



Data-centric security.

Enabling business objectives to drive security

*Mike Bilger
Luke O'Connor
Matthias Schunter
Morton Swimmer
Nev Zunic*

Contents

2 Introduction
4 Business strategy and security
8 The IBM data-centric security model
16 Maturity levels for data-centric security
19 Implementation architecture
24 Conclusion

Introduction

Many companies' attitude toward computer security is ambivalent. On the one hand, the business threats associated with inadequate security policies and practices are more significant than ever. The realization of these threats, such as network outages or the exposure of customer data, may not only lead to the interruption of business services, but may also damage business reputation – especially if security breaches are publicized. On the other hand, companies that are seriously committed to supporting a well-defined security strategy often do not have convincing business metrics for evaluating a strategy's effectiveness. Security spending is then viewed as pure cost without a tangible business benefit; therefore it is to be minimized, similar to other pure costs, such as insurance. Consequently, a security conundrum arises: "security cannot be ignored," and at the same time, "security must be cheap."

Security-aware enterprises understand that managing IT security risk is essential to overall business resilience. Without proper IT security, the entire enterprise may be at risk. Today, IT security controls are not linked to business objectives; consequently, it is difficult to determine the right level of IT security. Meanwhile, traditional paradigms of computer security are becoming obsolete:

- **Integration or federation** opens enterprises to their partners – and to attacks and fraud originating from their networks.
- **Resource sharing, componentization and virtualization** reduce barriers that once protected applications from each other.
- **Provisioning engines and centralized directories (identity, policy)** become prime targets for hackers and single points of failure.
- **Openness** makes it easier for hackers to connect to and plug in to broadly deployed IT systems.

Highlights

- *Automation*, for example automatic adjustment of bandwidth, computing resources and security defenses, allows faster (and easier) propagation of security threats.
- *Speed and adaptiveness* amplify security problems.
- *Business process transformation and outsourcing* increase dependencies on third parties.

An enterprise's main challenge is to implement the correct level of security that addresses these threats and is driven by business requirements. That is, for each business asset, the appropriate level of protection is implemented, which results in controls that are cost efficient and effective, without being overprotective.

The IBM data-centric security model (DCSM) uses the business value of data to determine and implement the appropriate level of overall IT security.

In this white paper, we introduce the IBM data-centric security model (DCSM), which leverages the business value of data to determine and implement the appropriate level of overall IT security. The major obstacle that DCSM allows organizations to overcome is the disconnect between IT security technology and the objectives of business strategy. We propose to link security services directly to business processes by relating security services directly to the data they implicitly protect—a relationship that is often obscured by the presentation of security as an end in itself. The focus in the DCSM is on deriving the right security level, based on a business analysis of the data being handled. This data classification then drives the properties and access control policies governing the use of data by applications that implement business processes. Security services and their underlying mechanisms can be abstracted into interfaces that directly support data-handling policies. The DCSM does not require major changes to security services, but instead takes existing functionality, then casts and integrates that functionality in terms that can be directly understood by people who define and manage business processes. In this manner, security

Highlights

A direct interdependence between the DCSM and the business processes is established from model conception, by way of the data acted on by processes.

IT and security technologies, such as intrusion detection systems, antivirus software, firewalls and virtual private networks, are critical to efficient protection of systems that implement defined business objectives.

can be seen as directly supporting business processes and, in turn, business objectives. Rather than relying on traditional risk management methodologies or other informal linkages between security and business processes, a direct dependency between the DCSM and business processes is established from model conception, via the data acted on by processes.

Business strategy and security

A business strategy is a plan for a company to obtain and sustain a competitive advantage. Business strategy objectives, which provide a context in which to measure and evaluate a strategy, typically encompass the following issues:

- *Maximizing shareholder value*
- *Retaining and attracting clients*
- *Reducing the costs of business processes*
- *Maintaining and improving marketplace competitiveness*
- *Maintaining business continuity and resilience*
- *Achieving and maintaining regulatory compliance*
- *Managing and enhancing marketplace reputation*
- *Establishing new investments*
- *Identifying and exploiting new business opportunities*

Information is vital to these strategic objectives. IT and security technologies, such as intrusion detection systems, antivirus software, firewalls and virtual private networks (VPNs), are critical to efficient protection of systems that implement these objectives. But neither IT nor security is a strategic objective on its own. For business strategists (and, in fact, most people) these technologies are mere components of a complex IT infrastructure designed to support the reliability and integrity of business processes.

Highlights

The first security priority is to protect critical data, core processes and the trust that other enterprises, customers and stakeholders place in an enterprise.

For clients, privacy is a paramount trust issue, and therefore clients need to be reassured that their data is protected from release or modification and is used only for intended business purposes.

If we look beyond the details of technologies and practices, we see that IT security is a large contributor to the business notions of trust and risk mitigation, which impact most of the business objectives previously enumerated.

The first security priority is to protect critical data, core processes and the trust that other enterprises, customers and stakeholders place in an enterprise. Clients and companies are more inclined to establish business relationships with a company they trust, and this is a subjective evaluation. A company, particularly one that promotes itself as a brand, will be very concerned about maintaining its reputation as a trusted business partner. With respect to IT, trust manifests itself mainly in the way data is created, collected, stored, processed and distributed. Clients view companies as the custodians of their data, and expect trustworthy treatment of their data. Companies that outsource processes expect the same privileged treatment from the outsourcing service provider.

For clients, privacy is a paramount trust issue. Clients need to be reassured that their data is protected from release or modification and is used only for intended business purposes. Recently, several high-profile disclosures of client data, through poorly protected databases accessible via the Internet, have caused a significant loss of reputation for the companies involved. The companies themselves are concerned with the integrity of their business processes and the data that supports these processes. In particular, if a business process involves interactions with a business partner, then additional care must be taken to ensure trust in the process as a whole.

Highlights

Risk analysis and methodologies for operational risk management provide a bridge between security technologies and their impact on business processes in terms of expected losses due to threat realization.

From a business perspective, the level of security protection applied must be based on the business value of the information that is protected.

The dependencies between security and business objectives manifest themselves in the execution or support of business processes. But how can these dependencies be expressed, measured and optimized using language that makes business value evident? Risk analysis and, in particular, methodologies for operational risk management provide a bridge between security technologies and their impact on business processes in terms of expected losses due to threat realization. Many companies are now adopting enterprise-wide risk-management strategies in response to regulatory and compliance requirements (particularly the Sarbanes-Oxley act in the United States). Control Objectives for Information and related Technology (CobIT) is one of the few well-developed methodologies for supporting such a strategy.

Protecting key information assets

Today's enterprises operate on information. Information is a critical business asset within today's enterprises:

- *Information represents the know-how of an enterprise.*
- *Critical business processes operate on information.*
- *Trusted relationships are maintained by exchanging (possibly sensitive) information.*

As a consequence, if the confidentiality, integrity and availability of the information are not guaranteed, the business will no longer operate.

From a business perspective, the level of security protection applied must be based on the business value of the information that is protected. Since data is the core asset that must be protected by IT security, the business value of data must drive the IT security controls that are implemented. This idea is at the heart of the DCSM.

Highlights

Once the value of the data has been determined, security control requirements can be defined and justified from a business perspective.

One of risk management's important aspects is to implement an adequate level of baseline protection to ensure infrastructure availability.

To identify the business value of certain types of information, an enterprise can analyze the business value of the information; the business processes that operate on it; and the business relationships that it supports. Once the value of the data has been determined, security control requirements can be defined and justified from a business perspective.

Risk mitigation using data-centric security

Managing the overall IT risk that an enterprise faces is another important business objective of IT. Enterprises are willing to bear a well-defined risk of a particular severity. Nevertheless, they want to ensure that they can afford the cost of exposures (that is, damage to assets and brand) and that major incidents are unlikely and do not threaten the enterprise as a whole. One of risk management's important aspects is to implement an adequate level of baseline protection to ensure infrastructure availability.

Security management methodologies, such as ISO 17799, are applicable to some of the previously enumerated business objectives, but there are no common metrics for comparing security methodologies with business objectives. This is not surprising, given that businesses such as banking and insurance have been developed over several hundred years, while computing is less than 50 years old and commercial IT security is much younger. ISO 17799 presents a methodology for providing and managing security services, as opposed to furnishing security professionals with a means to communicate security business value to their stakeholders. ISO 17799 can be viewed as a segmented island in IT management, which needs to evolve to become more integrated with business processes and strategy.

Highlights

There are interdependencies between IT security services and business objectives, but there is no unifying principle to express and evaluate these interdependencies.

The purpose of the IBM DCSM is to directly align business strategy and IT security through the common thread of data.

Unfortunately, IT security risk methodologies are immature and do not appear to be converging toward the analytical and predictive power of more established models, like credit risk models. Security risk practitioners are quick to point out that their task is severely handicapped by a lack of accurate long-term security data, as compared with the voluminous data available for financial risk models. While this is true, there are no credible security risk models available that could process long-term security data, even if such data were available. The main issue seems to be that security professionals are not well versed in risk techniques that are quantitative and predictive.

In summary, there are dependencies between IT security services and business objectives, but there is no unifying principle to express and evaluate these dependencies. Security technologies are too arcane to be of central interest to strategists, and the importance of IT security may simply be relegated to the IT infrastructure. Risk methodologies are not advanced enough to provide a convincing bridge between security technologies or services and business processes. However, this may change in the future.

The IBM data-centric security model

The purpose of the IBM DCSM is to directly align business strategy and IT security through the common thread of data. We emphasize that the DCSM approach does not create this link based on data, but brings to the fore the security methodology data components that are all too often obscured by security technicalities and terminology. All security technologies seek to protect data, and all security functions and protocols target appropriate data use. The DCSM is mainly a restatement—in terms of the data-control capabilities supported by security services—of current security models that focus on security

Highlights

The DCSM does not depend explicitly on specific security products or technologies and may be seen as independent of the underlying security infrastructure.

The first consideration of a DCSM is to determine a set of guidelines for enterprise-wide data handling, based on business policies.

mechanisms and management. Typically, these data-control capabilities are not emphasized, but it is exactly this aspect of security services that will provide the linkage to business processes. Importantly, the DCSM does not depend explicitly on specific security products or technologies and may be seen as independent of the underlying security infrastructure.

The first consideration of a DCSM is to determine a set of guidelines for enterprise-wide data handling, based on business policies. The next consideration is to determine which security services are required to support these guidelines. We structure these guidelines into two parts. The first part classifies business data. A class can be based on the owner and on given security requirements.

- *Where did the data originate?*
- *Who owns the data?*
- *Who controls the data?*
- *Who or what holds the data?*
- *What type of data is it?*

Then, for each class, business-oriented security requirements are defined that describe how a certain class of data shall be handled and protected. Example policy decisions that define how data is handled are:

- *Who or what can use the data?*
 - *For what purpose?*
 - *Can it be shared?*
 - *Under what conditions?*

Highlights

The interdependence between guidelines for enterprise-wide data handling and security services is evident: confirmation of data origin and ownership will rely on authentication services; data modification will rely on authorization and access control services; data safeguarding will rely on confidentiality services; data storage will rely on integrity and disclosure control services.

- *Where will the data be kept?*
- *How long do we keep the data?*
- *Does it need to be safeguarded?*
 - *At rest?*
 - *When backed up?*
 - *During use?*
- *How can the data be disclosed?*
 - *What subset can be disclosed?*
 - *What protection must be implemented?*
 - *Does the data need to be distorted or watermarked?*

Each of these data issues has direct business significance: for protecting intellectual and business knowledge, maintaining the integrity of business processes, or adhering to and complying with jurisdictional regulations. The interdependence between such guidelines and security services is also evident: confirmation of data origin and ownership will rely on authentication services; data modification will rely on authorization and access control services; data safeguarding will rely on confidentiality services; data storage will rely on integrity and disclosure control services. The mechanisms that support these security services may be complex and are part of the IT infrastructure services, but these details are hidden in the DCSM.

Security emphasis is shifting from network-based to host-based defenses. If we extend this layered defense approach further, beyond host-based security to the data that is protected on those hosts, we arrive at the DCSM. To keep these multiple defense layers manageable, DCSM defines an integrated requirements and policy approach. Figure 1 illustrates the DCSM, in which data is placed at

Highlights

In the DCSM, data is placed at the center, and the first objective in creating a DCSM is to identify the owner of the data, whether it's an individual, a customer or a line of business.

the center of the model. The first objective in creating a DCSM is to identify the owner of the data, whether it's an individual, a customer or a line of business (LOB). Requirements are gathered from both business and legislation governing usage and handling of specific types of data. These requirements will influence the policies that are defined and applied to the data. Data is classified using business terminology, while access control policies are defined using organizational roles. The rest of this paper analyzes this model in more detail.

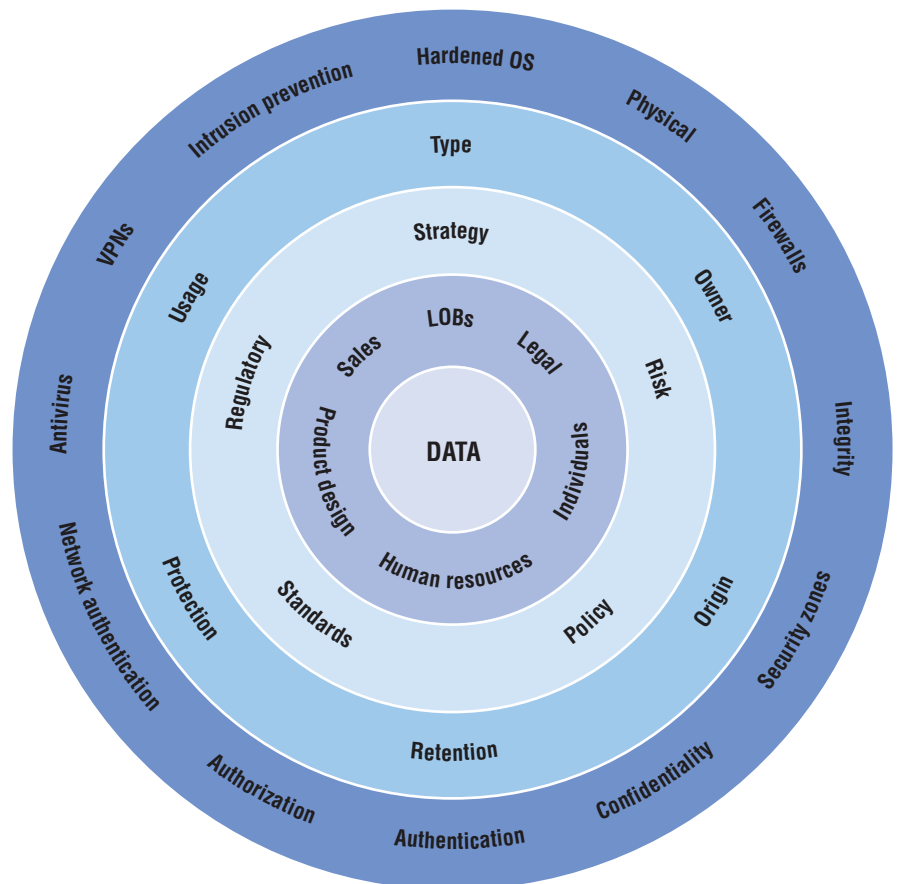


Figure 1. IBM data-centric security model

Highlights

The main components of the abstract DCSM are separated into the policy pillar and the data pillar.

Components of the DCSM

Figure 2 shows the main components of the abstract DCSM, separated into the policy pillar and the data pillar. The policy pillar starts by summarizing the business requirements and regulations that will be addressed by the security architecture. Both requirements and regulations are unified into a description of the desired security policies and procedures for different data classes. The corporate and regulatory policies express data-handling policies in terms of requirements, both internal and external to the enterprise, which, for example, may dictate obligations for data owners and custodians, or may state data-retention periods. The next step is to use the security and business requirements to define an overall business data classification (BDC), which represents the labels or attributes of data that are used to determine the data classes. Data will also be classified by criteria such as ownership and origin time and location. The data will have well-defined owners, typically expressed in terms of a business purpose or business line function. The goal is to identify the overall data governance that needs to be implemented. The data classification and the policy rules are encoded into data control rules (DCRs). These DCRs represent the unified data-handling policies expressed in terms of BDC. They are used to establish appropriate access policies and practices to support corporate data-handling policies.

Highlights

The policy pillar starts by summarizing the business requirements and regulations that will be addressed by the security architecture, and the data pillar rests on a security infrastructure that provides basic security functions.

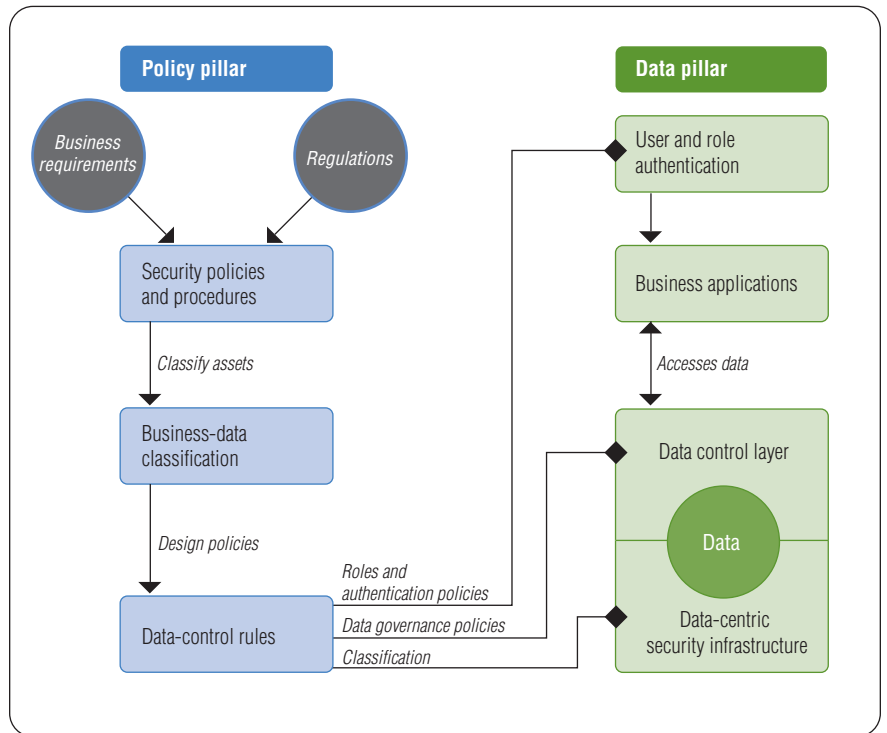


Figure 2. The components of the DCISM

Highlights

The DCSM provides layers of protection that are consistent with corporate or organization policy and regulations; corporate standards are used to restrict data access to authorized users.

The data pillar of DCSM rests on a security infrastructure that provides basic security functions, such as perimeter defense, protection of data at rest or disclosure rules, or encapsulation of data during transmission. The corporate data is then classified in terms of the BDC scheme. Access to the data and permissible actions on the data are controlled by the data control layer (DCL). The DCL is designed to implement the (abstract) policies expressed in the DCRs and relies upon security services in the IT infrastructure. Its fine-grained security controls can implement a wide range of DCRs. The DCL obtains the access context (such as authenticated users) and uses this context to decide whether the data can be accessed. The IT infrastructure is configured to support the security policies that have been derived from the DCRs. Business applications access the data through the DCL, which uses the data governance policies. On top is a role-based authentication component that identifies users and assigns roles to the users based on authentication policies provided by the policy pillar. To enable protection with only minimal changes to the applications, we leverage an application abstraction model that maps terminology between application-specific contexts to the corporate data governance rules. This enables the DCL to understand application context without requiring that this context be adapted to the security policies.

The DCSM provides layers of protection that are consistent with corporate or organization policy and regulations; corporate standards are used to restrict data access to authorized users. The sensitivity of the data will dictate the appropriate protection measures at every phase of a data request. The infrastructure security services are utilized to protect critical data, and the corporate risk acceptance plan will determine the appropriate use of technical safeguards at the infrastructure and application layers.

Highlights

When a DCSM is deployed, the security infrastructure provides services to the data control layer (DCL) that are defined in terms of the data control policies, and the details are hidden from the DCL.

Deployment of the DCSM

Figure 3 shows an example of a logical deployment of the DCSM. The security infrastructure provides services to the DCL that are defined in terms of the data control policies. Here, a policy statement, such as data of type X that must be securely transported, would be translated into a request from the DCL to the secure transport service of the security infrastructure. This service in turn may rely on a protocol such as Secure Sockets Layer (SSL), which itself makes use of certificate-based authentication, but these details will be hidden from the DCL. If the data requester is a mobile employee, then the safe transport requirement may, for example, be satisfied by using a tunneled VPN connection, again a detail hidden from the DCL.

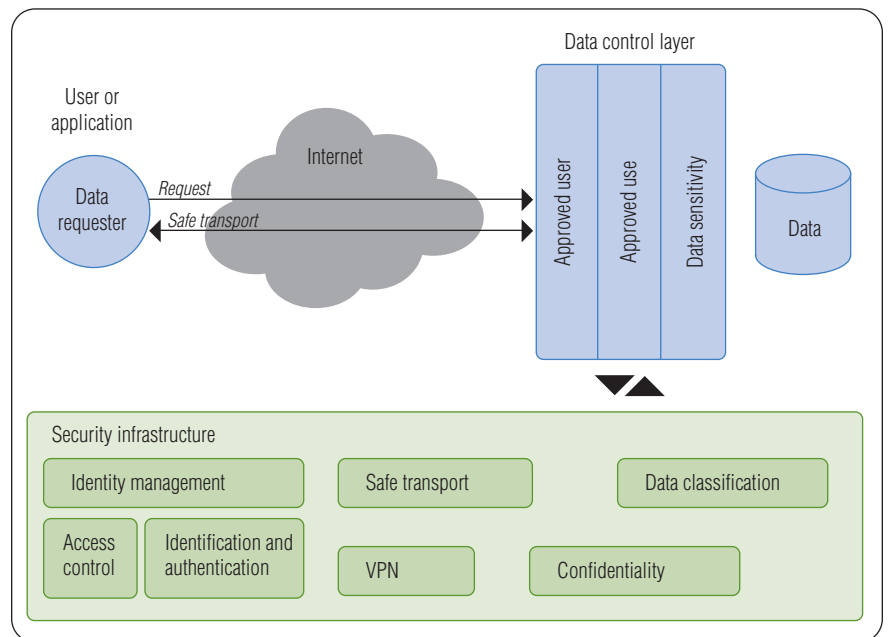


Figure 3. A logical deployment of the DCSM

Highlights

Best practice when implementing a DCSM is to stage the deployment according to the current business risk and the business requirements for different parts of the enterprise.

The DCSM thus depends on an enterprise-wide BDC scheme, consistent deployment of the DCL at the point of access to all data, and adherence to data classification during capture, transmission and storage. The last requirement implies that data labels are persistent and must reside with the data that is labeled.

Maturity levels for data-centric security

Enterprises need not implement the DCSM all at once. To align with the business objectives, best practice is to stage the deployment according to the current business risk and the business requirements for different parts of an enterprise. To guide this staged deployment, we outline the basic maturity levels for data-centric security. An enterprise can then choose at which level of maturity to implement the DCSM and in which parts of its operations. The maturity levels can be classified according to the matrix shown in Figure 4.

Adoption levels	Basic	Intermediate	Advanced	Full
Security infrastructure	■	■	■	■
Business data classification		■	■	■
Role definitions		■	■	■
Policies by classification		■	■	■
Data is labeled			■	■
Data flow analysis			■	■
Automated policy provisioning				■

Figure 4. Maturity matrix for data-centric security

Highlights

At the basic maturity level, the security functionality is not driven by the business requirements on the data handled by the IT systems.

For intermediate maturity, the run-time classification is not reflected in the system, and consequently, policies will be designed per system and need to sufficiently protect all data handled by a system.

Basic: global IT security requirements

Basic maturity is the prevalent state in many enterprises. The security functionality is not driven by the business requirements on the data handled by the IT systems. Instead, general IT security requirements have been defined that implement a protection level designed to protect critical information assets. As a consequence, many assets are overprotected, while the most critical information assets are usually not sufficiently protected.

Intermediate: using data-centric security for designing security policies

For adoption of data-centric security, IT security investments must be driven by the protection needs derived from business requirements on the data. The first step is for business and IT to agree on which data categories will be protected. In addition, business must define the protection requirements for each data category, including requirements for baseline protection. Given these business objectives, basic data-centric security is implemented by determining the most critical data that is handled by a system. Then the security controls that correspond to the required protection level are implemented. For intermediate maturity, the run-time classification is not reflected in the system. As a consequence, policies will be designed per system and need to sufficiently protect all data handled by a system.

Highlights

The next maturity level enables runtime labeling of channels and data, while enabling automated policy selection.

Full data-centric security implements automated policy management, designed so that systems can adapt their security controls to the data they need to handle.

Advanced: labeled data

The next maturity level in adopting data-centric security is to enable run-time labeling of channels and data while enabling automated policy selection. For example, an application server on this maturity level will be able to apply different access control rule sets for different types of data. The labels are used to select the appropriate policy to protect given data.

Full: data-centric security

A full implementation of data-centric security comprises the mechanisms of the previous two maturity levels. Policies are designed from a data-classification perspective and data is labeled in the run-time system. Full data-centric security implements automated policy management. The goal is for systems to adapt their security controls to the data they need to handle. A system will have multiple policies that are applied depending on the classification of the data that is handled. These policies will be designed independently and then provisioned for the different system types. The core security requirement is that each data classification's corresponding policies satisfy the security requirements for that classification. There are two main approaches to guarantee compliance with this security requirement. The bottom-up approach collects all corresponding policies and audits them for their compliance with the overall security requirements. A top-down approach formalizes the security requirements into baseline policy rules. These rules are then translated into system policies that can be automatically provisioned to the individual systems handling the data.

Highlights

To a large extent, data-centric security does not require new technology.

Implementation architecture

We now discuss the essential technical components needed to implement the DCSM. To a large extent, data-centric security does not require new technology.

Design of classification and policy

The first phase is an initial execution of the policy pillar. This execution includes identification of the critical data types that exist in an enterprise, as well as the business and regulatory requirements that apply to the data. Based on these consolidated security requirements, specific security requirements for each data category can be derived. To implement the required protection, the security staff then designs critical-data-system policies that meet the security requirements put forward for each of the categories. This flow is depicted in Figure 5.

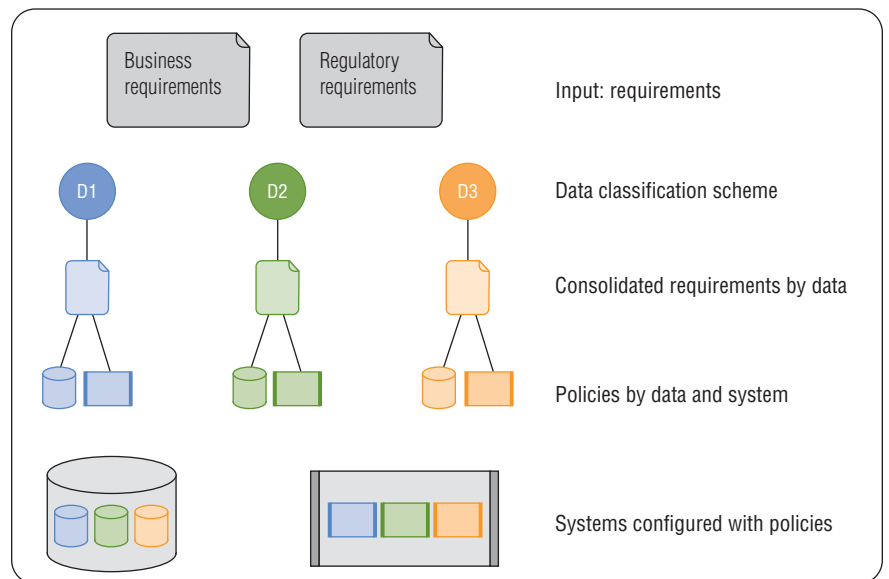


Figure 5. Security analysis and policy design

Highlights

Data handled by an enterprise must be classified, and classification can be done on several levels: security zones can be labeled with the data classifications that they are allowed to process; systems and channels can be labeled with the data classifications that they are permitted to process; databases and channels can be labeled in detail; or individual instances can be labeled.

Migration: classifying business data

The first technical challenge is to classify the data. Data handled by an enterprise must be associated with classifications. Classification can be done on several levels. The most coarse-grained approach is to label security zones with the data classifications that they are allowed to process. The next-finer-grained approach is to label systems and channels with the data classifications that they are permitted to process. The next refinement is to label databases and channels in detail. This approach requires that, for example, the classification of the columns of a database be determined and stored. The most fine-grained approach is to label individual instances, for example, to identify which files are classified confidential.

The DCSM is based on the ability to classify data according to a common schema. We recall that the original goal of the DCSM was to provide a direct linkage between security services and the data of business processes. Clearly then the data classification of the DCSM must be defined in terms of business data, as opposed to any existing security classification schemes, because in the DCSM security requirements are subordinate to the data's business value. Therefore, sensitivity labels commonly associated with mandatory access control (MAC) are unsuitable to form the basis of a data-classification schema. In military security models based on MAC policies, information assurance policies dictate data-handling practices independent of the use of data in various processes. In a commercial setting, this approach is inappropriate.

Highlights

A data model based on the operation of business processes can be linked downward in the enterprise architecture to security services and linked upward to the business modeling and architecture layers.

A data model based on the operation of business processes can be linked downward in the enterprise architecture to security services and linked upward to the business modeling and architecture layers. Such a business data-classification schema can provide closer affinity to corporate security policies for data classification in agreement with business processes and may lead to increased security awareness for employees who can directly understand the business purpose of data they are handling. Also, such a data model is expected to ease the definition of interenterprise agreements for data exchange. An example BDC scheme is shown in Figure 6.

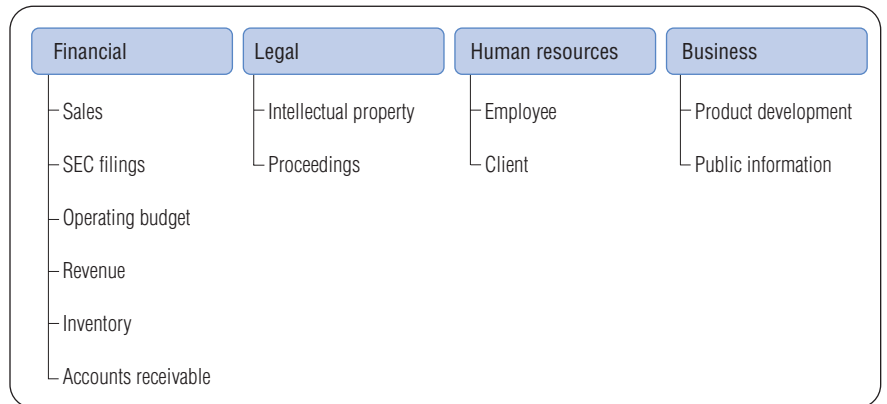


Figure 6. An example BDC scheme

Highlights

Authentication, authorization and disclosure control are at the heart of the DCSM.

Data-centric security is based on a new approach to policy management, in which policy design is federated between multiple authorities inside an enterprise.

Authentication and authorization: role-based data-access control

Authentication, authorization and disclosure control are at the heart of the DCSM, and several components are needed. An authorization component asks the user for authentication and issues corresponding user credentials. A monitor component observes accesses to critical data and requests authorization to perform the desired operations. A role-based data-access component decides whether a policy allows or denies a certain operation on a given data category.

This policy enforcement engine is a core component of a DCSM design. It obtains the roles of the user accessing a data category, the business context of such a business process and the operations to be performed on the data. The rules-based engine then returns a decision: whether the access is allowed, denied or filtered. The engine can also determine if transformations should be performed on the data before release. Depending on the criticality of the data, authorization may either prevent unauthorized access or generate corresponding noncompliance events.

Policy management

Data-centric security is based on a new approach to policy management, in which policy design is federated between multiple authorities inside an enterprise. It is essential for compliance that the overall enterprise enforces certain baseline policies. The security team and the business process owners define a baseline policy for business classification along with mandatory rules for handling the data categories. Each business owner can further refine the policies and make them more granular, if necessary. Additional policies can be added by the business process owners. The policy management system then ensures that these local refinements do not violate the mandatory enterprise-wide policy.

Highlights

For interenterprise transactions, data must be seamlessly protected, no matter where it is currently located.

Higher security requirements for data protection will require higher infrastructure security.

Interenterprise transactions

Enterprises are increasingly moving toward value networks in which groups of equal partners form short-term coalitions similar to virtual enterprises. Business trends suggest that this model, in which each enterprise concentrates on its core competency while most transactions cross organizational boundaries, is expected to be the rule rather than the exception.

For such interenterprise transactions, data must be seamlessly protected, no matter where it is currently located. From a data-centric approach, this requires that labels can be transmitted, and that corresponding security requirements can be globally enforced. In enabling such a unified enforcement in a heterogeneous environment, it is essential to note that each partner will use different policy implementations. The only common requirement is that the enterprises follow a data-centric approach and that these policy implementations satisfy the given requirement.

Foundation: infrastructure security

Data-centric security requires a secure infrastructure. If servers and systems are affected by worms and viruses, the ability to enforce a given policy is limited. As for all other secure systems, the higher the security requirements on data protection, the higher the infrastructure security requirements. As a result, any implementation of data-centric security will require a basic level of system security. This means perimeter defense, patch management, identity management, virus and intrusion detection, and additional security capabilities. Nevertheless, data-centric security can reduce the cost of infrastructure security and of adhering to compliance requirements.



By labeling data, data-centric security enables enterprises to actively assess and manage their information assets. An enterprise will know the business value of the data handled by different systems on different networks. An enterprise will be able to split its infrastructure into different zones that correspond to the business value of the data that is handled within each zone. For zones that handle only low-value data, infrastructure protection can be reduced to the bare minimum, allowing investments to be focused on zones handling higher-value data.

Conclusion

This white paper has presented a new approach to security. The primary goal of data-centric security is to drive security controls from a business requirements perspective. This goal is achieved by separating policy and classification from data protection. For each data class, appropriate controls can be defined that reflect the business requirements that have been identified by an enterprise.

Overall, data-centric security enables cost-efficient protection of information assets. Unlike today's approach of providing unified protection to all assets, data-centric security uses business requirements to design and implement a specific level of protection for each asset class that an enterprise holds.

The ability to update security policies in operational systems provides the flexibility needed to adapt to changing regulatory and business requirements. IBM's easy and intuitive way to maintain overall security policies is designed to be cost effective, while allowing businesses to flexibly address changing security requirements in a dynamic business environment.

For more information

To learn more about the IBM data-centric security model, visit:

ibm.com/services/security

© Copyright IBM Corporation 2006

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
12-06
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both.

Other company, product, or service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.