



SOLUTION OVERVIEW



Security Solutions

to Minimize Risk of Breaches of Personal Information



Where it all comes together.™



KEY BENEFITS

Reduces Exposure Under Breach Reporting Laws

VeriSign solutions minimize risk of penalties, and damage to reputation and customer loyalty, associated with security breaches.

Minimizes New Security Investments

Enterprises can reduce the costs of planning, developing, and implementing the security infrastructure needed to help achieve compliance.

Establishes a Flexible, Extensible Security Program

VeriSign establishes policies, procedures, guidelines, and technologies that help in complying with breach reporting laws and other regulations and achieving business priorities.

The California Security Breach Notice Act (formerly Senate Bill 1386) requires any agency, business, or person owning, licensing, or maintaining a computerized database of personal information on California residents to immediately notify the customers if the security of their personal information is breached. This requirement, which became operative on July 1, 2003, has been duplicated by other states and the federal government and applies even if no personal information is stolen. In addition, it authorizes lawsuits and injunctions if breaches are not reported in a timely manner.

Enterprises recognize the difficulty of providing written or electronic notices to customers in the event of a breach. Accordingly, most enterprises operating in states that have breach reporting laws recognize the need to prevent security breaches that necessitate reporting and may potentially damage their reputation. To minimize risk exposure caused by unauthorized access to or disclosure of information, enterprises are acting quickly to identify and assess security risks, plan and implement services to protect sensitive information, and establish measures to monitor and manage security systems.

VeriSign offers a suite of services to support enterprises in preventing breaches of security systems covered by the California Security Breach Notice Act and similar statutes:

- **VeriSign® Global Security Consulting** – Enables enterprises to design and implement an information security program to minimize the risk exposure of networks and applications that may contain personal information.
- **VeriSign® Managed Security Services (MSS)** – Help ensure the security of networks that hold customers' personal information through 24/7 management of the network-security infrastructure. Regular vulnerability assessments help ensure that potential vulnerabilities are detected and remedied proactively before attackers can exploit them.
- **VeriSign® Unified Authentication** – Enables enterprises to leverage existing infrastructure for authenticating a variety of digital credentials—including digital certificates, dynamic one-time passwords (OTPs), and universal serial bus (USB) tokens with smart card technology—to minimize, if not eliminate, unauthorized access, while reducing costs.

+ Compliance Assessment and Gap Analysis

Identifying and assessing threats to customer information and evaluating the effectiveness of current safeguards is a complex task that requires in-depth knowledge of security technology and practices, as well as continual identification of ever-changing security threats and requirements. VeriSign leverages deep expertise, proven methodologies, and state-of-the-art tools to thoroughly assess the current state and vulnerability of existing network security implementations, including policies, technology, operations, use, performance, and physical security. VeriSign identifies immediate security concerns and pinpoints gaps between the current infrastructure and identified requirements, overall system security, and projected growth. Using the assessment and gap analysis, VeriSign provides prioritized recommendations for improving performance and mitigating risk, thereby helping ensure compliance with breach reporting laws.

+ Security Breach Protection

VeriSign MSS allow enterprises to offload security infrastructure management to a team of experts whose core business is security. The suite of services (e.g., firewalls, intrusion detection systems, intrusion prevention, and log monitoring), which can be utilized individually or as a set, includes assessment, monitoring, management, and reporting.



Working from globally linked VeriSign Security Operations Centers (SOCs), security teams use sophisticated tools to monitor, correlate, and analyze data across multiple levels of the organization in order to rapidly identify and prevent attacks. Enterprises maintain full control of security policies and decisions and can access network data 24/7 via the Web-based VeriSign® Enterprise Security Portal.

+ Authentication and Access Control

A 2005 survey on security conducted jointly by the U.S. Federal Bureau of Investigation (FBI) and the Computer Security Institute (CSI) found that nearly half of all cyber security breaches originate from outside the target organization's boundary. To protect customer information against unauthorized access, enterprises must be able to control not only who accesses networks, applications, facilities, and other resources, but also which resources each user can access. VeriSign Unified Authentication enables enterprises to significantly reduce the risk of unauthorized access. Along with its technology partners, VeriSign enables enterprises to easily deploy and manage a variety of strong authentication solutions such as digital certificates, smart cards, USB tokens, and biometrics. In addition, Unified Authentication can be seamlessly integrated with leading access control and directory applications.

The VeriSign® Identity Protection (VIP) suite of services is designed to strengthen and protect consumer's digital identities and is for enterprises that interact electronically with consumers' personal data. The VIP suite is comprised of VIP Fraud Detection Service and VIP Authentication Service. These complementary services form a flexible, layered solution that provides both visible and invisible mechanisms for securing online transactions and preventing identity theft. VIP Fraud Detection Service provides invisible server-side monitoring capabilities. VIP Authentication Service provides a more visible, standards-based strong authentication solution for online commerce applications. Both services help ensure that a person is who he or she claims to be.

+ Learn More

For more information about VeriSign® Security Services, please call 650-426-5310, email enterprise_security@verisign.com, or visit us at www.Verisign.com.

+ About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at www.verisign.com.

Visit us at www.Verisign.com for more information.

This Solution Overview provides only a general description of VeriSign services for informational purposes and does not comprise a legal opinion or representation regarding the status or sufficiency of the VeriSign services under any applicable law. Customers should obtain independent legal advice on the scope and applicability of any legal requirements to which they may be subject.

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. IBM and Tivoli are trademarks of IBM Corporation. All other trademarks are the properties of their respective owners.