AURORA

Symantec

SAMPLE REPORT

Data Classification Technical Assessment

Update: February 13th, 2015

aurorait.com
888.282.0696
info@aurorait.com

2510 W. 237th Street | Suite 202 | Torrance, CA 90505

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Statement of Confidentiality

This Confidential Information is being provided to Customer ABC as a deliverable of this consulting engagement. The sole purpose of this document is to provide you with the results of, and recommendations derived from this consulting engagement. Each recipient agrees that, prior to reading this document, it shall not distribute or use the information contained herein for any purpose other than those stated.

aurorait.com
888.282.0696
info@aurorait.com

2510 W. 237th Street | Suite 202 | Torrance, CA 90505

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Table of Contents

aurorait.com
888.282.0696
info@aurorait.com
2510 W. 237th Street | Suite 202 | Torrance, CA 90505
© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Executive Summary

Company ABC has contracted with Aurora to provide technical consulting services for Data Classification. The engagement leverages Symantec's Data Loss Prevention suite, a world class technology designed to protect a company's valuable data. Data Classification and Data Loss Prevention work hand in hand to limit risk and exposure of sensitive data.

The engagement began on March 1st, 2014 and includes planning, business requirements and data gathering, data classification technical assessment, and reporting activities.

Aurora has worked with the customer to perform a Data Classification Assessment. This assessment includes an initial Business Requirements workshop, followed by a technical assessment leveraging Data Loss Prevention and Data Insight technologies. The objective of the assessment is to determine the customer's current data classification posture, and provide information for improving data classification and limiting data loss.

Based on the Business Requirements Workshop performed March 15th, 2014, Company ABC has identified three (3) high-risk repositories that are in scope for this engagement:

- **Server 01 Users Share (\\server01.domain.local\Users$)**
  This server stores the End Users redirected My Documents folders
- **Server 02 HR Department Share (\\server02.domain.local\departments\HR)**
  This server stores the HR departments shared data
- **Business Reconciliation Server01 (busrec01.domain.local)**
  This server process banking reconciliation and is subject to PCI compliance

Currently, Company ABC classifies newly created data as sensitive and non-sensitive. However, these classifications do not currently have technical handles in place to ensure the proper handling of the data. As well, older data has not been classified, and process do not exist to retroactively classify this data.

For the purpose of this engagement, Company ABC focused on the following types of data:

1. Sensitive data older than 18 months
2. Non-sensitive data older than 36 months
3. Credit Card Numbers
4. Internal HR Forms and Social Security Numbers

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

AURORA

Symantec

SAMPLE REPORT

Aurora Data Classification Technical Assessment

As a result of the Data Classification Technical Assessment, Company ABC would be able to quickly reduce its risk to data loss. The following was determined:

- Approximately 30% of all data found on the in-scope repositories was older than 36 months, and based on business guidelines, can be safely deleted or archived.
- Approximately 2600 files were found to be sensitive and had not been access in the last 18 months (both Server01 and Server02). Using the data ownership determination from Data Insight, Company ABC can quickly determine if this data can be deleted or moved with the input of the true data owner.
- Credit Card data does not exist in bulk outside the Banking Reconciliation Server, with only a few cases of Credit Cards existing on the Server 01 and Server 02 shares. However, the Banking Reconciliation Server had a logical flow misconfiguration, and thousands of copies of credit card numbers were being stored in temp files within the Windows System directory. A correction to this business process can drastically reduce the risk associated with this machine.
- Approximately 400 HR forms were found outside the standard location where they should be stored. Using the Network Protect portion of Symantec Data Loss Prevention, these files could be automatically moved to the correct location with the correct ACL permissions.

aurorait.com
888.282.0696
info@aurorait.com

2510 W. 237th Street | Suite 202 | Torrance, CA 90505

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Project Contacts

Customer Contacts

Role	Name	Phone	Email
Project Managers			
Technical Team Leads			
Network Infrastructure Representative			
Information Security Representative			
System Administrator			
Server Management Representative			
Desktop Management Representative			
Audit Representative			
Database Administrator			
LDAP Administrator			
Business Unit Team Leads			
Risk, Privacy, and Compliance Representatives			
Investigations / Forensics Representative			

Aurora Contacts

Role	Name	Phone	Email
DLP Consultant			
DLP Account Manager			
DLP System Engineer			

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

AURORA

Symantec

SAMPLE REPORT

Aurora Data Classification Technical Assessment

Data Classification Overview and Best Practices

Data Classification is used to develop and implement processes to continually assess and classify information assets. This is necessary to truly implement precautions that must be taken to ensure the availability, integrity, and confidentially of information assets based on their value. Certain information about an asset is required to properly classify it:

- Data Owner
- Archive Requirements
- Compliance Requirements
- Associated Business Function
- Sensitivity

According to Carnegie Mellon, data can be classified into one of three sensitivity levels or classifications:

- **Restricted Data**
  Restricted data is that which the unauthorized disclosure, alteration, or destruction would cause a significant level of risk to the company. This type of data should be protected with the highest level of security controls.
- **Private Data**
  Private data is that which the unauthorized disclosure, alteration, or destruction would cause a moderate level of risk to the company. This type of data should be protected with a reasonable level of security controls.
- **Public Data**
  Public data is that which the unauthorized disclosure, alteration, or destruction would cause little or no risk to the company. This type of data should be protected with a reasonable level of security controls.

Data Classification Maturity Level

The Data Classification Maturity Level is a practical way to assess a Company's current Data Classification capability.

Data Classification Maturity Stage	Description of Maturity Stage
0	No information assets are classified or assets are randomly classified.
1	Assets are classified at a high level or organizational level, assets are unidentified.
2	Processes are developed and implemented allowing assets to be classified in detail.
3	New assets are classified in detail.
4	Legacy assets are classified in detail.
5	Assets are classified, and processes exist that allow for asset reassessment and new asset classification.

Symantec DLP Network Discover and Protect

Typically residing in the data center, Symantec DLP Network Discover identifies sensitive data exposed on or residing on file servers, databases, collaboration platforms, web sites, desktops, laptops, and other data repositories. Symantec Repository Scanners allow detection of confidential content on SharePoint, Exchange, LiveLink, Documentum, and Web servers.

Typically residing in the data center, Symantec DLP Network Protect automatically relocates, copies, or quarantines exposed confidential data.

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

AURORA

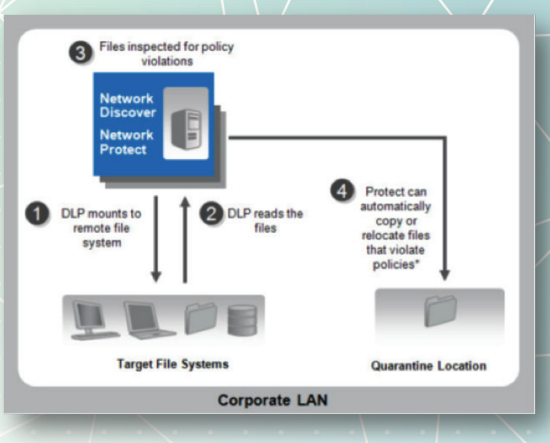
Symantec

SAMPLE REPORT

Aurora Data Classification Technical Assessment

Symantec Data Insight

Symantec Data Insight helps organizations improve unstructured data governance through actionable intelligence into data ownership, usage and access controls. Data Insight's reporting, analytics and visualization capabilities help drive efficiency and cost reduction across the data lifecycle as well as help drive improved protection of sensitive data and achieve compliance.



Business Requirements

The business requirements of the assessment include limiting data loss in the following areas:

- The Users share on Server01
- The HR Department share on Server02
- One of the Banking Reconciliation Servers

Limiting data loss will be done by analyzing both the content of the data, as well as the metadata surrounding the files. Leveraging Data Insight to determine last access dates and true data ownership based on access patterns, Company ABC can age out older data quickly and safely.

Another major driving factor for the Data Classification Technical Assessment is PCI compliance. Company ABC has a number of servers that process credit card data on a regular schedule. While these servers and the data they processes are already classified as sensitive, Company ABC wants to ensure the correct technical handles are in place to process the data securely.

Across all repositories, the following types of data are to be protected:

- Credit card information
- Social Security Numbers
- Internal HR forms

Customer Privacy Requirement

Company ABC is tasked with protecting its Customers information. Initially, the focus is on Credit Card numbers to ensure PCI compliance.

Metadata and Data Aging Requirement

Company ABC will be leveraging information gathered in this assessment to effectively age out old sensitive data. This will be done by looking at the last access date and true data ownership of discovered sensitive data.

Employee Privacy Requirement

Company ABC wants to make sure that sensitive employee information doesn't exist on open file shares. As part of this assessment, Company ABC would like to see if any internal HR forms exist on open file shares.

aurorait.com

888.282.0696
info@aurorait.com

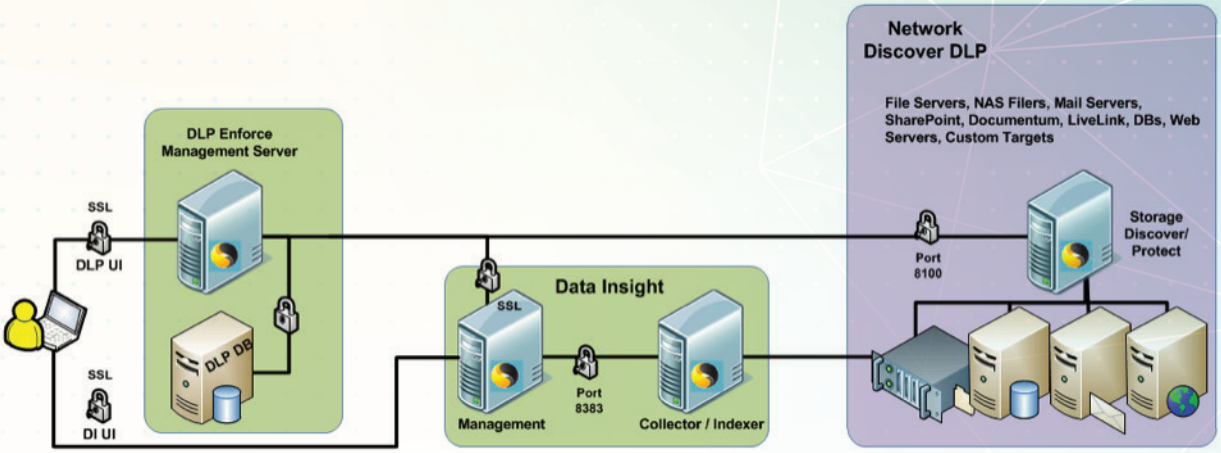
2510 W. 237th Street | Suite 202 | Torrance, CA 90505

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Technical Information and Configuration

Network Architecture

The diagram below shows the overall network architecture of the tools used during the Data Classification Technical Assessment. Please note that all items pertaining to Symantec DLP and Data Insight are running on a single physical server for the purpose of this assessment.



Customer Network Details

IP Address for DLP Network Discover	10.1.1.50
IP Address for Data Insight	10.1.1.51
DNS Server(s)	10.1.1.20, 10.1.1.21
Active Directory Server	10.1.1.10
Scanning Hours	7pm – 7am
Pause during Business Hours	Yes

Repositories Scanned

Server	Share	Credential Used	Agent Installed
server01.domain.local	Users%	DOMAIN\svc_backup	Yes
server02.domain.local	Departments\HR	DOMAIN\svc_backup	Yes
busrec01.domain.local	Entire System	DOMAIN\Administrator	No

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Results and Reports

This section details the findings for each of three repositories within scope. This includes summaries of the findings for each server in scope, along with any important details. For detailed export reports, please see Appendix A.

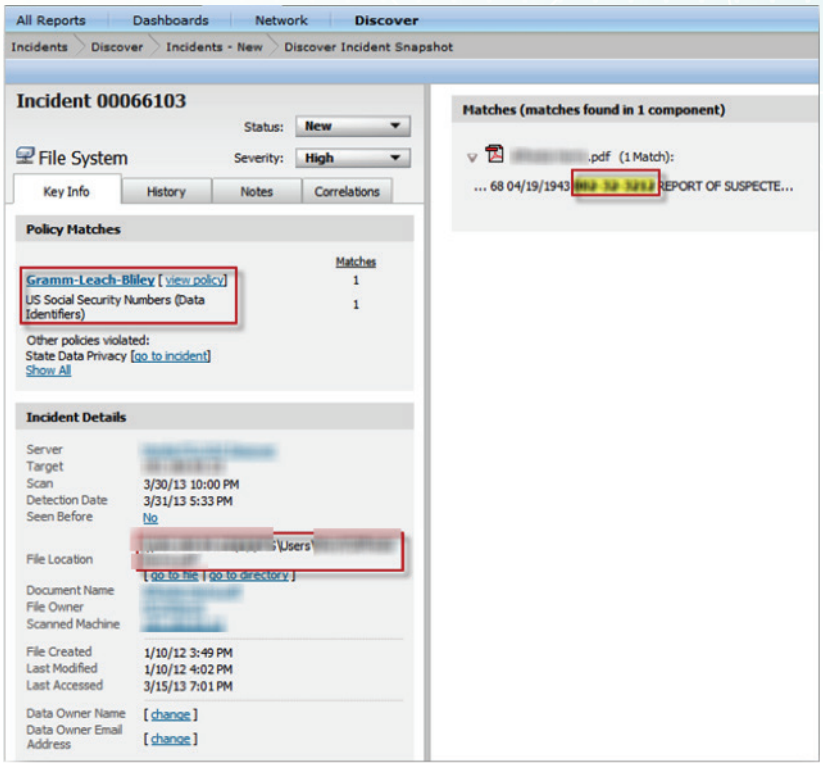
Server01 Users Share

Server01 houses the re-directed My Documents folders for all the internal Users at Company ABC. While the company's Acceptable Use Policy states that Users should not store sensitive data on these shares, many Users have been found to violate this requirement. Using Symantec DLP and Data Insight, the following summarization of data was determined.

Total Data	1 million files / 300 GB
Data over 36 months old	250,000 files / 100 GB
Data over 18 months old	350,000 files / 150 GB
Data considered sensitive	1,700 files / 1.1 GB

The locations of these files are specified in the reports in Appendix A. For many of the files, it was determined they were backups that the User's had placed on the share when backing up or migrating their Desktops. As a whole, the permissions on the different folders in the share were correct.

An example of a sensitive pdf is shown below, which contains an external partner's Social Security Number.



© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Server02 HR Department Share

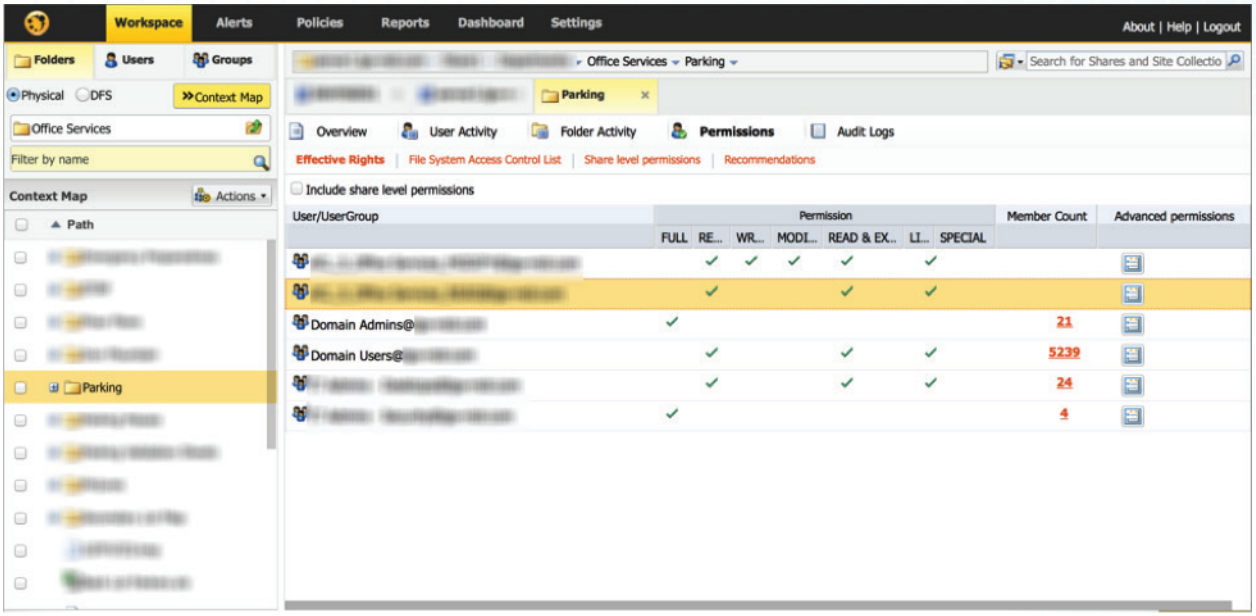
The HR Department share on Server02 is known to contain sensitive data. However, Company ABC was interested in determining how much was sensitive, and who was accessing the data. A summarization of the scanning results are shown below.

Total Data	10,000 files / 2 GB
Data over 36 months old	5,000 files / 1 GB
Data over 18 months old	5,800 files / 1.2 GB
Data considered sensitive	1,100 files / 0.2 GB
Most common ACL	Domain Users

Specific path permissions and scan result reports can be found in Appendix A.

Finding sensitive data on the HR Department share was expected. However, the ACL permissions and access patterns were surprising. Many Users who should have access to the folder were accessing it through incorrect ACLs. For example, on many folder Inheritance was broken and valid Users were gaining access through the "Domain users" ACL.

In remediating one of the folders, effective permissions were removed from the Domain Users group and given to only those who needed access. This required access was determine in part by the AD Security Group as well as the access patterns over the past 6 months. This is shown in the screenshots below.



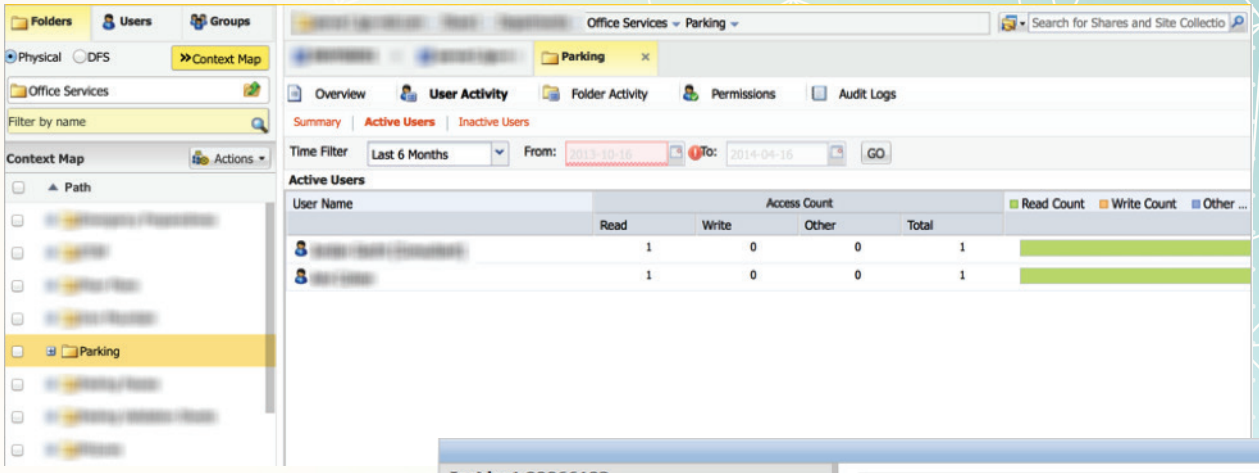
© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

AURORA

Symantec

SAMPLE REPORT

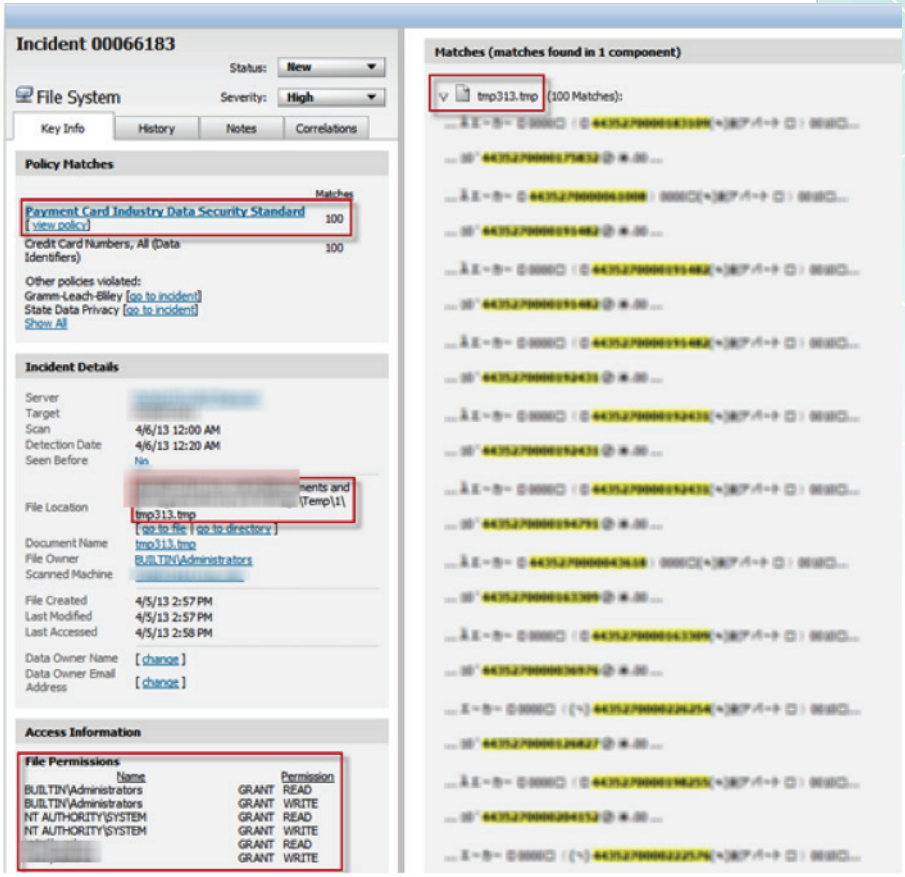
Aurora Data Classification Technical Assessment



Banking Reconciliation Server

The Banking Reconciliation Server is known to handle sensitive data, and was meant to act as a baseline for a server that does not store sensitive data. However, during the course of the assessment, it was determined that the server temporarily stored processed data in a location the company did not know about.

After processing credit card data, the server used PGP to securely wipe all working directories that held credit card data. What was not known is that the Windows Operating System was storing the computational values in temporary files during the encryption process. These temp files were not identified during the initial setup of the process, and therefore were not wiped using PGP like the final output files.



As a result of the Data Classification Technical Assessment, Company ABC added the C:\Windows\System32\Temp directory to the list of directories that are PGP wiped after processing. This greatly reduces the risk associated with this machine and helps maintain PCI compliance.

aurorait.com

888.282.0696

info@aurorait.com

2510 W. 237th Street | Suite 202 | Torrance, CA 90505

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Assessment Summary and Next Steps

The Data Classification Technical Assessment started with a Business Requirements discussion with Company ABC. It was determined the company's Data Classification Maturity Level was between 1 and 2, since a classification scheme existed, but processes were not in place to actively classify and monitor new or old assets.

Substantial sensitive data was found in both expected and unexpected locations. A number of situations have quick resolutions that can put into place to quickly reduce overall risk and exposure:

- Users backup local and old data to their Users$ share and then forget they stored it there. This data can be aged out, or the User can be contacted and asked to delete/move the data.
- The HR Department Share (and other similar shares) can have their ACL permissions drastically reduced to limit unexpected exposure.
- The Banking Reconciliation Server should have an additional process put into place to ensure temporarily stored data is destroyed or encrypted. This was implemented as part of the assessment, since the resolution was easily handled by Company ABC's Admins.

At the conclusion of the Data Classification Technical Assessment, a number of items were identified that would be beneficial for Company ABC to implement. Based on a Data Classification Maturity Level between 1 and 2 for Company ABC, better practices for finding and assessing data should be put into place. This includes:

- Increasing the data classification levels from either sensitive or non-sensitive to a three-level classification will help further categorize assets. For example, Restricted, Private, and Public.
- Actively monitor and re-assess both new information assets as well as older assets. This should be done both as a business process as well as a technical handle:
  - Employees should be regularly reminded of what type of data can reside on which network locations.
  - Technical solutions such as Symantec Data Loss Prevention and Data Insight should be used to constantly monitor and remediate unclassified or misclassified data. The solution can also be used to move data to the correct protected location.

Aurora would be honored in assisting Company ABC in implementing any of the above mentioned business processes and technical solutions.

aurorait.com
888.282.0696
info@aurorait.com

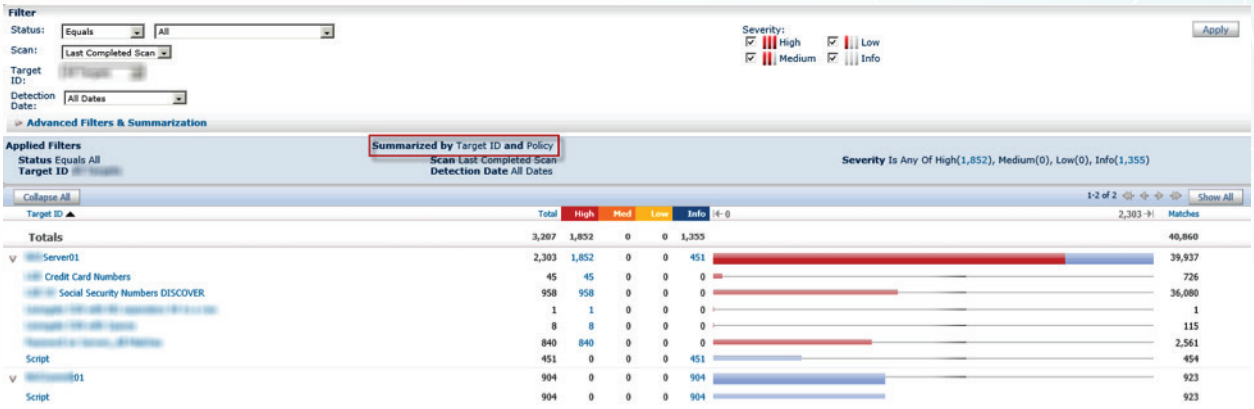
2510 W. 237th Street | Suite 202 | Torrance, CA 90505

© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.

Appendix A: DLP and Data Insight Exported Reports

Not included as part of sample report, but included in Data Classification Technical Assessment. These reports can be used by Companies to quickly address high-risk repositories. A screenshot of access details and DLP incident details are shown below as examples.

HeaderTable													
Created By	Report Type	Report Name											
Symantec Data Insight 4.5.	Access Summary for Paths	Access Summary											
ParamTable													
Name	Value												
max_row_count:	100000												
Paths:	\\server01.domain.local\Users$\												
Show Custom Attributes:	FALSE												
Start Time:	Nov 19, 2011, 11:55 AM												
End Time:	Feb 17, 2014, 11:55 AM												
TopN													
Access Path	Account Name	User	Activity Count	Top Activity Count	Top Activity Percent								
Aabrams	aabrams	aabrams	103	56	30								
Access Path Summary													
File Server \ Web Applicat	Access Path	Path Type	User Name	Account Name	Create	Delete	Read	Write	Rename	ipaddress	BU Name	BU Owner	Total Access
server01.domain.local	\Users%\aabrams	CIFS	aabrams	aabrams	3	12	56	32	2	192.168.100.40	Finance	ttaylor	103



© 2015 Aurora. All Rights Reserved. All other logos and trademarks are the property of the respective trademark owners.