Overview

The cloud is here to stay. And that means data will remain mobile and people can access it from virtually anywhere. To compete in today’s digital world, you must share sensitive information outside your organization. You also need to share data with external users while it remains protected and simple to access.

It’s imperative that you keep this data safe—wherever it is. But traditional tools are struggling to keep up, resulting in more data breaches:

- 2016 was a record year for data breaches, up 40 percent from 2015.
- There were 1,209 total breaches in 2016, 15 mega-breaches, and 1.1 billion exposed identities, almost double the 564 million exposed in 2015.

The damage is not only financial; it erodes trust among your customers, bruises your brand, and can result in fines and penalties for noncompliance.

So what can you do? To manage these risks, you need a new approach to data protection. Symantec advises organizations to move to an information-centric security model—no longer is it enough to rely on the older approach of just securing the network and data center.

The perimeter no longer exists, as competitive pressure demands that you move your data to the cloud and allow employees, or other external users, to access information from anywhere on their PCs, smartphones, and other devices.

Explore more:
Symantec 2017 Internet Security Threat Report

The cost of breaches is rising as well. The average breach cost $4 million in 2016, according to Ponemon Institute.

Explore more:
2016 Was a Record Year for Data Breaches

Hardening your network and data center is not enough. Today’s organizations are working with more third-party partners and constantly exchanging data outside their four walls. Tracking and protecting this data as it moves among multiple locations, users, and devices becomes complex and introduces the risk of data loss.
Some organizations are in the dark

Too often, organizations don’t know what data is sensitive, much less where it is. Typically, it’s not classified correctly and not handled appropriately:

- **Two-thirds** of security professionals don’t have complete visibility into where their organization’s sensitive data resides.
- **More than half** of organizations don’t understand the full risk to their data.

### Integrated security is the answer

What’s needed is a new approach to data security, an inside-out strategy that starts with the data itself. We call it **information-centric security**.

To start, you need to identify the what and where of your sensitive data. When employees send files to the cloud that contain personal information about customers, how do they know what data is sensitive and what is the adequate level of protection?

#### Three key questions you need to ask

1. **Where is my sensitive data and how much is stored on-premises and in the cloud?**
2. **How do I protect my data should it fall into the wrong hands?**
3. **Who is accessing my data and what is the risk of account takeover?**

---

**See**

data where it lives.

**Control**

user access to data.

**Protect**

data from being leaked.

---

Explore more:

[11 Data Issues That Keep IT Security Pros up at Night](#)
Data loss can be a thing of the past

Even if your staff has full data protection knowledge, is it realistic to rely on them to consistently apply policies and never make a mistake? Integrating data monitoring, protection, and access control policies ensures consistent and always-on protection that follows your data—wherever it goes, on whatever device.

One way to know what data is sensitive and if you are protecting it correctly is with Symantec™ Data Loss Prevention.

It lets you instantly

- Discover
- Monitor
- Protect

sensitive data, wherever and whenever you use it—in the office, on the road, or in the cloud.

Symantec Data Loss Prevention finds any data and determines whether it is sensitive and adds policies around it. For example, it makes sure that certain data is not allowed to leave your organization.

And if data does leave, it can be encrypted. Data Loss Prevention gives you complete visibility and control across the broadest range of potential data loss channels:

- Cloud apps
- Endpoints
- Data repositories
- Email and web communications

Better way to identify sensitive data

While Data Loss Prevention delivers a powerful combination of data detection technologies—from data fingerprinting to image analysis—there are some types of sensitive data that a defined data loss prevention policy may not detect. In this case, the best way to identify sensitive data is via the users who created it. Symantec Information Centric Tagging empowers your employees to help identify and classify the value of the information that they create. Information Centric Tagging can also automate data protection, in the form of automatic watermarking of email and documents, to leave a visual indication of the classification level, as well as encryption.
“Symantec offers the most comprehensive sensitive-data detection techniques in the market, with advanced functionality such as form detection, image analysis, and handwriting recognition that can cover a wide breadth of data loss scenarios.”

— “Magic Quadrant for Enterprise Data Loss Prevention,” Gartner, February 2017

**Symantec CloudSOC** lifts security to the cloud

Symantec CloudSOC, a cloud access security broker, extends the granular Symantec Data Loss Prevention policies to the cloud, allowing sensitive data to be discovered in motion. Furthermore, the integration of Symantec Data Loss Prevention and CloudSOC allows our leading Data Loss Prevention engines to scan cloud data and apply consistent policy controls.

Uncover data-loss blind spots and discover sensitive data in more than 60 cloud apps, including Microsoft® Office 365®, Box, and Dropbox.

Symantec CloudSOC keeps your cloud apps and services secure and compliant. It delivers visibility into shadow IT and manages data in cloud apps and protects against threats targeting cloud accounts.

Remote key access: For users who sit outside an organization’s perimeter, obtaining a decryption key can be cumbersome, pushing them to use shadow data systems.

Vulnerable data: Encrypted data is only protected when it remains encrypted. Once decrypted, users have full access to that data, and they can share it inappropriately (accidentally or maliciously).

Encryption keys that protect resting persistent data must also be persistent and stored with the data they protect, which makes them vulnerable to theft. Plus, encryption provides no protection against misuse of data by insiders.

Passwords are the weakest link

81 percent of all confirmed data breaches still involve hackers using weak, default, or stolen passwords.

**Encryption alone is not enough**

Encryption is one approach; and while encrypting data can safeguard it against loss, it can impact productivity. Depending on how you manage decryption keys, it can be difficult to access data remotely. In addition, once data is decrypted, it can be shared in clear text form, with no way to apply further controls.

Explore more:
**Symantec Data Loss Prevention – Now in the Cloud with CloudSOC**

Explore more:
**2016 Verizon Data Breach Investigations Report**
Another crucial step in your chain of security is to ensure that those who receive data are in fact who they say they are and that your employees can work securely any time, anywhere, on any device.

So why not just make sure that only the right people can access important corporate data? Because even the right people do the wrong things. In 2016, even Facebook founder and CEO Mark Zuckerberg’s Twitter and Pinterest accounts were hacked because, the hackers said, he was sloppy with his password practices.

Perhaps stronger passwords are the answer. Or perhaps not. The head of the U.K.’s National Cyber Security Centre has questioned the wisdom of public guidelines on internet passwords, claiming they require the average citizen to memorize the equivalent of a 600-digit number every month.

Complementing passwords, no matter how strong, with additional layers of authentication significantly reduces the risk of account takeover and eases the user experience.

Symantec Validation ID and Protection Service multifactor authentication prevents unauthorized access to networks, applications, and the cloud, with easy-to-use multifactor and risk-based authentication. It stops account takeover when, for example, an employee uses the same password for his LinkedIn account and his Salesforce account.

Symantec Validation ID and Protection Service intelligently authenticates users by interpreting logon patterns, location, and risk. It simplifies security with a broad range of multifactor options such as one-tap push authentication and fingerprint verification.

Validation ID and Protection Service eliminates up to 81 percent of hacking-related breaches through strong, trusted enterprise authentication. With it, you can positively identify a user by enhancing passwords with a dynamic second factor of authentication that cannot be predicted or stolen.

Symantec Validation ID and Protection Service works not only with a virtual private network but can adapt to nearly any network, cloud, or mobile app with built-in integrations.

Symantec secures users

Tactics used in cyber attacks

62% of breaches feature hacking.

43% are social attacks.

51% of breaches include malware.

14% of breaches are from casual events. The same proportion involves privilege misuse.

81% of hacking-related breaches use either stolen or weak passwords.

8% of breaches include physical actions.


Explore more: www.symantec.com
Today, organizations of all sizes demand the ability to share data but frequently lack the right controls. What if you have a team that’s sharing confidential financial information with a potential acquisition target and then the deal falls through? Suddenly a lot of people have access to your sensitive data who should not. In the past, you would be stuck. There was no way to delete files retroactively or deny further access.

Symantec Information Centric Encryption denies all access to private data retroactively:

- **Integrates** with data loss prevention and cloud access security broker technology to ensure sensitive data is discovered and appropriately protected.
- **Ensures** that protection follows sensitive data wherever it goes.
- **Limits** data access only to intended users with simple-to-use identity-based decryption.
- **Monitors** who is accessing data and understands abnormal access behaviors.
- **Controls** data wherever it resides at any time by blocking file access.

Put all these pieces together and you get Information Centric Encryption. You won’t waste resources on ineffective perimeter defense—instead, Symantec protects all your data, wherever it is and wherever it’s going.

Why is an integrated approach so beneficial? Because it allows you to confidently share sensitive data with anyone.

“Gartner Magic Quadrant” has named Symantec a leader in data loss prevention for the past 10 years. Forrester Research has also rated Symantec a leader.
Components of information-centric security

Existing Symantec customers can use their Data Loss Prevention and CloudSOC policies to detect sensitive data and automatically encrypt it. This ensures a consistent approach to data protection that spans

- **On-premises**
- **Cloud**
- **Mobile environments**

It eliminates the risk of users circumventing data protection policies or making innocent mistakes.

Store or move encrypted files anywhere—on-premises, in the cloud, or in email—because only authorized users have permission to open the files.

Verify identity with multifactor authentication, ensuring you’re sharing information only with intended users.

Central monitoring allows you to see exactly who is accessing data, when and from where. And administrators can revoke access to any document on a per-user basis, so you can protect access to documents over the lifetime of that information.

Strong security protects today’s business

Our tightly integrated information-centric security gives you the confidence to do business in today’s environment of always-on data sharing.

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

Contact your local Symantec sales representative or business partner: www.symantec.com

About Symantec
Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Copyright ©2017 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.