DATA SHEET

Symantec™ Information Centric Encryption

Powered by PGP™ Technology

Digital Rights Management for Data 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 persistent protection, monitoring and access control 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. Encryption helps protect data while at rest and in transit, but such protection vanishes after decryption, making it impossible to ensure data integrity and track further data distribution.

Increased regulation, customer scrutiny, and risk awareness are driving the need to protect information. Data breaches continue to increase, with a cost of $3.9 million per breach, on average, according to a 2018 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.

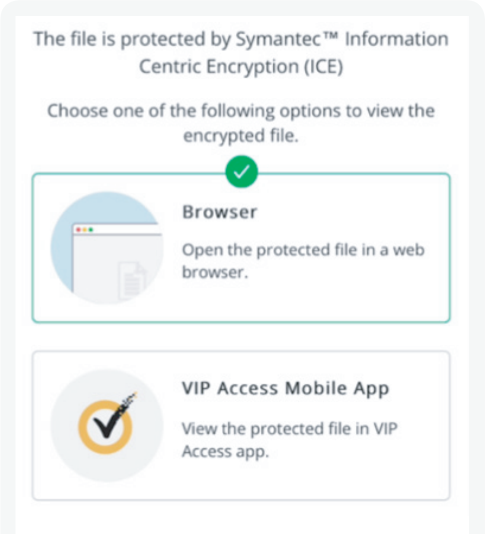
Enterprise-grade Protection

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, email 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.

Identity-based Access

To access a protected file or email, the recipient uses a "one touch" process that protects data even if multiple users share a device. In fact, proof of identity must be provided, and two-factor authentication can be enforced further to validate the user is the intended recipient. Two options can be provided: a one-time agent download or agentless viewing. Policy-based digital rights, such as edit and print, are only available via agent download, while browser-based agentless viewing provides the invaluable benefit of reducing friction and relieving possible trust obstacles when a document only requires it be viewed.

Options: Browser View or Agent Download



The file is protected by Symantec™ Information Centric Encryption (ICE)

Choose one of the following options to view the encrypted file.

Browser

Open the protected file in a web browser.

VIP Access Mobile App

View the protected file in VIP Access app.

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 cloud-based 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.
- Protects sensitive emails and attachments sent through Office 365 and Gmail for Work.
- Use permission sets to define which users can access a file, how long the file is accessible, and what actions the users can take (such as view, edit, print and offline access) on the file.

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 or an on-premises key store.
- Governments must contact you to decrypt any of your data.
- You can revoke access to sensitive data if malicious insiders or hackers obtain it, or when partnerships end.

Deployment Considerations

Information Centric Encryption is built on integrations with Symantec CloudSOC, Symantec Data Loss Prevention or Symantec Information Centric Tagging. Refer to the implementation guides for specific requirements.

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
- Cloud Email (with Symantec Data Loss Prevention 15.1)

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), Sierra (10.12) or High Sierra (10.13)
- MacOS X iOS 9.x to 12.x

For Symantec Data Loss Prevention or Information Centric Tagging system requirements:

https://www.symantec.com/products/data-loss-prevention/

https://www.symantec.com/products/information-centric-tagging/

Summary

Enterprise Strength, Consumer Simplicity

- **Automatic data protection** – using Data Loss Prevention, CloudSOC or Information Centric Tagging to drive encryption
- **Persistent data protection** with strong encryption (AES 256 & RSA 4096)
- **Dynamic monitoring and protection** – control data accesses and revoke user access remotely as requirements change
- **Identity access and strong authentication** – share data safely only with authorized users
- **Extensive coverage** – enable broad protection for cloud apps, email, storage and endpoint

Symantec

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