Trustwave®

Trustwave Data Loss Prevention

Trustwave's Data Loss Prevention (DLP) Solution is a content discovery and control solution designed to monitor and prevent data loss across your network.

Overview

Every day, companies are faced with demands for protection against data exfiltration. First, regulatory and industry mandates require certain organizations to inventory sensitive data or monitor and mitigate data exfiltration. Second, companies have found their confidential source code posted on the Internet, hackers have gained access to customer data, and executives have been charged with stealing confidential information. Government regulations, hacker attacks and unauthorized corporate postings have made it imperative that a business be aware of exactly what is transmitted over its corporate network. In today's digital economy, averting this kind of risk is crucial to protecting the data and reputation of any business.

Data Risk Solution

Recent high profile breaches have been accomplished with malware that ultimately allowed attackers to download sensitive information. The theft of customer records, confidential information and valuable intellectual property can result in a damaged reputation, loss of customer trust, and a multitude of fines and fees. Trustwave's Data Loss Prevention (DLP) solution helps prevent the outflow of such valuable data. It is the outbound content control solution that enables businesses of all industries to gain complete visibility into all risks of potential data leakage, whether inadvertent or malicious, and to control violations before they occur.

An extensive suite of detection and analysis capabilities, Trustwave's DLP Solution identifies, classifies, correlates, captures and mitigates information outflow. With visibility and control across the entire network, Trustwave's DLP provides maximum protection against state and federal compliance violations, customer data loss, intellectual property theft, insider hacker activity, fraudulent employee lawsuits, inappropriate Internet usage and corporate espionage.

Trustwave's DLP solution helps you to gain immediate visibility and control over:

- The unauthorized release of private customer information
- The leaking of confidential documents
- Unencrypted transmission of personal health information (PHI) or cardholder information
- The posting of financial reports and source code
- Insider hacker planning and activity
- Internet misuse causing legal exposure
- Damaging blogs by a trusted insider
- Resignation and intellectual property theft

The DLP Solution

Preventing exfiltration begins with a comprehensive solution to answer 3 fundamental questions - Where? What? Who? The Trustwave DLP products—Monitor, Protect and Discover—provide visibility and control of sensitive data throughout the entire enterprise. These products comprise the Trustwave DLP solution to provide the following capabilities for protection of your valuable information assets:

Monitor Trustwave DLP Monitor analyzes all Internet-based communications and attachments including e-mail, IM, P2P file sharing, chat rooms, blogs, Web postings, FTP and Telnet for violations of a company's corporate governance, compliance and acceptable use policies. Utilizing Trustwave's proprietary suite of content detection technologies and more than 70 predefined Risk Categories, Monitor detects and monitors the insider threat to help you protect an organization from compliance, productivity, reputation and legal risk.

Protect Defend against unauthorized data leakage over many channels with DLP Protect. Based on Trustwave risk categories, custom categories or CANDL (Content Analysis Description Language) categories, policies can easily be set to control how information flows out from the organization. This solution is available for both e-mail and Web:

- **DLP Protect E-mail** provides automatic encryption, block, quarantine or self-compliance capability for e-mail communications and attachments identified as violating corporate and compliance policies. Self-compliance and user alerts can be used to train users on corporate policy; alerts inform the sender of a policy violation and that encryption, blocking or quarantine, was performed.

- **DLP Protect Web** automatically blocks HTTP, HTTPS and FTP traffic violating corporate and compliance policies. Deployed with an ICAP-enabled proxy server, Protect Web can help save organizations from expensive compliance violations, litigation and theft of intellectual property that could harm future revenue streams.

Discover Gain visibility into what sensitive data you have (structured and unstructured) and where it located across the enterprise. DLP Discover analyzes data at rest utilizing the Risk Categories to identify and capture violations of the corporate and compliance policy, and provide additional "proof positive" evidence. It will also remediate risks from data loss by moving, quarantining and encrypting sensitive information.

Visibility and Control

Most content monitoring solutions provide visibility into only a fraction of the risk, leaving your organization still open to attack. With Trustwave, an organization gains visibility of all insider risk to identify potential threats, investigate them before an event becomes an issue and control them without impeding the flow of business. Trustwave's visibility and control provides organizations and corporations protection against compliance violations, customer data loss, intellectual property theft, Internet abuse, insider hacker activity, sexual harassment, racism and other forms of insider risk.

Trustwave also provides visibility into the location, access and movement of sensitive data based on sophisticated content classification and analysis technologies. An enterprise can apply its data security policies to govern sensitive data movement within or out from the network and also be alerted to potential leakage events. By correlating the risk in different areas,Trustwave's DLP suite is the solution to provide complete visibility and control of malicious or inadvertent insider activity.

Advanced Control In order to control content, you must first identify it. Working in combination with the content detection technologies and Risk Categories, Trustwave provides content control without impeding the flow of your business with the following features:

- Automatic E-mail Encryption for compliance and confidential documentation protection
- Unique self compliance alerting senders to policy violations and allowing them to decide whether to continue the action
- Automatic protections of data upon detection for greater security and less manual intervention.
- E-mail Quarantine and Block, to immediately stop unauthorized transmissions
- Enforcement of persistent protection of the data
- Minimized disruptions to user workflow

Investigation Management The Trustwave DLP solution goes beyond basic monitoring and control. It provides investigative reporting and analysis tools to help investigate a violation after it has been identified. Trustwave's suite of investigation management tools includes reporting, violation identification, and "proof-positive" evidence collection and case management. In addition, Trustwave DLP simplifies management and operations with dashboards, robust event search and archiving to allow reviewers to quickly identify risk information that empowers them to take appropriate action.

Real-Time Identity Match—Identity Match is a powerful technology which instantly associates the individual with the violation, regardless of protocol, handle or alias used. Identity Match captures user identity, host name, and logon time and scales with large multi-site enterprise deployments.

Features of the Trustwave DLP Solution

- Monitors all TCP traffic and stored data
- Monitors content, user, system and drive activity
- Protects content in motion and at rest
- Stops damaging information outflow
- Over 70 risk categories, out-of-the-box
- Easy custom category creation
- Full and partial file matching
- Exact content match
- Correlation of suspicious activity
- Advanced search capability
- Highlighting, risk dashboards and reporting
- Sophisticated reporting and analysis to support forensic investigation
- Real-time identity match
- Flexible policy and data management
- Simple integration with SIEM solutions

Trustwave®

For more information: https://www.trustwave.com