SOLUTION BRIEF

It's Time to Rethink Your Data Protection

As your sensitive data moves, your security must move with it

Symantec™

Introduction

The cloud is here to stay. Data remains mobile and people are accessing it from virtually anywhere. Competing effectively in today's digital world requires you to share sensitive data with external users in a simple way while keeping it protected, and in compliance with new regulations like the EU GDPR (General Data Protection Regulation).

But traditional security tools are struggling to keep your data safe, as Symantec's Information Security Threat Report (2018) shows:

- Stolen user credentials are used to attack organisations, with spear phishing being the most widely employed technique.
- In 2017, the vast majority (**90%**) of attacks appear designed to gather information from targeted organizations.

The cost of breaches remains high. The average breach cost $3.6 million in 2017, according to Ponemon Institute.

Explore more ›
Symantec 2018 Internet Security Threat Report

Explore more ›
GDPR: A New Era in Privacy and Data 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. Who is accessing my data and what risks do they present to my data?
3. How do I protect my data should it fall into the wrong hands?

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.

Explore more ›
11 Data Issues That Keep IT Security Pros up at Night

What to Do When Employees Send Data to the Cloud

- Know when data is sensitive.
- Provide consistent protection (manual processes are error-prone).
- Understand your overall data risk posture, and identify which activities or users need investigating.
- Allow third-party or roaming users to access protected content without adding undue risk.
- Preserve identification integrity, such as verifying that user accounts haven't been compromised.
- Protect data that falls into the wrong hands, even if that data no longer resides on your network.

Explore more
7 Types of Insider Attacks

Information-Centric Security Is the New Approach

To manage security risks, you need an enhanced approach to data protection. Symantec's information-centric security model doesn't just secure the network and data center, it secures the data. This allows data to move between multiple locations, with many users sharing it, all while you track and protect it, reducing the risk of data loss.

With a leading portfolio of data protection technologies, spanning data loss prevention, tagging (or classification), cloud access security broker, encryption, analytics, and identity authentication, Symantec brings it all together in our information-centric security model. Our approach integrates functionality to provide enhanced protection, automated workflows, and visibility into what really matters.

Explore more
Visit the Information Centric Security website

Sensitive Data Gets Automated Protection

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

Symantec Data Loss Prevention finds data and determines whether it is sensitive and adds policies around it. For example, you can set policies to make sure that certain highly sensitive data is not allowed to leave your organization, unless it is encrypted. Data Loss Prevention gives you complete visibility and control across the broadest range of channels including cloud apps, endpoints, data repositories, and email and web communications.

“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**

Human Intelligence Detects Sensitive Data

While Data Loss Prevention delivers a powerful combination of automated data detection technologies (from data fingerprinting to image analysis), it relies on appropriate policies being defined. When sensitive data is created before a policy exists, the Symantec approach lets the data owner classify it. Symantec Information Centric Tagging empowers your employees to identify and classify how sensitive their data is, thereby extending protection to sensitive data where policies may not yet exist. Information Centric Tagging also automates data protection, applying automatic watermarks to email and documents, leaving a visual indication of the classification level, as well as the protection state.

This blended approach increases your ability to automatically and intelligently detect data.

Valuable Insights Reveal Risky Behaviors

Monitoring and understanding risk is essential. Symantec Information Centric Analytics (powered by Bay Dynamics) provides an integrated, contextually enriched view of your enterprise’s cyber risk. It correlates and distills Symantec Data Loss Prevention security event data, uncovering valuable insights into user behaviors to reveal persistent threats and risky activities.

Information Centric Analytics helps you become more resilient to data breaches or account takeover by dynamically analyzing large numbers of security alerts and delivering a prioritized list of users whose behaviors are elevating your risk level. This helps reduce the likelihood of a breach and improves your compliance with data protection regulations.

Security Resides in the Cloud

Symantec CloudSOC, a cloud access security broker, keeps your cloud apps and services secure and compliant. It delivers visibility into shadow IT—hardware or software that is not supported by the IT organization—and manages data in cloud apps and protects against threats targeting cloud accounts.

Symantec CloudSOC extends Symantec Data Loss Prevention detection policies, removing blind spots from more than over 75 cloud apps, including Microsoft® Office 365®, Box, and Dropbox. 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.

Explore more

Symantec Data Loss Prevention – Now in the Cloud with CloudSOC

Passwords Are the Weakest Link

More than 80% of all confirmed data breaches involved hackers using weak, default or stolen passwords (2016 Verizon Data Breach Investigations Report). 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. For example, in 2016, Facebook founder and CEO Mark Zuckerberg's Twitter and Pinterest accounts were hacked because, the hackers said, he was sloppy with his password practices.

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

Explore more ›

Your Data is Only as Safe as Your Weakest Password

Encryption Gets Stronger

Encrypting data safeguards it against loss, but it can impact productivity. Depending on how you manage decryption keys, it can be difficult to access data remotely. This cumbersome and frustrating experience pushes users to shadow data systems. And once you decrypt data, users have full access and can share it inappropriately (accidentally or maliciously) with no way for you to apply further controls.

Symantec Information Centric Encryption delivers visibility into who is accessing data, while providing a better user experience. It also allows you to manage protection dynamically and control user access remotely:

- **Deny** all access to private data retroactively.
- **Integrate** with data loss prevention, information centric tagging and cloud access security broker technology to ensure sensitive data is discovered and appropriately protected.
- **Ensure** that protection (including digital rights management) follows sensitive data wherever it goes.
- **Limit** data access only to intended users with simple-to-use identity-based decryption.
- **Monitor** who is accessing data.
- **Control** data wherever it resides at any time by blocking file access.
- **Own** your encryption keys, choose whether to store them on-premises or in the cloud.

Multi-Factor Authentication Prevents Unauthorized Access

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.

Symantec Validation ID and Protection Service keeps data from falling into the wrong hands by preventing unauthorized access to networks, applications, and the cloud, with easy-to-use multi-factor 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.

Explore more ›

Enterprise-Grade Authentication Made Easy for Everyone

"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.

Strong Security Protects Today's Business

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

For more information, contact your local Symantec sales representative or business partner

go.symantec.com/ICS

Components of Symantec Information-Centric Security

Data Loss Prevention: Discovers sensitive data across all channels with central policy controls

Information Centric Tagging: Augments classification and protection with user-driven data tagging

Information Centric Analytics: Identifies risky users accessing sensitive data

CloudSOC: Extends existing data loss prevention policies, workflows, and detection to cloud apps

Information Centric Encryption: Integrates policy-driven encryption, digital rights management and identity access.

Validation and ID Protection Service: Secures access to critical data with multi-factor authentication

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.

Symantec™

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

19A173304_SB_ICS_EN