

## 6.7 Enterprise Security Services

---

This pattern guides an enterprise in selecting security services for protecting its assets, after the required security approaches—prevention, detection, response—have been identified. It helps to establish the level of strength or confidence each security service should offer, based on priorities. Primary examples of such services are identification and authentication, accounting/auditing, access control/authorization, and security management.

---

### **Example**

A new wing of an existing museum of gemstones is to be opened. The museum's management has already identified security as an enterprise concern and determined appropriate security properties and approaches to be supported. Now the management needs to identify what security services will be used. A specific asset group is used in this simple example problem.



The museum has identified three specific gems as irreplaceable due to their financial value. They can only be insured for approximately two-thirds of their actual monetary value. The museum wants to provide integrity and availability for physical protection of the gems, but also confidentiality for the real value of the assets. The museum has determined that prevention will be the primary approach to providing integrity and availability of the gems. Prevention will also provide confidentiality for information that stipulates real monetary values. Detection and response will provide secondary approaches to protecting these gems and resources will be allocated to prevention first. The museum now needs to determine what abstract security services will support the desired properties and approaches.

### **Context**

Business strategies, plans, and operations are understood. These include disaster recovery and continuity of operations strategies, a semantic data model, high-level business process and workflows, business locations, organizational units, and business cycle models. Security approaches (prevention, detection, response) and their priorities have been selected to satisfy the identified security needs of enterprise assets. The approaches might have been selected by applying ENTERPRISE SECURITY APPROACHES (148). The pattern user has a basic awareness of potential security services.

### **Problem**

To fully integrate security into the business model, business planners need to identify the security services needed to protect each category of enterprise asset. Selection of security services will need to balance the resources the museum is willing to allocate in order to address security approaches appropriately. At the business level, planners provide direction about how much emphasis to focus on preventing security incidents, detecting incidents after the fact, and the level of focus for responding to security incidents. Some services, such as access control, emphasize a prevention approach. Other services, such as accounting, emphasize detection and response. Still others, such as identification and authentication, support both prevention and detection.

How do you select and integrate security services across the organization to support security properties using preferred security approaches?

The forces applicable at the business model level of concerns are still abstract and are strongly intertwined with business processes. The enterprise needs to resolve the following forces:

- Customers and clients expect suitable protection of their assets
- Unauthorized access to critical assets that require prevention as the primary protection must be prevented
- A strong ability to discover security incidents provides protection for assets that require detection as a primary approach
- It is necessary to be able to recover from, or actively respond to, incidents for assets where prevention is not suitable or where prevention fails
- Accurate actor identification provides more protection when actors access critical assets
- Strong security services provide greater asset protection, but tend to be harder to use
- Weak security services tend to be easier to use, but provide less asset protection

### ***Solution***

Specify an integrated set of security services to address identified security approaches and security properties for each asset type. This process emphasizes two perspectives, namely, the individual perspective of each asset type, and a holistic perspective of the overall organization. Assets can vary greatly. This pattern therefore focuses on associations of security approaches and security services to assist the user in understanding relationships that can then be applied to asset categories. The Implementation section below provides examples. The examples are to help the pattern user to establish a particular set of security services to address all asset security needs for a given organization. From a holistic perspective, it ensures that the various approaches for asset types complement and reinforce each other, rather than work against each other.

The process of defining security services is typically performed by an enterprise architect and systems engineer. The first step is to collect all necessary information, including the asset types and security approaches that have been defined—for example, by applying ENTERPRISE SECURITY APPROACHES (148). Next, services are selected for each asset type and integrated. Finally, a ‘human touch’ is involved in applying an enterprise level pattern such as ENTERPRISE SECURITY SERVICES (161). Its application helps to shape thoughts about security, but it never can be a one-shot solution. You need feedback and conscious re-visiting of your decisions, because the world and organization change continually. Any of the earlier steps in this process might be revisited. In addition, if circumstances change sufficiently, feedback can extend to the beginning of the reasoning chain, to re-apply previous patterns such as ENTERPRISE SECURITY APPROACHES (148). More details on the process are provided in the Implementation section below.

After applying this solution, the next step typically is to specify requirements for the selected security services—for example, by applying one of these patterns: I&A REQUIREMENTS (192), ACCESS CONTROL REQUIREMENTS (267), or SECURITY ACCOUNTING REQUIREMENTS (360). It is important to note that ENTERPRISE SECURITY SERVICES (161) is organization-wide, while the scope of each service requirements pattern is a system or security domain within the organization.

### ***Structure***

Table 6.31 shows elements of the structure of this solution. Participating elements include humans involved in defining the solution for a specific situation. Participants also include primary elements of the process of defining a solution: security approaches, selection criteria, and security services. More details of these three primary elements are also given in the table. The implementation section below gives additional common examples of selection criteria. Multiple criteria apply to each security approach and to each security service. More than one service can be selected for each approach.

**Table 6.31** Elements of enterprise services solution

PARTICIPATING ELEMENT	SECURITY APPROACH	SELECTION CRITERION	SECURITY SERVICE
<ul style="list-style-type: none"> <li>• Business planners/controllers</li> <li>• Enterprise architect</li> <li>• Enterprise security officer</li> <li>• Asset</li> <li>• Security approach</li> <li>• Selection criteria</li> <li>• Security service</li> </ul>	<ul style="list-style-type: none"> <li>• Prevention</li> <li>• Detection</li> <li>• Response</li> </ul>	<ul style="list-style-type: none"> <li>• Assets are irreplaceable</li> <li>• Continuous record of asset protection is required</li> <li>• Need for daily asset access accounting</li> <li>• System cannot be down more than 8 hours</li> <li>• Financial data could harm partnerships</li> <li>• ... (see implementation section)</li> </ul>	<ul style="list-style-type: none"> <li>• I&amp;A</li> <li>• Access control</li> <li>• Accounting</li> <li>• Security management</li> <li>• ...</li> </ul>

## Implementation

This section first provides further detail on the process that was summarized in the Solution section, then presents criteria for selecting security services.

### Process Guidelines

1. Collect necessary input information:
  - Critical enterprise asset types.
  - Basic security needs or properties for each asset type. Asset types and basic security needs might be obtained as a result of applying SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89).
  - Specific security approaches for each asset type, including prevention, detection, and response, and the business priority for the approach in each case. Specific approaches and priorities might be obtained as a result of applying ENTERPRISE SECURITY APPROACHES (148).
2. Determine which security services to use for each asset type and approach:
  - Determine the factors that apply to your organization
  - Identify services that support the approaches, based on applicable factors

Note that one possible response is to take no action, that is, to accept the risk or ignore the incident, in which case no security service is designated.

More details on relating security approaches to security services are provided below.

3. Revisit security services for each asset type as circumstances change:
  - Decisions to revisit may be time-driven, for example annually.
  - Decisions to revisit may be event-driven. Examples are: (1) an organization makes a significant change to its business process, (2) a major law is passed that requires specific security measures, (3) an organization experiences a major security incident that calls into question its security services.

### Approach criteria

Tables 6.32–6.34 correlate security approaches with security services and a business priority. The criteria indicating selection provide typical examples of instances when

**Table 6.32** Correlating prevention with security services and business priorities

SECURITY SERVICE	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION	EXAMPLE SECURITY MECHANISMS
Access control	High	Enterprise has irreplaceable assets	Categorize access to assets according to roles and responsibilities, and restrict access to individuals via their roles/responsibilities
	Moderate	Assets can be damaged deliberately or inadvertently	Encapsulate assets (for example, envelope, encrypt, vacuum)
	Low	Assets require basic level of protection for insurance purposes	Provide physical protection controls
Accounting	High	Continuous record of asset protection is required (for example by a contract)	Real-time audit trail for information assets or sensors for physical assets
	Moderate	Asset access limited and must be accounted for	Pre-defined job functions in organization associated with user roles
	Low	Asset access physically limited but videotapes of area-access required	Videotape of assets, predefined job locations

**Table 6.32** Correlating prevention with security services and business priorities (*continued*)

SECURITY SERVICE	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION	EXAMPLE SECURITY MECHANISMS
I&A	High	Enterprise has irreplaceable assets (for example, extremely costly, value lost if modified, not insurable, one of a kind)	Use multiple authentication layers (for example biometrics and passwords) Store identities on smart card with biometric authenticator
	Moderate	Assets replaceable at significant cost	Use token generator for identity authenticator Restrict access to I&A information
	Low	Assets can be replaced as long as problems are detected	Use unguessable authenticator (for example randomly-generated passwords)
Security management	High	User I&A information alterable by single identified person	Only security officer can alter I&A information All I&A information is encrypted in storage and transfer
	Moderate	Only select roles may alter I&A information	SSO and System Administrator can alter I&A information All I&A information is encrypted in transfer
	Low	I&A information should not be easily modified	Access to server where I&A information can be altered is restricted

**Table 6.33** Correlating detection with security services and business priorities

SECURITY SERVICE	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION	EXAMPLE SECURITY MECHANISMS
Access control	High	All events needing immediate attention can be specifically identified	Accounting service mechanisms will need extreme granularity Access controls will relay to real-time audit trail
	Moderate	Normal/abnormal functionality is identified and controlled	Accounting service mechanisms provide daily audit trails for all information system functionality

**Table 6.33** Correlating detection with security services and business priorities (*continued*)

SECURITY SERVICE	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION	EXAMPLE SECURITY MECHANISMS
Accounting	Low	Prevention is highest priority for organization	Select access control activities are reported to accounting service mechanisms for documenting
	High	Business records need to be accurate and support any/all legal needs	Document all initial business records, any changes to them, and actor involved, in non-repudiable manner
	Moderate	Inability to recover from incident could weaken reputation	Ensure audit trails are reviewed for early detection of incidents
	Low	Need to recover from environmental disruptions	Maintain a history of all business records so that emergencies can be recovered from
I&A	High	Critical interactions are only authorized for specific staff	Use intrusion detection to detect any unauthorized interactions
	Moderate	Sensitive information restricted	Keep complete audit trails for all access to sensitive information
	Low	Need for daily asset access accounting	Assets need identifiers for differentiation
Security management	High	All security management information is company sensitive	Access control is enforced continuously for all this information This information for accounting cannot be altered
	Moderate	All security management information is selectively accessible	Access control with roles ensures the information is current and valid
	Low	Security management information must be periodically reviewed and changes documented	Audit trails must include changes by security officer and system administrators

**Table 6.34** Correlating response with security services and business priorities

SECURITY SERVICE	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION	EXAMPLE SECURITY MECHANISMS
Access control	High	Assets are nationally sensitive (for example nuclear plants)	Access requires specific permissions and is restricted by time of day, location, and so on
	Moderate	Financial data could harm partnerships	Access is restricted to a specific community of interest
	Low	Only HR employees should access corporate personnel data	Access authorizations are established by department functions
Accounting	High	Location/condition of specific assets must not be altered	Accounting records must provide continuous monitoring (for example videotape) with immediate alert locking asset location on any change
	Moderate	Any unauthorized changes to asset must initiate notification	If detection indicates unauthorized asset change, accounting service mechanism must send notification to system administrator
	Low	Only physical disasters need immediate responses	Accounting service mechanism only notifies select staff if physical catastrophe occurs
I&A	High	Unknown users must be immediately locked out permanently	Identification used with biometrics secured on a token I&A service mechanism does not have high false positive or negative ratios I&A part of layered defence
	Moderate	When user I&A provides warning, additional means are used to reduce possibility of false positive	Front door human guard, badging system with photo, and identifier and password on automated system
	Low	Users are not allowed to repeatedly provide invalid log-in information	Computer system locks down after preset number of invalid attempts



**Table 6.34** Correlating response with security services and business priorities (*continued*)

SECURITY SERVICE	BUSINESS PRIORITY	CRITERIA INDICATING SELECTION	EXAMPLE SECURITY MECHANISMS
Security management	High	System cannot be down more than eight hours	Security management plans and procedures for contingency operation are in place and assure response in 8 hours
	Moderate	System cannot be down more than twenty-four hours	Security management plans and procedures for backup and recovery will restore a functioning system in twenty-four hours
	Low	System information must be accessible on line in two weeks	System backups with all security management information must be run every two days and recovery plans are in place

the organization has set a business priority at a certain level. Example mechanisms that may be employed to offer the service are also provided. Note that these tables could not possibly address all possible security services—instead they focus on fundamental services that will provide a basis for security.

Rows of the tables may be interpreted as follows, using as an example Table 6.32, which addresses prevention as the approach. An organization has identified a need for prevention. I&A is a security service selected as a means of supporting prevention of unauthorized operations on assets. The organization has established prevention as a high business priority for a given asset category, such as irreplaceable assets. In this circumstance a strong I&A service is needed. It may be implemented through the use of both biometrics and passwords structured as multiple authentication layers. Suppose another asset category has a moderate need for prevention, such as assets replaceable but at significant cost. In this case a moderately strong I&A service is needed. It may be implemented through use of biometrics by itself, or use of a token generator. Finally, if the prevention priority for an asset category is low, then a weaker I&A service is needed. This may be implemented through randomly-generated passwords.

The example implementations are not decided in this pattern. The first three columns—service, priority, and criteria—represent organization-wide decisions made in the scope of this pattern. The fourth column, example mechanisms, represents system decisions made in the scope of each system security architecture.

### ***Example Resolved***

This example expounds on the problem example provided earlier. As noted, the museum has gems that are irreplaceable and only partially insurable. They have a business priority for ensuring their integrity and availability by preventing their theft or any damage. The museum will therefore need to have strong I&A, access control, accounting, and security management services to protect the gems. Detection and response security approaches will also be provided as backups for the prevention approach. To provide integrity and availability for the detection approach, both I&A and accounting security services will be needed. For the response approach the security management service will also need to be dependable.



The museum also indicated a real need to protect confidentiality of the real value of these gems by preventing that information from being easily obtained. In addition, the museum will need to ensure integrity of that information. This additional consideration for integrity of gem values to have a high business priority will need to be fed back into the earlier work to ensure it is captured. There is a high business priority for prevention of any lapses of confidentiality and integrity of gem data on insurance contracts, attributes (carats), purchase amounts, and appraisal values. To achieve the required prevention approach, stringent I&A, access control, and security management services will be needed. To achieve the required prevention as well as detection and response for preventing integrity violations of gem data, strong mechanisms for all four identified services will be needed.

The museum has now reached a point at which they can begin to determine refinements for security services appropriate to support abstract selected services. Table 6.35 captures the museum's resolution of abstract security services to be used.

### ***Known Uses***

The prevention-detection-response approaches identified in this pattern are well established functions in the security community. Likewise, security services identified in this pattern are well-established, although there is lack of consensus on names for some of them, notably accounting. The security services in this pattern are aligned with services in the taxonomy in Chapter 2. To a significant degree, criteria details in the Implementation section of this pattern are based on extensive MITRE Corporation experience with our customers. There are also some standards that include related information. For example, [ISO13335-4] discusses services and mechanisms—under the name 'safeguards'—such as I&A, access control, audit, and security management, and associates these with security properties such as confidentiality and integrity. [NIST800-33] describes a security services model that includes identification, authentication, access control, audit, non-repudiation, and security administration services. The latter also maps services to a set of primary purposes or approaches: prevent, recover, and support.

**Table 6.35** Protecting museum assets

MUSEUM ASSET	SECURITY PROPERTY	SECURITY APPROACH	BUSINESS PRIORITY	SELECTED SERVICE
	Integrity availability	Prevention	High	<ul style="list-style-type: none"> <li>■ I&amp;A</li> <li>■ Access control, e.g., locked glass display</li> <li>■ Accounting</li> <li>■ Security management</li> </ul>
	Integrity availability	Detection	Medium	<ul style="list-style-type: none"> <li>■ I&amp;A</li> <li>■ Accounting, e.g., surveillance camera</li> </ul>
	Integrity availability	Response	Medium	<ul style="list-style-type: none"> <li>■ I&amp;A</li> <li>■ Accounting</li> <li>■ Security management</li> </ul>
	Gem insurance contracts, attribute data (i.e., carats), purchase data, and appraisal data	Confidentiality	High	<ul style="list-style-type: none"> <li>■ I&amp;A</li> <li>■ Access control, e.g., a safe</li> <li>■ Security management</li> </ul>
	Integrity	Prevention Detection Response	High	<ul style="list-style-type: none"> <li>■ I&amp;A</li> <li>■ Access control</li> <li>■ Accounting</li> <li>■ Security management</li> </ul>

A specific example of how a prevention approach leads to use of the access control service is the Cisco use of Access Control Lists to protect networks, described in [ACL]. Examples of how accounting in the form of audit software supports detection of fraud are described in [CPA].

## Consequences

The following benefits may be expected from applying this pattern:

- The pattern fosters management level awareness: all enterprise security patterns help management to better understand security as an overall issue, and gives them terminology and simple understanding of the underlying concepts without relying on details of the technology used to implement them.
- It facilitates conscious and informed decision making about security services to support identified security approaches.

- It promotes sensible resource allocation to protect assets.
- It allows feedback in the decision process to better adjust security services to the situation at hand by traceability back to business factors and security needs.
- It encourages better balance among security, cost, and usability of an asset.
- It shows that you can combine services to better and more cheaply protect an asset.

The following potential liabilities may result from applying this pattern:

- It requires an investment of resources to apply the pattern, including time to analyze enterprise assets and security approaches. In some cases the cost of applying the pattern may exceed its benefits.
- It requires the involvement of people who have intimate knowledge of assets, and basic knowledge of asset security needs and security approaches. These people typically have high positions in the enterprise and their time is valuable. On the other hand, the pattern allows more people to be aware of the issues, so that after the initial investment of time, other people can be in a position to maintain and evolve the service selection.
- It is possible for an organization to assign people to this task who have less than adequate knowledge of assets, approaches, or services, because they may have more available time or are less expensive. If the people applying the pattern do not have good knowledge of enterprise assets and their value, the pattern results may be inaccurate or not useful.
- Perception of security needs can differ throughout an organization. This may make it difficult to reach agreement on priorities of services. On the other hand, bringing such disagreements to the surface may be a benefit, because then they can be properly discussed and resolved.