DATA LOSS PREVENTION FOR GOVERNMENT

AVOID LOSS AND STAY COMPLIANT

Trustwave Data Loss Prevention (DLP) Solution is a content control solution designed to monitor and prevent data loss across government networks and supports both FISMA Compliance and Continuous Monitoring.

OVERVIEW

The cyber threat to the U.S. critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. Trustwave Data Loss Prevention (DLP) solutions are engineered to not only help government agencies avoid data loss that can lead to compliance violations and intellectual property loss, but also to provide the versatility to protect sensitive information. With predefined compliance packages that specifically address government standards such as FISMA, Continuous Monitoring, NIST 800-53, DoD 8500.2, BYOD and the new Presidential Policy Directive 21 (PPD 21), the Trustwave suite of solutions helps to ensure that sensitive and confidential data is shared, used, stored and transmitted appropriately—while helping to ensure that relevancy is not diminished with inaccurate data discovery.

COMPLETE INSIDER RISK SOLUTION

Based on information reported by The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), malicious code continues to be one of the most widely reported incident types across government agencies. Measures need to be taken to identify and mitigate weaknesses in the federal infrastructure that can be exploited by malware. Improper usage, policy violations, and non-cyber incidents are all factors which can lead to the unauthorized disclosure of Personally Identifiable Information (PII)—and/or sensitive information. Trustwave Data Loss Prevention (DLP) solution helps prevent the outflow of such valuable data. It is the only inbound and outbound content control solution that enables government agencies to gain complete visibility into all insider risk, whether inadvertent or malicious, and to control violations before they occur. Offering an extensive suite of detection and analysis capabilities, Trustwave DLP solution also identifies, classifies, correlates, captures and stops information outflow. With visibility and control across the entire network, Trustwave DLP provides maximum protection against compliance violations, data loss, intellectual property theft, insider hacker activity and inappropriate Internet usage.

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

- The unauthorized release of Personally Identifiable Information (PII)
- The leaking of confidential and sensitive documents
- Insider hacker planning and activity
- Internet misuse
- Damaging blogs by a trusted insider
- Intellectual property theft

THE DLP PLATFORM

Complete security begins with a comprehensive platform. The Trustwave DLP solutions—Monitor, Protect and Discover—provide total content control throughout the entire government enterprise from the desktop to the network perimeter. This integrated and scalable platform is comprised of these solutions for maximum protection over your valuable information assets.

Monitor
Based on the patent-pending Intelligent Content Control Engine, Trustwave DLP analyzes all Internet-based communication and attachments including e-mail, IM, P2P file sharing, chat rooms, blogs, Web postings, FTP and Telnet for violations of an agency's governance, compliance and acceptable use policies. Utilizing the Trustwave proprietary suite of content detection technologies and more than 70 predefined risk categories, Monitor helps to instantly identify, capture and control the insider threat to protect government agencies from compliance, productivity, reputation and legal risk.

Protect

Defend against unauthorized data loss over many channels with 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 outside of the network. This solution is available for both e-mail and Web:

- Protect E-mail provides automatic encryption, blocking, quarantine or self-compliance capability for e-mail communications and attachments identified as violating government compliance policies. Self-compliance and user alerts can be used to train users on government data protection policies; to inform the sender of policy violation and to notify that encryption, blocking or quarantine was performed.
- Protect Web automatically blocks HTTP, HTTPS and FTP traffic violating government compliance policies. Working in conjunction with an ICAP-enabled Proxy Server, Protect Web can help save government agencies from costly compliance violations, litigation and theft of intellectual property that could cause harm to mission-critical operations.

Discover

Investigate data-at-rest to discover additional violations residing in stored data on desktops, laptops and file servers. Based on the Intelligent Content Control Engine, Discover analyzes data-at-rest utilizing the risk categories to identify and capture violations of the government compliance policy, and provide additional “proof positive” evidence.

VISIBILITY AND CONTROL

Most content monitoring solutions provide visibility into only a fraction of the risk, leaving your agency’s network still open to attack. With Trustwave, a government agency 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 network operations. Trustwave visibility and control provides government agencies maximum protection against compliance violations, data loss, intellectual property theft, Internet abuse, insider hacker activity and other forms of insider risk.

Trustwave also provides content, user and system visibility, drives activity to control sensitive data outflow and alerts to potential security breaches or laptop theft. By correlating the risk in different areas, Trustwave DLP suite is the only solution to provide complete visibility and control of malicious or inadvertent insider activity.

DATA LOSS PREVENTION

DLP helps to avoid data loss that can lead to compliance violations and intellectual property loss, while also providing the versatility needed to protect sensitive data in motion, at rest and in use.

Advanced Content 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 mission-critical operations.

- Early identification of violations with visibility and insider risk correlation
- Automatic E-mail Encryption for compliance and confidential documentation protection
- Unique E-mail and Desktop Self-Compliance, alerting senders to policy violations and allowing them to decide whether to continue the action
- E-mail Quarantine and Block, to immediately stop unauthorized transmissions

Investigation Management

The Trustwave DLP platform goes beyond basic monitoring and control. It provides a suite of investigation management tools to help with analysis, discovery and forensic analysis after a violation has been identified. Trustwave suite of investigation management tools includes reporting, violation identification, and “proof-positive” evidence collection and case management. In addition, the Trustwave DLP Management Center provides executive dashboards, powerful event search and archiving to allow reviewers to quickly identify risk information and empower them with a forensic trail to take action.

Real-Time Identity Match

Identity Match is a powerful technology that 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 government agency deployments.

DISCOVER ONCE, PROTECT FOREVER: INTEGRATED DLP AND ENCRYPTION

In addition to our leading Trustwave DLP solution, Trustwave can deliver the strongest levels of information-centric security through DataControl. DataControl seamlessly combines our DLP Discover software with state-of-the-art encryption, specifically our Smart Tag™ technology. It allows government agencies to systematically identify at-risk data and automatically protect it to reduce the risk of data breaches. With DataControl, organizations can “Discover Once, Protect Forever” the data that is critical to daily agency operations.

Advantages of Trustwave DataControl:

- Automatically protect data upon detection and reduce manual intervention requirements.
- Encrypt and protect data wherever it goes with Smart Tag™ technology.
- Enforce persistent protection on the data.
- Apply encryption and group access controls based on specific policy violations.
- Ensure no disruptions in user workflow.
- Reduce risk across government networks; even if data were to leak, it remains encrypted and thus protected.

Components of the Trustwave DLP Solution:

- Monitors all tcp traffic and stored data
- Monitors content, user, system and drive activity
- Protects content on the network, desktops and via e-mail
- 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
- Investigation management and forensic analysis tools
- Real-time identity match
- Exact replica of original event
- Flexible policy and data management

Trustwave®

Smart security on demand

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