INFORMATICA

WHITE PAPER

Safeguarding Sensitive Data in the Federal Government

Advancing Cybersecurity with the Informatica Solution for Data Privacy

This document contains Confidential, Proprietary and Trade Secret Information ("Confidential Information") of Informatica Corporation and may not be copied, distributed, duplicated, or otherwise reproduced in any manner without the prior written consent of Informatica.

While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. Informatica does not accept responsibility for any kind of loss resulting from the use of information contained in this document. The information contained in this document is subject to change without notice.

The incorporation of the product attributes discussed in these materials into any release or upgrade of any Informatica software product—as well as the timing of any such release or upgrade—is at the sole discretion of Informatica.

Protected by one or more of the following U.S. Patents: 6,032,158; 5,794,246; 6,014,670; 6,339,775; 6,044,374; 6,208,990; 6,208,990; 6,850,947; 6,895,471; or by the following pending U.S. Patents: 09/644,280; 10/966,046; 10/727,700.

This edition published March 2013

Table of Contents

Executive Summary 2

Implementing a Data Privacy Strategy 3

Data Privacy: Challenges and Trends 4

Revenue Agencies—Perforated with Privacy Weaknesses 4
Department of Defense—Vulnerable from the Inside and Out 5
Intellectual Property, Trade Secrets, and Competitive Intelligence 5
Legislative Mandates and Initiatives 5
Department of Homeland Security—
Warnings of Web Browser Vulnerability 6
Government-Wide Social Security Number Remediation 6

Acknowledging Insider Threats 6

Exposure in Nonproduction Environments: Test and Development 7
Exposure in Production Environments: DBAs and Privileged Users 7

Addressing the Data Privacy Lifecycle 8

Using and Combining Data Protection Technologies 9

Data Masking 9
Data Encryption + Data Masking 10
Database Activity Monitoring + Data Masking 10
SIEM + Data Masking 11

Assessing Data Privacy Solutions 11

The Informatica Solution for Data Privacy 12

Informatica Data Subset 12
Informatica Persistent Data Masking 12
Informatica Dynamic Data Masking 13
The Informatica Advantage 14

Conclusion 15

Executive Summary

Cybersecurity has become one the highest priorities today in federal government. The sharp increase in legislation recently proposed to this end indicates a renewed and intense focus on securing personally identifiable information, protected health information, and sensitive data and intelligence. Cybersecurity laws are critical to securing our national and economic interests and protecting citizens from harm or loss.

Yet despite recent actions by Congress and the White House, little progress has been made in formulating and enacting a comprehensive cybersecurity policy across the federal government. This has left numerous agencies and organizations vulnerable to cyberattacks and attempts to breach data, which have been growing at record pace. The General Accounting Office (GAO) estimates that attacks on the U.S. government have increased 680 percent over the last six years. In addition, around 94 million citizens' records under the care of government agencies have been lost or breached since 2009.[1]

The sources of threats to government cybersecurity are numerous and varied. They include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, espionage, or information warfare. While outside of our control, these threats are heightened by otherwise resolvable vulnerabilities in federal data systems. Specifically, according to a recent GAO report, significant weaknesses in information security controls continue to undermine the confidentiality, integrity, and availability of critical information and systems supporting the operations, assets, and personnel of federal government agencies.[2]

In fiscal 2011, 22 of the 24 federal government's inspectors general identified information security as a major management challenge for their agency. Moreover, GAO, agency, and inspector general assessments of information security controls during fiscal year 2011 revealed that most major agencies had weaknesses in most major categories of information system controls. On this issue, Leon Panetta, U.S. Secretary of Defense has stated:

"It is critical to strengthen our cyber capabilities to address the cyber threats we're facing. I view this as an area in which we're going to confront increasing threats in the future and thus we have to be better prepared to deal with the growing cyber challenges that will face the nation."[3]

This white paper discusses the challenges to securing information in federal government organizations and outlines common sources of data breaches. It discusses the effectiveness and versatility of data masking—both traditional, persistent data masking and the newer, breakthrough technology of dynamic data masking—in addressing the data privacy requirements of the public sector. It also examines the pros and cons of complementary data protection techniques such as encryption and database activity monitoring, and how they can be used alongside data masking software to provide optimal protection in specific scenarios. Finally, the paper outlines what to look for in a data privacy solution and advocates implementing Informatica® data masking products to achieve robust, transparent, and cost-effective data privacy.

[1] Rapid 7 LLC, *Data Breaches in the Government Sector* (September 2012).

[2] Gregory C. Wilshusen, Director Information Security Issues, "Cybersecurity: Threats Impacting the Nation," *Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives* (2012).

[3] Office of the Assistant Secretary of Defense (Public Affairs), U.S. Department of Defense, *News Release: DOD Announces First Strategy for Operating in Cyberspace* (July 14, 2011).

Implementing a Data Privacy Strategy

The security of infrastructure, networks, and systems is essential to protecting national and economic security, public health and safety, and the flow of commerce. To this end, federal government agencies should implement a comprehensive data privacy strategy that addresses three types of cyberattacks (in ascending order of invasiveness):

- Denial of service attacks that affect the operability of networks
- Destructive actions that threaten to destroy and degrade networks or connected systems
- Theft or exploitation of data

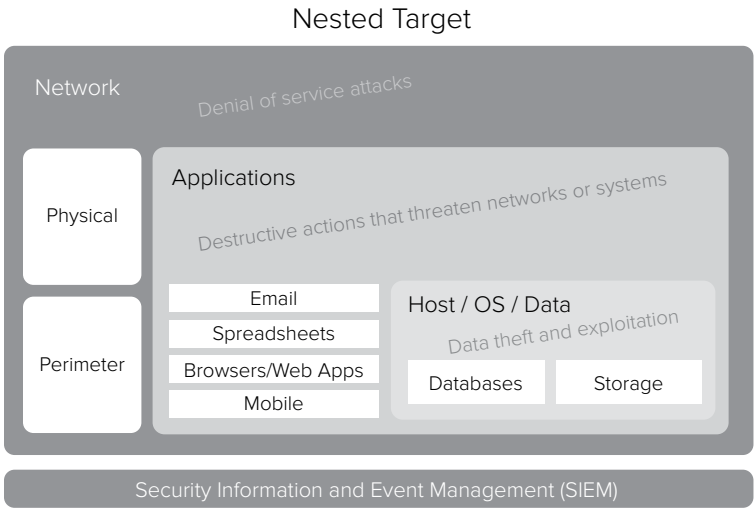


Figure 1: Cyberattacks target three types of nested targets: networks, applications, and host data.

The GAO report on cybersecurity identifies that ineffective information security controls can result in significant risks, including:

- Loss or theft of resources, such as federal payments and collections
- Inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personal taxpayer information, or proprietary business information
- Disruption of key operations supporting critical infrastructure, national defense, or emergency services
- Undermining of agency missions due to embarrassing incidents that erode the public's confidence in government
- Use of computer resources for unauthorized purposes or to launch attacks on other computer systems

While not all government agencies deal with sensitive data related to defense or national security, most agencies do collect, store, and process personal, financial, health, and other information that must be protected. Entrusted with the many aspects of safety and security of the public, government agencies must consistently demonstrate the ability to be sound financial stewards and rigorous defenders of sensitive data or personally identifiable information (PII).

The effects of ineffective information security are profound. The average cost to the government of a data breach has been estimated at $5.5 million or $194 per individual record, according to the Ponemon Institute.[4] In addition to high costs to taxpayers, data breaches and cyberattacks are also costly to citizens directly and erode the public's trust. The unauthorized use or misuse of PII can impact an individual's ability to get a job, secure a loan, pay for education, become insured, defend against identity theft, or benefit from public programs. Citizens need to know that they can trust public organizations with their personal information, but each new high-profile public data breach or negative watchdog report shakes that faith.

Data Privacy: Challenges and Trends

Many U.S. government agencies have made major investments and significant strides in securing their systems against data breaches and cyberattacks, treating data privacy as a top priority. But securing data is becoming an increasingly daunting challenge because of vulnerabilities that remain.

Below are six of the top data privacy challenges and trends affecting the federal government.

Revenue Agencies—Perforated with Privacy Weaknesses

According to IRS Publication 1075, "The public must have and maintain a high degree of confidence that the personal and financial information furnished to us is protected against unauthorized use, inspection or disclosure." Yet a 2012 GAO report entitled *Information Security: IRS Needs to Enhance Internal Control over Financial Reporting and Taxpayer Data* states:

"Although IRS has made progress in correcting information security weaknesses that we have reported previously, many weaknesses have not been corrected and we identified many new weaknesses during fiscal year 2010. Specifically, 65 out of 88 previously reported weaknesses—about 74 percent—have not yet been corrected. In addition, we identified 37 new weaknesses. These weaknesses relate to access controls, configuration management, and segregation of duties."[5]

Specific weaknesses include the "excessive access" given some internal users to systems by granting permissions beyond what they need to perform their jobs. Furthermore, the GAO has uncovered poor segregation-of-duty practices and determined that some devices were sending unencrypted data over the IRS Network.

[4] Ponemom Institute LLC, *2011 Cost of Data Breach Study: Global* (March 2012).

[5] Office of the Assistant Secretary of Defense (Public Affairs), U.S. Department of Defense, *News Release: DOD Announces First Strategy for Operating in Cyberspace* (July 14, 2011).

Department of Defense—Vulnerable from the Inside and Out

Following a recent attack from a foreign intelligence service that gained access to over 24,000 records from a defense contractor with insider access to systems, the Department of Defense has outlined a new, more comprehensive strategy to defend against breaches and other cybersecurity related problems. In that case, the target records related directly to a highly sensitive weapons system. According to William Lynn, Deputy Secretary of Defense:

"The cyber threats we face are urgent, sometimes uncertain, and potentially devastating as adversaries constantly search for vulnerabilities. Our infrastructure, logistics network, and business systems are heavily computerized. With 15,000 networks and more than seven million computing devices, the DoD continues to be a target in cyberspace for malicious activity."

Given this vulnerability and the risks involved, defense and intelligence agencies must take a posture in protecting their data networks similar to that which they have in defending the domains of land, sea, and air. To do that, they must look at all possibilities of threat and understand the full breadth and depth of vulnerabilities from both inside and outside their organizations.

Intellectual Property, Trade Secrets, and Competitive Intelligence

Pharmaceutical manufacturers regard most of their research data as confidential commercial information, intellectual property, or trade secrets. As part of the drug approval process, much of this confidential information must be submitted to the Food and Drug Administration (FDA) as background and clinical trial data. Many federal statutes recognize that companies' proprietary business information must be protected. For example, the Food, Drug, and Cosmetic Act prohibits FDA employees from disclosing any method or process acquired during review that is entitled to protection as a trade secret.

Similar statutes apply to other agencies that test and approve products or conduct public surveys with confidentiality commitments. The U.S. Energy Information Administration is responsible for collecting sensitive information about the nation's energy supply across all commercial partners. Information on energy location, supply, drilling, storage, reserves, and production rates is not only highly sensitive but also considered extremely valuable commercially with both competitive and financial implications.

Legislative Mandates and Initiatives

Federal Information Security Management Act (FISMA). With the passing of FISMA, the National Institute of Standards and Technology became responsible for developing guidelines on information security for all civilian federal agencies. The institute now produces security controls for information systems, which are the safeguards necessary to protect the confidentiality, integrity, and availability of data produced and used by federal agencies.

Health Insurance Portability and Accountability Act (HIPAA). The requirements of HIPAA privacy rules apply to all government healthcare organizations, including programs like Medicare and Medicaid, Tricare, Military Health, and Veterans Insurance. One of the HIPAA privacy rules calls for "minimum necessary" use and disclosure of protected health information (PHI). It mandates that policies and technologies be implemented to hide, protect, or mask any individually identifiable health information that's not otherwise required to fulfill a specific purpose or request.

Department of Homeland Security—Warnings of Web Browser Vulnerability

Following a series of attacks on government computer systems, presumably by Chinese intelligence and other hackers, the Computer Emergency Readiness Team of the Department of Homeland Security recently issued the following warning about infected systems vulnerable to data breach:

"A vulnerability in the Java Security Manager allows a Java applet to grant itself permission to execute arbitrary code. An attacker could use social engineering techniques to entice a user to visit a link to a web site hosting a malicious Java applet. An attacker could also compromise a legitimate web site and upload a malicious Java applet (a 'drive-by download' attack). Any web browser using the Java 7 plug-in is affected. The Java Deployment Toolkit plug-in and Java Web Start can also be used as attack vectors. Reports indicate this vulnerability is being actively exploited, and exploit code is publicly available."[6]

Government-Wide Social Security Number Remediation

Government organizations with a broad range of functions—revenue, benefits, healthcare, and security, for example—have relied on Social Security numbers (SSN) as a unique identifier in their systems for years. In recent years, agencies have implemented extensive remediation initiatives to remove SSNs as the prime identifier or key. But they widely report that SSNs continue to be collected and stored without a thorough understanding of the business requirements for that data. A comprehensive SSN remediation program must be part of an overall governance plan that includes removing and securing personally identifiable information, including SSNs, and a process review of all systems to determine the actual business requirements of SSNs.

Acknowledging Insider Threats

According to Forrester Research, 70 percent of data breaches today occur from inside an organization. Because these threats are just as likely as external ones to expose data to a cybersecurity attack or loss, agencies need to put as much thought and effort into securing data from the inside as they have traditionally done from the outside. Public sector entities must enhance their internal privacy protection techniques to guard against data misuse, leakage, or theft.

The sources of insider threat are numerous and varied. They include contractors hired by the organization as well as careless or poorly trained employees who may inadvertently introduce malware into systems. Agencies are further challenged to balance the adoption of new technologies and transformation initiatives with the critical need to protect information from the vulnerabilities often inherent in these technologies. In particular, government organizations often need to block access to social media on government equipment, prevent employees from sending attachments externally, and even limit or ban the use of portable storage devices.

But blocking social media, monitoring technology, and securing devices address only a fraction of the vulnerabilities that lead to data theft and exploitation. Two additional areas of exposure stand out as significant threats to data security:

- Access to copies of production data in nonproduction environments by test and development personnel
- Access to data in production environments by database administrators (DBAs) and privileged users

[6] United States Computer Emergency Response Team, U.S. Department of Homeland Security, *Alert (TA13-010A): Oracle Java 7 Security Manager Bypass Vulnerability* (January 10, 2013), http://www.us-cert.gov/ncas/alerts/TA13-010A.

Exposure in Nonproduction Environments: Test and Development

Test data plays a vital role in measuring the effectiveness of databases. IT organizations spend an enormous amount of time and effort to create or provision data for testing purposes. But poor quality software—costing organizations worldwide $500 billion annually—complicates these efforts.[7] Research has shown that testers spend more than 30 percent of their time on test data–related activities, including setup of data for multiple environments, downtime due to corrupt data, replacement of missing data required for testing, and correction of defects that often cost hundreds of millions dollars.[8]

In addition to the complications and costs of defects, test and development environments typically contain multiple copies of production data in its entirety—frequently, as many as 10 copies. The sheer volume of data being exposed in these circumstances makes an organization vulnerable immense risk of breaches, whether that data is used by developers internally or via third-party contract. If the development work is done overseas, the risks are further elevated. To mitigate the risks of such large-scale exposure, the data used in test and development environments must to be de-identified or obfuscated while keeping it as true as possible to the original production data from which it was copied.

For example, HIPAA Privacy Rule 164.502 (b)(1) states, "When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." It is imperative for organizations to understand that this rule applies to all test and development environments as well. As such, organizations must de-identify or mask sensitive data, personally identifiable information, financial information, and protected health information so that test and development personnel do not see or access individuals' identities.

Exposure in Production Environments: DBAs and Privileged Users

Another significant exposure risk involves internal users with access to data and systems beyond what is required for their jobs. Personal and other sensitive data needs to be protected proactively from excessive or unnecessary access by DBAs, support teams, contractors, and end users—and not just in databases, data warehouses, clones, and backups, but also within application screens. Because there are several types of data requiring protection, as well as many different user and administrative roles and privilege levels, protecting this data presents a significant challenge. Making the challenge even more formidable is the need to extend protection without impacting application performance and without requiring new application code or any database changes. Furthermore, organizations need to audit who is accessing which data and must be alerted in real time to unauthorized access so that appropriate steps can be taken.

[7] Caper Jones & Associates LLC, *Software Quality in 2011: A Survey of the State of the Art* (August 31, 2011).

[8] Gartner, Inc., *IT Key Metrics Data 2012: Key Applications Measures: Application Development: Current Year* (December 15, 2011).

Addressing the Data Privacy Lifecycle

Data privacy protection has a lifecycle that aligns with best practices for data governance (see Figure 2). For effective protection, each step of the cycle needs to be addressed:

1. **Discover** where sensitive data resides and understand how it is used and by whom.
2. **Define and Classify** private and sensitive data across the organization, along with requirements for its protection, from data creation to destruction
3. **Apply** privacy protection policies and implement technologies to support those policies across the organization's systems and data classifications in support of compliance.
4. **Measure and Monitor** the use of information and those who access it, and implement an audit process to prove that the data is being protected; similarly, organizations need to show compliance for retention policies.

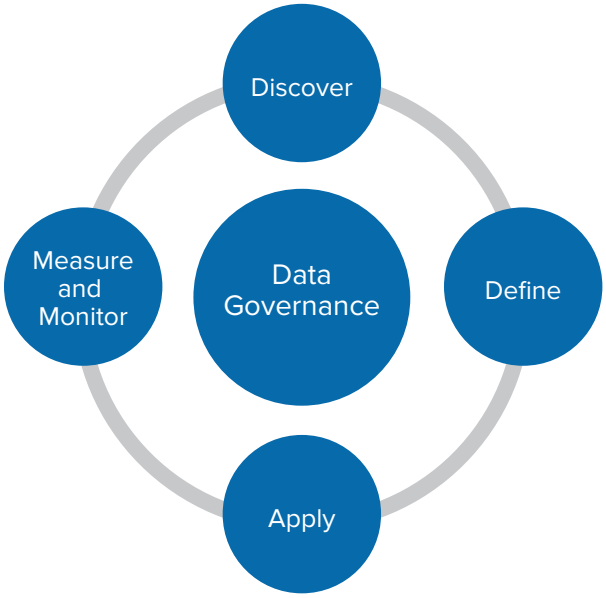


Figure 2: Each of four steps of data governance best practices needs to be addressed for effective protection.

Once past the first step, Discover, each subsequent step of the data privacy lifecycle is enabled by a technology or set of technologies, along with a specific set of best practices for their use. These technologies, their respective strengths, and how they can be used to meet various protection criteria in production and nonproduction environments, are discussed in the following section.

Using and Combining Data Protection Technologies

Several proven data protection technologies are available and of particular relevance to federal government organizations aiming to secure their systems against data breaches and cyberattacks. Data masking has emerged as one of the most versatile of these technologies, both on its own and in its ability to work in concert with other protection techniques.

Data Masking

Persistent Data Masking—Broad-Based Protection of Nonproduction Data

Traditional, or persistent, data masking protects sensitive data by using a range of techniques and algorithms to permanently obfuscate that data while at rest or in transit. This enables fully functional, realistic data sets to be used in development, test, training, and other nonproduction environments because all of its identifying information has been hidden. The masked data retains its original form and possesses full referential integrity so that developers can work with realistic data while its sensitive elements are shielded to eliminate the risk of a privacy breach.

Dynamic Data Masking—Selective, Policy-Based Shielding of Production Data

Dynamic data masking uses data protection rules in real time to keep privileged personnel, such as DBAs, production support staffers, and business users, from accessing sensitive and personally identifiable information that they do not require to perform their jobs.

The value of dynamic data masking lies in its ability to apply different masks to different types of the data found in production databases, applications, and reporting and development tools. Because masking is applied dynamically based on user roles and privilege levels, only individuals with a need to see the fully exposed data could do so; all others see masked data. In a public sector organization, this would mean that a DBA or unauthorized user would not be able to see real Social Security numbers, individual student grades, or tax payers' modified adjusted gross income figures because these values and other personally identifiable information would be selectively scrambled, hashed, masked, or blocked.

Data Masking Advantages

Among the key advantages of data masking, both persistent and dynamic, is its freedom from requiring changes to databases or application source code. This means that masking can be applied quickly and unobtrusively to protect private data across an organization, regardless of size. Data masking is also granular, in that it enables organizations to selectively mask data down to the row, column, or cell level. Furthermore, data masking technology can integrate with existing authentication solutions, including ActiveDirectory, LDAP, and Identity Access Management software. And it complements other data protection technologies such as encryption, database activity monitoring (DAM), and security information and event management (SIEM), collectively providing comprehensive data privacy protection.

Data Encryption + Data Masking

Encryption can solve many data protection problems. In fact, mass encryption of databases is practically mandatory to guard sensitive data against outside intrusion. But it's not a perfect solution for all problems; on its own, it poses several limitations. Encryption cannot prevent access to private information by DBAs and systems administrators or by authenticated applications and reporting tools. Nor can it selectively protect down to the row, column, or cell level; rather, it encrypts the entire database, which can be problematic. Additionally, while it's easy to encrypt structured data such as that found in databases, encryption cannot protect unstructured data found in spreadsheets, documents, and emails, or data in semistructured formats. Finally, the process of continually encrypting and decrypting can degrade system performance considerably.

Encryption alone has its limitations, but by combining it with data masking, organizations are able to address a far greater range of data privacy issues while minimizing the performance degradation. For example, structured data within databases can be mass encrypted to protect the data at rest, while dynamic data masking can be simultaneously employed to selectively protect sensitive data:

- Within the screens of authorized tools and applications
- From access by DBAs and users who do not need to see such data as part of their jobs

Similarly, data masking can be used to extend protection to unstructured and semistructured data. Persistent data masking can also be used in conjunction with encryption to make encrypted data more realistic-looking for development and testing purposes. In either case, masking data as opposed to encrypting it exerts little to no performance penalty.

Database Activity Monitoring + Data Masking

Database activity monitoring (DAM) solutions monitor database access and activities and help organizations better understand how and where their database security can be breached. DAM, however, does nothing to physically or logically secure data. By adding data masking on top of a DAM solution, organizations gain the ability to mask sensitive data from developers, DBAs, and unauthorized internal users and contractors (see Figure 3). This capability can be refined based on the results of DAM monitoring and auditing of masked data.

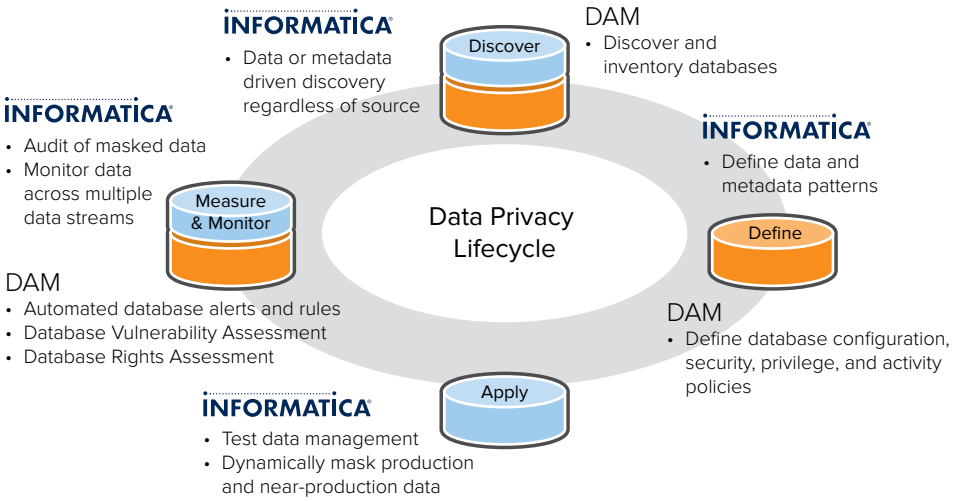


Figure 3: Data masking can be seamlessly incorporated into an existing database activity monitoring solution.

SIEM + Data Masking

Security information and event management (SIEM) solutions consolidate data on network, application, database, and security events. They provide both historical and real-time correlation and analysis of the data to drive security reports and improvements. When combined with event processing software, the data can be used to drive real-time alerts and responses. A data masking solution will feed monitoring and audit data to a SIEM solution as part of an end-to-end security-monitoring environment.

Assessing Data Privacy Solutions

Whether an organization is looking for a data masking, encryption, DAM, SIEM, or other kind of data protection, certain questions need to be posed about a data privacy solution that's being considered. These include:

- Is it from a vendor with a proven record of success working with public sector organizations?
- Will it work with, complement, and/or extend other types of data protection solutions?
- Does it deploy quickly and deliver a rapid ROI?
- Can it scale to protect increasingly large volumes of data?
- Is it easy to use and administer?
- Does it support cloud environments?

Data privacy solutions have a further set of requirements specific to their use. Organizations should look for a solution that achieves the following:

- Protects data in production and nonproduction environments
- Delivers both persistent and dynamic data masking
- Scales to support hundreds of databases with a single installation
- Supports all applications and reporting and development tools running on the most popular database platforms
- Exacts no penalty on database and application performance
- Integrates with existing authentication software
- Provides policy-based and role-based data protection
- Simplifies the creation of data masking rules
- Applies several types of real-time data masking, blocking, and alerting actions
- Supports structured, unstructured, and semistructured data
- Supplies granular protection down to the level of row, column, or cell
- Works seamlessly in concert with encryption, DAM, and SIEM technologies
- Implements quickly to furnish broad data privacy protection in a matter of days
- Customizes easily to specific public agency requirements

The Informatica Solution for Data Privacy

Informatica offers one solution that meets all the requirements for robust data protection. The Informatica solution for data privacy is based on proven technology that substantially reduces the risk of a data breach and helps federal government organizations protect against cyberattacks. The solution consists of three products:

1. Informatica Data Subset
2. Informatica Persistent Data Masking
3. Informatica Dynamic Data Masking

Together, these products mask or block sensitive and confidential information from unauthorized access in both production and nonproduction environments. Used individually or in concert with other data protection solutions, they empower your IT organization to comply with data privacy policies, regulations, and mandates at lower costs. They enable your application end users, database administrators, developers, testers, trainers, production support, and business analysts to perform their functions without sacrificing data security.

Informatica Data Subset

Informatica Data Subset is flexible, scalable software for creating data subsets. It enables your IT team to create, update, and secure data subsets—smaller, targeted databases—from large, complex databases. With referentially intact subsets of production data, your IT organization dramatically reduces the amount of time, effort, and disk space needed to support nonproduction systems.

Informatica Data Subset quickly replicates and refreshes production data with only the most relevant, high-quality application data. This means your IT team doesn't need to create a full database copy—you separate out only functionally related data from interconnected systems.

Informatica Persistent Data Masking

Informatica Persistent Data Masking is scalable data masking software that helps your entire IT organization manage access to your most sensitive data. The software shields confidential data, such as financial information, health data, Social Security numbers, names, addresses, and phone numbers, from unintended exposure to reduce the risk of data breaches. It provides unparalleled enterprise-wide scalability, robustness, and connectivity to a vast array of databases.

Informatica Persistent Data Masking minimizes the risk of data breaches by masking test and development environments created from production data regardless of database, platform, or location. The software furnishes sophisticated, but flexible, masking rules that allow your IT team to apply different types of masking techniques to various data used in testing, training, and other nonproduction environments.

Informatica Data Subset and Informatica Persistent Data Masking together form Informatica Test Data Management (see Figure 4). A purpose-built tool, Informatica Test Data Management enables security administrators, QAs, and other users to discover where sensitive data lives across the organization, make subsets of production data to create smaller copies for testing or training, mask the data, and then substantiate that the data was masked according to specified privacy policies.

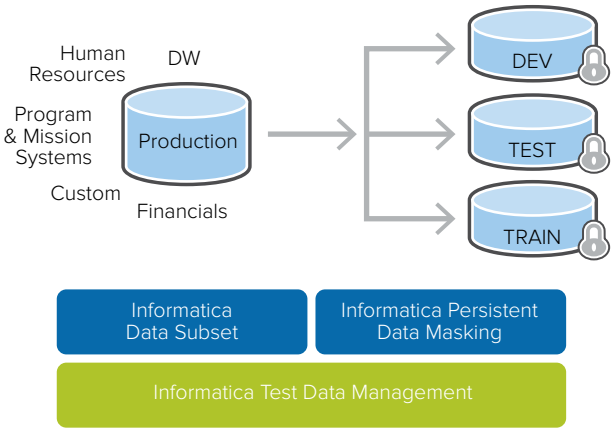


Figure 4: With Informatica Test Data Management, your IT team can apply different subset and masking techniques to production data.

Informatica Dynamic Data Masking

In production environments, privileged users such as DBAs or functional business users often have inadvertent access to sensitive data that they don't actually need to perform their jobs. To help organizations proactively address this data privacy challenge in production, Informatica offers Informatica Dynamic Data Masking—the only true dynamic data masking product on the market. The software dynamically masks sensitive information in production data and blocks, audits, and alerts end users, IT personnel, and outsourced teams who access sensitive information.

With Informatica Dynamic Data Masking, your IT organization can apply sophisticated, flexible data masking rules based on a user's authentication level. Through a simple yet elegant rules engine, criteria can be specified to identify which SQL statements are to be acted upon (rewritten). When there is a match, Informatica Dynamic Data Masking applies one or more actions—including mask, scramble, hide, rewrite, block, or redirect—to prevent unauthorized users from accessing sensitive information in real time.

The Informatica Advantage

What makes the Informatica solution for data privacy unique is its basis on the industry-leading Informatica Platform. This comprehensive, open, unified, and economical data integration platform supports a centralized data management approach, so your IT organization can leverage the solution across multiple business lines to conduct audits and comply with data privacy policies and regulations enterprise-wide.

Leveraging the Informatica Platform, the Informatica solution for data privacy enables you to address each part of the data governance lifecycle: discover; define and classify; apply; measure and monitor (see Figure 3). It empowers your IT organization to ensure that data privacy is not just a one-time initiative but also part of an overall, ongoing data governance program by:

- Addressing all database applications, on or off premises, including both production and nonproduction databases
- Providing a centralized management and control center for consistent enterprise-wide data privacy protection
- Featuring coarse and fine-grained encryption to support a variety of custom and packaged applications, databases, and data center policies
- Handling data volume growth—either organic growth or as new applications are deployed in the data center

Conclusion

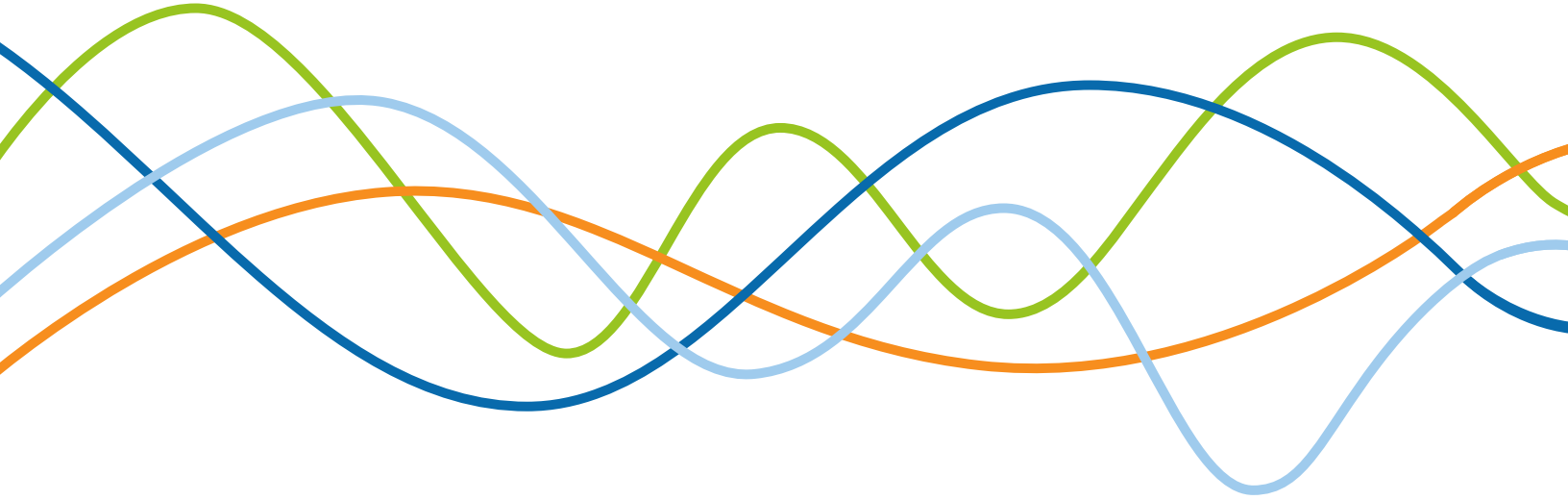
Cyberwarfare is a grim reality increasing in its frequency and sophistication. Federal agencies in particular are constantly targeted by cyberattacks that often result in significant data breaches. But they don't need to be left vulnerable. Several proven data protection technologies are available and of particular relevance to government organizations aiming to secure their systems against data breaches and cyberattacks. Data masking has emerged as one of the most versatile of these technologies.

Informatica offers one solution that includes data masking and meets all the requirements for robust data protection. The Informatica solution for data privacy is based on proven technology that substantially reduces the risk of a data breach and helps government organizations protect against cyberattacks.

With this solution, you can mask or block sensitive and confidential information from unauthorized access in both production and nonproduction environments. It can be quickly implemented on its own or seamlessly with other protection technologies to provide broad data privacy. It also scales to support hundreds of databases with a single installation and supports all applications and reporting and development tools running on the most popular database platforms. And because it is easily customized, the Informatica solution for data privacy can meet the specific requirements of public agencies, supplying them with robust protection against the cyberattacks facing them today.

ABOUT INFORMATICA

Informatica Corporation (NASDAQ: INFA) is the world's number one independent provider of data integration software. Organizations around the world rely on Informatica for maximizing return on data to drive their top business imperatives. Worldwide, over 4,630 enterprises depend on Informatica to fully leverage their information assets residing on-premise, in the Cloud and across social networks.



INFORMATICA®

Worldwide Headquarters, 100 Cardinal Way, Redwood City, CA 94063, USA
phone: 650.385.5000 fax: 650.385.5500 toll-free in the US: 1.800.653.3871
informatica.com linkedin.com/company/informatica twitter.com/InformaticaCorp

© 2013 Informatica Corporation. All rights reserved. Printed in the U.S.A. Informatica, the Informatica logo, and The Data Integration Company are trademarks or registered trademarks of Informatica Corporation in the United States and in jurisdictions throughout the world. All other company and product names may be trade names or trademarks of their respective owners.

IN09_02381_0313