Cisco Services.
Making Networks Work.
Better Together.

Unified Security – A New Way to Protect Financial Service Institutions through a Unified Security Strategy and Architecture

CH Hariharan, Senior Director / Enterprise Architect, Cisco Advisory Services
Anuj Kumar, Technical Leader / Enterprise Architect, Cisco Advisory Services

It's a fact—Financial Service institutions are under attack. The seemingly endless barrage of threats to the sanctity of the corporate databanks comes daily from new and varied sources. The Chief Security Officer or Chief Information Officer are most often reacting to a multitude of operational issues that make tackling the bigger security picture feel out of reach. Yet with the continually evolving dynamics of modern financial transactions, an enterprise-wide security strategy is precisely what is needed to move beyond the trap of reaction and toward a safer future. Consider this a wake-up call.

The current business environment poses a number of distinct challenges to both assessing the present state of enterprise information security and creating a sound model for protecting the enterprise going forward —

- Financial institutions traditionally take a 'stove pipe' approach, where various components of security are carefully assessed and solutions tailored to each. For example, securing laptop computer access to enterprise systems involves many different security parameters– authentication, authorization, encryption, mobile access, application access control, firewalls, and security policy management. Access for other computing devices may have different parameters to be accommodated. This device-centric approach, however, doesn't take into consideration the impact of the network or the application server on security – yet they are equally important parts of the picture. The challenge, then, is how to develop a unified, enterprise-wide security strategy and technology architecture that encompasses all points of vulnerability, and not perpetuate the stove pipe approach.

- There is no common model and framework through which the Security Organization can communicate and collaborate with other organizations in the enterprise, whether they are business or technology focused. This leads to different groups pursuing disparate approaches to security requirements in support of their own business needs. Unfortunately, many of these needs are replicated throughout the organization, resulting in a hodge-podge of solutions. What's really needed is an industry-standardized model that fosters and encourages better, more effective collaboration across the enterprise.

- Several emerging business models are being discussed in the financial services industry, especially the transformation from transactions to interactions. As these models evolve, the challenge will be leveraging them into the existing corporate security strategy and architecture. One possible approach may be to implement a Service Oriented Architecture (SOA) into the enterprise technology infrastructure to facilitate the transformation.

- In the United States and certainly elsewhere in the world, financial institutions are viewed as one of the critical infrastructures that support the health and economic well-being of the nation. U.S. Federal compliance requirements and information security standards are constantly updated to address new and changing threats worldwide – while compliance and standards in other countries vary for each. Many financial institutions today have an international footprint. Therefore, it is vital for a successful enterprise security strategy to enable the seamless application of government compliance requirements and information security standards in a way that fits a global business model.

Given these imposing challenges, financial institutions are faced with some imminent and significant decisions – *What is* the right methodology and process to sustain an enterprise security strategy and architecture? *How should* institutions aggressively address new threats to customers, partners, suppliers and employees? *How will* they successfully manage security in the face of ongoing changes to business demands, from competition and from changing service offerings? And, *how will* the institution meet or exceed the changing requirements of government compliance? All of these issues must be resolved, and piecemeal solutions ultimately will not serve for the long term.

Future Vision: Unified Security Makes for a Trusted Enterprise

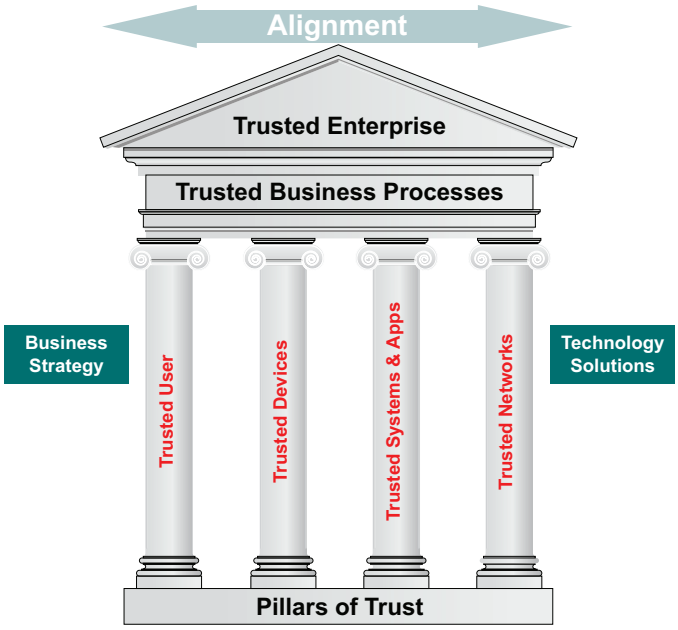
To survive and thrive, a new vision and a bold approach are required. The successful financial institution will develop a comprehensive, unified security strategy and architecture that —

- Enables secure business transactions and interactions both within the enterprise and externally with customers and business partners
- Protects the firm's critical assets, including customer information, corporate information and intellectual property
- Provides the capability for threat control and rapid containment
- Prevents unauthorized access to the firm's physical facilities and technical infrastructure
- Complies with government regulatory requirements for information security
- Enables efficient security monitoring and management

Only when these challenges are successfully addressed can a financial institution become a truly trusted partner to all members of its ecosystem. So what does a Trusted Enterprise look like?

The Trusted Enterprise comprises key structural components that have access to, store or carry corporate-sensitive information that must be protected. These include four virtual 'pillars' — users, user devices, systems & applications, networks — and fifth, like a virtual 'truss' touching each of these access points, the business processes on which the organization runs. To create a truly trustworthy operating environment for employees, customers and partners, the financial services firm must ensure that each of these structural components are individually secure within an architecture that embraces and protects the entire structure.

Structural Components of the Trusted Enterprise



Business Processes – the formalized methods and accompanying infrastructure through which the firm conducts its business operations

Users – The people that access a firm's resources for conducting its business – including employees, contractors, customers and business partners

User devices – The physical tools people use to access a firm's systems and applications in order to perform business operations. Devices include workstations, laptops, PDAs, phones and specialized hardware

Systems and Applications – A firm's servers and business applications infrastructure

Networks – The communications infrastructure, either owned by a firm or publicly shared, that is used to access the firm's systems and applications. Networks can include Enterprise WAN / LAN, the Internet, and associated network equipment

An Evergreen Process Keeps Security Current for the Long-Term

The vision for the Trusted Enterprise cannot be fulfilled without two critical components — a sustainable process that addresses adapting security threats over time, and a comprehensive but flexible architecture defined through the process. The 5-step, Evergreen Strategic Planning and Implementation Process for Unified Enterprise Security drives an enterprise-wide security infrastructure that remains current and viable even as security threats evolve.

Evergreen Strategic Planning and Implementation Process for Unified Enterprise Security

The process begins with the identification of corporate security threats. This includes existing threats within the organization as well as emerging threats to users, end devices and networks. The identification process must incorporate an understanding of the impact of each identified threat on the Trusted Enterprise 'pillar and truss' components and ultimately on the core business itself.

Once the threats are recognized, security needs must be established. These should be integrated closely with regulatory requirements such as Sarbanes-Oxley or HIPAA, as well as with internal corporate polices and goals.

What is a Security Service?

- A Security Service is a software module that performs a business security function and that can be created by integrating one or more security products or technologies with the different layers of an enterprise architecture
- Security Service capabilities should be architected as shared, integrated services that meet the information security requirements of an enterprise
- Security Services should integrate the principles and guidelines of Service-Oriented Architectures
- Security Services should support—
  - * Provisioning consistent security capabilities across an enterprise
  - * Avoiding duplication of capabilities
  - * Sharing of a single solution across an enterprise

Following these discovery phases, the Enterprise Security Architecture is defined. This phase includes establishing an architectural framework if one does not exist. If one does exist, then this is the step for defining and integrating the Security Service framework into it. A detailed description of these Services is mandatory in order to avoid confusion regarding the security solution requirements.

The next phase in the process is to create a Security Deployment Roadmap. In this step, the Security Services identified in the previous phase are mapped to the overall enterprise architecture, the pillars of the Trusted Enterprise, and the technologies that will deliver the Services. The roadmap should be multi-year to clarify a broad view of the complete organizational deployment strategy.

The final phase of the process is to deploy the Security Services into the enterprise. This involves various design and implementation steps, including creating detailed architectural designs, testing integration capabilities, conducting pilots, and completing production rollouts.

Although this is the last detailed phase, the process does not end here. Identifying and responding to new threats will be a constant dynamic within the enterprise, so the process must continuously perpetuate. However, because the process yields a modularized, integrated architecture, updates to specific components can be 'plugged in' to holistically mitigate new threats without requiring a broad foundational change. This unified approach extends the usability and value of the architecture for the long term, increasing ROI on the original development investment.

The balance of this paper explores each phase of this evergreen process and its related architectural impact in more detail.

Evolving Business and Technology Trends Heighten Enterprise Security Vulnerabilities

As technology plays an increasingly business-critical role, enterprise security risks become more prevalent. Today, technology is reshaping the financial industry's approach to traditional business needs of increasing revenue, improving customer relationships and increasing productivity and efficiency, in ways that both benefit financial firms and customers but also continually create new security vulnerabilities.

Business Need: Increasing revenue

While there are many ways to increase revenue, the two most prevalent methods are reacting in real-time to customer demands, and driving innovative products and services to market as quickly as possible.

Both of these methods require greater automation of business processes and procedures, so that institutions will be nimble enough to meet market demands and sufficiently oriented toward doing more online transaction-based or interaction-based business. However, the results of greater automation and increased online business activities are a corresponding increase in both the exposure of online users and in the amount of information that needs protection in transit.

For example, the traditional banking model (up through the 1990s) was face-to-face contact between bank staff and customers at branch offices, and not online transactions. The amount of information exposed online was minimal and the types of attacks attempted were not sophisticated. But now, as remote banking becomes more prevalent, we see an increase in both horizontal (number of users) and vertical (number of services) online usage. We also see an increase in the amount of information exposed online. Furthermore, security attacks have matured to be sophisticated in nature and immediate in effect.

Given the business imperative of providing online transactions, the security architecture is now forced to accommodate new requirements—the amount of sensitive customer data stored on a firm's databases is increasing, as is the amount of information to be secured in transit across the network.

Business Need: Improving Customer Relationships

As financial institutions look to improve customer service through relationship building, they must rely on the highly flexible use of all resources – time, location and service level – to interact with customers. The need is not just around improving services, but also increasing the level of trust between the firm and the customer. The firm must also work to improve partner relationships, such as those with clearinghouses and loan originators, and to integrate the virtual aspects of these partner services into improving overall customer service.

Here, the business need is clearly improving collaboration with customers in an 'anytime, anywhere' mode. This is an appropriate place to leverage Customer Relationship Management software and establish metrics for understanding better methods of customer interaction. The net effect will be an interactive firm-to-customer dynamic that fosters new and innovative financial products – ultimately helping the institution achieve greater competitive differentiation and hopefully increase market share.

For example, financial service contact centers were traditionally organized around geography or product set, i.e. a card products call center handled card products but not mortgages. Now, digitally enabled, 'virtualized' communications and related technologies easily allow contact centers to cross-sell and up-sell other products, servicing customers any time, anywhere. In doing so, rich data may be obtained that can drive new or improved product offerings.

However, in this broadened service dynamic, protecting customer information becomes an even higher priority because the amount of information and the extent to which it travels greatly increases. Systems that were previously stove-piped are now opened up to other parts of the organization, or even to business partners, increasing targets for malicious activity. This forces a critical focus on identity authentication and access so the financial firm can determine who is looking to perform an action and on what systems.

Business Need: Increasing staff efficiency and productivity

All financial firms seek the cost reductions and increased ROI that come from improving process and staff efficiency. Re-using 'modularized' business processes, and virtualizing the resources that use them, are major steps toward realizing this benefit. For example, enabling mortgage applications to be processed by branch and regional office personnel rather than only by a centralized mortgage processing group represents a substantial efficiency improvement.

But for every re-use of a modularized business process, the number of corresponding system access points increases, exposing the vulnerability of each and compounding the security challenge. In our mortgage example, access to both the mortgage application software and the customer data multiplies across field offices, and must be tightly controlled according to user authority level. So, when planning re-use of multiple processes, an organization needs to carefully determine how the sheer number of systems it virtualizes will interoperate and be made available to all users that require them.

The changing nature of application development is what even makes this possible. Traditionally, most financial firms wrote monolithic applications created for a single purpose running on dedicated infrastructure resources. For instance, with credit card transactions, an application might validate a transaction through the card sponsor such as Visa or Mastercard. Also in the traditional model, lead times for new applications were long, and every new application would have its own module and unique security capabilities – a highly inefficient approach. This paradigm is now changing.

Today, we see rapid application deployment made possible through a Service Oriented Architecture (SOA) and through Web 2.0, where application modules are more easily re-used. In our credit card example, if we've already written a module for credit card validation with Visa or Mastercard, and then we create a separate application that needs the same functionality; there is no need for rewriting the application. Rather, the existing module is simply re-used as a service in the common repository.

Dollar Amount of Losses by Type of Incident

According to the Computer Security Institute, the top three types of security breach incidents accounted for over $1B in direct losses to business in 2005

Computer Virus:	$42,787,767
Unauthorized Access:	$31,233,100
Theft of Proprietary Info:	$30,933,000

Source: CSI/FBI 2005 Computer Crime and Security Study

Given this cleaner service-oriented model, security architectures must then focus on the need to be consistent across applications, infrastructure, and geography. This creates an opportunity to deploy security solutions as shared services rather than as separate point solutions.

Identify Security Needs

The next step in the evergreen cycle is to identify all of the enterprise security needs. Unfortunately it has become necessary to maintain a continuous look at emerging threats in the marketplace and how those may impact the business services and offerings of the firm. These threats define the security needs for each pillar in the Trusted Enterprise. Consequently, it becomes imperative to regularly reassess corporate security policies, because the risk profile of corporate data can change as new threats emerge — so, security needs become based on the firm's use of information.

One of the biggest challenges for today's financial service firms is managing the amount and complexity of regulatory and industry requirements. From Gramm-Leach-Bliley to Sarbanes-Oxley and Basel II, financial firms are tasked

U.S. Regulatory Compliance Impact on Structural Pillars of the Trusted Enterprise

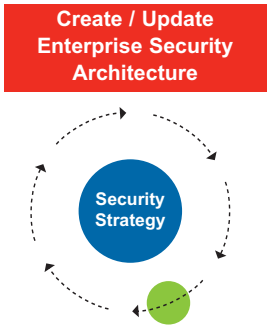
Regulation	User	End User Device	Systems & Apps	Network
Gramm-Leach-Bliley Act				
Encrypt electronic customer information		X	X	X
Monitor systems to detect intrusion into customer information systems		X	X	X
Use action plan when unauthorized access has occurred	X	X	X	X
Sarbanes-Oxley Act				
Control internal interactions between people and applications	X	X	X	
Implement authentication and control mechanism to know who can access what systems and data and what they may do with those resources	X	X	X	
Apply application-to-application access controls		X	X	
Audit and report on compliance for internal control implementations	X	X	X	X
FFIEC Guidance				
Identify and assess risks associated with Internet-based products and services	X	X	X	X
Identify risk mitigation actions including authentication strength	X	X	X	X
Measure and evaluate customer awareness efforts	X			
PCI Data Security Standard				
Build and maintain a secure network				X
Protect cardholder data	X	X	X	X
Maintain a vulnerability management program		X	X	X
Implement strong access control measures		X	X	X
Regularly monitor and test networks				X
California Security Breach Information (SB 1386)				
Notify consumers when their unencrypted personal information has been compromised	X	X	X	X
Bank Secrecy Act				
Report suspicious activities to appropriate regulatory and law enforcement agencies	X	X	X	X
USA Patriot Act				
Verify identity of customers opening new accounts to prevent money laundering and terrorist activities	X		X	
Basel II				
Measure 'Operational Risk' and quantify the economic value across key risk areas	X	X	X	X
Move from perimeter-centric security risks to end- to-end transactional risks	X	X	X	X
Conduct real time measurements of security controls and processes	X	X	X	X
Use simplified and consistent security architecture across enterprise applications to reduce complexity in measuring operational risks	X	X	X	X

with following a plethora of rules that mandate new processes, systems and external interfaces, multiplying points of vulnerability in an organization. Each of these regulations has a distinct impact on one or several of the Trusted Enterprise structural pillars, and must be taken into account when designing corporate policies and security infrastructure. A security architecture that identifies and successfully addresses each regulation's impact on each pillar will ensure that a firm is compliant with all of the mandated directives.

Proper regulatory compliance also means establishing appropriate controls around both physical and IT security systems. These controls require formal governance to ensure that compliance is met. Given the complexity of the regulations game board, this can be daunting. Fortunately, there already exist two leading global standards for financial firms to use in monitoring regulatory compliance –

- CobiT, the Control Objectives for Information and related Technology, offers a widely accepted IT control framework. It provides a set of measures, processes and best practices to use for choosing the best level of security and control that will protect corporate assets through an IT governance model
- COSO, the Committee of Sponsoring Organizations of the Treadway Commission (sponsored by five major professional accounting organizations), offers common internal rules and practices to assess the effectiveness of IT control systems in identifying factors that cause fraudulent or mistaken financial reporting

Given these existing and broadly adopted standards, financial firms have an excellent starting place from which to approach their security architecture development and governance, without reinventing the wheel.

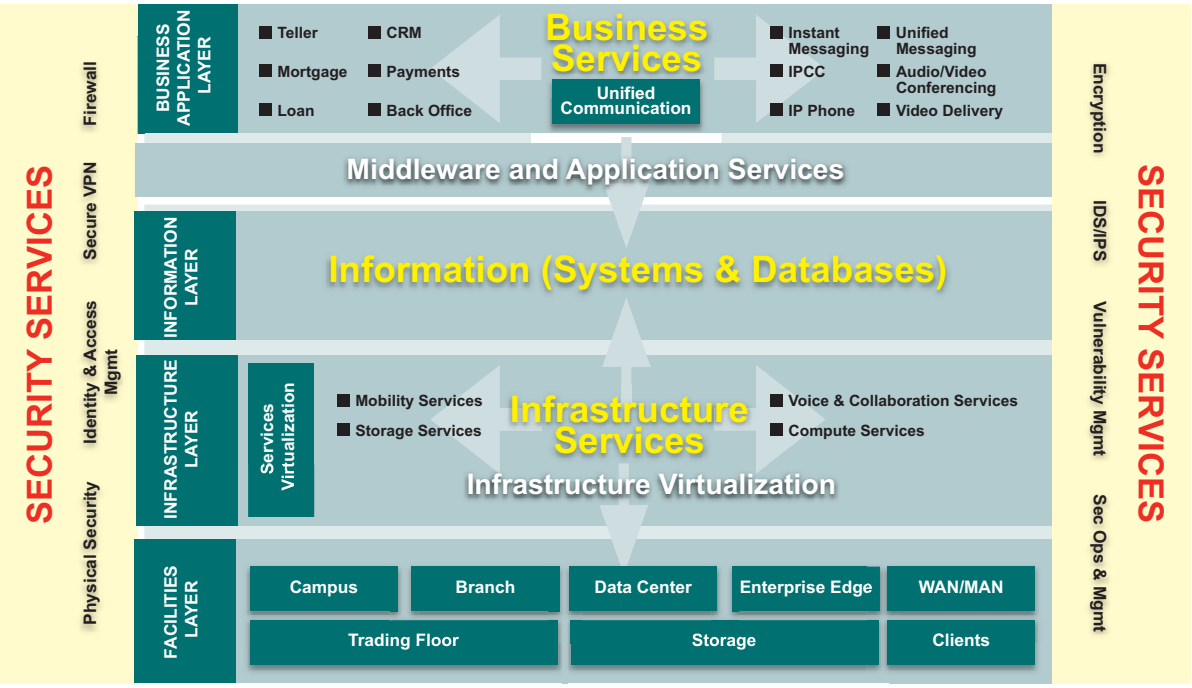


Once the threats and needs are identified, it is time to create the security architecture that will ensure the Trusted Enterprise. The architecture should be approached strategically to allow for continually changing business requirements over the long term. The chosen solution will need to be integrated across all access points, collaborative among all services and devices, and adaptive to automatically prevent new threats. In this critical step, a Service Oriented Architecture (SOA) offers the most comprehensive and cost-effective method for meeting end-to-end security requirements.

First, consider SOA in a business development context. Financial firms may seek to launch new business services quickly, without enduring the traditional IT backlog that can significantly lengthen time to market. As an example, a merger of two companies with their own unique customer databases and contact systems requires the creation of a third contact system blending the two. Traditionally, this would take months if not years to achieve. But using SOA, existing modularized business services can be easily knitted together and adapted as needed, creating a brand new, unique business service. In our example, modularized customer contact applications from each merged company could be quickly combined to yield the new application for the merged entity. This ability to design and deploy in near real time is a major SOA advantage.

However, with the SOA approach, every new business process that touches any or all of the Trusted Enterprise pillars also brings a new security service requirement, such as identity and access management, a virtual private network, a firewall, or even physical security. Because new business processes that affect the pillars are continually developed, associated new security services are also continually required. If approached through the stove pipe model discussed at the beginning of this paper, the sheer volume of components involved will result in skyrocketing implementation and maintenance costs. However, if using SOA, security services are treated as an enterprise-wide set, and can be reused and leveraged across the enterprise, producing significant cost savings and increased efficiency.

Security Services Framework—
Service Oriented Enterprise Architecture View



The security capabilities are architected as shared, integrated services that meet information security requirements of the enterprise.

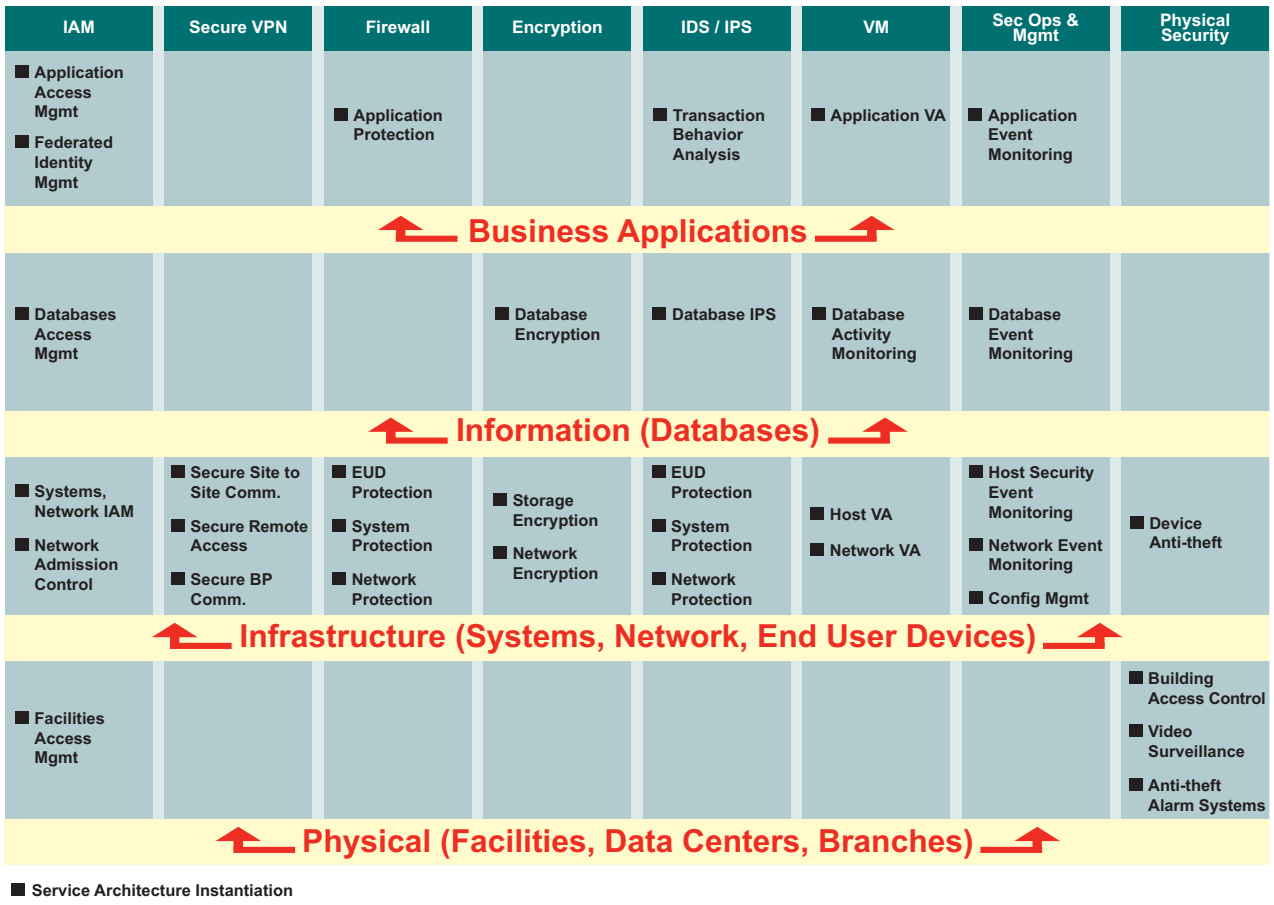
Given the SOA opportunity, Cisco Systems has embraced and applied the SOA approach and philosophy to the networked environment through a new architecture framework called SONA—the Cisco Services Oriented Network Architecture. The Security Services Framework Model above shows how SONA links all layers of the enterprise security architecture together. In this framework, security capabilities operate as shared, integrated services that will meet the information security requirements of today as well as tomorrow.

Create / Update Services Deployment Roadmap

The next phase in the evergreen strategic planning process is to create the roadmap for deploying security services within the enterprise. This process requires a gap analysis of an organization's existing enterprise architecture against the security architecture requirements defined in the previous phase. The following diagram offers a useful guide for approaching this analysis. It shows the ideal target state for security services applied to the four layers of the Enterprise Architecture framework. Specific functional elements are required for each security service at each layer. The task is to assess the existing organizational capability at each of these points, and identify the gaps that must be filled to complete the security architecture and ensure all points of vulnerability are covered. The technology deployment requirements for filling these gaps will be unique to every organization's situation.

Going through this assessment for an entire enterprise and then building out the needed infrastructure will be a major undertaking involving substantial commitment of resources. One potentially useful and efficient way to approach it is to use the Security Services Architecture Elements chart as the basis for scoring and prioritizing all of the security services a firm will need.

Security Services Architecture Elements within an Enterprise Architecture



The scoring process begins with considering the various architectural elements within a given security service as 'risk controls.' Each risk control is assessed by the firm and assigned 3 scores that reflect various attributes of the firm's current status for the control The scores rate the Architecture Maturity, which includes the firm's architecture consistency (have security functions been architected with consistent principles across the firm) and service orchestration ability (has the control been architected and deployed as a service), and the Deployment Maturity, which examines the firm's ability to deploy risk control architecture elements across the Pillars of the Trusted Enterprise. We suggest the following scoring system:

Architecture Maturity	
Architecture Consistency Score [60% weighting]	**Risk Control Current State**
1	Non-existent architecture
2	Disparate architecture model
3	Consistent architecture model
Service Orchestration Ability Score [40% weighting]	**Risk Control Current State**
1	Not deployed as a service
2	Partially deployed as a service
3	Fully deployed as a service
Deployment Maturity	
Score	**Risk Control Current State**
1	No current deployment
2	Partial deployment
3	Full deployment

Note that for Architecture Maturity scoring, architecture consistency is given a slightly higher weighting than service orchestration ability because of the criticality of getting the architecture right. Without the correct and comprehensive architecture, even the best service-oriented deployments will still leave a firm with security gaps.

EXAMPLE

Security Services Architecture Elements Score Card

Security Architecture Risk Controls	Architecture Maturity					Deployment Maturity
	Architecture Consistency	Architecture Consistency Weighted Score (B*0.60)	Service Orchestration Ability	Service Orchestration Ability Weighted Score (D*0.40)	Final Score for Architecture Maturity (C+E)	
IAM						
Application Access Mgmt	1	0.6	3	1.2	1.8	1
Federated Identity Mgmt	1	0.6	2	0.8	1.4	2
Database Access Mgmt	2	1.2	1	0.4	1.6	3
Systems Access	1	0.6	3	1.2	1.8	1
Network Access Control	1	0.6	1	0.4	1	1
Facilities Access Mgmt	3	1.8	2	0.8	2.6	3
Secure VPN						
Secure Site to Site Commn						
Secure Remote Access						
Secure BP Commn						
Firewall						
Application Firewall						
EUD Firewalls						
System Firewall						
Network Firewall						
Encryption						
Database Encryption						
Data in store Encryption						
Network Encryption						
IDS/IPS						
Transaction Behavior Analysis						
Database IPS						
EUD IDS/IPS						
Systems IDS/IPS						
Network IDS/IPS						
VM						
Application VA						
Database Activity Monitoring						
Systems VA						
Network VA						
Sec Ops & Mgmt						
Application Event Monitoring						
Database Event Monitoring						
Host Security Event Monitoring						
Network Security Event monitoring						
Configuration Management						
Physical Security						
Device Anti Theft						
Building Access Control						
Video Surveillence						
Antitheft Alarm Systemterrorist activities						

Once the scores are assigned, the Architecture Maturity for each risk control within a security service can then be plotted against Deployment Maturity using the following Action Map. By doing so, the firm can establish an order of priority in which to build out the architecture, with a clear picture of the existing levels of protection and vulnerability across the entire enterprise.

Security Services Architecture & Deployment Maturity Action Map

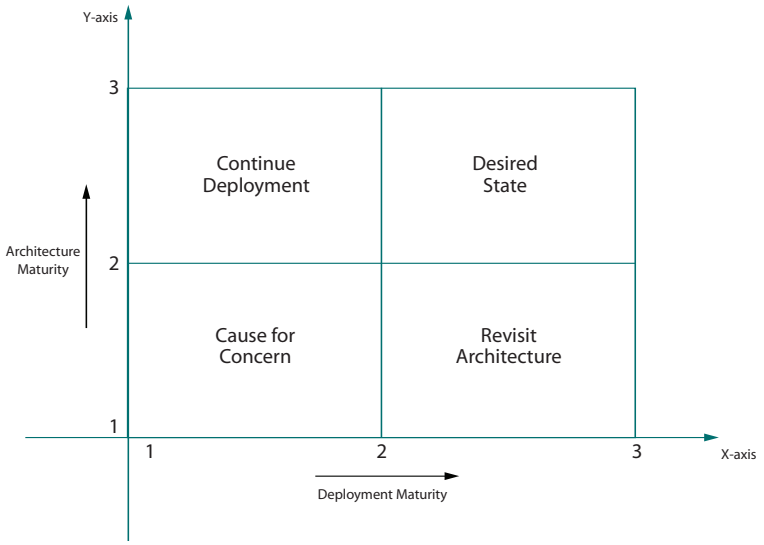
Action Map Legend

Desired State: The risk control elements are architecturally mature and provide firm-wide coverage.

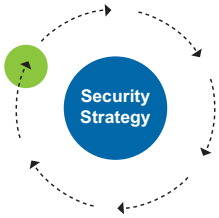
Revisit Architecture: The security solutions are deployed through an inconsistent architecture across the firm. Revisit the architecture to make functionality consistent.

Continue Deployment: The risk control elements follow a consistent architecture, but do not provide required coverage across the firm. Provide more coverage to make the firm secure.

Cause for Concern: The risk control elements neither have a consistent architecture nor provide sufficient coverage. These should be the high priority items for correction.



Deploy and Operate Security Services



After the roadmap is clearly defined, the final step in the initial implementation of the evergreen planning process is to deploy the security services into the architectural framework. In this phase, detailed security solution designs are created, solutions are tested, pilots deployed and production systems rolled out. The security infrastructure is momentarily complete, but the continuing emergence of new threats perpetuates the evergreen cycle of identifying and addressing the end-to-end security situation. If a SOA architecture has been deployed, this process is simplified by an order of magnitude.

Conclusion

Information security is a three dimensional problem driven by business model changes, the sophistication of emerging threats, and increasingly stringent regulatory requirements. An enterprise information security architecture must address all three of these dimensions in order to effectively meet the needs of the modern financial services firm. A strategy that incorporates a Service Oriented Architecture will enable rapid deployment of consistent, flexible, and adaptable security services that work across the enterprise, rather than propagating a collection of one-off point solutions. When creating this architecture, the 5-phase evergreen strategic planning process helps to identify and mitigate new threats on a continual basis, keeping the firm always current in defending the information at the heart of its existence.

About the Authors

CH Hariharan is a Senior Director / Enterprise Architect in the Advisory Services group of Cisco Systems, Inc.
Anuj Kumar is a Technical Leader / Enterprise Architect in the Advisory Services group of Cisco Systems, Inc.

For More Information

If you would like to learn more about how the Cisco Services Oriented Network Architecture can help your organization meet the challenge of enterprise security, please contact CH Hariharan at chhari@cisco.com.

Acknowledgements and References

The following is a partial list of references used in researching and writing this paper. We would like to sincerely thank the many brave people on the front lines of the security wars who shared their personal experience and creative thinking with us to as we formulated the ideas presented herein. We salute you

- Five business drivers for IAM – Gartner, ID: SPA 21-3673
- Hype cycle for IAM - Gartner 2005
- Client Security – A framework for protection , Forrester paper 2006
- Payment Card Industry – Self assessment is not enough, Forrester 2006
- Self Defending Networks – Cisco White paper
- Cisco products and technologies white papers
- Structure and content of an EISA – Gartner 2006
- Trends 2006: Identity Management, Forrester
- Separating fact from fiction: Security technologies for Regulatory Compliance – Burton Group
- California Security Breach Senate Bill
- FFIEC Information Security Booklet
- Bank Secrecy Act/ Anti Money Laundering
- Cisco SONA Architecture Framework
- USA Patriot Act