Symantec.

Symantec™ Information Centric Encryption

Powered by PGP™ Technology

Dynamic Monitoring and Control

Once data leaves your organization, how can you retain control of it? With Information Centric Encryption, you can keep data safe though monitoring and controlling access in real time, dynamically revoking user access or remotely wiping access to a document.

Data Protection Challenges

Organizations are moving sensitive data out of their physical perimeters and into the cloud where they can share it with users across multiple organizations and locations. But it's difficult to keep data safe and usable once it leaves your traditional control.

Increased regulation, customer scrutiny, and risk awareness are driving the need to protect information. Data breaches continue to increase, with a cost of $4 million per breach, on average, according to a 2016 report from Ponemon Institute. The damage is not only financial but also impacts customer trust and brand reputation and can result in fines and penalties for noncompliance.

New Approach

Information protection that encompasses discovery, protection, and user authentication provides a complete approach. By integrating these capabilities in a way that follows the data, you get true information centric security. It protects your sensitive data, making it only visible to the intended recipient.

Enterprise-grade Protection

Information Centric Encryption delivers strong, simple protection that follows data wherever you store, use, or move it.

It protects data with enterprise-strength techniques through the integration with Symantec Data Loss Prevention, Symantec CloudSOC (Cloud Access Security Broker) or Symantec Information Centric Tagging technologies. Using highly accurate data discovery engines, sensitive data is detected on-premises, in cloud and mobile locations. Alternatively, users can identify and classify files and emails that contain sensitive data.

You can apply enterprise-grade encryption automatically by policy, ensuring consistent compliance. And this protection follows the data, regardless of device or location.

To access a document, the recipient uses a "one touch" process that protects data even if multiple users share a device.

Key Benefits

Protects sensitive data in the hands of third parties

- Your organization's information ecosystem includes third parties such as partners, customers, contractors, and investors. With Information Centric Encryption, you get visibility into shared data as well as effective collaboration controls so trusted third parties can access your data securely.
- Information Centric Encryption supports application data and a broad set of file formats to meet the needs of your information ecosystem.

Finds and deletes rogue copies

Information Centric Encryption finds and wipes copies of data accessed by an unauthorized user.

Keeps you in control

- You can use your keys stored in a customer-managed Amazon Web Services account.
- Governments must contact you to decrypt any of your data.
- You can revoke access to sensitive data if a malicious insider or hacker obtains it.

Deployment Considerations

Information Centric Encryption is built on integrations between Symantec CloudSOC, Symantec Data Loss Prevention or Symantec Information Centric Tagging. It requires CloudSOC, Data Loss Prevention (v15) or Information Centric Tagging v15.

CloudSOC, Data Loss Prevention and Information Centric Tagging integrations have their own system requirements, supported applications and platforms, and deployment instructions. Refer to their implementation guides for those requirements.

Supported applications and platforms

Application & Requirements
Administrator Access
• Google Chrome 45 or higher
• Mozilla Firefox 36 or higher
• Safari 10 or higher
Supported Environments
With Symantec CloudSOC:
• Box
• OneDrive
• SharePoint Online
With Symantec Data Loss Prevention 15:
• Microsoft SharePoint
• On-premises File Stores
• Removable USB Drives
With Symantec Information Centric Tagging 15:
• Protect email bodies and attachments via Outlook plug in
• Protect a wide variety of file formats with a mouse-click
Information Centric Encryption Utility
• Windows 7, 8, 8.1, or 10
• MacOS X Yosemite (10.10), El Capitan (10.11), or Sierra (10.12)
• MacOS X iOS 9.x or 10.x
For Symantec Data Loss Prevention or Information Centric Tagging system requirements:
• www.symantec.com/products/data-loss-prevention/requirements
• www.symantec.com/products/information-centric-tagging/requirements

Summary

Enterprise Strength, Consumer Simplicity

- **Automatic protection** – using Data Loss Prevention, CloudSOC or Information Centric Tagging to drive encryption
- **Persistently protect data** with strong encryption (AES 256 & RSA 4096)
- **Dynamic protection** – wipe user access remotely as requirements change
- **No passwords** – One Touch access and strong authentication
- **Extensive coverage** – enable broad protection for cloud apps

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com