Vontu Response to NIPP Framework

Vontu Data Loss Prevention solution enables government agencies to demonstrate compliance with DHS directives
Vontu Data Loss prevention solution enables government agencies to demonstrate compliance with the NIPP framework and DHS directives

In June of 2006, the Federal Department of Homeland Security (DHS) announced the completion of the National Infrastructure Protection Plan (NIPP). The NIPP is a framework intended to help governmental agencies and their partner organizations protect the nation’s critical infrastructure and other key resources against damage or loss due to terrorist attack, natural disaster, or other catastrophe. 14 federal agencies, called Sector-Specific Agencies (SSAs), are particularly affected, as they’re tasked with securing critical infrastructure and key resources.

The NIPP is in effect a set of blueprints, specifying key initiatives, milestones, and metrics required to demonstrate compliance with DHS directives and directs SSAs to submit Sector-Specific Plans (SSPs) to DHS within 180 days. The NIPP not only requires SSAs to secure their own internal networks against any unauthorized transmission of sensitive data that could damage the United States, but also addresses the interdepartmental sharing of secure information. Without robust data security, there cannot be the free flow of sensitive information between SSAs and their security partners that’s necessary for collaboration.

Secure information sharing requires more than just network security and/or broad-based encryption—the data itself must be protected. Government agencies must be equipped to answer questions such as:

• Can you currently assure the integrity and confidentiality of all of your sensitive information?
• If you had to begin exchanging sensitive data tomorrow with another agency, via any Internet protocol, could you do it without non-encrypted sensitive data exiting your network sight unseen?
• Do you know which laptops, desktops, data repositories, or endpoints contain the most sensitive information in your agency?
Vontu helps federal agencies protect critical information resources within the NIPP framework

Vontu’s Data Loss Prevention technology enables SSAs to reduce the risk of sensitive data loss and demonstrate compliance with DHS directives regarding critical infrastructure and key resources (CI/KR) protection. Vontu’s Federal Risk Assessment Program and Data Loss Prevention software solutions help agencies prevent malicious and unintentional data breaches regardless of whether data is stored on the network or on a disconnected endpoint, as well as prevent data from exiting any network gateway or endpoint. How Vontu specifically addresses each NIPP security activity is outlined below.

The NIPP framework

The NIPP risk management framework specifies six broad activities which, undertaken in order, represent a roadmap to achieve compliance with the DHS directives within the specified 180-day timeframe. The six activities are:

1. Set Security Goals
2. Identify Assets, Systems, Networks, and Functions
3. Assess Risks (consequences, vulnerabilities, and threats)
4. Prioritize
5. Implement Protective Programs
6. Measure Effectiveness

All six activities are integrated into a feedback loop for continuous improvement. Areas specified to be protected include: Physical (such as ports and water supplies), cyber (such as data security and network security), and human.
Activity one: Set security goals

SSAs must define specific outcomes, conditions, end points, and/or performance targets that combined will indicate “…an effective protective posture.” Vontu’s Data Loss Prevention system is an essential countermeasure to reduce the risk of sensitive data loss. Vontu’s ability to identify the unauthorized flow of sensitive data helps establish an effective protective posture at every stage of the NIPP risk management framework.

Vontu solution:
As the diagram above illustrates, the broader process of CI/KR protection is designed for ongoing and continuous improvement. Vontu supports this process by combining comprehensive risk assessment with effective data security technology:

- Vontu enables government agencies to discover unsecured sensitive data and measure their level of data security risk so they can better set security goals.
- Vontu’s Data Loss Prevention solution provides comprehensive security measures for stored data (at rest on file servers, databases, Microsoft® SharePoint®, Lotus Notes®, Documentum®, LiveLink®, web servers, Microsoft® Exchange, end-user laptops and desktops, and other data repositories); data that is being transmitted (in use) outside the agency via email, IM, Web, Secure Web (HTTP over SSL), FTP, P2P, and generic TCP; data copied to USB, burnt to CD/DVD, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications (data on the endpoint); plus robust risk and compliance reports that demonstrate risk reduction over time.

This combination delivers valuable insight on activities two through six (see below) so as to improve perspective and deepen knowledge of the real risks SSAs may face. The SSAs can then in turn better review and revise their security goals and set new ones as needed to more accurately reflect their situation, and repeat this process as necessary, further closing the loop of continuous improvement.

Activity two: Identify assets, systems, networks, and functions

In this procedure, SSAs must inventory the components that comprise their unique CI/KR security requirements and gather information about those components that can facilitate risk management.

Vontu solution:
Data flow discovery is a fundamental component of asset identification, as well as to risk assessment and goal setting. Vontu’s Data Loss Prevention solution provides insight into where sensitive data is stored throughout your network as well as through what network protocols (e.g. e-mail, webmail, and FTP) sensitive data is exiting the agency. Vontu also delivers immediate visibility into sensitive or classified data that is copied to removable media such as a USB drive. A Vontu Network Discover scan will examine laptops, desktops, servers, and network file shares throughout your organization—including offline machines, large numbers of distributed machines, and desktops at branch offices.
with low-bandwidth connections—so you can pinpoint exactly where sensitive data is exposed. In addition, Vontu Network Monitor and Vontu Network Prevent monitor and prevent data loss on the network including email, IM, Web, Secure Web (HTTPS), FTP, P2P, and generic TCP. Vontu Endpoint Discover detects and inventories confidential data stored on laptops and desktops and prioritizes high risk endpoints for additional protection, and Vontu Endpoint Prevent monitors and prevents confidential data from being copied to USB, burnt to CD/DVD, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications.

Vontu classifies potential risks as they’re identified, as defined by the individual SSA, and automatically quarantine or relocate data to a secured location, depending on classification.

**Activity three: Assess risks (consequences, vulnerabilities, and threats)**

In this procedure, SSAs must identify vulnerabilities in their assets, systems, and network, determine the level of risk in each case, and assess the potential consequences of corresponding data security breaches.

**Vontu solution:**

Vontu enables government agencies to identify sensitive or classified data and measure the level of risk across several key areas:

- On laptops or desktops that could be lost or stolen
- On removable media such as USB drives, CDs and DVDs, or iPods® that can easily be transported, lost or stolen
- Downloaded to local drives
- On file servers, databases, Microsoft® SharePoint®, Lotus Notes®, Documentum®, LiveLink®, web servers, Microsoft® Exchange, end-user laptops and desktops, and other data repositories
- Exiting the network via email, IM, Web, Secure Web (HTTP over SSL), FTP, P2P, and generic TCP

Vontu’s methodology enables agencies to demonstrate compliance with government standards such as export controls (e.g. EAR, OFAC, and ITAR) and NIST guidelines. Vontu first creates a policy template based on the specific SSA’s requirements, which are based in turn on DHS directives. Then, Vontu Network Discover scans for exposed data stored in file servers, databases, Microsoft SharePoint, Lotus Notes, Documentum, LiveLink, web servers, Microsoft Exchange, and other data repositories to detect data that violates SSA policy. Vontu enables high-performance, parallel scanning of thousands of desktops and laptops, including offline machines and remote office systems, with only minimal network impact. To better secure data throughout agency networks, Vontu Network Data Monitoring and Prevention monitor and prevent data loss on the network with comprehensive coverage including email, IM, Web, Secure Web (HTTPS), FTP, P2P, and generic TCP. Vontu Endpoint Discover provides added security by discovering sensitive data stored on the endpoint, and Vontu Endpoint Prevent prevents it from being copied to USB, burnt to CD/DVD, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications.
Endpoint Discover also provides insight into what sensitive data is being downloaded to local drives. The final output is an executive level report that quantifies data loss frequency, severity, and risk by data type, user, department, policy, and regulation, as well as compliance scorecard. SSAs can also conduct this risk assessment as an ongoing process to continuously size risk and identify vulnerable areas.

Activity four: Prioritize
Based on the results, SSAs must clearly understand all areas of risk, prioritize them accordingly, and identify initiatives that will best enable them to mitigate risk.

Vontu solution:
If you don’t know what’s wrongfully exposed, you won’t know how to prioritize Data Loss Prevention efforts. Vontu helps you pinpoint areas of risk and quantify the potential impact. As incidents are detected, Vontu automatically classifies the severity level—high, medium, low, and informational—to drive the appropriate level of enforcement and remediation. Vontu Endpoint Discover also helps prioritize encryption efforts. A Vontu Endpoint Discover scan will discover and inventory confidential data stored on laptops and desktops and prioritize high risk endpoints for additional protection.

Activity five: Implement protective programs
After undertaking the first four activities, SSAs must next take appropriate action to reduce or manage their risk and secure the resources necessary.

Vontu solution:
Vontu provides numerous safeguards to enable SSAs to secure data storage and data access, and prevent unauthorized data transmission between various CIOs:

• Vontu provides a pre-built Federal Government Solution Pack based on agency data protection best practices. This Solution Pack jump-starts data loss prevention with packaged best practices that include federal agency-specific policies, user roles, recommended response rules to remediate incidents, and pre-defined compliance and risk reports.

• Vontu Network Discover and Vontu Network Protect detect and limit unauthorized access to and download of sensitive data, quarantine or move exposed data, and ensure data is encrypted in accordance with security policy. These solutions further detect any unauthorized data flow that indicates access control policies aren’t being enforced.

• Vontu Network Monitor and Vontu Network Prevent monitor network communications and can block transmission of sensitive data that violates policy, or route it for encryption prior to transmission.
Vontu Endpoint Discover and Vontu Endpoint Prevent deliver real-time control over sensitive data at the endpoint. They can discover and inventory confidential data stored on laptops and desktops—regardless of whether the employee or contractor is on or off the network—and prioritize high risk endpoints for additional protection, and monitor and prevent confidential data from being copied to USB, burnt to CD/DVD, downloaded to local drives, attached to network transmissions, or encrypted or concealed using high risk applications.

Activity six: Measure effectiveness
For this procedure, SSAs must evaluate the methods and procedures they’ve put in place to measure their own progress, and also assess their effectiveness with regard to the national CI/KR protection program. The goal of this activity is to continuously improve protection, manage risk, and increase resilience.

Vontu solution:
- Vontu’s pre-built compliance and risk management reports provide historical and trend analysis to demonstrate risk reduction over time. Executive dashboards, role-based reports, and a wide range of incident filters (e.g. senderID, severity, destination, etc.) enable you to benchmark performance across multiple departments and help maintain confidentiality as incidents are reviewed.
- Run reports anytime, or schedule them to be automatically run at any future point, and then automatically distribute the reports.
- Detailed audit trails provide an account of changes made to policies, policy violations, and what actions were undertaken.
- Vontu’s auto response and manager notifications educate employees immediately when policy violations are detected and drive ongoing behavior modification to continuously improve internal policy compliance.
Vontu Federal Risk Assessment program helps get you started

Once you’ve set your security goals, Vontu enables you to assess areas of risk in order to prioritize Data Loss Prevention efforts and begin to reduce risk of exposure. To address this need, Vontu provides a 48-hour Federal Risk Assessment Service that enables government agencies to identify unsecured sensitive data and measure the level of risk. Vontu’s risk assessment will quantify your data loss frequency, severity, and risk by data type, user, department, policy, and regulation. A risk assessment will help you answer questions such as:

- Which employees are carrying large amounts of sensitive data on their laptops?
- Who and what sensitive or classified data is being copied to USB drives or downloaded to local drives?
- How well is my current information security policy being enforced?
- Has my access control system assigned the right privileges?
- Are there any unauthorized copies of sensitive data exposed on file servers or databases?

For more information, and to get started immediately, visit the Vontu Risk Assessment page, at http://www.vontu.com/services/risk_assessment.asp, or call 415.364.8100.
How to get started

Our team of Data Loss Prevention experts will work with you to understand your unique data security requirements, priorities, and share insight into our industry best practices. Contact Vontu to get started at +1.415.364.8100 or email info@vontu.com.

About Vontu

Vontu, now part of Symantec, is the leading provider of Data Loss Prevention solutions that combine endpoint and network-based technology to accurately detect and automatically protect confidential data wherever it is stored or used. By reducing the risk of data loss, Vontu solutions from Symantec help organizations ensure public confidence, demonstrate compliance and maintain competitive advantage. Vontu Data Loss Prevention customers include many of the world’s largest and most data-driven enterprises and government agencies. Vontu products have received numerous awards, including IDG’s InfoWorld 2008 Technology of the Year Award for “Best Data Leak Prevention,” as well as SC Magazine’s 2006 U.S. Excellence Award for “Best Enterprise Security Solution” and Global Award for “Best New Security Solution.” For more information, please visit http://go.symantec.com/vontu.