Syntergy Webinar:
Your OpenText Content Server Data is at Risk

Vijay Sharma, VP Sales & Business Development
Ivan Gudov, Solutions Specialist
Robbie Spencer, Product Manager

- It’s 3am - who’s accessing our documents?
- Somebody downloaded 50GB of content – who & why?
- How do we monitor Content Server for unusual or nefarious activity?
- How do I monitor classified and records management documents for access
- How do I prevent data breaches to avoid negative impact on our corporate brand and lawsuits
- How do I Identify and secure sensitive content in Content Server libraries?
- What content do we have, where does It reside & who is using it?
- How is our customer’s data securely being handled inside our organization?
- How do I safeguard
    - ➢ Personal Identifiable Information (PII)?
    - ➢ Protected Health Information (PHI)?
    - ➢ Payment Card Industry (PCI) and other confidential data in Content Server?

Agenda

SYNTERGY

- Introduction
  - Syntergy Overview
  - Why Implement a Data Loss Prevention (DLP) Strategy
  - Impact of a Data Breach
- Syntergy Content Sentry Demo
  - Next Generation Datacentric DLP Solution for OpenText Content Suite
  - Future Roadmap
- Q&A

SYNTERGY

Syntergy Corporate Profile

- 20 Years Experience Serving Global Customers
- Headquarters in San Diego, CA
- Key Executives and Engineers from OpenText and other ECM leaders.
- Distributed Staff & Partners throughout USA/Canada/Europe/Asia Pacific
- OpenText Technology Partner
- SkySync Elite Partner
- Microsoft Gold Partner

OPENTEXT Partner
TECHNOLOGY

SKYSYNC

Microsoft Partner
Gold Portals and Collaboration
Gold Web Development

- Leader in OpenText Content Suite Data Moving Solutions
- Enhance the Use, Performance & Security of OpenText ECM Software
- Provider of more than 20 Content Suite Products to Increase Usability & Adoption
- Consulting Services Expertise in Upgrades, Migrations, Custom Module Development, Deployment Assistance, Performance Tuning, Taxonomy Consulting, Integration, Systems Analysis, Training and Support
- Key Differentiators – Technical Expertise, Responsiveness & Value

Content Suite - Popular Technology Solutions

SYNTERGY

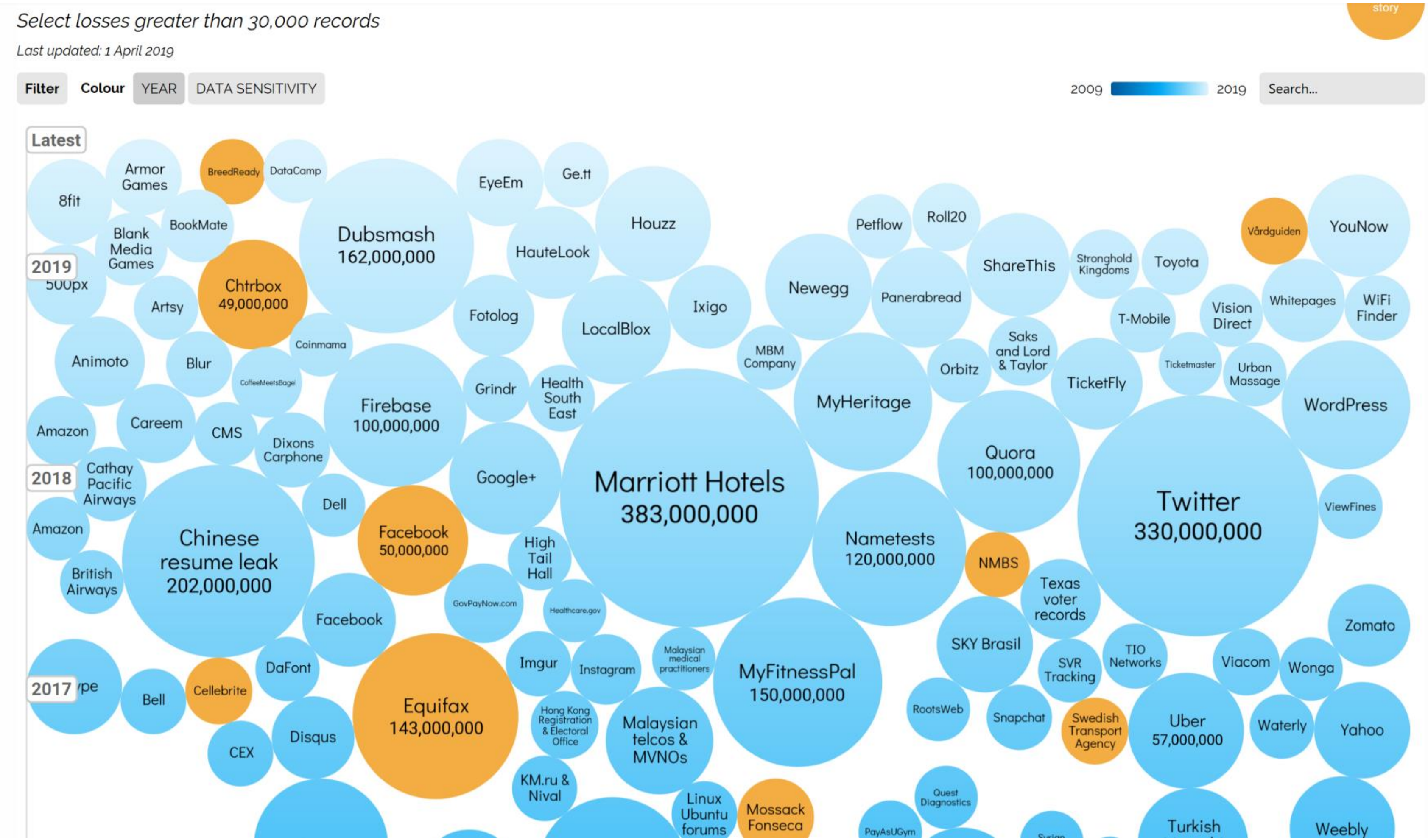
- Zero Downtime, One Hop Upgrade to Content Server 16.X
- Consolidation of Livelink/Content Servers to Content Server 16.X
- Change Content Server Infrastructure - Unix to Microsoft Windows or Database Vendor (e.g. Oracle to SQL)
- 7x24x365 "Always-On" Content Servers for High Availability/Disaster Recovery
- Powerful Bulk Data Loading & Meta Data Management Solutions
- Synchronize Geo-Distributed OpenText Content Servers in Real Time – Making Content Server Global, Fast and Highly Available
- Data Centric Data Loss Prevention (DLP) for Content Server
- Sync & Integrate Content Server with major Cloud Services, ECM platforms and Network File Systems e.g. BOX, OneDrive, Microsoft O-365, SharePoint, Google, Dropbox using SkySync **New

What is Data Loss Prevention (DLP)?

SYNTERGY

- **Data Loss Prevention (DLP)** is a strategy to assist System/Network Administrators and Security Teams to:
  - Control what data end users can access & transfer
  - Detect anomalous/nefarious user activity and take action
  - Identify where does sensitive data reside
  - Control what data users can view and transfer so that users cannot accidentally or maliciously share data that could put the organization at risk.

World's Biggest Data Breaches



Select losses greater than 30,000 records

Last updated: 1 April 2019

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Impact of Data Breaches

Ponemon Institute Research Report (August 26, 2018) - https://www.ponemon.org/

- Data Breaches Caused by Insiders Increase in Frequency and Cost
- Companies need to intensify their efforts to minimize the insider risk because of rising costs and frequency of incidents.
- Global Study, on what companies have spent to deal with a data breach caused by a careless or negligent employee or contractor, criminal or malicious insider or a credential thief.
  - 717 IT and IT security practitioners in 159 organizations in North America (United States and Canada), Europe, Middle East and Africa, and Asia-Pacific were interviewed.
- While the negligent insider is the root cause of most breaches, the bad actor who steals employees' credentials is responsible for the most costly incidents.
- If the incident involved a negligent employee or contractor, companies spent an average of $283,281.
- The average cost more than doubles if the incident involved an imposter or thief who steals credentials ($648,845).
- Hackers cost the organizations represented in this research an average of $607,745 per incident.
- It took the companies more than two months on average to contain an insider incident. Only 16 percent of incidents were contained in less than 30 days.

Company & Personal Impact

- Damage to the Company Brand, Reputation and Revenue Loss
- Resignations and Job losses
- Nearly 70% of breaches impact a secondary victim

Content Security and the Insider Threat

- The majority of SECURITY spending is to prevent external attacks
- Perimeter-based security can't provide security or protect privacy
- However, the impact of INSIDER THREATS, although less frequent, are often more damaging
- Businesses need TO RE-EVALUATE RISK ASSESSMENT and align resources appropriately
- As collaboration technologies move to MULTIPLE DEVICES and THE CLOUD this becomes even more important.
- Clients/Partners are demanding proof of implementation of Data Loss Prevention (DLP) solutions to ensure that their personal information and Intellectual Property is adequately protected

Challenges of Protecting Business Data

SYNTERGY

Activity Based Monitoring

- The "Snowden" conundrum

Location vs Content

- Are we sure where our sensitive content is located?
- What happens when someone moves the sensitive content?

Partial Protection & Check Box Mentality

- Will our policies, procedures and implementation stand up to scrutiny?
- Are we truly protecting our sensitive content or checking a feature box?

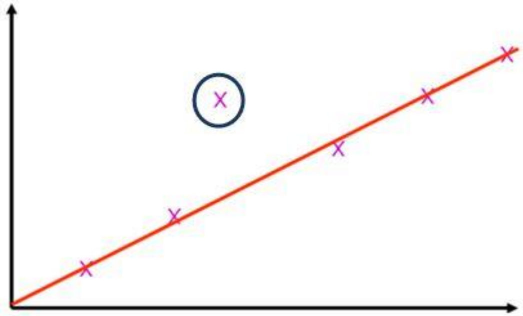
Users, Users, Users

- Changing workforce – New Apps, Mobile, BYOD
- Productivity Hindrance
- Using "Shadow IT" to get their jobs done
- Weak Passwords & Management Practices

Data Loss Prevention in Content Server

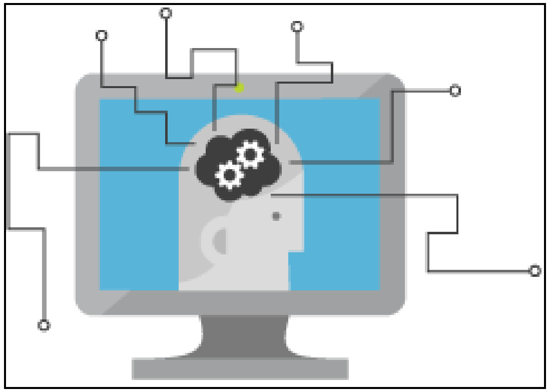
Anomaly Detection

- Differences from established baselines
- Location variations
- Volume of activity

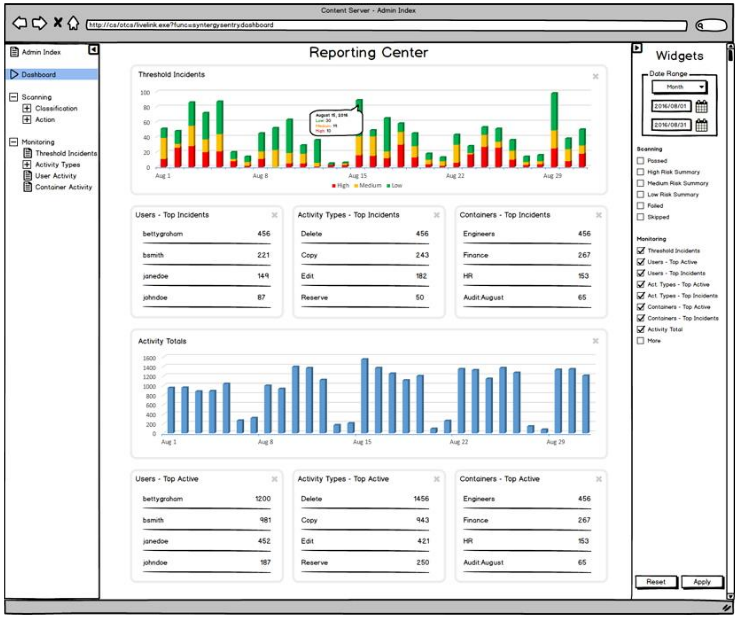


Continuously Detecting Sensitive Content (Scanning) *Future

- Machine Learning
- Content Analytics
- Real Time Detection Option



Content Sentry Demo



- Admin Index
- Dashboard
- Scanning
  - Classification
  - Action
- Monitoring
  - Threshold Incidents
  - Activity Types
  - User Activity
  - Container Activity

Reporting Center

Threshold Incidents

Users - Top Incidents	
bettygraham	456
bsmith	221
janedoe	149
johndoe	87

Activity Types - Top Incidents	
Delete	456
Copy	243
Edit	182
Reserve	50

Containers - Top Incidents	
Engineers	456
Finance	267
HR	153
Audit:August	65

Activity Totals

Users - Top Active	
bettygraham	1200
bsmith	981
janedoe	452
johndoe	187

Activity Types - Top Active	
Delete	1456
Copy	943
Edit	421
Reserve	250

Containers - Top Active	
Engineers	456
Finance	267
HR	153
Audit:August	65

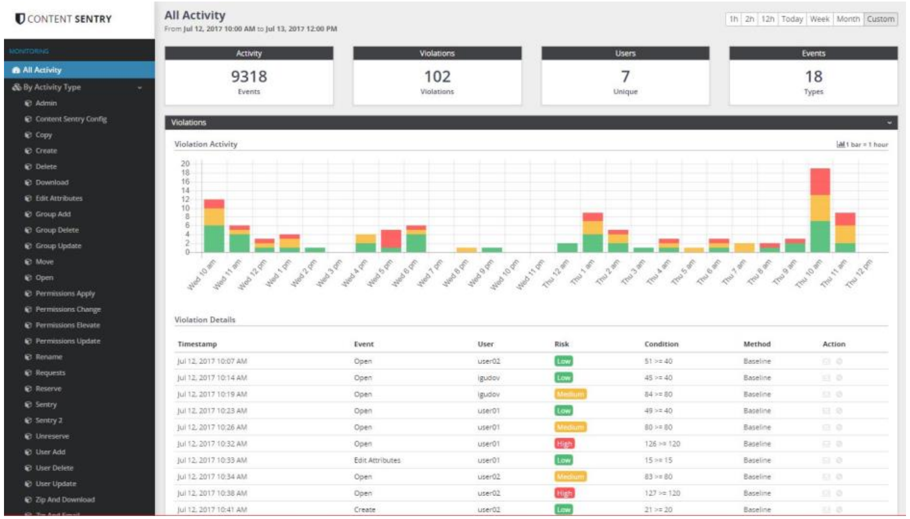
Widgets

Date Range: Month
2016/08/01
2016/08/31

Scanning
- ☐ Passed
- ☐ High Risk Summary
- ☐ Medium Risk Summary
- ☐ Low Risk Summary
- ☐ Failed
- ☐ Skipped

Monitoring
- ☑ Threshold Incidents
- ☑ Users - Top Active
- ☑ Users - Top Incidents
- ☑ Act. Types - Top Active
- ☑ Act. Types - Top Incidents
- ☑ Containers - Top Active
- ☑ Containers - Top Incidents
- ☑ Activity Total
- ☐ More

Reset | Apply



MONITORING
- All Activity
- By Activity Type
  - Admin
  - Content Sentry Config
  - Copy
  - Create
  - Delete
  - Download
  - Edit Attributes
  - Group Add
  - Group Delete
  - Group Update
  - Move
  - Open
  - Permissions Apply
  - Permissions Change
  - Permissions Elevate
  - Permissions Update
  - Rename
  - Requests
  - Reserve
  - Sentry
  - Sentry 2
  - Unreserve
  - User Add
  - User Delete
  - User Update
  - Zip And Download
  - Zip And Email

All Activity

From **Jul 12, 2017 10:00 AM** to **Jul 13, 2017 12:00 PM**

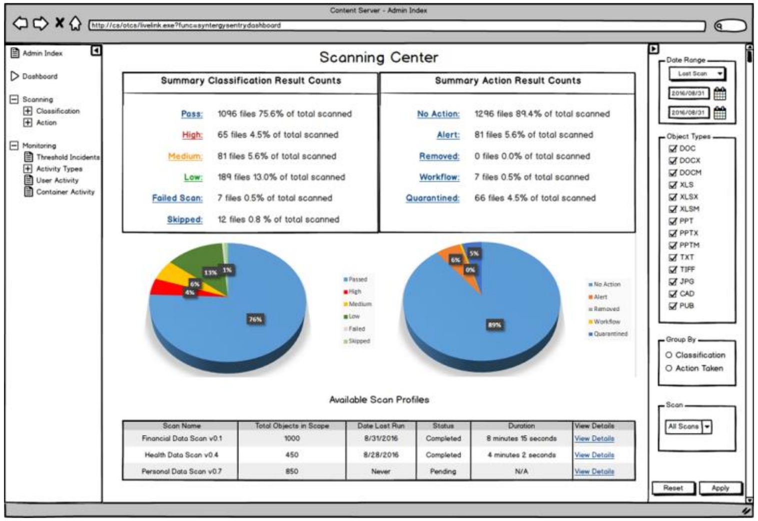
Activity	Violations	Users	Events
9318 Events	102 Violations	7 Unique	18 Types

Violations

Violation Activity

Violation Details

Timestamp	Event	User	Risk	Condition	Method	Action
Jul 12, 2017 10:07 AM	Open	user02	Low	51 >= 40	Baseline	
Jul 12, 2017 10:14 AM	Open	igudov	Low	45 >= 40	Baseline	
Jul 12, 2017 10:19 AM	Open	igudov	Medium	84 >= 80	Baseline	
Jul 12, 2017 10:23 AM	Open	user01	Low	49 >= 40	Baseline	
Jul 12, 2017 10:26 AM	Open	user01	Medium	80 >= 80	Baseline	
Jul 12, 2017 10:32 AM	Open	user01	High	126 >= 120	Baseline	
Jul 12, 2017 10:33 AM	Edit Attributes	user01	Low	15 >= 15	Baseline	
Jul 12, 2017 10:34 AM	Open	user02	Medium	83 >= 80	Baseline	
Jul 12, 2017 10:38 AM	Open	user02	High	127 >= 120	Baseline	
Jul 12, 2017 10:41 AM	Create	user02	Low	21 >= 20	Baseline	



- Admin Index
- Dashboard
- Scanning
  - Classification
  - Action
- Monitoring
  - Threshold Incidents
  - Activity Types
  - User Activity
  - Container Activity

Scanning Center

Summary Classification Result Counts	
Pass:	1096 files 75.6% of total scanned
High:	65 files 4.5% of total scanned
Medium:	81 files 5.6% of total scanned
Low:	189 files 13.0% of total scanned
Failed Scan:	7 files 0.5% of total scanned
Skipped:	12 files 0.8 % of total scanned

Summary Action Result Counts	
No Action:	1296 files 89.4% of total scanned
Alert:	81 files 5.6% of total scanned
Removed:	0 files 0.0% of total scanned
Workflow:	7 files 0.5% of total scanned
Quarantined:	66 files 4.5% of total scanned

Available Scan Profiles

Scan Name	Total Objects in Scope	Date Last Run	Status	Duration	View Details
Financial Data Scan v0.1	1000	8/31/2016	Completed	8 minutes 15 seconds	View Details
Health Data Scan v0.4	450	8/28/2016	Completed	4 minutes 2 seconds	View Details
Personal Data Scan v0.7	850	Never	Pending	N/A	View Details

Date Range: Last Scan
2016/08/31
2016/08/31

Object Types
- ☑ DOC
- ☑ DOCX
- ☑ DOCM
- ☑ XLS
- ☑ XLSX
- ☑ XLSM
- ☑ PPT
- ☑ PPTX
- ☑ PPTM
- ☑ TXT
- ☑ TIFF
- ☑ JPG
- ☑ CAD
- ☑ PUB

Group By
- ○ Classification
- ○ Action Taken

Scan: All Scans

Reset | Apply

Product Roadmap

- Sensitive Content Detection in Content Server & Other Systems (e.g. PII, PCI, PHI, Custom)
- Geolocation / IP Address Monitoring
- Monitoring Policies
- Security Clearance Support
- Incident Management Center (Workflow)
- Integration with Microsoft Outlook
- SIEM Integration - Splunk, ArcSight, QRadar

SYNTERGY

Questions?

Vijay Sharma

vsharma@syntergy.com

Tel: 415-543-0602