: IBM (PwC) has done a version of this for European Banking.

•**Application Substrate Services**—which handle the management of (1) security (Identity, Authorization and Role), (2) messaging protocols among components (both within and outside the enterprise, e.g., Web Services, E-Mail, IM, VoIP), (3) session/work flow, (4) personalization, and, (5) the collection, integration, storage and delivery of data to components of the Stack: all these functionalities “just happen” which allows the creator of functionality of the components to focus on business requirements



Example message sequence and flow

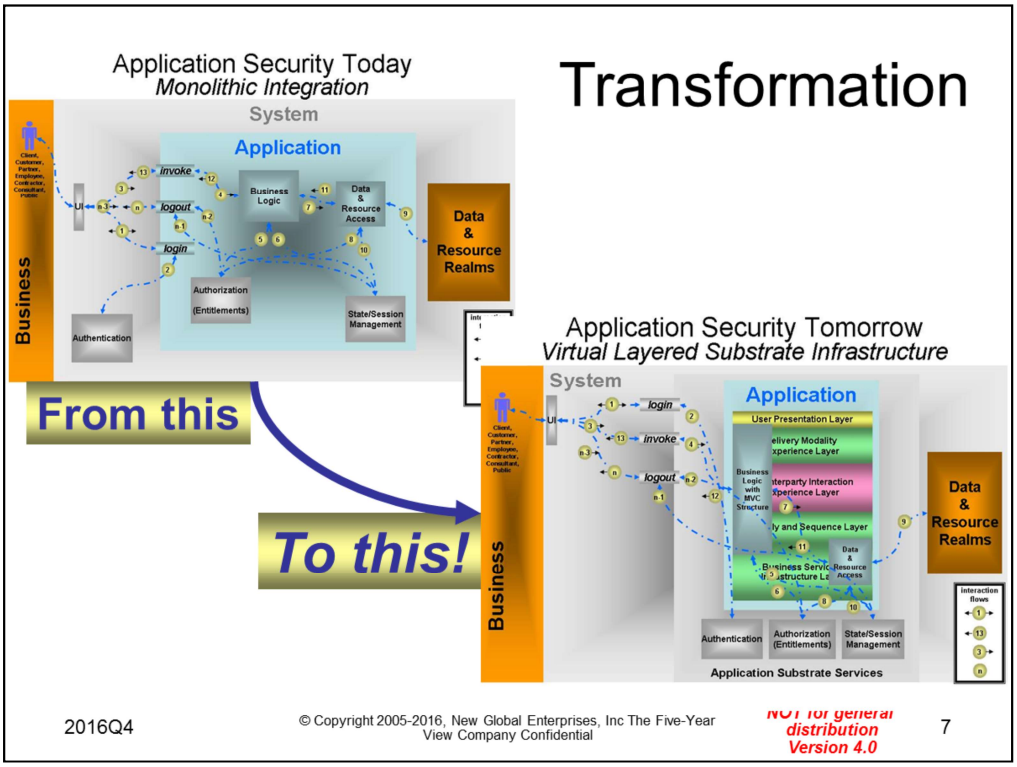
1. Credential presentation protocol (https put ***login*** form + password factor and role resolution sequence: rich client?), ends with a Navigation Window
2. Verification Protocol, produces a Certificate which expires if not used within a variable but fixed period of time and always in a variable but fixed period of time
3. Selection protocol in navigation Window (https put ***invoke*** form)
4. Method invocation in app server of a Java Process: Application Function object
5. Verify credential for use in function (method invocation to Authorization Enterprise Java Bean)
6. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
7. Request object profile from Data Manager (method invocation to Data Realm Enterprise Java Bean)
8. Verify credential for access to data (method invocation to Authorization Enterprise Java Bean)
9. Send SQL statement to Data Base (e.g., Oracle PS SQL)
10. Update State and Session Context (method invocation to State/Session Enterprise Java Bean)
11. Return Protocol for Result Set
12. Formatting protocol for User View (JSP dhtml)
13. Presentation protocol for User (Browser)
14. Yada yada yada

-
-
-

n-3. Logout protocol
n-2. Destruction Protocol for Certificate
n-1. Destruction Protocol for State/Session
n. User Notification of exit from Application

Etc., etc., etc.

Transformation



We know about the Application Layer 7.

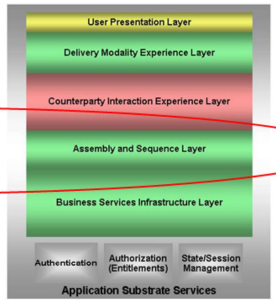
But I thought Layer 8 was the People!

It is!

People AND Workflow using Applications

- Layer 8 is about what the **People** assemble & sequence executing **Business Processes** within Layer 7
  - **Workflow**
    - and all the ancillary protocols among peer components in this Layer

A Scalable Application Infrastructure
Service Oriented Software Architecture
to Support a Distributed Operational Organization



Process Implementation Focus

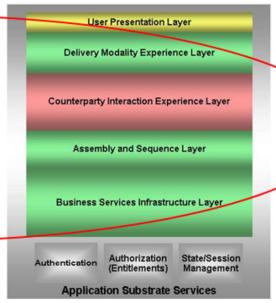
If People and Workflow are Layer 8, then what is Layer 9?

Business Process Engineering!

Business Process Engineering

- Business Processes, in economic terms, produce Significant Results
  - Layer 9 is engineering for Significant Results
    - This is Business Design and Optimization
      - Interaction Contracts with Counterparties

A Scalable Application Infrastructure
Service Oriented Software Architecture
to Support a Distributed Operational Organization

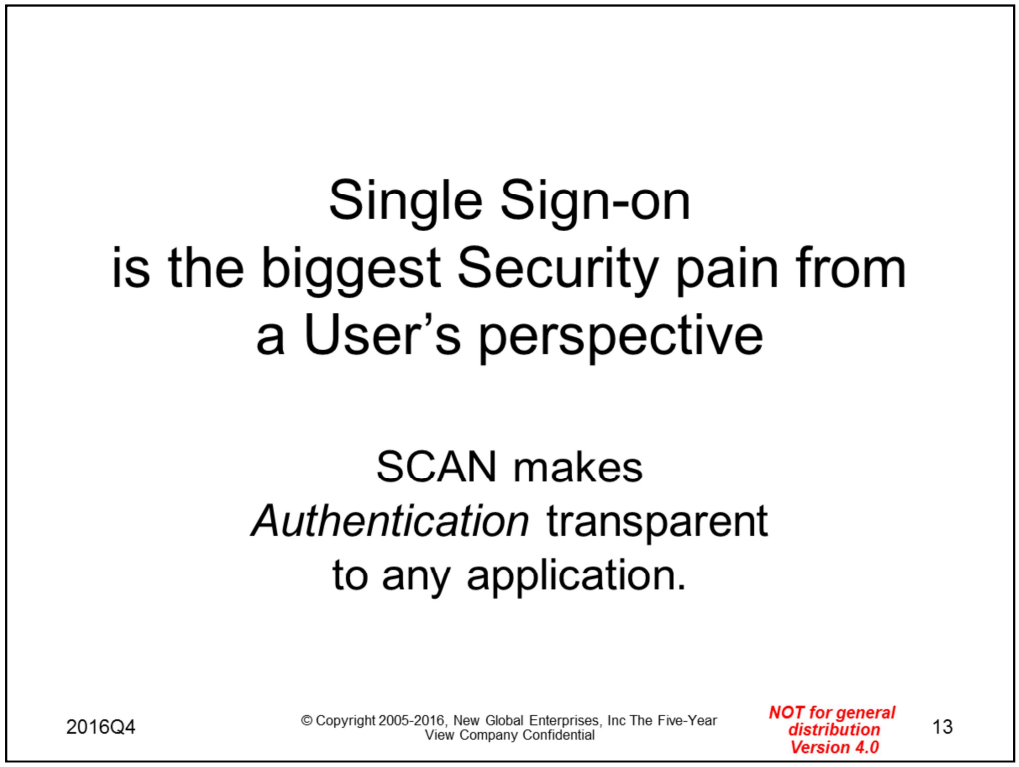


Level and Scope

Up the Stack and Aacross the Applications

Application Security Tomorrow

Functional Decomposition
around
Messaging Protocols



And Authority Happens.

All Security Services need to operate independently of the Functional Logic, in other words it is more of a Feature of the environment.

Security Message Categories
Factored Functionality

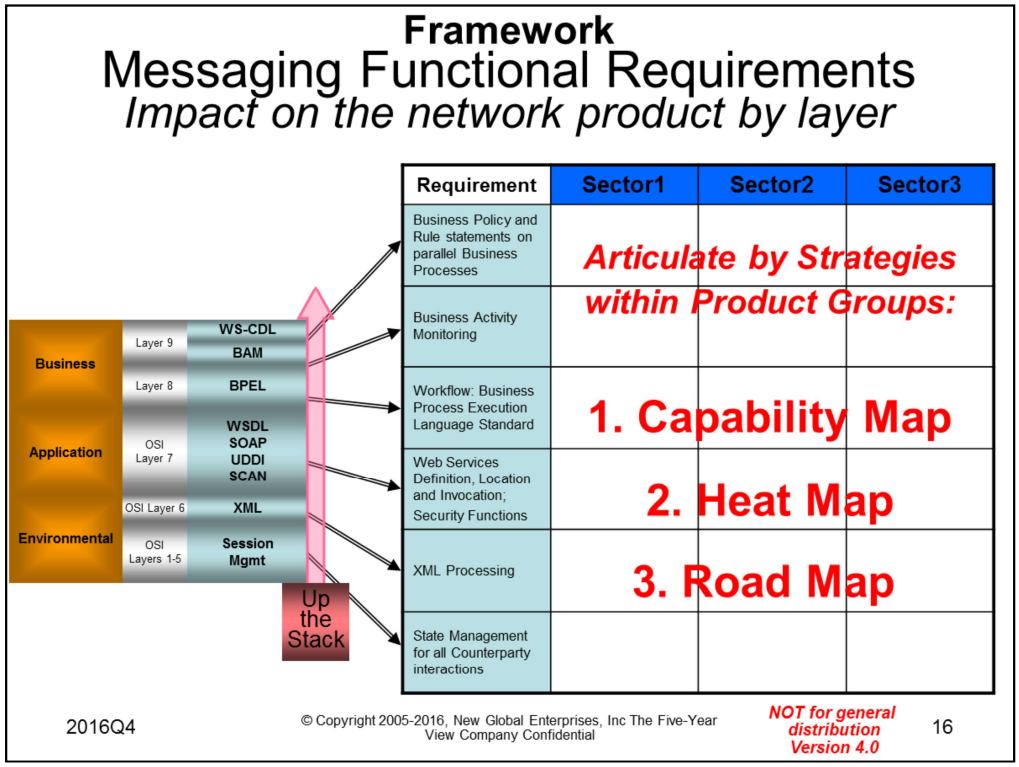
Security Protocols	**Service Invocation (SI)**	**Event Dispatch (ED)**	**Data Distribution (DD)**
Business			
	login	***login***	***login***
Application	***login***	***login***	***login***
	login	***login***	***login***
Environmental			

S C A N

e.g., ***login*** plays in every Category

How does all this fit into a Services Architecture?

What does it mean for Company?

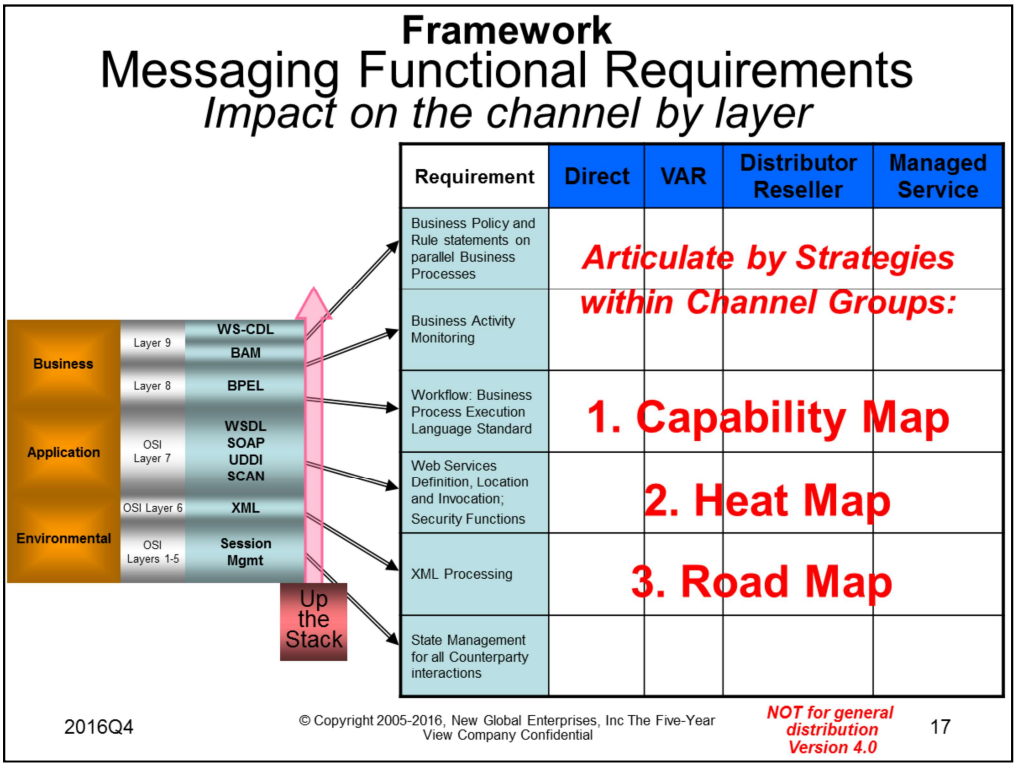


1. Capability Map
   What knowledge, skills and processes are required to deliver the functionality?
2. Heat Map
   What is state of Capability to Provide in Juniper?
3. Road Map
   How do we get there in 3-5 years?

WS-CDL:

Equally applicable to Channel Services:

1. Direct
2. VAR
3. Distributor/Reseller
4. Managed



1. Capability Map
   What knowledge, skills and processes are required to deliver the functionality?
2. Heat Map
   What is state of Capability to Provide in Juniper?
3. Road Map
   How do we get there in 3-5 years?

Equally applicable to Channel Services:

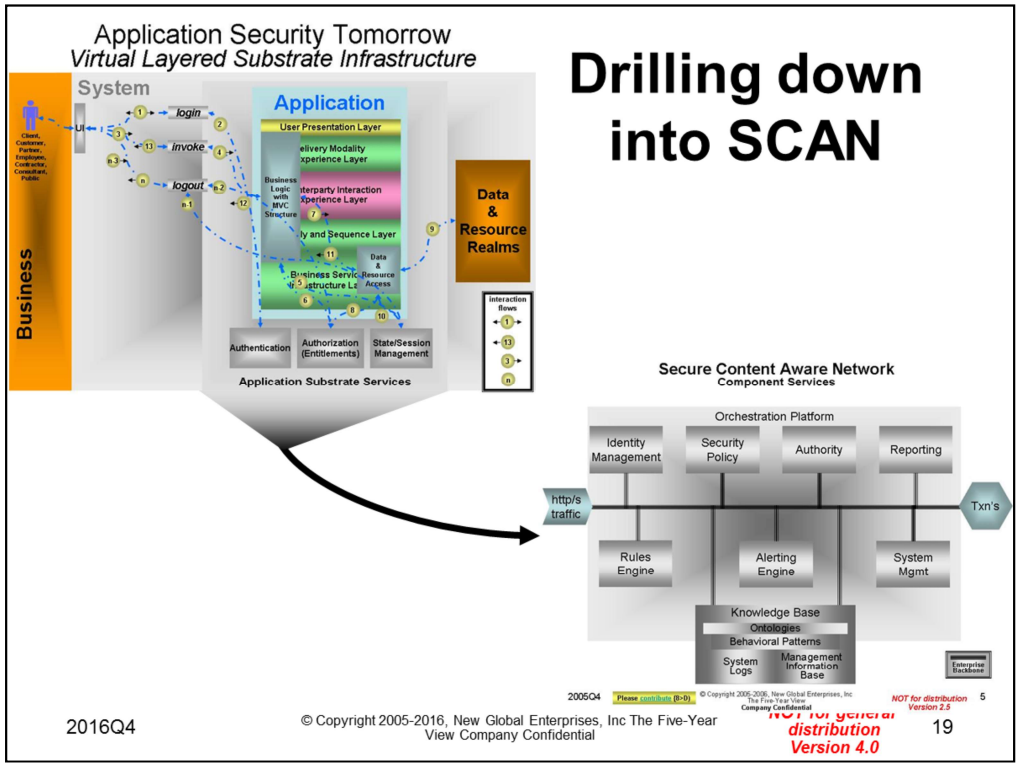
1. Direct
2. VAR
3. Distributor/Reseller
4. Managed Service

- Service

- Experience

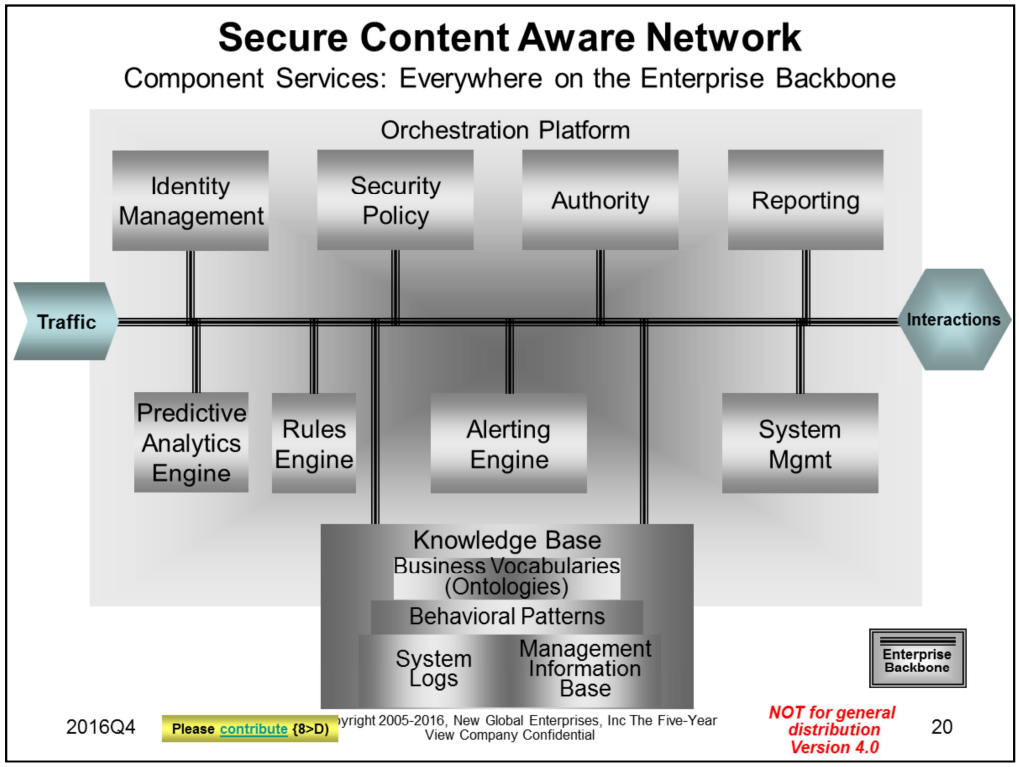
Full Set of Functional Categories for SCAN

Well-Architected
Component
Service Point Suites
in the Application Layer 7.0



2016Q4

19



Technology Portfolio Sectors of the Services that Implement the Instruction and Control Points: possible third party suppliers, including Open Source

SCAN tracks the messages and sessions that result in create, read, update and delete of Enterprise Resources, CRUD being a transaction. Enterprise Resources include money, digital information, client data and goods.

Orchestration Platform

Functions to integrate data and processes amongst the component services in tracking of the traffic and interaction sessions.

Digital Harbor

Identity Management

Authentication services and key and certificate management services ,e.g., PKI or X509

Open X509

Security Policy

Server that contains the set of rules, notification event dispatch, and possibly autonomic actions to intercede, prevent and/or correct.

RiskInsight

Authority Server

Manager of role based permissions

SOA Software

Reporting

Structured Reports: Business Sessions Alert Reports; Active real-time dashboards; Visualizations

Quantum 4D

Rules Engine

Inference management capability based on ontologies like OWL

Protégé, JESS, ActiveBPEL

Alerting Engine

Server that oversees patterns of interest and raises events to be handled by appropriate process

Cydelity

System Management

Services to collect and store instrumentation data and provide visibility on system processes

New Global Enterprises (Instrumentum/ARM-1)

Knowledge Base

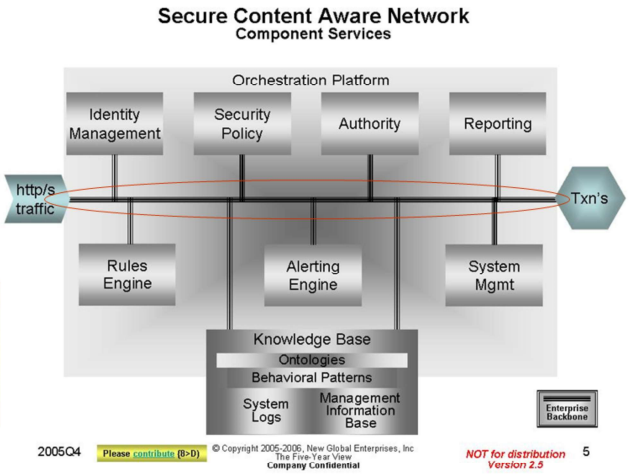
Persistent store of semantic information (ontologies), behavioral patterns of interactions, log of system access and use and base of instrumentation data

XML, RDF, OWL, XDI, PostgreSQL, sceptreTalk™

Services that Implement the Instruction and Control Points for a Secure Content Aware Network (SCAN)

SCAN tracks the messages and sessions that result in create, read, update and delete of Enterprise Resources, CRUD being the transaction.

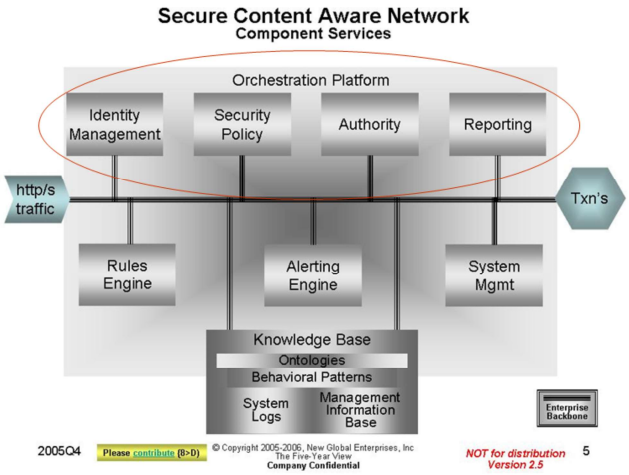
- Enterprise Resources include money, digital information, client data and goods.



Functionality Descriptions

Possible third party suppliers, including open source

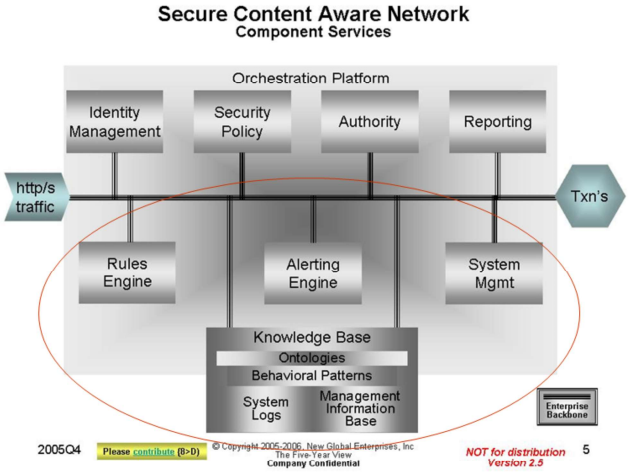
- Orchestration Platform
  - Functions to integrate data and processes amongst the component services in tracking of the traffic and interaction sessions.
    - PI Calculus based (assertions on parallel processes)
- Identity Management
  - Authentication services and key and certificate management services ,e.g., PKI or X509
    - Open X509
- Security Policy
  - Server that contains the set of rules, notification event dispatch, and possibly autonomic actions to intercede, prevent and/or correct.
    - Reactivity, RiskInsight
- Authority Server
  - Manager of role based permissions
    - SOA Software
- Reporting
  - Structured Reports: Business Sessions Alert Reports; Active real-time dashboards; Visualizations
    - Quantum 4D



Functionality Descriptions

Possible third party suppliers, including open source

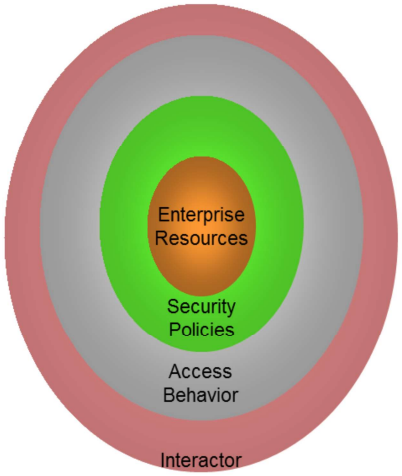
- Rules Engine
  - Inference management capability based on ontologies like OWL-based
    - Protégé, JESS, ActiveBPEL
- Alerting Engine
  - Server that oversees patterns of interest and raises events to be handled by appropriate process
- System Management
    - Cydelity
  - Services to collect and store instrumentation data and provide visibility on system processes
    - New Global Enterprises (Instrumentum/ARM-1)
- Knowledge Base
  - Persistent store of semantic information (ontologies), behavioral patterns of interactions, log of system access and use and base of instrumentation data
    - XML, RDF, OWL, XDI, PostgreSQL, Protégé, Jess, sceptreTalk™



Talking Enterprise Application Security

Component Objects

- **Enterprise Resources**
  - The things to protect: Money, Digital Property, Client Information, Shipment of Merchandise
- **Security Policies**
  - Business rules on who can do what with what by when
- **Access Behavior**
  - Streams of http/s traffic, logs of actual and attempted entry into Enterprise Zones of Trust and actual and attempted access and usage of the Enterprise Resources
- **Interactor**
  - Identity/Role of person or system engaging in the Behaviors



Enterprise resources

The things to protect: Money, Digital Property, Client Information, Shipment of Merchandise

Security Policies

Business rules on who can do what with what by when

Access Behavior

Streams of http/s traffic, logs of actual and attempted entry into Enterprise Zones of Trust and actual and attempted access and usage of the Enterprise Resources

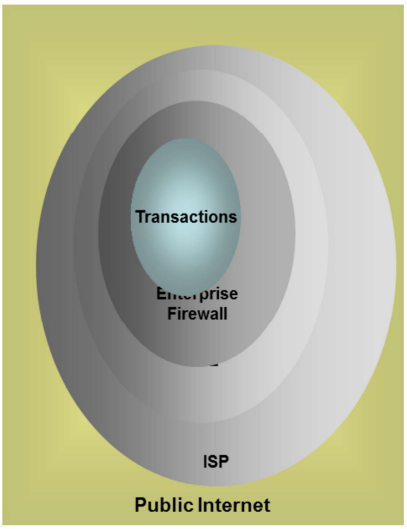
Interactor

Identity and Role of person or system engaging in the Behaviors

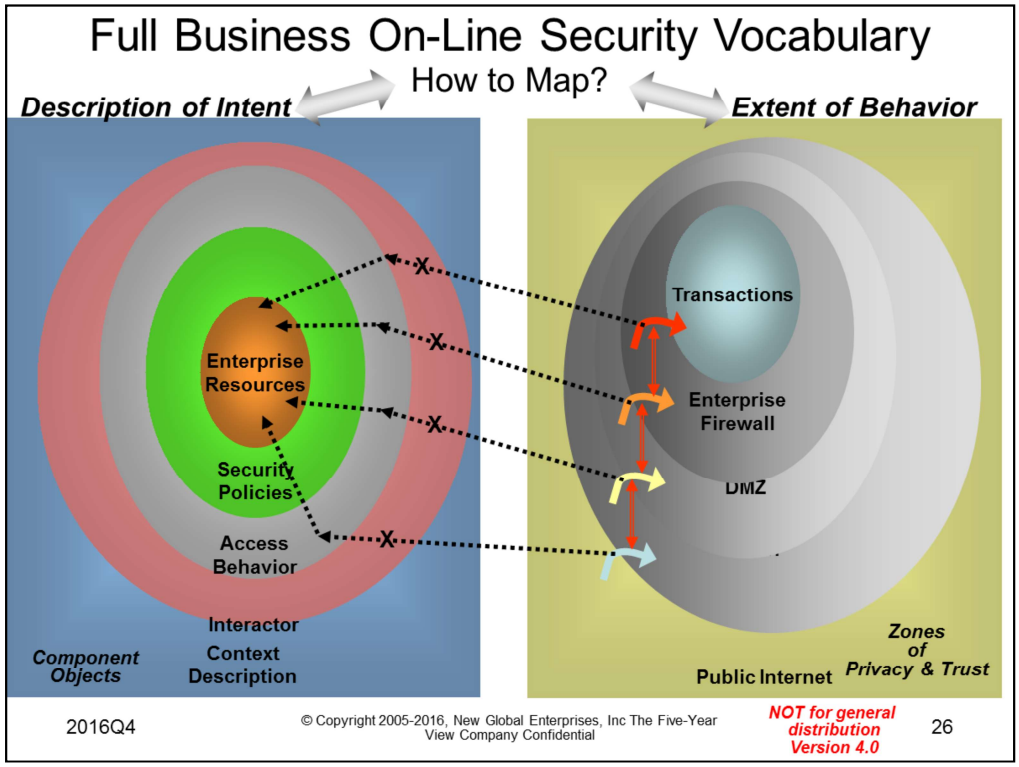
Concentric Spheres of Privacy &Trust

Interactional Lines of Defense

- **Public Internet**
  - Maximum visibility, Zeroth Zone of Privacy and Trust
- **ISP**
  - Perimeter of First Zone of Privacy & Trust
- **DMZ**
  - Perimeter of Second Zone of Privacy & Trust
- **Enterprise Firewall**
  - Perimeter of the Third Zone of Privacy & Trust
- **Transactions**
  - Access and change



Thanks to John Macauley (jmacauley@insignisconsulting.com) for this observation



Do retinal scans: What you see is what you get.

Enterprise Resources (Thanks to Bob Ciccone (Bob.Ciccone@cydelity.com) for these categories

Control over Money, Digital Property, Customer Information, Shipments of Merchandise

Surveillance: Security, Risk and Regulation

Transactions

Instruction (Order, Delivery, Payment, Information Request)

There is a business even more in this network architecture. IPV6 is still a dream.