

California's Breach Disclosure Law Solution Overview



Entrust
Securing Digital Identities
& Information

A National Issue: California's Breach Disclosure Law

Solutions to Protect Data and Help Prevent SB1386 Disclosures

In response to the dramatic rise in identity theft and privacy concerns across the country, in 2002 the California legislature passed a Breach Disclosure Law, commonly known as SB1386¹. This law, in effect as of July 1, 2003, applies to all organizations with California customers, thereby creating implications for companies across the US. Under this law, companies and government agencies are required to notify customers if **their unencrypted personal information** has been acquired by an **unauthorized entity**.

In order to avoid the negative consequences resulting from notifying customers of a cybersecurity breach, companies and government agencies need to put measures in place, such as encryption and access control, to help protect personal information from unauthorized disclosure. Entrust solutions for **securing digital identities and information** can provide a way for organizations to proactively protect data while enabling new and extended business practices.

Avoiding having to issue notifications as required by CA1386 involves more than just protecting data at rest. Data should be protected throughout its lifecycle, including during:

- data submission via forms, web or e-mail
- data access via forms, web or e-mail
- data storage on workstations, databases, and e-mail servers

Entrust provides security solutions, including those with end-to-end encryption capabilities, to address data protection at all these stages of the data lifecycle process.

Beyond encrypting data in transit and at rest, organizations also have the need to implement **access control** measures to help verify that only authorized users can see personal customer information. This demands a centralized mechanism for defining and auditing access policy that complements organizational policy. This also involves assigning users specific access privileges to specific applications based on the individual's role in the organization, with decisions being made in accordance with a predefined workflow process. Likewise, when an individual's role changes or he or she terminates his or her relationship with the organization, processes must enable the user's access to be updated (or removed) accordingly.

From SB1386:

"This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

SB1386 defines "personal information" as a person's name in conjunction with his or her:

- social security number
- driver's license or state ID number
- credit/debit card or account number and access code

Entrust Security Solutions for SB1386

Security Requirement	Description	Solution
Data Submission	Via forms, web or e-mail	Secure Identity Management, Secure Messaging, Secure Data
Data Access	Via forms, web or e-mail	Secure Identity Management, Secure Messaging, Secure Data
Data Storage	Workstations, databases and e-mail servers	Secure Messaging, Secure Data
Policy and Audit	Deploying and managing identities across applications	Secure Identity Management

¹ Complete text of the bill can be found at: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Entrust Solutions to Protect Data and Help Prevent SB1386 Disclosures

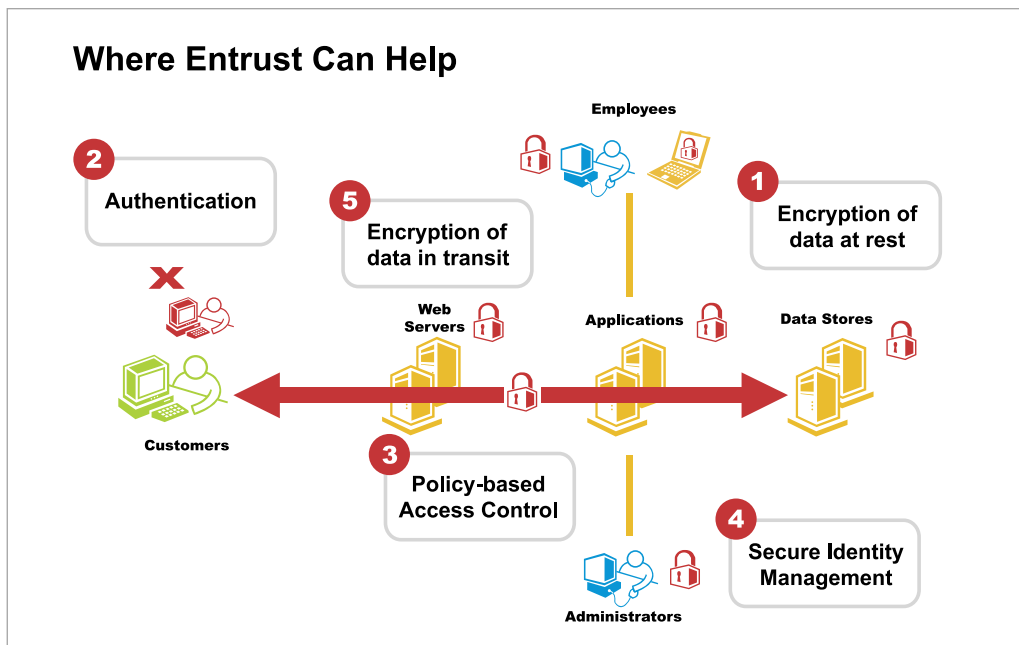
Beyond the Perimeter

To adequately secure their networks and online transactions, enterprises and governments need to deploy a variety of IT security products and capabilities. Traditionally, most organizations have focused primarily on securing the perimeters of their networks by using firewalls, intrusion detection, and anti-virus software. While each of these types of security is important for protecting networks from malicious intruders and software, none of them is effective at enabling businesses and governments to secure and protect identities and information while **transforming interactions** with customers, partners, and employees to drive new opportunities for productivity, revenue, and cost-effectiveness. Ultimately, businesses and governments interacting with constituents have the following fundamental requirements:

- they have to know who they are dealing with to ensure **accountability** and **integrity** for all types of information, including transactions.
- they need **privacy** for personal information (to prevent issues like identity theft, for example) and **confidentiality** for other types of sensitive information (for example, business plans, partner agreements, customer lists, ...).
- These essential requirements exist regardless of whether interactions occur in the physical or digital world.

To meet these business requirements in the digital world, Entrust provides the following capabilities across a broad range of solutions:

- authentication to ensure that users accessing applications are who they claim to be
- authorization to ensure information is only accessible to those that have a right to see it
- digital signature to ensure the integrity and authenticity of information
- encryption to ensure that information remains private and confidential as it travels across the network and wherever it is stored



For more information on Entrust solutions, please visit: www.entrust.com/solutions/