Symantec DLP Data Access Governance

Comprehensive data security and governance for file systems and SharePoint

At a Glance

Data discovery

- Identify sensitive data across file systems and data repositories with unmatched content detection capabilities that minimize false positives.
- Seamless integration of Data Access Governance and Data Loss Prevention for Storage.

Data activity monitoring

- Monitor activity across Windows file servers, NAS devices, and SharePoint so you know what data users are accessing and what they're doing with it.
- Identify probable owners so only the right people are put in charge of important data access decisions.

Data access governance

- Quickly assess and identify unsafe "open access" conditions that can lead to sensitive data getting into the wrong hands.
- Enable business owners to decide who should have access to their data and end users to request access to the data they need with Entitlement Reviews and Self-Service Access Requests.

Introduction

The majority of enterprise data exists as unstructured files stored in common content repositories such as network file shares on server and NAS infrastructure as well as Microsoft SharePoint. Gartner estimates there will be an 800% growth in the amount of data by 2021, with 80% of it being in the form of unstructured data. As a result, organizations are losing more and more visibility into this data every day and are struggling to control it, leaving it vulnerable to negligent employees and malicious attackers. Protecting unstructured data against loss and theft is a critical strategy to your data security program.

Solution

Symantec Data Loss Prevention (DLP) Data Access Governance addresses the unstructured data problem by delivering actionable intelligence into data ownership, usage and access for unstructured data. For file shares and SharePoint sites, Symantec DLP Data Access Governance provides powerful reporting, analytics, and visualization capabilities that shine a light on the data by giving organizations visibility into where their sensitive data resides, who owns and accesses it, as well as how it is being used.

Data Access Governance is part of the comprehensive Symantec DLP for Storage solution, which includes DLP Network Discover and DLP Network Protect to allow you to discover and protect confidential data across virtually any storage system.

Key Use Cases

- **Find and fix sensitive files access.** Data Access Governance integrates with Network Discover to find sensitive files stored on your network, identify data owners, and automatically restrict access or engage data owners in the data cleanup process.
- **Fix overly permissive file access.** Data Access Governance and Network Discover find sensitive folders and shares with the greatest risk of exposure based on their accessibility and content. Data Access Governance also provides actionable recommendations for tightening permissions and change analysis capabilities to lockdown access to align with business need.

Integrated Data Discovery

- **Sensitive Data Discovery** – Identify files containing sensitive content with industry-leading content detection capabilities - such as Vector Machine Learning, Indexed Document Matching and Sensitive Image Recognition – through Data Access Governance integration with DLP Network Discover.

Auditing and Reporting

- **Permissions Auditing** – Gather full permission details across every share, folder, and file, highlighting toxic conditions such as Broken Inheritance, Historical and Unresolved SIDs, Direct User Permissions, and Open Access.
- **Open Access Reporting** – Quickly assess the open access in your organization to understand what is over-exposed and at risk, including file shares on premises and in the cloud.

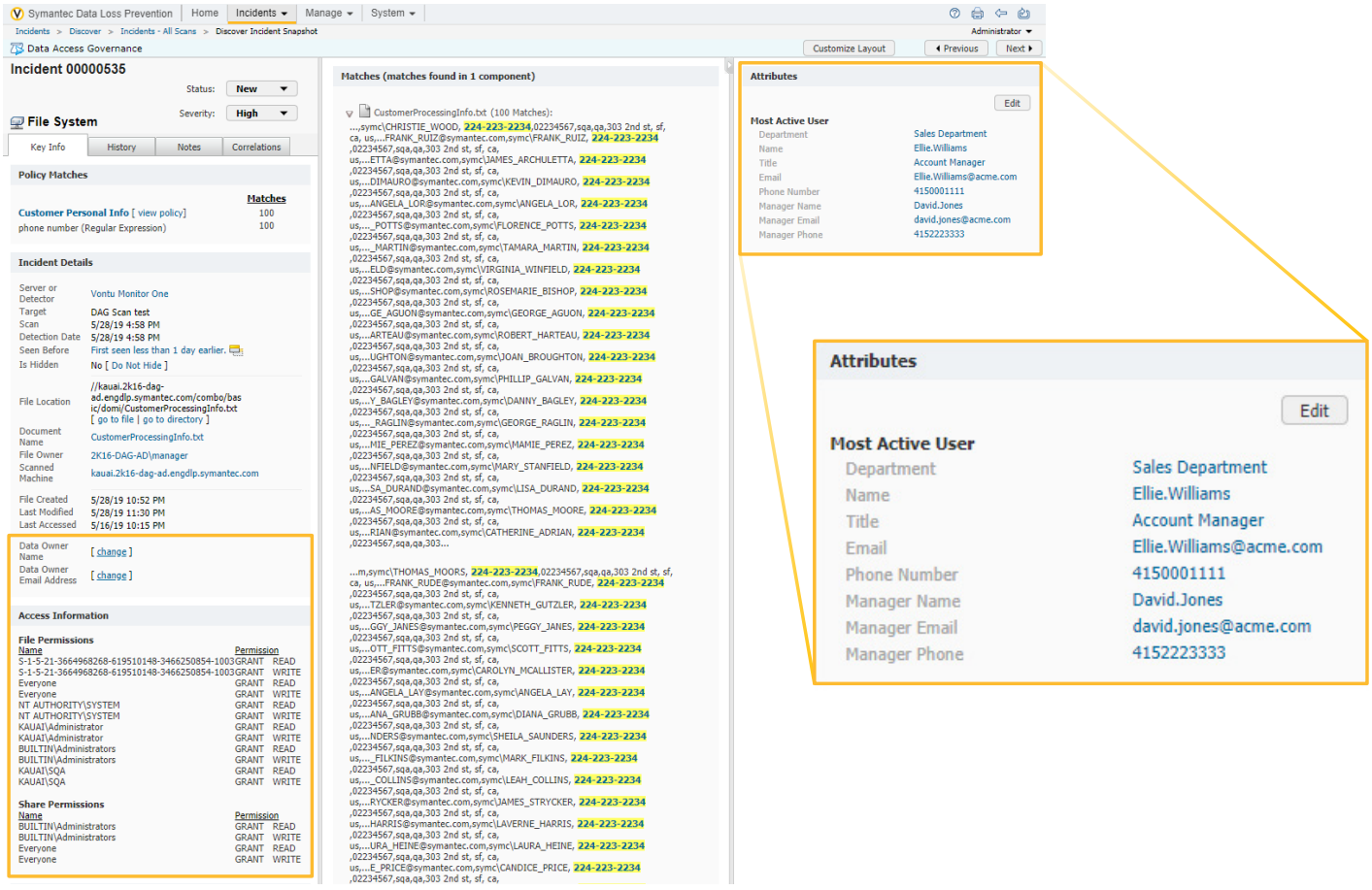
- **Effective Access Calculation** – Gather all user permissions to shared folders and correlate the information with Active Directory, system-level rights, and policies to effectively determine each way a user can access a given resource, as well as the level of permission each access avenue grants.
- **File Metadata Collection** – Understand everything there is to know about every file, including file types, attributes, owner info, and even tags applied by other products or processes.

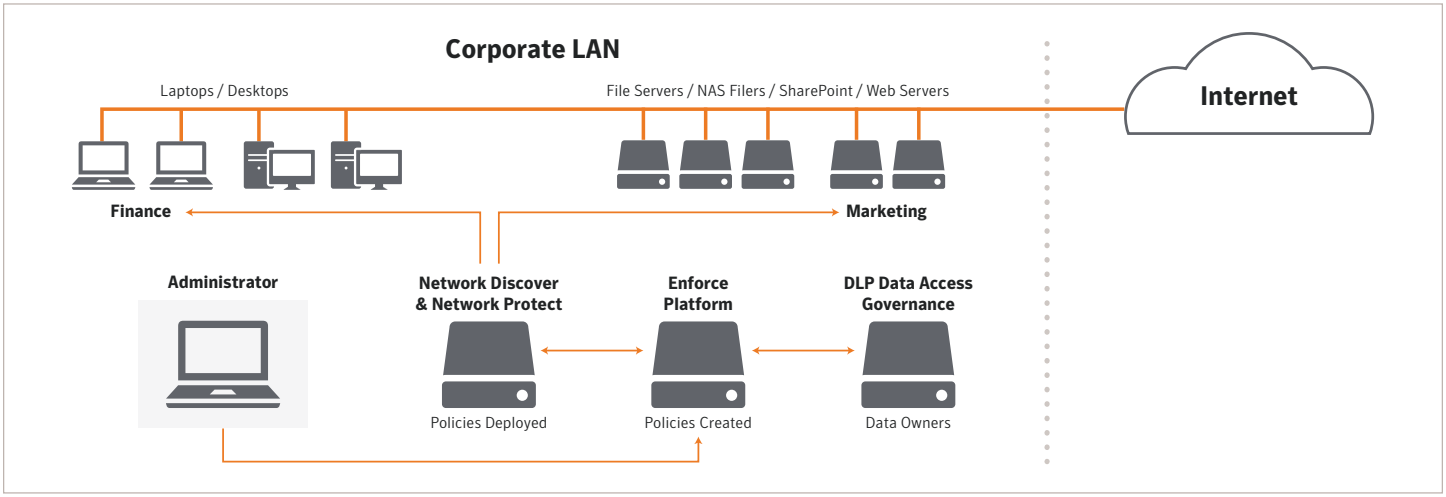
File Activity Monitoring

- **Activity Monitoring** – Monitor activity across Windows and NAS file systems, and SharePoint sites for complete insight into which files, folders, and shares users are accessing, as well as what they're doing with the data.
- **Probable Owner Identification** – Identify the Most Probable Owner of every share or folder via multiple layers of context, including common managers, content creators, and most active users.

Access Governance

- **Governance Workflows** – Easily implement governance workflows like Entitlement Reviews and Self-Service Access Requests to safely provide data custodians the ability to control access to the data they own and end-users the ability to request access to the data they need.
- **Access Transformation** – Automatically assign a least privilege model to your file shares that can be used to govern access going forward. Do all this without interrupting regular business operation and user access to the files and folders they use the most.
- **Access Change Modeling & Recommendations** – Simulate the impact of changes before you make them and receive recommendations on where access can be reduced or revoked based on real user activity.





Architecture

DLP Data Access Governance consists of a Management Console and a reporting portal. It is based on a distributed client-server architecture that is designed to scale to the demands of large enterprises.

DLP Data Access Governance works with a wide range of data sources: NetApp®, DellEMC®, Microsoft® Windows® and SharePoint®. It uses native APIs to collect file transaction data, while minimizing server performance overhead. File activity data is indexed and made available for search. Symantec DLP Data Access Governance supplies data ownership and data access information to Symantec DLP's Enforce console for correlation with network file incidents generated by Network Discover, thus helping practitioners make informed decisions on remediation actions. It also provides a management console for visualizing data access and reviewing permissions and detailed logs.

Supported Platforms

- Windows File Servers
- Unix/Linux File Systems
- Network Attached Storage (NAS) Devices
- Microsoft SharePoint
- Symantec Data Loss Prevention 15.1 and 15.5

Product Requirements

- Required: No DLP prerequisites but Symantec DLP Network Discover is recommended
- Microsoft SQL Server

About Symantec Data Loss Prevention product family

Symantec DLP is a content-aware solution that discovers, monitors and protects confidential data wherever it is used or stored across cloud, and on-premises environments. It safeguards your brand and reputation, protects you against insider threats, and enforces security and compliance policies across borders.

About Symantec Data Loss Prevention Network Discover: it finds exposed sensitive data by scanning network file shares, databases, and other enterprise data repositories including local file systems on Windows, Linux, AIX, and Solaris servers, NAS filers, Lotus Notes and SQL databases, and Microsoft Exchange and SharePoint servers.

About Symantec Data Loss Prevention Network Protect: it adds file protection capabilities on top of Network Discover. It automatically cleans up and secures the exposed files found by Network Discover. Network Protect offers a broad range of remediation options including quarantining or moving files, copying files to a quarantine area, or applying policy-based encryption and digital rights to files. It informs and educates business users about policy violations by leaving a marker text file in the file's original location to explain where and why it was quarantined.

To learn more about Symantec Data Loss Prevention visit go.symantec.com/DLP.

Threatscape

To learn more, contact us via info@threatscape.com or on 0203 653 0000 (UK) or 01 901 7000 (Ireland) | www.threatscape.com

Symantec

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

20A252415_DS_DLP_AccessGovernance_EN