

8 Steps to data security compliance

A step by step guide to protect the privacy of confidential customer and employee information assets in today's heightened regulatory environment



What every security and compliance team should know to protect confidential data and demonstrate compliance

The rise in data security breaches and trade secret violations over the past year is a wake-up call for executives—network security is not enough. Organizations must protect the data itself, not only to avoid financial loss and brand damage, but also to demonstrate regulatory compliance. Several international and federal data privacy regulations, such as Gramm-Leach-Bliley (GLBA), Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) Data Security Standard, and the European Union (EU) Data Directive, as well as more than 35 state laws require organizations to safeguard confidential customer and internal data. Vontu Data Loss Prevention (DLP) from Symantec also enables Government agencies to comply with regulations such as the Federal Information Security Management Act (FISMA), the National Infrastructure Protection Plan (NIPP), and White House OMB and NIST PII Requirements. To mitigate the risk of compliance violations, security teams must implement processes and technology that reduce the frequency and severity of data loss incidents.

Vontu Data Loss Prevention helps organizations such as Charles Schwab, Equifax, and Raymond James Financial, as well as federal agencies and customers in energy and utilities, financial services, insurance, high technology, retail, telecommunications, manufacturing, media and entertainment, pharmaceuticals, and healthcare, demonstrate compliance with these external regulations as well as internal data security policies. To help you reduce your risk of confidential data loss and demonstrate regulatory compliance, Vontu, now part of Symantec, has developed the following guide. This report outlines specific steps you should take to evaluate and strengthen your data security processes, policies, and technology systems.

STEP 1 Quantify and qualify risk

The first step to protect confidential data—such as customer and employee information—and demonstrate compliance is to know your risk. The latest statistics show that 1 in 400 emails and 1 in 50 network files contain confidential information. However, few organizations have such clear visibility into their data. Most are unsure where it is stored, where it is being used, and what to do once they find it. In order to quantify risk, security teams must have greater visibility into their exposed confidential data. What data is at risk—customer accounts, patient health data, financial records? Where is my confidential data stored on file servers, databases, laptops, desktops and other data repositories? How and what quantity of confidential data is transmitted outside my organization via e-mail, Instant Messaging, or FTP? What sensitive data is being downloaded to local drives, burned to CD/DVD or copied to USB devices and other removable media and who is responsible? How severe are the incidents? Answers to these questions enable security teams to quantify and qualify risk so they can take the next steps to implement protective processes and technologies.

Vontu DLP helps organizations take the first step to demonstrate data security compliance, identify threats to information assets and potential compliance violations, pinpoint specific confidential data wherever it is stored or used—across endpoint, network, and storage systems—and quantify the frequency and severity of the potential impact of a security breach. With Vontu DLP, security teams have complete visibility into high risk areas such as:

- Location and exposure of stored confidential data—on file servers, databases, Microsoft® SharePoint®, Lotus Notes®, Documentum®, LiveLink®, web servers, Microsoft® Exchange, end-user laptops and desktops, and other data repositories
- Volume and types of confidential data (such as customer records, financial information, or intellectual property) leaving the network
- Frequency and severity of confidential information exposures that may violate policy
- Methods by which confidential data is transmitted outside the organization
- What confidential data is being downloaded to local drives or copied to storage devices such as USB devices, CDs/DVDs, or iPods®
- Parties responsible for, and related severity of, confidential data breaches
- Compliance regulations that may have been violated.

Once an organization quantifies risk through a Vontu Risk Assessment, it can establish data security policies, implement protective technology, and take proactive steps to demonstrate compliance.

STEP 2 Establish policies that address privacy and regulatory compliance

Government regulations and worker privacy laws play a significant role in how organizations structure and implement data protection policies. The more globally dispersed the organization, the more impact international law has on policy and workforce monitoring. Though privacy laws and regulations vary from country to country, there are a number of requirements that should guide the formation of policy that enables the organization to demonstrate compliance:

- Protect security of the data itself
- Demonstrate regulatory compliance
- Safeguard employee privacy.

Vontu DLP enables organizations to meet these requirements through policy-driven data discovery, protection monitoring, and prevention. Pre-defined policy templates inspect data wherever it is stored or used, for potential violations of over 50 international, federal, and state data privacy regulations such as GLBA, HIPAA, PCI Data Security Standard, FISMA, OMB, NIPP and PIPEDA, to name a few. Policy templates are also flexible which enables them to be tailored to an organization's unique data protection needs and jurisdictions of operation. Such flexibility also allows organizations to adapt policies to regulatory changes in order to demonstrate compliance over time.

STEP 3 Manage and control risk

Once security and compliance teams have identified risk and severity across the organization, they can deploy a Data Loss Prevention solution to reduce risk and demonstrate compliance. At this stage, requirements such as protection of data wherever it is stored or used, detection accuracy, policies that address regulatory compliance, and enterprise scale, among others, become key factors in the decision process. An effective Data Loss Prevention solution should:

- Accurately detect threats to reduce exposure and ensure compliance
- Prevent violation of worker privacy through targeted, policy-based monitoring
- Protect confidential stored data from unauthorized access, tampering and usage
- Prevent confidential data usage on the network or endpoints from leaving the organization
- Monitor confidential data stored on the endpoint, and prevent this data from being inappropriately used, sent out, or copied to storage devices such as USB devices, CD/DVDs, or iPods®
- Discover and protect confidential data that is exposed on file servers, databases, Microsoft® SharePoint®, Lotus Notes®, Documentum®, LiveLink®, web servers, Microsoft® Exchange, end-user laptops and desktops, and other data repositories
- Automatically enforce encryption policies
- Automate reporting and policy enforcement to demonstrate regulatory compliance and streamline system and incident response, notification, workflow, and compliance reporting.

With Vontu DLP, organizations are able to immediately reduce the threat of confidential data breaches. Data, wherever it is stored or used, is continuously inspected according to policies configured specifically to meet the organization's compliance requirements. As potential violations are detected, Vontu DLP automates remediation, through worker notifications and escalation, to help organizations change employee behavior and pinpoint compliance gaps in existing business processes. Vontu DLP also identifies unencrypted data that should be protected, and automatically routes it to an encryption server prior to being sent. Finally, centralized reporting and analytics enable security teams to demonstrate compliance and respond more quickly and confidently to audits.

STEP 4 **Oversee partners, suppliers, and service providers**

A comprehensive compliance strategy must extend beyond the four walls of the organization and include provisions for business partners, suppliers, and other external service providers.

For organizations that share data across multiple channel relationships, Vontu DLP delivers specific capabilities that protect confidential information and address compliance obligations. One example is our centralized policy management feature that covers multiple network exit points and includes partner locations. This enables organizations to deploy monitors at outsourced partner data centers and manage them centrally. From a single dashboard, security teams can identify potential data breaches, alert offenders, and fix processes immediately. Finally, because outsourcing often introduces the use of international entities, Vontu DLP has incorporated capabilities to meet global compliance requirements. Centralized policy management and reporting enables policies to be tailored to meet global worker surveillance and privacy regulations—such as the EU Data Directive—and still preserve the organization's need to protect data.

STEP 5 **Improve worker education and awareness**

Leading analyst firm Gartner reports that 70 percent of security incidents that incur losses are caused by insiders—employees, contractors, and other workers who have access to confidential information. In addition, most incidents aren't the result of malicious intent, but rather inadvertent mistakes and misunderstood policies. Organizations must change worker behavior through awareness and education in order to reduce this insider threat.

Vontu DLP enables organizations to reform worker behavior and fix broken business processes that routinely cause data loss. For example, as soon as an incident is detected, our sender notification feature automatically sends a customized message to inform the employee and remind him or her of organizational policy. If the incident is considered severe, the Vontu solution can be configured to automatically escalate the issue to management. Real-time worker education and escalation helps organizations reduce the risk of data loss and demonstrate regulatory compliance.

STEP 6 Support due diligence and audits

Security and privacy teams are required to certify their compliance with external regulations as well as internal policies. Compliance certification includes detailed accounts of processes and controls, which include detection, management, and control of confidential and classified information, as well as adherence to worker privacy regulations. While external regulations are often top of mind due to concern over penalties and public embarrassment, internal policy audits also cause concern because of the time and resources they can consume. Unlike external audits, internal audits aren't always precipitated by an incident and often carry greater scrutiny.

Vontu DLP enables security teams to respond to both internal and external audits more thoroughly and with minimal resources and time. For every suspected breach, the Vontu solution generates incident snapshots to support investigations and audits. In addition, the Vontu solution delivers a range of compliance reports that pinpoint and quantify risk areas and provide trend analysis to demonstrate risk reduction over time. Armed with this insight, security teams can demonstrate compliance, increase auditor confidence, and show that they've implemented processes and technology to address regulation requirements.

STEP 7 Report to the board and executive team

The negative publicity and brand impact that often accompanies a compliance violation has increased the awareness of Data Loss Prevention in the executive suite. For security teams, executive reporting is a key step to address compliance requirements and demonstrate risk reduction over time. Executives want primary insight that includes:

- **Current quantified risk.** This provides insight into data loss prevention risk so it can be considered in context with other organizational risk areas.
- **Risk by organizational area.** With clear knowledge of where risk is greatest, the organization can target specific areas of operation that must become compliant.
- **Potential regulatory exposure.** This requires the identification of the organization's liability as it relates to international, federal, and state data privacy regulations.
- **Risk reduction over time.** This insight is perhaps the most important because it demonstrates proof of proactive measures taken to reduce liability.

Our reports enable security teams to proactively address executive concerns. Through executive dashboards, analytics, and audit trails, our customers can present key executive-level metrics that quantify risk across the organization, inform management of regulatory liability, and demonstrate risk reduction over time. A small sample of Vontu DLP executive reports includes:

- Reports on risk by business unit
- Potential breaches by compliance regulation
- Potential breaches by business unit
- Potential breaches by outsource partner.

STEP 8 Continuously monitor and report to drive down risk

From a compliance perspective, regulators and internal and external auditors often look for proof that an organization has proactively and continually mitigated risk. To meet compliance goals, the organization must measure the effectiveness of data protection policies over time in order to identify potential violations, reveal salient trends, and fix broken business processes.

Vontu DLP enables organizations to continuously reduce their risk of data loss. Once Vontu solution is installed, customers baseline their risk, and begin to target policy to drive compliance in all areas where violations occur. As the system operates, violations are averted through features such as worker notifications, selective message blocking, and policy-based encryption. Through our historical reporting and trend analysis, security teams can address auditor requests and demonstrate risk reduction and compliance improvements.

Conclusion

Regulations such as GLBA, HIPAA, FISMA, OMB and the more than 35 state data privacy policies require global organizations and government agencies entrusted with private data to protect it from inadvertent or malicious disclosure. This regulatory oversight adds another dimension that organizations must incorporate as part of a comprehensive Data Loss Prevention strategy. Knowledge of regulatory provisions, however, is just a start. The mitigation of risk is an ongoing process that requires visibility into current exposure, implementation of processes and technology to protect data, and ongoing analysis and evaluation for continuous improvement.

Vontu Data Loss Prevention from Symantec enables organizations to reduce the frequency and severity of data loss incidents to protect brand and reputation, safeguard customer data, protect intellectual property, and demonstrate compliance. Vontu DLP 8 is the industry's first integrated suite to prevent the loss of confidential data wherever it is stored or used—across endpoint, network, and storage systems. The layered architecture enables customers to 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 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>.



Vontu, Now Part of Symantec

475 Sansome Street, Suite 2000

San Francisco, CA 94111

Tel: +1.415.364.8100

Fax: +1.415.364.8190

info@vontu.com

www.vontu.com

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec, the Symantec logo and Vontu are trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.