

A FORSYTHE CASE STUDY

Data Loss Prevention: Security Technology Assessment

A Fortune 250 Energy Company

Business Challenge

The alarming rate of network breaches and stolen or misplaced laptops, portable devices, and media has caused many organizations to be concerned about the potential for transmission of sensitive information to unauthorized recipients outside the internal network. These issues were at the top of the agenda for the CIO of a major regional energy company. He sought to evaluate his organization's strategy for mobile-device encryption, e-mail encryption, and database monitoring, as well as their overall approach to data loss prevention (DLP). The CIO determined that experienced, objective, outside help was needed to analyze the environment and provide the best strategy and plan to protect and monitor its sensitive information.

The CIO's primary challenges were to:

- Determine encryption requirements for transmitting sensitive information to recipients outside of the network, whether from desktops, internal storage or portable devices
- Monitor information stores to pinpoint leakage of confidential information and unauthorized manipulation of confidential databases
- Determine the most appropriate technology solutions and the associated product and support costs
- Make the necessary policy and process changes to support the DLP strategy

Many DLP solutions exist. Most provide policy-based monitoring and enforcement for the movement of information within the internal network and on desktops, or if it traverses the corporate boundary. DLP products can be agent-based, network-based, or both. They typically monitor and/or block activities for information containing intellectual property, trade secrets, financial data, personal data, and other proprietary data. They apply technologies like fingerprinting, lexical analysis, and behavioral analysis to multiple protocols and on the various conduits through which sensitive business information can travel.

Solution

Through interviews with the CIO and key stakeholders, Forsythe gathered background on the company's supported platforms, operating systems and architecture; the types of information considered sensitive to the organization; the information lifecycle; and whether the information would be stored on the internal network, copied or stored on mobile systems or portable storage devices, or transmitted outside the organization. To gain additional context, Forsythe also reviewed the organization's information security policies, standards, practices and technologies related to encryption and information protection. From this, a proposed DLP strategy and architecture were created.

Forsythe researched and identified specific vendors and products that could meet the defined requirements. The research included a comparative analysis of the requirements for each security technology area: solutions for data-at-rest, data-in-motion, e-mail encryption, end-point encryption and database monitoring. Possible technologies were measured against the proposed architecture and against key criteria, including industry leadership, product features and cost.

Forsythe recommended a phased implementation plan for the proposed solutions. (Whenever a large and complex environment is interested in implementing multiple technologies, it is better to do this with a well-planned, phased implementation approach. If an enterprise were to try to implement several similar technologies at the same time, they may over-commit internal resources, leading to a higher rate of mistakes and errors.) As part of the phased implementation, Forsythe also recommended that some proof-of-concept trials be performed. This step would bring clarity to very specific requirements that may need to be tested before a full implementation or purchase occurs.

Results

Forsythe provided this client with a much more detailed understanding of their underlying requirements for information protection, and the specific technologies and investments that would need to be made to implement them. By identifying and benchmarking suitable products, this organization was able to refine its plans using unbiased, vendor-neutral technical recommendations to meet the strategy.

Forsythe's recommendations included commentary on the technologies and products available in the DLP space, which are all in a transitional or adolescent phase of maturity in the marketplace. Vendors continue to form partnerships with one another, or to be purchased by larger players. In addition, many new technologies are being developed and implemented in both the DLP and database monitoring sectors.

Armed with current knowledge, this engagement provided a go-forward plan that not only gave the

company a deeper understanding of sensitive information flows and potential leakage points, but also provided a customized architecture for addressing them. This enabled the CIO to move confidently forward to the proof-of-concept and implementation stages of his protection strategy.