



# **ENGINEERING FOR DATA PROTECTION AND ACCOUNTABILITY**

A Technical White Paper  
May 2007

## Table of Contents

Introduction — A Value Driven Business Imperative for Data Protection . . . . .	1
Safeguarding Data to Reduce Risk and Enable Business Growth . . . . .	1
Solutions That Can Add Value While Reducing Risk . . . . .	2
Addressing Both Security and Privacy . . . . .	3
Striving for Continuous Improvement . . . . .	3
Intelligent Handling of Data Over its Entire Lifecycle . . . . .	4
A Layered Approach to Data Protection . . . . .	5
Data Classification . . . . .	5
Systemic Perspective of Data Protection and Security Requirements . . . . .	6
Architectural Building Blocks for Systemic Security . . . . .	7
Network Security for Data Sources . . . . .	7
Identity Management . . . . .	8
Secure Data Storage and Encryption Approaches . . . . .	9
Portal-based Architectures . . . . .	10
Thin Client Architectures — Eliminating the Risk of Local Data . . . . .	11
Conclusion . . . . .	13
For More Information . . . . .	13

## Chapter 1

# Introduction — A Value Driven Business Imperative for Data Protection

As more and more devices are connected via the network and information is now easily available through open and ubiquitous access methods, a shift is happening in the way people are using technology. More and more people are using technology to connect with each other to participate and to share work flows, to compete for jobs, to purchase goods and services, to learn and create. This work flow will rarely, if ever, be entirely contained within traditional jurisdictional boundaries, thus creating a challenge to legislators, enforcement agencies and users of systems.

Sun calls this new era the “Participation Age” — an age where participants aren't just acquiring information, but are also contributing to the information, refining it, and sharing it. The Participation Age affects not only how people use information, but also how information technology (IT) systems and services must be designed to deliver and protect information. Today's IT services must support widespread access while also protecting the security and privacy of intellectual property (IP) and personally identifiable information (PII).

It is Sun's belief that these IT services and the organizations that use them must, in turn, develop methods to measure and correct the ability of IT systems to support fair and appropriate use of IP and PII. In other words, systems should be designed to promote accountability by leveraging secure architecture techniques and open standards that can be validated by third parties. This is security, privacy and accountability in a governance environment that is designed to meet the needs of businesses, consumers and governmental agencies.

This paper is not intended to be a comprehensive survey of these techniques and possible standards, nor is it intended as a specific technical road map. Instead, this paper is intended to explore how a policy and governance professional can seek to build accountability for governance into IT infrastructure given the existing constraints of the IT environment.

## Safeguarding Data to Reduce Risk and Enable Business Growth

Opening up access to applications and data via the network can also open vulnerabilities where malicious users may try to exploit system resources or data. To protect against this risk, the organization must safeguard its own IP and the many forms of PII that are being captured and used within IT systems. Further, this data must be protected throughout its entire lifecycle from the first point of collection and then everywhere that it flows through IT systems where it can be subject to unauthorized access and misuse or negligence. At the final stage of the data lifecycle, when the data has reached the end of its useful life, the best protection is to destroy the data.

Where data is not protected, there is virtually no accountability for privacy and organizations and users can have no assurance that data access, usage and deletion will happen according to policy and legal restrictions. The contrary is also true in that system level protection can contribute to an organization's ability to execute governance responsibilities and to be accountable for its privacy promises.

Safeguarding data that flows through IT systems and across various geographies has become increasingly complex in light of evolving business and technology trends, including the following:

- Evolving regulatory requirements require increased protection of personally identifiable information to prevent unauthorized collection, access, or use
- Legal liability and business consequences may be imposed for not adequately protecting data from unauthorized access, resulting in potential impact for both organizations and individuals
- Relationships with IT users such as employees, partners, customers and suppliers are dynamic and constantly changing, making it more difficult to maintain accurate and up-to-date authentication and access controls
- Business and organizational success is increasingly dependent on thriving communities that participate and share information over the Web
- Cost of IT services has become a major focus, so data protection strategies must balance risk against cost and effective expenditures of resources

These trends are changing fundamentals of how IT systems are created and governed. Everything with a digital heartbeat will have the ability to be connected through dynamically formed relationships.

Effective data protection and accountability can enable these dynamic relationships to be turned into Participation Age communities that drive business and organizational growth. Users, in turn, will join and participate in a community only if they trust that the community will conduct itself in ways that are not harmful to them. Consistent enforcement of effective privacy policies and practices can build trust by helping to ensure members that their personal information will be used appropriately. Information technology systems and system architecture should also play a significant part in the search for solutions in this new era.

### **Solutions That Can Add Value While Reducing Risk**

Data protection measures are not necessarily in conflict with ease of use, operational efficiency and IT flexibility. In fact, there are many cases where solutions that improve security and privacy also deliver greater value for an organization while reducing risk.

Some examples of data protection solutions that both reduce business risk and increase business value include:

- An enterprise LDAP directory can simplify management of user profiles and access rights to offer increased security through consistent access controls and improved operational efficiency for system administrators.
- Operating systems incorporating container technologies and other virtualization methods not only isolate application services to prevent system breaches from extending their reach, but also offer added flexibility for dynamically assigning or reassigning resources.
- Federated identity techniques can help protect privacy by minimizing unnecessary PII transfer and offer enhanced security for solutions that involve systems maintained by multiple partners.
- Hardware-based encryption offer enhanced security with virtually no performance penalty. Technologies that streamline creation and management of security keys also help prevent key misplacement or theft.
- Identity management solutions can be designed to help protect security and privacy as well as reducing complexity of reporting for compliance and governance purposes.
- Database management systems allow administrators to assign restrictive access to specific database tables while granting wider access to certain table views. This feature enables administrator to isolate PII and restrict

its access while enabling more widespread access to public data that contains no PII. Furthermore, if the PII must be encrypted, overall database performance is less impacted because other data can be safely maintained without encryption.

### **Addressing Both Security and Privacy**

Data protection may be defined as the combination of security and privacy — two topics that are intimately connected because protecting personal information is not possible without effective information, physical and organizational security. Organizations can control access to PII only if the organization's governance model, IT systems and applications that contain data are secure.

Addressing today's security and privacy challenges can be summarized as getting the right data to the right people at the right time. Security and privacy challenges can also be summarized as preventing unauthorized access throughout the data lifecycle. This implies simplifying access for the right people while making access by the wrong people cumbersome, expensive and easily detected. Success in this endeavor depends on a combination of people, processes and technology. Technology is designed to facilitate authorized access in a repeatable and auditable fashion, and the systems themselves can be designed to promote data governance in a way that enhances accountability for the organizations that build and manage them.

While this paper focuses primarily on the technical aspects of data protection and the importance of designing systems for data protection from the very beginning stages, it is also important to remember that the technical requirements will not be sufficient unless people are adequately trained and there are appropriate data management processes in place to help ensure consistent implementation of security and privacy policies over time. A dynamic system requires dynamic management and measurement.

### **Striving for Continuous Improvement**

It is also worth noting that regardless of the legislative schema, data protection may never be completely foolproof. Data protection strategies and implementations are often based on so called reasonable levels of protection given the risks involved. In other words, risk management must be applied where an organization understands that data in general, and PII in specific, has value and that securing and preserving that value requires following the data throughout its lifecycle, from collection to deletion and at every point between those defining events.

Privacy and security standards and legislation designed to protect PII has not yet become harmonized across individual jurisdictions and is certainly not consistent across different cultures worldwide. Thus there is a need for continual and ongoing dialog and experience with complex multinational data manageability requirements so that such standards and best practices can be realized. Technology cannot improve upon these process requirements until further standardization or harmonization is built into the processes themselves.

Furthermore, there may be multiple steps involved to establish or bring existing information technology and management systems in line with reasonable, standardized and auditable policies and procedures. Therefore, organizations should strive toward continuous improvement in data protection and should maintain realistic expectations about time lines and the levels of protection that technology can bring to their environment.

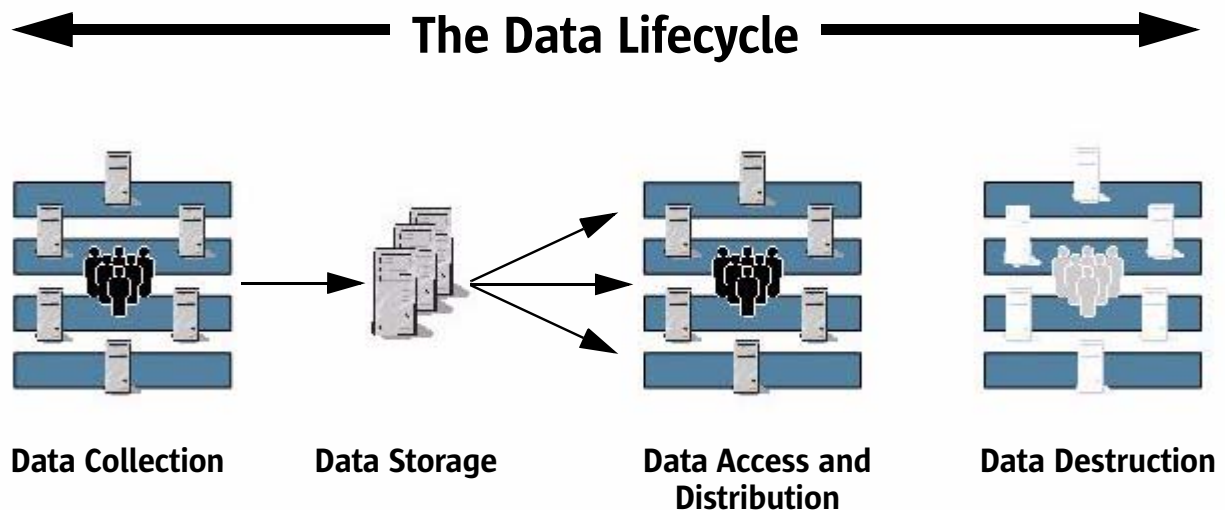
## Chapter 2

# Intelligent Handling of Data Over its Entire Lifecycle

Protecting data within today's most common IT infrastructures is quite different from earlier days when systems were implemented as islands of automation and data was self-contained within discrete systems. Traditional self-contained systems made it difficult to send or retrieve from a system. Therefore, it was relatively easy to inventory these system and draft policy that governed the data housed within them.

Today's systems enable remote access and often store information that is accessible by many systems and users over a network. New threats have emerged where copies of data can be downloaded to sites outside of an organization's primary network and to mobile devices. Business continuity planning may require that duplicate copies of data be retained in remote geographies — often crossing and re-crossing jurisdictional boundaries. To add to this growing complexity, emerging government and industry regulations have intensified the focus on access control and distribution and some include specific controls over where information may and may not flow. Addressing these challenges requires a comprehensive view of data management and data protection that encompasses the entire data lifecycle.

As shown in Figure 2-1, a data lifecycle begins at data collection or creation and continues through access control and dissemination, and finally, destruction. Whether protecting the privacy of PII or the integrity and security of IP, data protection must span this entire lifecycle.



*Figure 2-1. Data protection must be enforced throughout the data lifecycle from collection to destruction*

It is not necessary to begin planning and implementation of data protection in the early stages of the lifecycle. In fact, legacy systems that were designed without data protection in mind can be systematically converted to achieve accountability and governance by applying layers of security building blocks as discussed in the next section. In other words, where one begins is less important than that one begins at all.

## A Layered Approach to Data Protection

To implement a strategy to protect PII based on the principles described above, a layered approach to data protection can be very effective. The techniques and tools described below offer a set of secure building blocks that can be implemented in any order and integrated together to improve high priority control areas. Regardless of the current levels of protection in existing systems, an organization can begin to utilize these building blocks for their governance and data protection strategy. Some of the currently available techniques and tools for data protection include:

- Data classification to mark PII to help recognize varying levels of required protection
- A systemic perspective to security architectures
- Network security for data sources
- Identity management including authentication, authorization and the ability to audit records
- Secure data storage and encryption approaches
- Portal solutions for remote and secure access to applications
- Thin client solutions to minimize unnecessary duplication and theft of PII

The following sections describe how each of these layers can reinforce data protection throughout systems and organizations. It should be remembered that the level of protection, and thus the cost of protection, should be in line with governance principles, the value of the data and the business risk associated with its loss.

### Data Classification

Data classification is a technique whereby data is organized according to its value to the organization, how it will be used and the risks associated with its loss or theft. Different types of data may be subject to differing degrees of risk and have different value to the organization. Data can thus be labeled according to its risk profile, usage characteristics and value to the organization. When data is labeled as belonging to a specific class that shares a common set of characteristics and similar value to the organization, future users of the data will be more informed and can better protect the data.

For data that contains PII, specific privacy protections may triggered upon collection based on the analysis of the data. Data can be classified at the time of data collection to inform the planning for governance over an IT system. This will help ensure that the data is properly treated throughout later stages of the data lifecycle when that data will be stored, accessed, and distributed.

As an example, it is important to identify PII associated with patient health care because there is an ethical and legal obligation to protect patient records, And it is important to recognize that many different groups interact with patient data. Doctors must use the data to provide care, patients have a personal interest in accurate data so they can be more active in promoting their own health, still others document medical visits to pay costs or plan hospital facilities and so on. Each of these interactions with this class of PII must be protected. The consequences of failing to do so can be severe, including poor healthcare services for patients and unsatisfactory patient experiences. A breach of privacy for patient records can also result in regulatory fines, possible lost business, recovery costs, and potential damage to an organization's reputation in the marketplace. When PII is classified at the collection point, these risks can be minimized by planning for role-based access and defining permissible usage patterns for users and systems that must access the data.

Other types of data may be less sensitive and therefore may not warrant heroic measures for security or privacy. In addition, some types of data may change in value as they move throughout the lifecycle.

Classification schemes should include marking the data in a manner that enables a classification code to travel with the data through internal systems and in some cases to outside parties. When the classification code travels with the data, the data is more likely to be properly handled regardless of where it is distributed and accessed. Each different classification code can correspond to a set of access rules and protection measures that are to be implemented for that class of data.

Classification codes can also be used to identify an appropriate type of storage medium for each class of data. Storage media can be selected based on appropriate cost, required protections and the speed with which a given class of data must be retrieved.

*Table 2-1. Benefits of data classification*

<b>Benefits from a Privacy Perspective</b>	<b>Benefits from an IT Perspective</b>
<ul style="list-style-type: none"> <li>• Classification during the data collection process helps to ensure that PII is properly protected</li> <li>• Fine grained control during access and distribution phase can help reduce the risk of PII being accessed by an unauthorized source</li> <li>• Simplified management of data helps content owners be better stewards of their data</li> </ul>	<ul style="list-style-type: none"> <li>• Classification increases control during access and distribution phase to help reduce the risk of unauthorized access</li> <li>• Simplified reporting for regulatory compliance purposes</li> <li>• Provides the foundation for efficiently storing and managing data using information lifecycle management (ILM) methodologies</li> </ul>

## Systemic Perspective of Data Protection and Security Requirements

Security measures are best handled by systems that fail smoothly. In other words, one component of a security system can be broken without rendering the entire system defenseless. Single point-of-failure security methods such as perimeter firewalls or encryption technologies are not completely foolproof. Therefore, the biggest mistake an organization can make is to believe that they are secure when they have a single point of failure in their security architecture. Rather than trying to make firewalls or encryption more secure, multiple layers of defense should be used.

A systemic perspective of data protection and security for PII takes the notion of basic systemic security one step further by ensuring that all system components and applications that contain, utilize or manipulate PII are viewed in tandem with governance policies and user requirements and across organizations. A systemic perspective to protection provides the foundation for privacy governance and accountability across the entire data lifecycle including protecting data that is at rest within individual system components as well as data that is in motion between system components or between users and systems. Even data that flows across various geographic jurisdictions is considered within the data governance scheme.

While many of the system based security components may be managed and implemented by information technology professionals, privacy professionals should have a working knowledge of how security can be implemented to effectively communicate with IT staff and to properly define privacy requirements for IT systems.

It may be helpful to consider that a systemic perspective of security is conceptually a series of interrelated building blocks that are fit together to build the right IT architecture to match the level of data protection and data governance required for the types of business risk that are anticipated. From this secure foundation, additional layers of protection can be added as required in a networked environment.

### Architectural Building Blocks for Systemic Security

Sun's approach to systemic security is to implement multiple layers of security based on the concept of architectural building blocks. These building blocks consist of common design patterns and integrated system-level components that offer a repeatable framework for designing, deploying, and managing network infrastructure solutions. An architectural building block has well-defined properties and interfaces so that it can be easily integrated into the IT environment and can be deployed in a variety of ways depending on the requirements. When properly applied, these architectural building blocks can result in flexible infrastructure designs that provide high performance, scalability, availability, security, flexibility, and manageability for the overall IT environment.

Some examples of architectural building blocks that can be used to enhance systemic security include:

- Highly secure operating system
- Secure execution containers (isolated application environments within the OS)
- Network security and segmentation (restricting access within network segments)
- Centralized instances of core services such as directory and email
- Centralized management solutions

Organizations can implement all available architectural building blocks or only those that are most appropriate for the anticipated business risks. In either case, these architectural building blocks can act as layers of security that can be combined or overlapped to provide the right level of protection to meet an organization's needs and to build an environment that will assist efforts to govern PII throughout its lifecycle.

*Table 2-2. Benefits of secure building blocks*

Benefits from a Privacy Perspective	Benefits from an IT Perspective
<ul style="list-style-type: none"> <li>• Data at rest is better protected from unauthorized access</li> <li>• A security breach won't necessarily put PII in immediate danger</li> </ul>	<ul style="list-style-type: none"> <li>• Helps prevent malicious attacks to an individual system</li> <li>• Maintains security within the internal network</li> </ul>

### Network Security for Data Sources

Today's sophisticated network environments offer an additional layer of security that can be used to reinforce the security of identity management and systemic security layers by further restricting the ways in which data may be accessed. It is easy to make the mistake of thinking that a database sitting on an internal LAN is safe from malicious users or applications because the only sanctioned way of getting to the database is through its application server. However, if an application gets compromised or a hacker penetrates the LAN, another layer of protection could be the difference between a costly data theft incident and a non-critical intrusion detection.

In the early days of the Internet, network security consisted primarily of perimeter defenses made up of firewalls and sometimes intrusion detection solutions. Once inside the firewall, an application or user was generally trusted

and could do just about anything. Today's networking technologies can restrict communication over a given network segment by limiting it to protocols that are pre-approved and communication that is directed between approved parties.

For example, a finance system that contains paycheck information for employees may be on a network segment that restricts communication to system administrators and specific components of the financial application. Approved components of the financial application might include its application servers and the back-end database. If a user were to try to get a login prompt to the application's database server via telnet, the secure network would block that communication. Users could therefore gain access to the financial system only by coming in through the proper channels and not by other means.

The primary benefit of this approach is to contain breaches and prevent malicious applications from spreading throughout an enterprise.

*Table 2-3. Benefits of network security for data sources*

<b>Benefits from a Privacy Perspective</b>	<b>Benefits from an IT Perspective</b>
<ul style="list-style-type: none"> <li>• Greater protection of PII due to increased control over access and distribution of data</li> </ul>	<ul style="list-style-type: none"> <li>• Increased enterprise security due to compartmentalized security for each network segment</li> <li>• Lower risk of spread of a malicious attack or damage from a compromised application</li> </ul>

## Identity Management

One of the primary challenges in controlling data access and distribution lies in the difficulty of properly maintaining access rights to data that may be scattered throughout the enterprise. In particular PII may be spread across the organization or even shared outside the organization. A centralized identity management system can provide an enterprise directory that can be used by all enterprise applications to authenticate users and to control access to data as well as features of IT applications.

Traditional IT environments used a decentralized approach to access controls wherein each individual system maintained its own directory of user profiles and access controls. This approach created fragmented silos of identity data that were difficult to maintain. For example, a user that required access to three different applications on three different systems would likely have required a separate login and password for each system. In turn, each system would have maintained an identity profile for that user to indicate the types of data and application functions that the user was granted permission to access. If the user then changed roles or moved to a different job, the access profiles in all three systems might have required an update to reflect the change.

Planning an information technology environment with centralized identity management can eliminate the need for these fragmented silos of identity data. Identity management solutions can also automate the process of provisioning and deprovisioning user profiles to enable greater efficiency in managing access rights for users and help improve the accuracy of user profiles, enabling better governance of access to PII. This is an important factor for organizations that have large and rapidly changing user populations because it can help reduce the risk of security vulnerabilities due to inaccurate or outdated user profiles.

It is not uncommon for access rights and methods to change as data traverses the stages of the data lifecycle. For example, employee records may be accessible by fewer people to serve that employees needs after an employee leaves the company. These records must also be maintained in archives to preserve accurate records for the company. In other cases, PII may lose all of its value as it ages and would be best destroyed to protect the individual identified by the data and to avoid unnecessary risk to the organization. Identity management should make it easy to track data throughout the lifecycle and provide a simple and efficient means to change access rights as appropriate.

An identity management solution should also simplify regulatory compliance by recording the activities of users and simplifying report generation for audit or compliance purposes. Global regulatory initiatives designed to protect the privacy of individuals require adherence to consistent procedures and strict control mechanisms. While these procedures and controls can be implemented without an identity management solution, a well designed identity solution can raise the level of transparent compliance and accountability for systems and their owners.

Some of the key features of a governance-driven identity management strategy typically include:

- A secure directory infrastructure that provides role-based access control and acts as a single source for managing user identity profiles for multiple different enterprise applications
- User-defined workflows to help create consistent management for user profiles that may change over time
- Automated password reset and synchronization
- Federated identity management to enable seamless and secure access to data while reducing unnecessary transfer of PII between organizations or applications
- Compliance reporting through system-wide auditing
- Heterogeneous environment password synchronization that works with multiple vendor directory products for more consistent enterprise password policy enforcement

*Table 2-4. Benefits of identity management*

<b>Benefits from a Privacy Perspective</b>	<b>Benefits from an IT Perspective</b>
<ul style="list-style-type: none"> <li>• Greater protection against unauthorized access to PII due to increased enterprise security</li> <li>• Easier support for changes to data access rights in different stages of the data lifecycle</li> <li>• Federated identities make it easier to exchange information with outside parties without disclosing PII</li> </ul>	<ul style="list-style-type: none"> <li>• Increased enterprise security due to centralized authentication and centralized user access profiles that can be used by all enterprise applications</li> <li>• Lower risk of errors in maintaining user access privileges which reduces the risk of security vulnerabilities</li> <li>• Reduced costs for maintaining user profiles due to automated work flows</li> <li>• Simplified regulatory compliance</li> </ul>

## Secure Data Storage and Encryption Approaches

Encrypting archival data has become important because of the risks of losing portable or remote media such as tape cartridges and due to requirements for reporting lost PII. Advances in tape encryption technologies are also making it more cost-effective to encrypt tape data. Hardware accelerated encryption devices now enable performance that is virtually on par with writing unencrypted data to tape.

With advancements such as this, the biggest issue in using taping encryption has become managing encryption keys. Encrypted data is worthless if its key is lost or stolen. And yet it would undermine the whole concept of encrypting the data if plain text keys were transported along with the tapes of encrypted data.

The following best practices can be used with encryption systems to help ensure maximum protection of archival data:

- Keys must be shared only on a need-to-know basis.
- Data center locations that do not need access to data should not have a key for that data.
- Keys should never appear in clear text even to authorized users. They should be encrypted when passed between system components and masked when displayed as part of a user screen.
- The key database (a database that maintains the encryption keys) must be encrypted and must have very restricted access.
- A redundant key database should be maintained and it should be located in a separate facility.
- There must be an easy means to change write keys quickly if security is compromised.

*Table 2-5. Benefits of secure data storage and encryption*

<b>Benefits from a Privacy Perspective</b>	<b>Benefits from an IT Perspective</b>
<ul style="list-style-type: none"> <li>• Better protection and increased control over PII by isolating it from non-personal information</li> <li>• Improved protection of PII through encryption</li> </ul>	<ul style="list-style-type: none"> <li>• Enhanced security through best practices for managing encrypted data and keys</li> </ul>

## Portal-based Architectures

Portal based architectures provide an aggregation point that can allow an organization to focus its access requests on a single (or small set) of locations where security can be closely monitored. Some portal technologies can also detect the type of device used to access the portal, thereby providing an additional criterion to be used for access control decisions. For example, a user may be allowed access to sensitive information or functions when the request is originated from a trustworthy source such as a dedicated system within the organization's internal network and denied access when requesting the same data from a PDA that is connected over the Web via an unknown third party service provider.

Portal-based architectures can provide a consistent and centralized interface for users wishing to access services offered by the organization. Should a user no longer need access to a service, a portal also provides a centralized inspection point where access can be revoked.

Portals are also in the position to leverage a centralized identity and access management service to grant access to those services to which a user is entitled. While a portal can perform initial authentication for users, some applications may require that a user re-authenticate using the same or different mechanisms to grant access to specific services or functions.

*Table 2-6. Benefits of portal-based architectures*

Benefits from a Privacy Perspective	Benefits from an IT Perspective
<ul style="list-style-type: none"> <li>• Greater protection of PII throughout the data lifecycle due to the security advantages of portal-based architectures</li> </ul>	<ul style="list-style-type: none"> <li>• Protects internal systems and networks by restricting each user's view based on their access rights</li> <li>• Improves security by aggregating user entry points to a limited set of servers that can be isolated from the rest of the network and closely monitored</li> <li>• Can provide an extra layer of authentication</li> <li>• Enables cost-effective support for multiple types of devices</li> <li>• Can be combined with centralized authentication to enable single sign-on to applications</li> </ul>

### Thin Client Architectures — Eliminating the Risk of Local Data

Desktop systems that are based on a traditional fat client architecture, where each personal computer or other input device has its own hard drive or other storage media, have several shortcomings when it comes to security. The security risks are greatest when large numbers of fat client desktop systems are deployed because there is a greater amount of locally stored data and greater likelihood of security vulnerabilities. For example, it is typically difficult and costly to ensure that OS updates and patches are consistently applied to hundreds or thousands of fat client systems. And, in many cases, organizations lack sufficient control over the software that is installed by individual users of these systems.

As a result, organizations often operate with security vulnerabilities that are invisible to governance professionals. Fat clients can also increase the risk of privacy violations because they can store or cache PII on these devices locally where it stands a greater risk of loss or theft.

By contrast thin client architectures hold no local data. Instead, a user accesses PII and other data types through a server configured to manage all of this information. As a result, thin client architectures eliminate the need to deploy security controls on each and every desktop because those controls can be accomplished centrally and with a degree of transparency. Thinner client architectures also have a much lower intrinsic value to thieves looking for hardware to resell and are therefore a less interesting target.

Another advantage of thin client architectures relevant to governance and accountability for privacy controls is their use of centralized management and administration. This means that configurations and software can be more rapidly updated or patched in response to security alerts. For example, a security patch could be applied to one system to correct a security flaw impacting hundreds of users rather than having to distribute and implement the fix to hundreds of desktops individually.

And lastly, thin client systems can also be deployed with a virtual desktop environment using Smart cards for user authentication. The virtual desktop environment can enhance security and privacy by enabling users to securely move from one desktop to another, taking their virtual desktop environment with them. This provides a means for access to PII and confidential IP in many locations without ever caching the data on a client system, thus greatly reducing the risk of lost or stolen data while providing mobility.

*Table 2-7. Benefits of thin client architectures*

<b>Benefits from a Privacy Perspective</b>	<b>Benefits from an IT Perspective</b>
<ul style="list-style-type: none"><li>• PII cannot be stored on a local disk, but stays on the server where it can be more easily protected</li></ul>	<ul style="list-style-type: none"><li>• Reduced risk of security vulnerabilities due to easier administration</li><li>• Lower total cost of ownership due to simplified maintenance and administration</li></ul>

## Chapter 3

# Conclusion

Designing for data protection and accountability requires forethought about the overall system design and architecture. The only way to successfully protect organizational and individual PII subject interests is to design security in to the IT architecture and to implement multiple levels of security so that there is no single point of failure. Security methods must also be integrated with the interests and capabilities of people and processes to provide effective governance for the sensitive data and the overall IT environment.

Data has become one of the most valuable assets in today's Participation Age business environment. Protecting data using the strategies and best practices outlined in this paper can help reduce the risk associated with loss or theft of PII and important IP while moving organizations toward a model of strong governance and transparency. A strong foundation for data protection can be built using open standards and open interfaces and by designing IT solutions for systemic security using secure architectural building blocks. Additional layers of protection can then be added using strategies such as data classification, identity management, and encryption.

Not all of these data protection strategies will be appropriate for every situation. They should be selected and prioritized according to the unique risks facing each organization. The strategies can then be phased in over time as resources permit. When organizational needs change, data protection strategies can be reevaluated and re-prioritized based on then current risks and requirements.

Finally, data protection and privacy controls should be implemented by aligning governance practices with other organizational goals such as ease of use for IT systems, flexibility to adapt systems to changing organizational needs, and maximum operational efficiency. When technologies are designed to promote these interests, tools can be used more effectively to protect the privacy of individuals who are fellow employees, customers and citizens.

## For More Information

Visit the Web sites below for additional information about Sun building blocks.

*Table 3-1. Web Links for Additional Information*

<b>Web Site URL</b>	<b>Description</b>
<a href="http://sun.com/">sun.com/</a>	Sun Microsystems home page
<a href="http://sun.com/privacy/">sun.com/privacy/</a>	Sun online privacy policy
<a href="http://sun.com/security/">sun.com/security/</a>	Sun security solutions
<a href="http://sun.com/identity/">sun.com/identity/</a>	Sun identity management solutions
<a href="http://sun.com/solaris/">sun.com/solaris/</a>	Solaris™ Operating System
<a href="http://sun.com/storagetek/">sun.com/storagetek/</a>	Sun storage solutions
<a href="http://sun.com/javaenterprisesystem/">sun.com/javaenterprisesystem/</a>	Sun Java™ Enterprise System

Copyright © 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A.

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Sun, Sun Microsystems, the Sun logo, Solaris and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.