FROST & SULLIVAN

Data Security:
The Next Big Security Focus in India

Presented by
Frost & Sullivan in
Association with Websense

TABLE OF CONTENTS

Table of Charts

1. Introduction

The volume of user-generated content and data in organizations has been growing exponentially. This includes, but is not limited to, rich media content, voice and video traffic resulting from consumerization of IT, and increasing mobility. These trends correlate to more devices being connected to enterprise networks to provide anytime-anywhere information access and support bring your own device (BYOD) in the corporate culture—all contributing to the era of "big data."

The importance of data to consumers and business decision-makers is huge. Consequently, with increasing amounts of data in an organization's infrastructure, the amount of storage needed to support it needs to be increased at a faster rate. As a result, accessibility, data security and value delivery have emerged as crucial factors for business success worldwide.

Today, where petabytes of data are being generated every second, the need to accurately identify big data and protect its confidentiality has become a prime concern. Efforts to monitor and protect confidential data and intellectual property and safeguard it from insider threats, malware, hackers and advanced persistent threats (APTs) are assuming pivotal importance.

2. Data Security: The Next Big Thing?

Data explosion and advent of big data are phenomena, the result of economic development of nations and increase in digital footprint of organizations. Business intelligence applications are being developed to convert this heap of data (either un-structured, semi-structured or structured) into meaningful information to deliver better services and achieve sustained competitive advantage.

2.1 Trends driving data explosion

Data explosion is not only limited to the growing need for digitization, but also, to a greater extent, to emerging technologies and trends that are impacting the information technology landscape today.

a. Proliferation of mobile devices accessing corporate data

As data is increasingly becoming an essential component of wireless communication, smartphones, tablets and other data-centric devices are making a foray into the business world in a big way. Today's mobile workforce uses myriad devices to improve productivity and flexibility. According to Frost & Sullivan, smartphone and tablet PC penetration in India will register compound annual growth rates (CAGRs) from 24.8 percent in 2011 to 106.7 percent in 2017. This increasing mobility and surge of portable devices and ultra-books is resulting in growth of data traffic per device, adding to the magnitude of generated data that flows through any corporate network.

b. 'Big data' invasion

Companies are generating large amounts of information about customers, stakeholders and suppliers, and huge volumes of data are being generated every second. Contributing further is the need for digitization of text, music and video into rich media content. Data is also plentiful due to enterprises that use social media to connect consumers with their brands. Other principal technology trends that feed on big data are web services that are enabling data accessibility via the Internet and cloud storage, and virtualization, which is raising performance at a lower cost by letting a single server function as multiple computers. This advent of big data is pushing enterprises to invest in business intelligence and analytics like never before.

c. "Always on" networks with seamless connectivity

Another significant trend is the always-networked enterprise. The increase of wireless and networking capability in handhelds and portables has resulted in connectivity of workgroups to the main corporate network at anytime and from anywhere. Trend of extended office and workgroups has resulted in the need for continuous access to enterprise data. In addition, the blurring of professional and personal lives combined with the need for constant connectivity further defines today's enterprise workplace.

d. Adoption of cloud services

For ease of use, scalability and lower total cost of ownership (TCO), cloud solutions are increasingly being adopted. On-premises equipment and related services are gradually being complemented by such cloud offerings. In addition to the advantages of providing a more efficient and scalable way to store data, the increased adoption of cloud computing will continue to stimulate astronomical growth in storage requirements resulting from a data explosion.

e. Globalization leading to cross-border data flow

Globalization is not a new phenomenon, but has become a buzzword with the explosion of information taking place around us. Organizations becoming increasingly global translates into significant cross-border flow of data. Adhering to compliance regulations across geographies and protecting sensitive data from leakage has become a behemoth task. As levels of risk tolerance across facilities and locations are different, a weighted approach is needed to tackle risks.

2.2 Need to secure corporate data

Though data explosion has its positive attributes, issues such as categorizing data and attributing proper and sufficient security to it are a growing concern. Magnitude of threats to corporate data is increasing at an alarming rate, largely due to factors not limited to introduction of novel attack vectors, but also employee avarice and a global playing field.

Chart 1 highlights some key factors that signify the need for securing a corporation's data.

Chart 1: Factors Compelling Need to Secure Corporate Data

Source: Frost & Sullivan

a. Evolution of sophisticated threat vector

Along with increasing risk of zero-day vulnerability, threat vectors are becoming highly sophisticated. New attack paths are appearing almost every day. Introduction of security in the early stages of system development life cycle (SDLC) and information systems development can thwart proliferation of threat vectors, but only to an extent.

With limited applications designed with security in mind, increasing security threats continue to haunt the enterprise network. And security threats are not just limited to application security; they involve APTs and blended threats as well. Hence, a single layer of security with anti-virus firewalls and intrusion detection or prevention solutions is no longer sufficient. Today, developing foolproof software is a necessity, not an option.

b. Introduction of new technologies

Technologies that improve quality and enhance ease have revolutionized modern work culture. Collaboration, online meeting, web conferencing, video conferencing and corporate instant messaging have enabled geographically dispersed teams to come together in real time, thus saving costs and enhancing work quality. But, these very same technologies are carrying malware and enabling leakage of sensitive data.

In addition, due to proliferation of mobile devices, emphasis on end point security has to be heightened due to exposure of devices to new environments. This is resulting in the adoption of application control and privilege management solutions within organizations. As the end-node problem has been magnified with introduction of BYOD, modification of security policies especially for the way data is accessed, stored and retrieved needs to be re-evaluated. This calls for robust end-to-end deployment of data security initiatives.

c. Governance, risk and compliance

Due to financial implications caused by recent high-profile data leakage incidents, enterprises are facing increasingly strict governance and compliance requirements. Adherence to such items is required not only to continue the business, but also generate value. Failure to protect the organizations' assets, especially critical data, may lead to heavy penalties and even disciplinary action.

Hefty fines can be imposed for non-compliance, especially in the financial sector and verticals such as telecommunications. In several instances (especially in health care institutions), penalty from the government and affected individuals (e.g., patients) could be so detrimental to the organization that shutting down of operations and filing for bankruptcy are probable outcomes.

d. Protecting against insider threats

Sensitive information is accessed by employees as a part of their daily jobs. But when the same information is sent out of the corporate network, it becomes a breach of organizational interests. Unauthorized access of sensitive information by insiders is another menace that organizations are finding hard to keep up with due to proliferation of mobile devices and initiation of BYOD. Malicious activities by dishonest employees for financial gain or backlash by disgruntled employees can increase the risk of unlawful insider activity. It is true that access controls and safeguards are implemented so as to curtail such behaviour. But with vulnerabilities and security gaps evident, insiders can commit breaches with ease, using legitimate means. Social engineering is evolving as yet another risk.

e. Loss of valuable intellectual property

Innovation through product technological leadership is critical for enterprises, especially in the high-tech vertical. Companies invest substantially in R&D, and their intellectual property must be safeguarded. Loss of IP is highly detrimental from both financial and market-positioning perspectives. Such losses can often be from theft of source code, blue prints and design documents.

f. Protecting reputation and maintaining competitive advantage

When sensitive data is lost and the data security breach is announced, there is loss of enterpise reputation and goodwill. Organizations need to draw attention to the irreparable damage that occurs, and this often has detrimental consequences such as loss of stakeholder and customer confidence, drop in share value and loss of business, to name a few; the additional cost of the security lapse itself is added to this. Recent incidents in India such as Chinese hackers' breach of Indian Navy's computers, Microsoft's Indian web store security breach and recent hacks on Government portals such as High Commission of India, have had quantifiable consequences, which run into millions of rupees.

2.3 Enterprise challenges

While enterprises are getting involved more than ever in protecting data, there are several challenges associated with the evaluation and implementation of a successful data loss prevention (DLP) strategy:

a. Cost of compliance and security implementation

Adhering to compliance has been a key reason for growing information security investments. Non-compliance has heavy penalties. Movement of the organizations' focus from compliance to security has been observed over time. It is true that there is no quick fix for the gaping security flaws in organizations. But, even with tightening security budgets, investment in current solutions is vital for enhanced protection of enterprises. The regulatory environment is becoming increasingly stringent, and compliance increasingly arduous.

b. Return on security investment (ROSI)

As return on security investment (ROSI) is not as straightforward as return on investment (ROI) of a financial asset, convincing executive management to invest in security solutions is becoming increasingly difficult. Even though it is understood that data security solutions are a "must-have" and no longer "good-to-have," adequate spend on security still remains a challenge, as it is still considered an expense rather than an investment in protecting business goals.

c. Management commitment

Commitment from executive management and their continued focus on fortifying security posture are essential for successful data security deployment. Without vision, success of a data security project is hard to achieve and the entire effort may not produce results commensurate with the investment in security.

d. Data security implementation is more of execution-driven success than technology-driven success

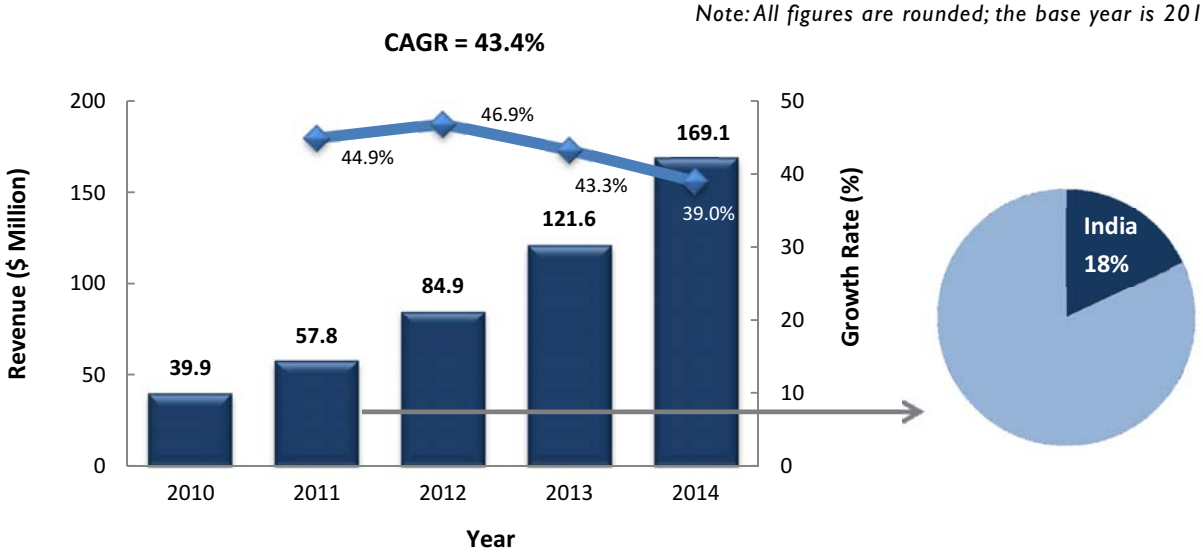
As a preliminary step, data classification and assigning security levels depending on sensitivity of the data are crucial to successful implementation of a DLP solution. As security levels change with data movement across its life cycle, commensurate levels of security classification is a challenge. Tailoring policies and regular expressions are vital to prevent an inordinate number of false positives.

2.4 Adoption trends

Over the years, the definition of DLP technology continued to evolve, as complexities in implementing a full-fledged end-to-end DLP deployment meant that many enterprises in India were more inclined to start with smaller and more basic DLP engagements. As such, many enterprises looked at having basic DLP capabilities being introduced into their security setup, and opted for a feature-based approach towards DLP adoption. Chart 2 depicts the Asia Pacific DLP market revenue statistics from 2010 to 2014, highlighting India's market share.

Chart 2: Asia-Pacific DLP Market: Revenue Forecasts, 2010-2014

Note: All figures are rounded; the base year is 2010.



Source: Frost & Sullivan

Among all Asia-Pacific markets, India is leading in adoption of DLP for 2011. The Indian DLP market experienced healthy growth in 2011, with several industry factors driving the importance of data security. Security compliance regulations by the government were implemented and there was high level of awareness of the importance of information security in the new business environment. This was chiefly due to rising concerns in online banking, enterprise mobility, Web 2.0 technologies and mobile computing, along with virtualization and cloud technologies. Demand for IT security became vital for enterprises to protect their virtual properties such as sensitive data or company reputation, and DLP technologies came to the fore as ideal solutions for the same. A few enterprises also grew more wary towards threats emanating from insiders due to the growing prevalence of the BYOD phenomenon in the enterprise arena.

Moreover, as awareness of technology was boosted by more publicized data loss incidents taking place in India, enterprises realized the urgency of adopting DLP technologies to not only protect assets, but also reputations. Dominant adopters were typically still verticals, which were particularly concerned about the integrity and security of corporate data.

As more enterprises express concerns about data security and risk management, adoption of DLP is expected to grow steadily. Frost & Sullivan estimates that DLP adoption in the Asia Pacific region is estimated to register a CAGR of 43.4 percent between 2010 and 2014.

3. Compliance and Government Regulations*

One of the reasons for the heightened need for data security initiatives is the mandate to adhere to several guidelines and the norms set forth by regulators. These include:

- The Information Technology Rules, 2011 (four sets of rules have been introduced under the Information Technology Act, 2000) by the Indian Government addressing the industry's concerns with data protection, creating a mandate for data protection and actions on cybercrime. Sensitive personal information of consumers, in digital form, is required to be protected through reasonable security practices by corporates. Moreover, the Act makes it mandatory for the organization to protect data under contracts. There is a defined penalty for breach of confidentiality and privacy.

- The Reserve Bank of India's guidelines on usage of information security to safeguard financial data have come into force in 2012, and swift implementation has been witnessed due to its fast-approaching deadline. Implementation of best practices is another reason behind the thought for investment in data security.

- Financial institutions came under Sarbanes-Oxley (SoX) and Gramm-Leach-Bliley Act (GLBA) requirements and were scrutinized for their consistency and adherence to the norms. This mandates them to adhere to the regulation and implement data security.

- Healthcare facilities like hospitals and pharmaceutical houses are regulated by the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act that mandate the use of security and privacy safeguards. Protected health information breach reporting has been a major move toward ensuring compliance and identifying incidents and breaches.

**Not intended to be legal advice. Please consult an attorney for legal advice.*

4. Case Study: Bharti Airtel

Executive Summary

Profile
Bharti Airtel Limited is a leading integrated telecommunications company with operations in 20 countries across Asia and Africa. Headquartered in New Delhi, India, the company ranks amongst top 5 mobile service providers globally in terms of subscribers. In India, the company's product offerings include 2G, 3G, and 4G services, fixed line, high speed broadband through DSL, IPTV, DTH, and enterprise services including national and international long-distance services to carriers.

Industry
Telecommunications

Challenge
Safeguard sensitive and company proprietary information and managing data loss exposure while having to comply with information privacy regulations

Solution
Websense Data Security Suite

Result
Increased pro-active and reactive handling of data leakage

Challenge

- The sheer geographical spread of Bharti Airtel Limited necessitated tighter monitoring and control over corporate data. In addition, there was greater need for control due not only to the evolving threat landscape, but also to legal and regulatory requirements peculiar to the telecommunication sector, as well as the IT (Amendment) Act.
- With the introduction of mCommerce into the telecommunication sector, the controls have justifiably been made more stringent. Bharti Airtel's venture into mCommerce with Airtel Money required data leak prevention to ensure robust security and compliance.
- Evolving trends such as remote and mobile workers have made traditional perimeter controls insufficient, thereby leading to the embrace of data-centric solutions that remain effective wherever data goes.

Solution

Recognizing the need for a comprehensive data loss prevention (DLP) strategy to address the above challenges, Bharti Airtel began evaluating data security vendors in 2009. The telecom operator sought a partner who could provide a complete solution with synergistic capability at both the network and end point layers. Websense, with its comprehensive solution and strong presence in India, was selected as the preferred partner. The Websense solution included the following highlights:

- Websense® Data Security Suite was deployed across all web and mail gateways and across more than 20,000 end points covering all offices of Bharti Airtel across India.
- Four integrated modules at hub level were implemented and managed under a single policy framework, which together provide visibility and control over network and end point data loss. The solution includes both incident management and remediation.

Testimonial

"While there were a few vendors offering compelling DLP products, in most cases strong presence in India and product integration were missing. After evaluation, we at Airtel were convinced that the DLP product from Websense suited our requirements of converged policy enforcement on network and end-points, strong and nimble support in India, and seamless integration with other DRM products."

- Aman Nugyal, Chief of Technology Assurance, Bharti Airtel

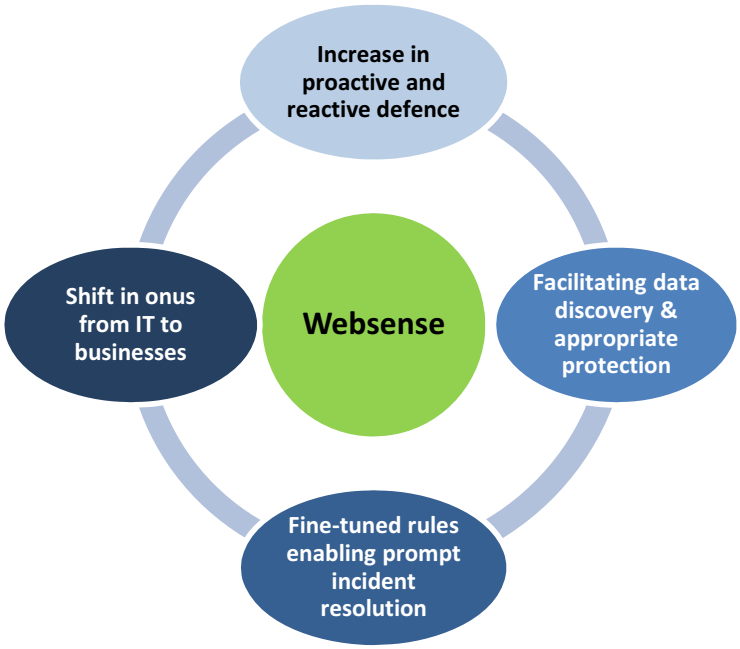
Of additional importance was Websense's robust change management and responsiveness coupled with best-in-class support, especially since Airtel was an early adopter of the solution. The technical expertise along with the vendor's strong reputation in the country strengthened its relationship with Bharti Airtel.

Result

Data Security Suite has provided numerous benefits to Bharti Airtel, including:

- **Enhanced proactive and reactive defences against data leakage through prompt alerts for anomalous action.** In particular, proactive prompts at end points for data-related requests led to about 60 percent of attempts being prevented.
- **The discovery and identification of sensitive data across the network.** Data discovery enabled the deployment of appropriate protection. As a result, risk mitigation was substantially improved. Breaches were dealt with more cautiously and effective consequence management was put in place to address these.

Chart 3: Business Value Provided by Websense Data Security Suite



Source: Frost & Sullivan

- **An improved crossover error rate due to the minimization of false positives and negatives.** This has made incident detection more effective and has helped prevent the "cry wolf" syndrome in the environment.
- **The setting of rules and prompt resolution of incidents has shifted from traditional IT to business units.** This solution has enabled business units to take charge of their data to safeguard their business and enhance compliance.
- **The Websense deployment enabled Bharti Airtel to successfully roll out its DLP strategy.** Bharti Airtel can now stay ahead of data threats, strengthen the culture of responsibility in handling of sensitive data, and enhance overall compliance.

5. Conclusion/Recommendation

The notion of security being a burden can change only when it is understood by organizations that robust security ultimately results in compliance and not vice versa. It must be realized that there is no silver bullet for securing enterprise data and deployment of DLP is a step towards safeguarding the enterprise.

While it is hard to justify the ROSI in a limited time frame, it is certain that a successful DLP implementation can have beneficial effects over time by reducing the number of breaches and protecting corporate data. A range of factors deliver business value to stakeholders, and security of organizational data is one of them. Business value can be derived from DLP investments; below are a few key points that aid in this journey toward achieving a secure enterprise through good practices in data security:

a. DLP should not be treated as a security solution, but as a business driver given its impact on organizations' competitiveness, compliance, brand and revenues.

b. Organizational processes are the key to the success of DLP implementation. Without the underlying processes, DLP implementation would just be like any other unproductive investment.

c. Every organization is different. Rather than relying on the bundled policies, introduction of content awareness using policies tailored to the organization would benefit the most.

d. Data classification and categorization are essential for assigning specific protection profiles for the data. This has also necessitated use of rigorous controls for its security. Base lining of these controls is also being looked into, so as to aid in bolstering security.

The principle business objective of data security is managing data loss exposure. Absolute security does not exist in practice; minimizing the residual risk to the organization should be the ultimate aim.

About Websense® Data Security Suite

Websense Data Security Suite includes four integrated modules managed under a single policy framework, which together provide visibility and control over network and endpoint data loss, as well as comprehensive data discovery across enterprise storage systems.

- **Websense Data Monitor:** Monitors for data loss on network (e.g., web, email, FTP).
- **Websense Data Security Gateway:** Enforces automated, policy-based controls to block, quarantine, route to encryption gateway, audit and log, or notify users of violations.
- **Websense Data Endpoint:** Monitors and enforces automated, policy-based controls for data in use via applications and peripheral devices on end points; provides local discovery and classification of confidential data.
- **Websense Data Discover:** Discovers and classifies confidential data stored in enterprise repositories, with customizable remediation action including file removal. Data Security Suite is the only solution with native enforcement of web (HTTP), secure web (HTTPS), and email (SMTP) traffic, reducing the need for additional expensive third-party proxy solutions.

Data Security Suite integrates with any Websense web security solution, which routes outbound web traffic to Websense Data Monitor for analysis.

How It Works

Websense data security solutions secure organizations against a wide range of data loss scenarios with a single policy framework for network and endpoint DLP and confidential data discovery using both local and network scans.

These solutions are available as individual modules, or an integrated suite, enabling the highest level of deployment flexibility. The individual modules available in Websense data security solutions offer specific DLP capabilities to suit organizations' unique needs.

Data Security Suite includes all the modules offering a comprehensive solution. Additionally, it embeds Websense enterprise-class DLP technology into the web and email security solutions to enable organizations to easily adopt an expandable, fully capable solution to help prevent inbound threats as well as manage outbound risks associated with data loss and regulatory compliance. Whether starting from the DLP solutions embedded in Websense web or email solutions or from deployment of individual data security modules, customers can quickly expand their deployment to Data Security Suite to secure other channels as well as leverage DLP capabilities.

About Websense

Websense, Inc. (NASDAQ: WBSN) is a global leader in protecting organizations from the latest cyber attacks and data theft. Websense® TRITON™ comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based Websense TRITON solutions.

For more information, contact:

Manish Bansal | E: mbansal@websense.com | P: +91 9819688007

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact us: Start the discussion

For more information, contact:

Ekta Aggarwal | E: ekta.aggarwal@frost.com

Legal Disclaimer