

A blurred background image of a woman in a dark blazer looking down at a laptop screen in an office setting.

Solution Brief: ArcSight ESM and SB 1386

ArcSight ESM and SB 1386 Protect Against Customer Data Security Breaches

ArcSight ESM allows companies to take charge of its security monitoring operations and protect the organization—and its customers—from an SB 1386 security breach

Highlights

- Provides peace of mind by protecting the personal and financial data of your customers
- Protects your organization from the disastrous ramifications of a SB 1386-related security breach
- Lowers successful attack rate by providing greater visibility into attacks on critical systems

Powerful Impact of SB 1386

Under a California law known as SB 1386, which took effect in July of 2003, any company in the world that collects personal or financial data on California residents is required to:

1. Notify customers when their unencrypted data has been exposed to a security breach.
2. Perform an investigation of the incident.

The impact of SB 1386 has been strongly felt since 2004. Required disclosures have resulted in a number of organizations making headlines after identity thieves penetrated their systems and obtained personal records of their customers. In accordance with SB 1386, these organizations were forced to notify tens of thousands of Californians that their records might have been compromised.

“Day after day we hear about new data breaches, each one worse than the last.”

Senator Dianne Feinstein, United States Senate

Nationwide Adoption of Consumer Protection Laws

In the wake of public outcry, similar legislation championed by U.S. Senators like Dianne Feinstein, Patrick Leahy and Charles Schumer has been proposed on a national basis to protect consumers from security breaches and identity theft.

“Day after day we hear about new data breaches, each one worse than the last,” said Senator Feinstein. “Not doing anything is not an option. It would be criminal to expose millions of additional people to the risk of their personal information falling into the hands of those who have no right to it. We need a national notification standard now.”

Crippling Costs of a Security Breach

Under SB 1386, the ramifications of a security breach involving customer data are ominous. One Forbes 100 financial services company estimates that an SB 1386 investigation would cost its organization \$6 million to \$8 million.



Beyond the high costs of investigation and disclosure, SB 1386 requirements result in damaged reputation, loss of consumer faith and bad publicity. In some cases, SB 1386 disclosures have resulted in cancelled contracts, lost revenue and class action lawsuits. Needless to say, an SB 1386 incident is unacceptable for any organization.

ArcSight Recognizes a Breach before It Causes Damage

ArcSight ESM helps companies stop SB 1386-related attacks and security breaches dead in their tracks. ArcSight serves as an early warning system to detect malicious actions before information thieves have an opportunity to target customer systems.

Take, for example, a typical Global 1000 organization. Its network emits hundreds of millions of security events per day, making malicious behavior an almost impossible task to recognize—until it's too late and the data has already been stolen.

With ArcSight ESM, however, companies can leverage security profiles to immediately and accurately recognize typical network probing and pre-attack behavior. Upon notice, ArcSight ESM adds the malicious entity to a suspicious list for tracking. If the attack escalates, ArcSight ESM's intelligent behavioral monitoring escalates the issue to security analysts, signifying that the attacker has gone beyond the typical port scan and fingerprinting methods.

Taking Action to End Security Threats

Once a security breach has been identified, your security team can quickly take the appropriate actions. Whether the attacker is an internal employee or an external malicious entity, any actions related to the incident are tracked

by ArcSight ESM to ensure that each team member is performing the necessary tasks. By automatically pulling together a composite report of these events, ArcSight ESM allows your organization to determine the attack methods and the overall threat level to customer data systems, as well as identify strategies for remediation.

ArcSight ESM gives any company the means to take charge of its security monitoring operations and protect the organization from a SB 1386 security breach. ArcSight ESM customers report vast increases in efficiency, a shortened window of vulnerability, a successful attack rate of zero on their customer systems and the confidence that they can take the right action at the right time.

About ArcSight

ArcSight, the recognized leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading global companies across all verticals—and more than 20 of the top 30 U.S. federal agencies.

For More Information

To find out how ArcSight can help you with your enterprise security management needs, contact ArcSight at info@arcsight.com, call (408) 864 2600 or visit us online at www.arcsight.com.



ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
Email: info@arcsight.com
Phone: 408 864 2600

© 2005 ArcSight, Inc. All rights reserved. ArcSight and ArcSight ESM are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 06/05