
Eliminating Data Security Threats: *Combating Insider Threat*

Terry Boedeker, CISSP
Solutions Engineer, Varonis Systems
Professional Techniques – T32



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Agenda:

About Varonis

- ◊ Security Breaches & Industry Trends
- ◊ Drowning in the “Depths of Defense”
 - ◊ FBI’s Top 5 Lessons
- ◊ Closing the Vault & Behavioral Analytics
- ◊ Big Data: Challenges & Opportunities
 - ◊ Human generated data
-  *How can Varonis help?*
- ◊ Heckle and throw things / Q&A



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"



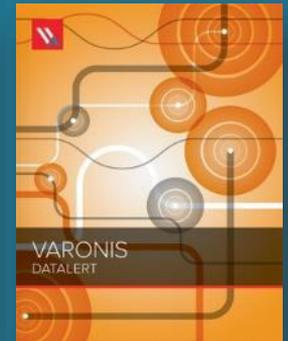
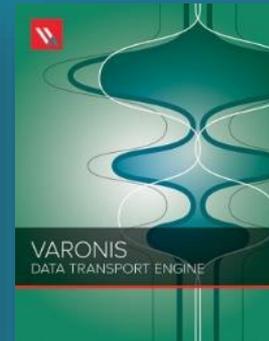
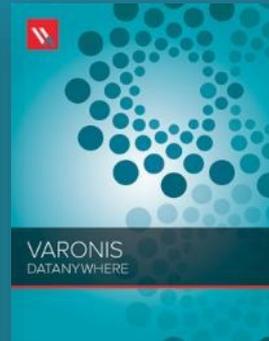
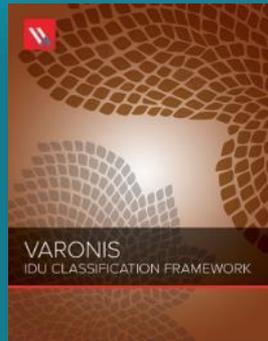
About Varonis

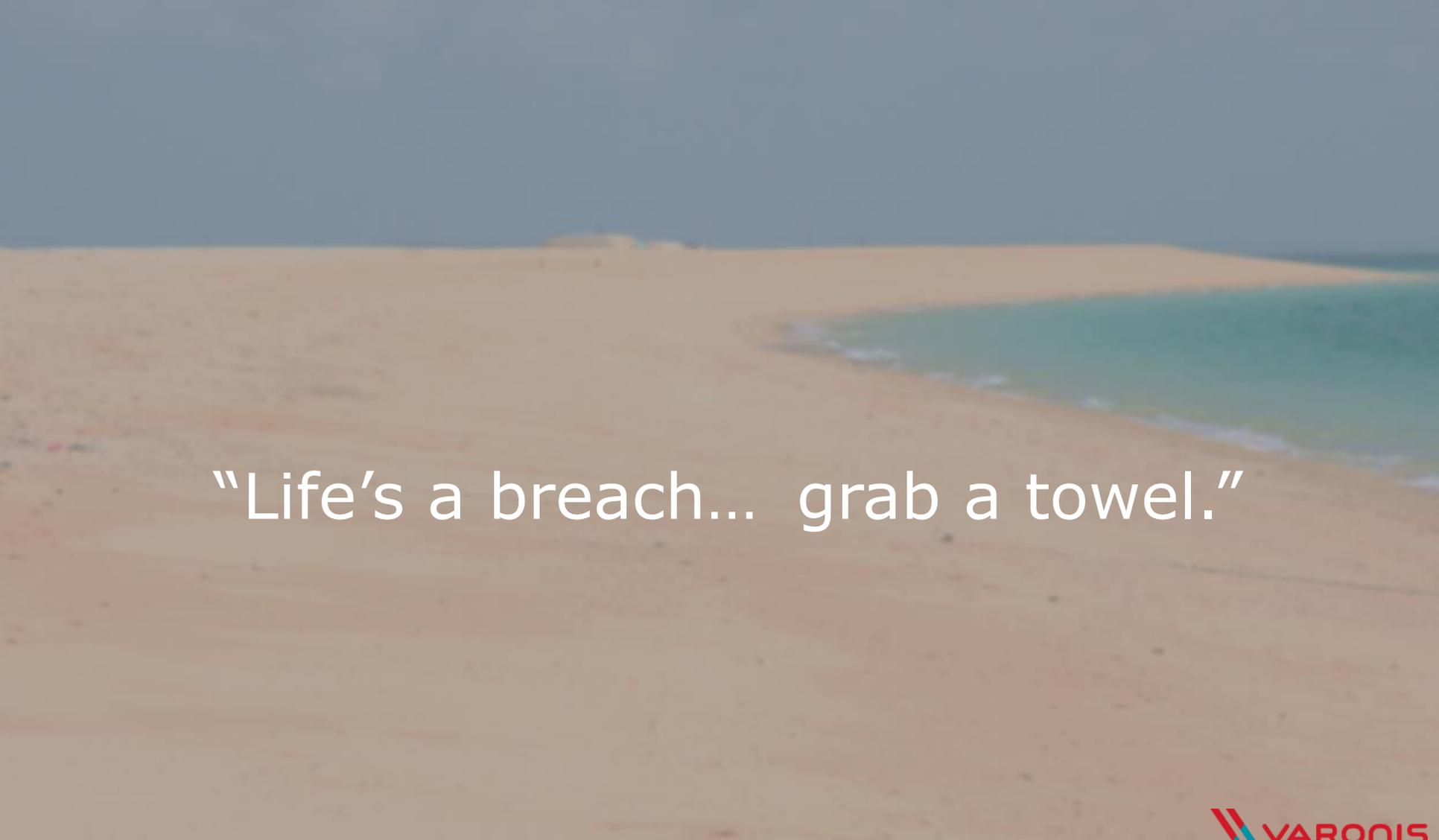




About Varonis

- Started operations in 2005
- Headquartered in NYC
- 10 Products
- Over 2500 customers world wide
- Publicly traded as of 2014 (NYSE:VRNS)
- Solutions for Human Generated Data





“Life’s a breach... grab a towel.”



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Security Breaches & Industry Trends

- ◊ The attack surface is transforming
- ◊ The most common source of breaches are not malicious attacks
 - ◊ Phishing attacks and advanced malware attacks are up 87%
 - ◊ The soft-center is still left unaddressed

The **average total cost** of data breaches to US-based organizations **is over \$5.4 million**

Sources:

1. http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year (Ugh... Long URL's are so 2005!)
2. <http://www.bankinfosecurity.com/interviews/data-breach-i-1953/op-1>



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



“Defense In Depth”



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Drowning in the Depths of Defense



"... A 'best practices' strategy in that it relies on the intelligent application of techniques and technologies that exist today.

The strategy recommends a balance between the protection capability and cost, performance, and operational considerations."
- National Security Agency

Sources:

1. http://www.nsa.gov/ia/_files/support/defenseindepth.pdf



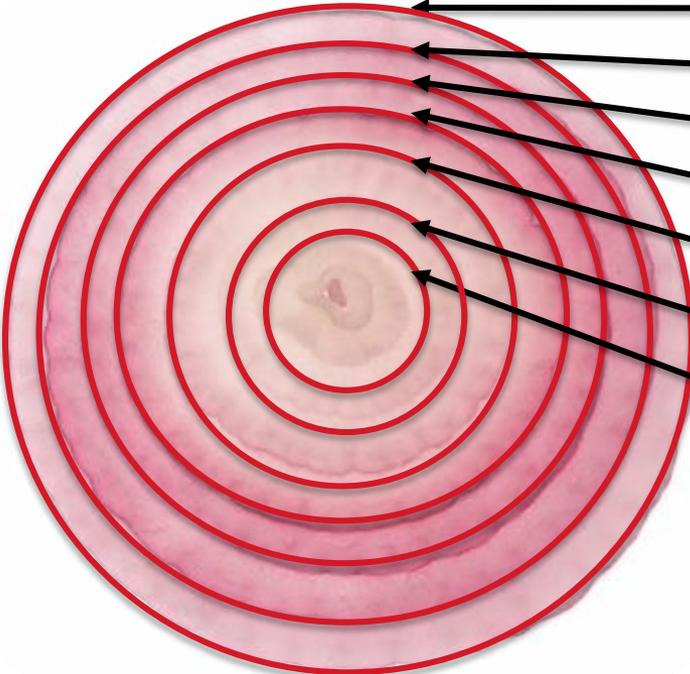
VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Drowning in the Depths of Defense



- Policies & Procedures
- Physical Security
- Network Perimeter
- Internal Network
- Host Based Security
- Application Security
- The Bank Vault**

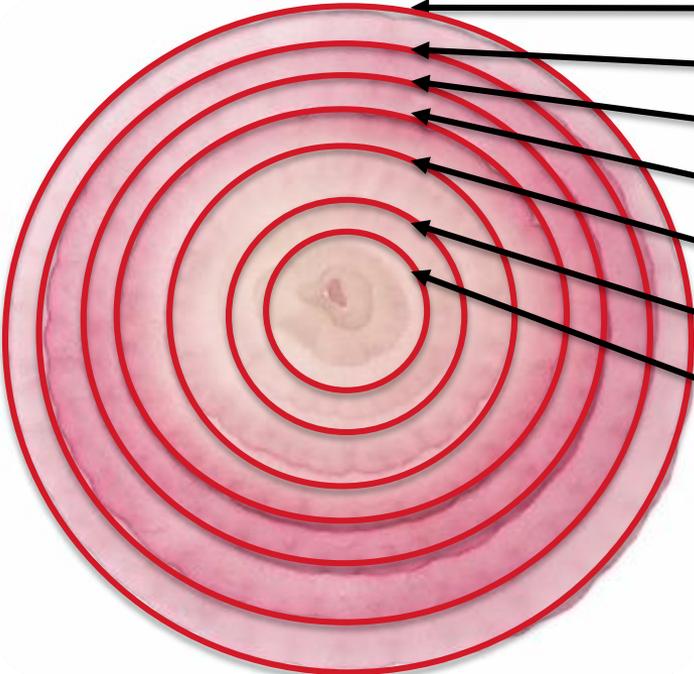
Does your "Defense-in-Depth" strategy **address your most valuable data?**



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



Drowning in the Depths of Defense



Policies & Procedures

Physical Security

Network Perimeter

Internal Network

Host Based Security

Application Security

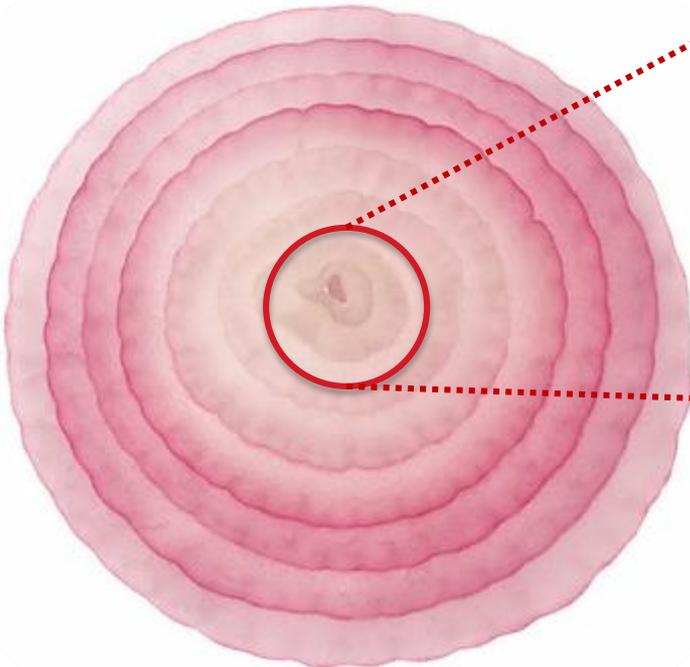
The Bank Vault



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



Drowning in the Depths of Defense



Users don't care about onions:

They care about access to data, which is exactly what they are doing.

Are you protecting the organization and its users from themselves?



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Wait a minute!

*“Did he just call our users
our biggest risk to our data?”*



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

I did.

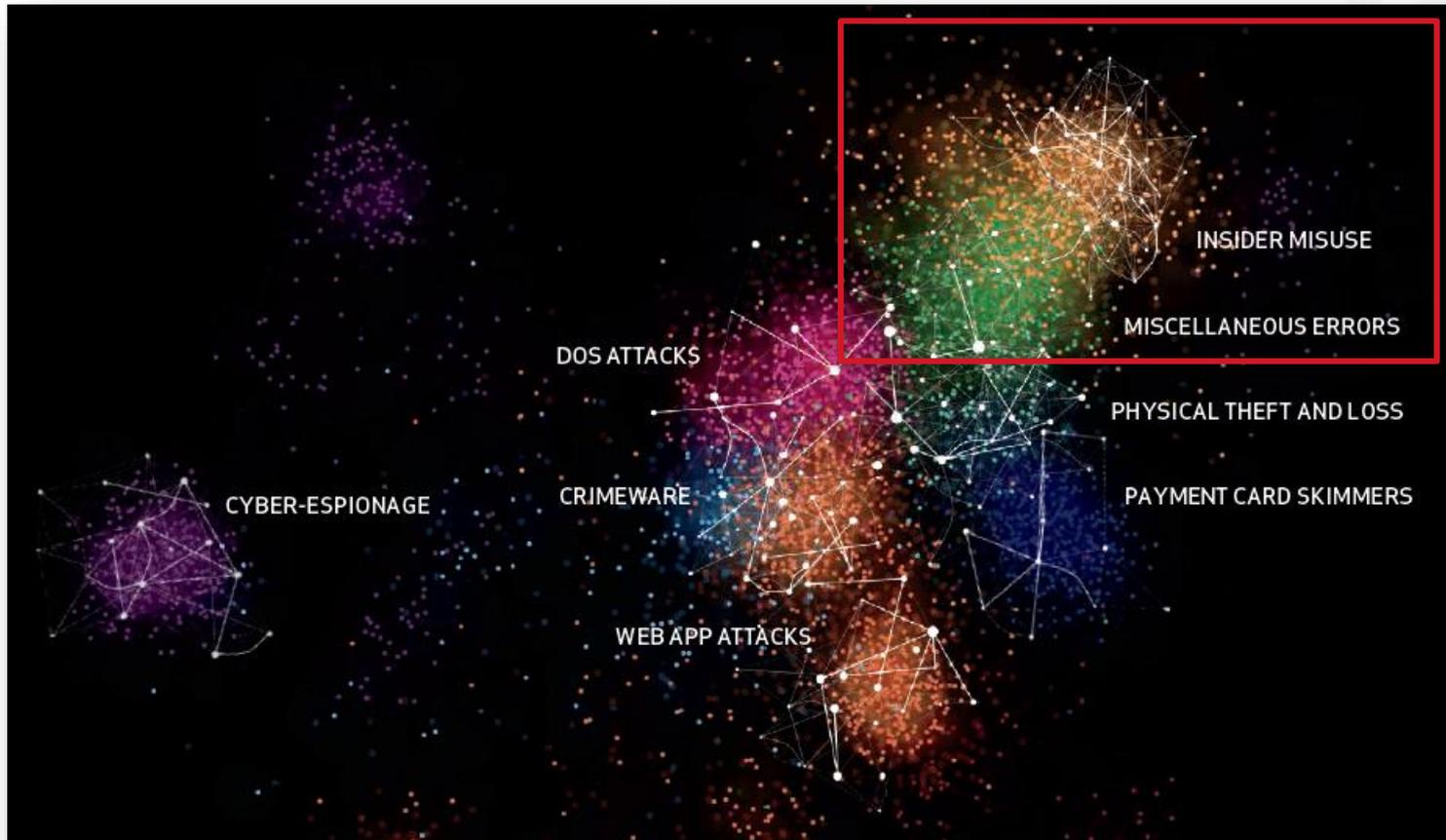
(And so do the numbers...)



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



2014 Data Breach Investigation Report



Source:

1. Verizon 2014 Data Breach Investigation Report

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL





FBI's Top 5 Lessons



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Insider Threat: The FBI's Top 5 Lessons

1. Insider threats *are not* hackers
2. Insider threat is not just a technical or a “cyber security” issue
3. A good insider threat program should focus on deterrence and not *just* detection
4. Avoid the *data overload* problem
5. Use *behavioral* analytics



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



Insider Threat: The FBI's Top 5 Lessons

Good news!

Insider threats are not responsible for the highest number of breaches...

("OK – so what is this guy so worked up about?")



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Insider Threat: The FBI's Top 5 Lessons

Bad news!

Insider threats are responsible for the most costly and damaging of breaches.

Source:

1. <http://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf>

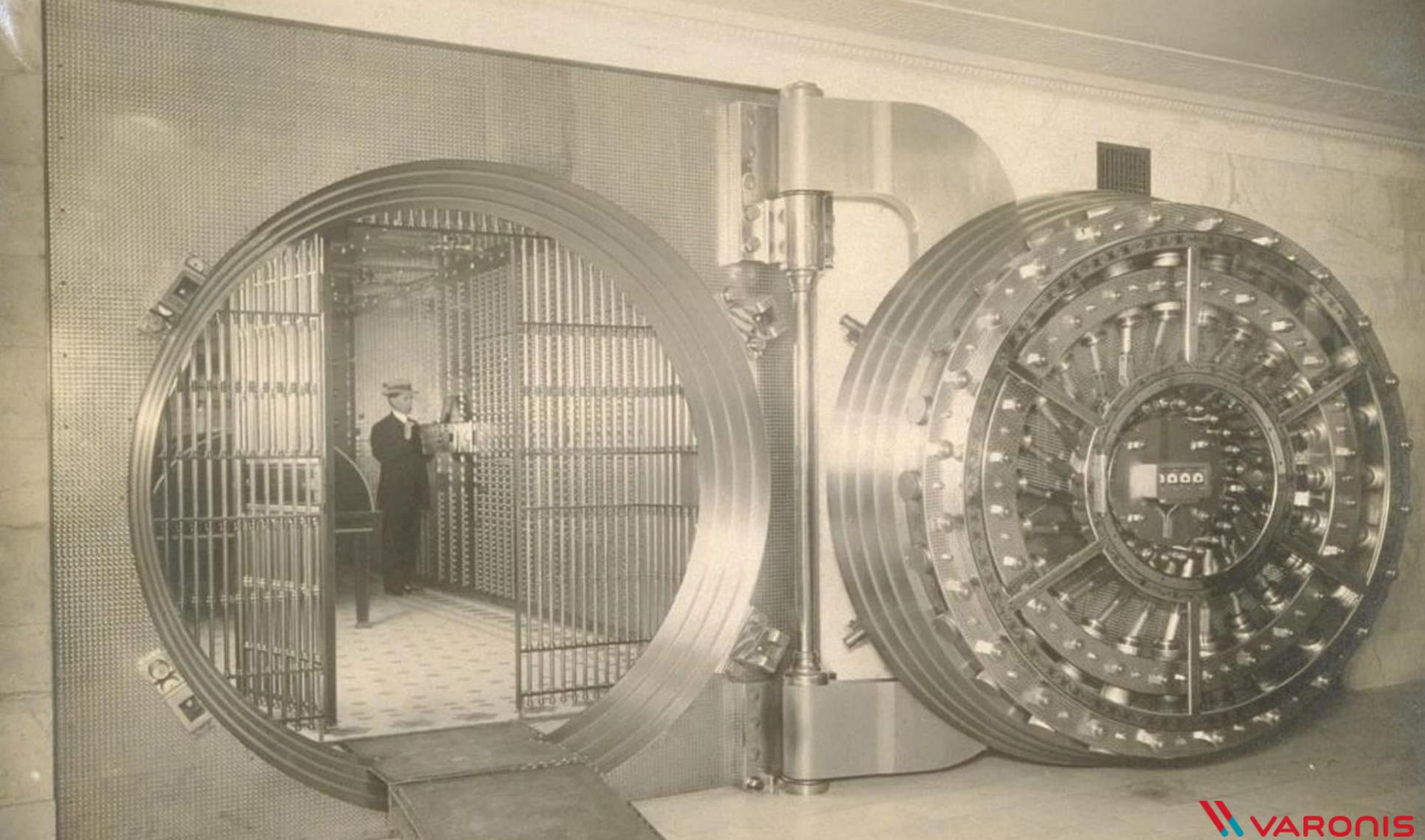


VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"



 VARONIS

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL


Trust in, and value from, information systems
San Francisco Chapter



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Closing the Bank Vault Door

Organizational Situations which increase the ease of the threat:

- Over permissive access controls
- Sensitive information is not labelled
- Sensitive information is easy to steal

***Oh. Is that all?
Just find the needle in the haystack?***

 VARONIS

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL

**ISACA**[®]
Trust in, and value from, information systems
San Francisco Chapter

**CRISC**
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Closing the Bank Vault Door



More like a needle in a stack of needles.



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



2014 Fall Conference - "Think Big"

CRISC
CGEIT
CISM
CISA

Behavioral Clues



- Taking stuffs without need or permission
- Looking for stuffs they don't need
- Asking about stuffs (*especially foreign stuffs*)
- Unnecessarily copying stuffs that isn't theirs
- Remotely access stuffs outside normal hours
- Disregard policies and install/download unauthorized stuffs
- Maintain an unusual schedule when its easier to steal stuffs
- Hang out with people who may want your stuffs

Source:

1. <http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat> (*heavily paraphrased...*)



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Big Data: Challenges & Opportunities



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Why is this a "Big Data" problem?

A Single Terabyte Contains:

- ◆ 1 million files
- ◆ 50,000 folders
- ◆ 2500 unique access control lists

A Single Access Control List Contains:

- ◆ Lists 4 groups

A Single Security Group Contains:

- ◆ 15 members

150,000 functional relationships in 1 TB of data!

That's ***before*** considering activity and content



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



Human Generated Data *IS* Big Data

STRUCTURED BUSINESS APPLICATIONS DATA



Relational Databases



Financial Records



Math Data



Multi-dimensional Data



Monthly Reporting Data
(Pre-Defined Schema)

UNSTRUCTURED HUMAN-GENERATED DATA



Emails



Word Files



Spreadsheets



Presentations

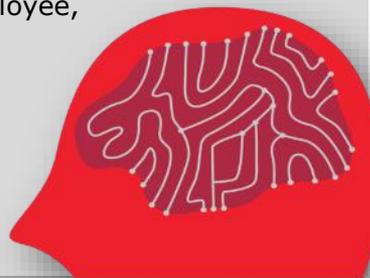


PDF Files



Image, Audio,
and Video Files

- Generated by every employee, in every organization
- Massive volumes



UNSTRUCTURED MACHINE-GENERATED DATA



Time Series Data
(No Pre-defined Schema)



Generated by
All IT Systems; Highly-
Diverse Formats



Massive Volumes

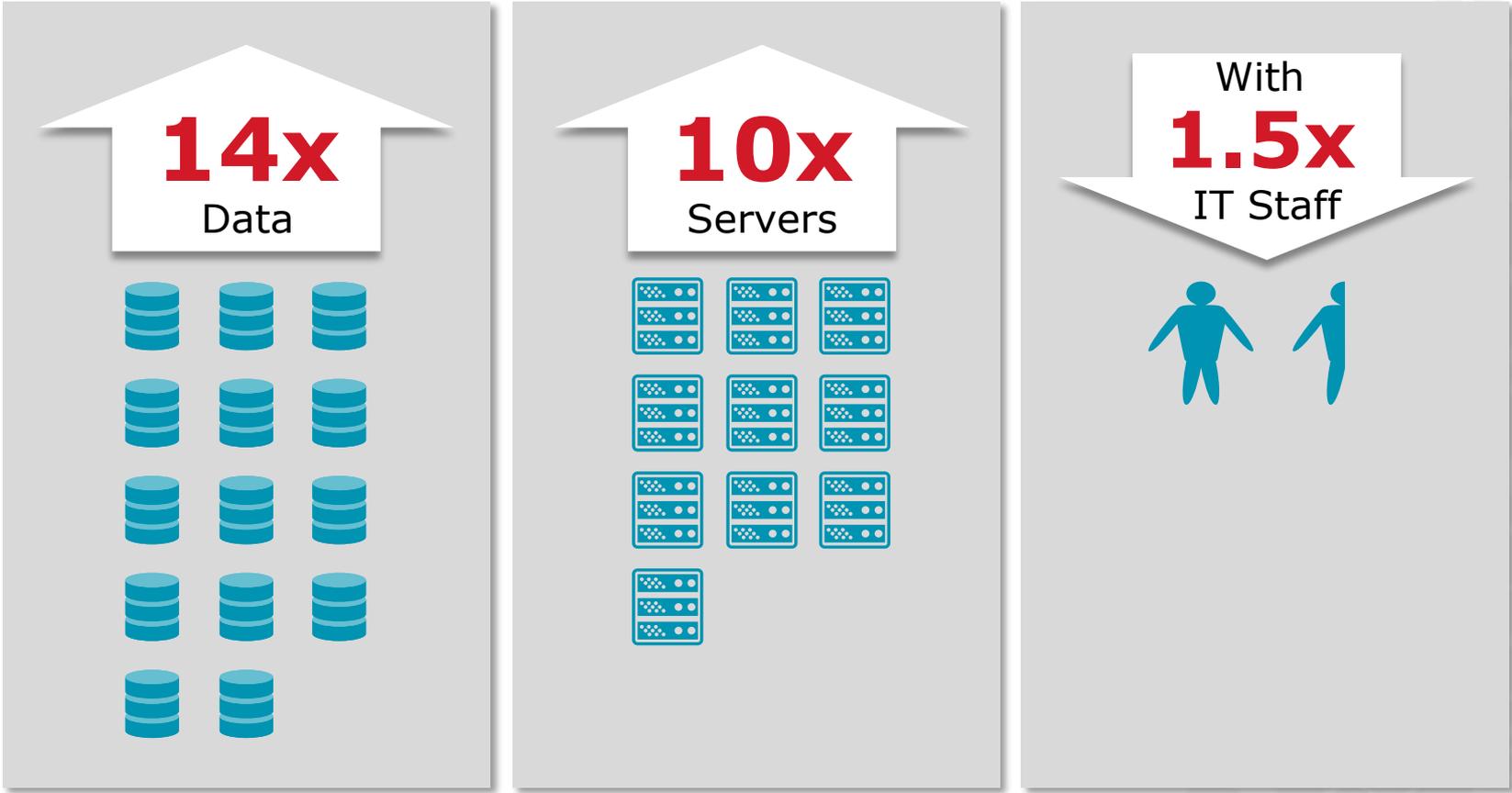
VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



CRISC
CGEIT
CISM
CISA

2014 Fall Conference - "Think Big"

Human Generated Data IS Big Data



Source:
1. IDC Digital Universe



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL

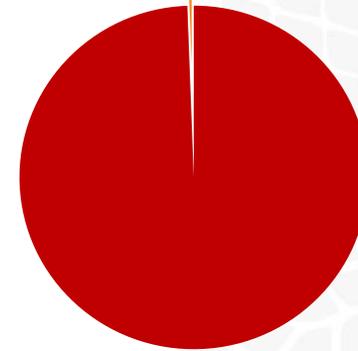


2014 Fall Conference - "Think Big"

Big Data: Challenges & Opportunities



Only 0.5% of the digital universe is analyzed



Enterprises are responsible for protecting 80% of all data

Opportunity to extract more value through tagging and analysis

Source:

1. IDC Digital Universe



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



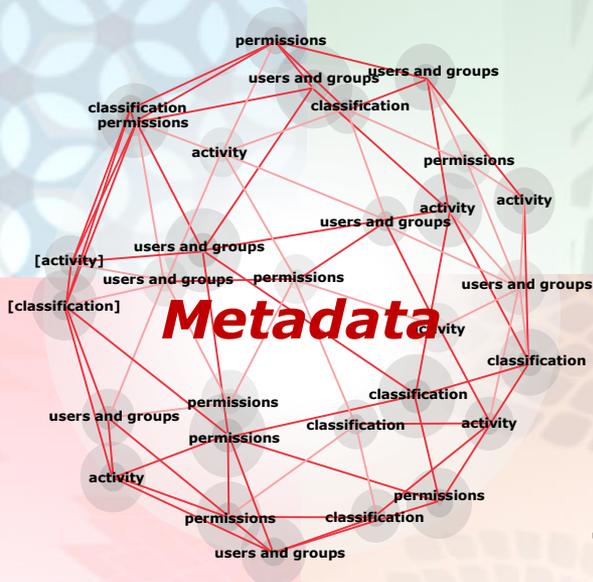
Big Metadata

1: User and Group Information:

From Active Directory, LDAP, NIS, SharePoint, etc.

2: Permissions Information:

Knowing who *can* access what data



3: Access Activity

Knowing which users *do* access what data, *when* and *what* they've done

4: Content Information

Knowing which files contain sensitive and important information



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL



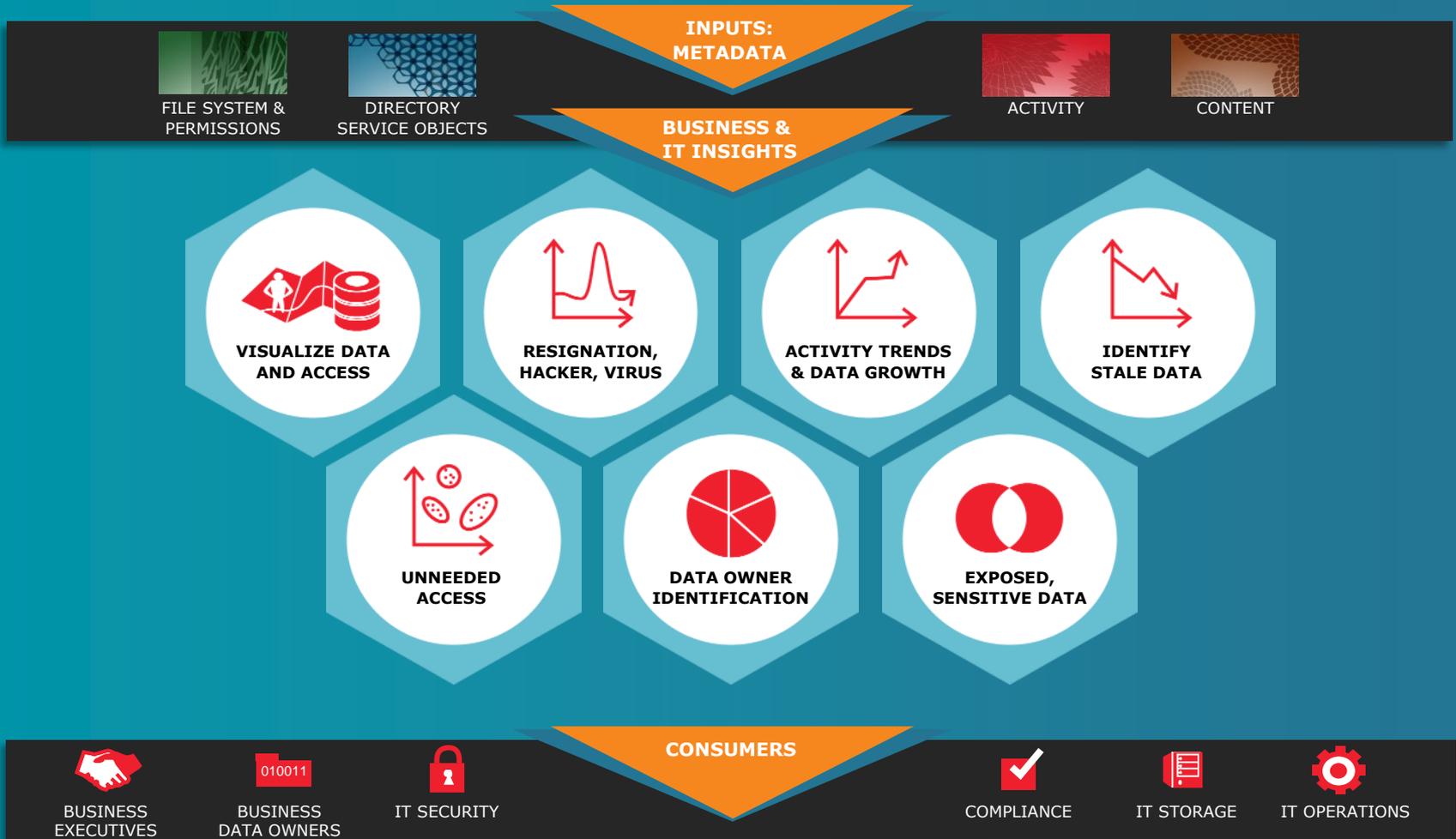
2014 Fall Conference - "Think Big"



So... What Might a
Solution Look Like?

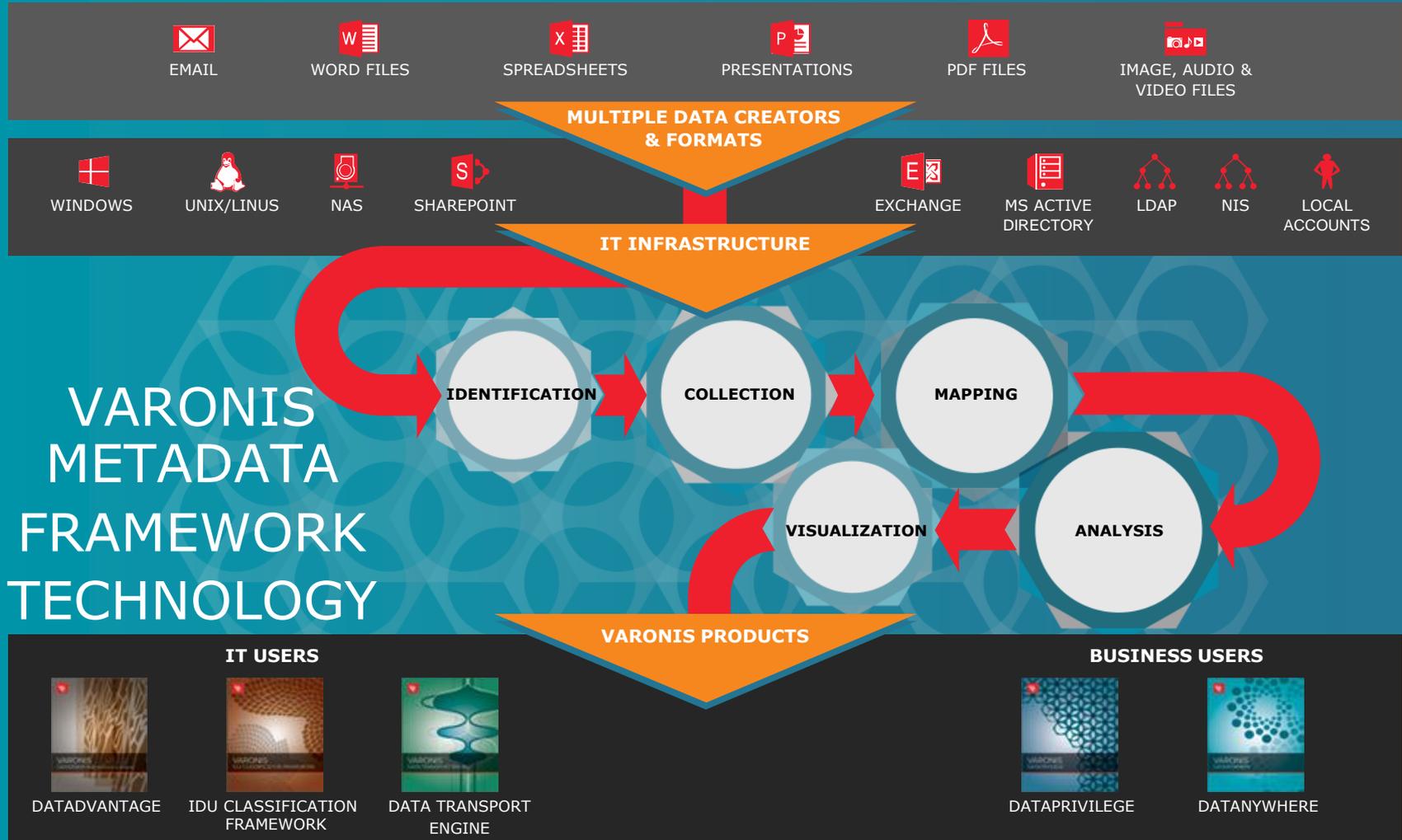


Big Data Intelligence



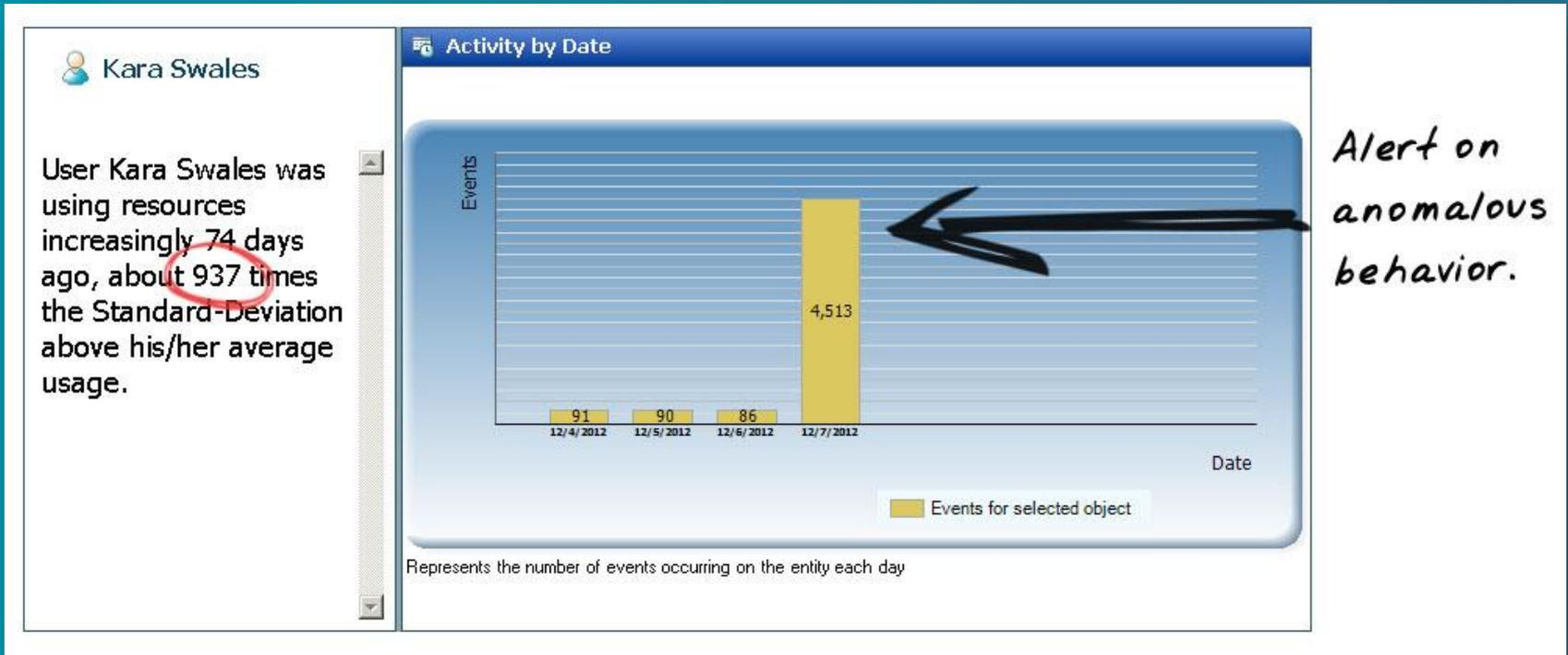


Metadata Framework





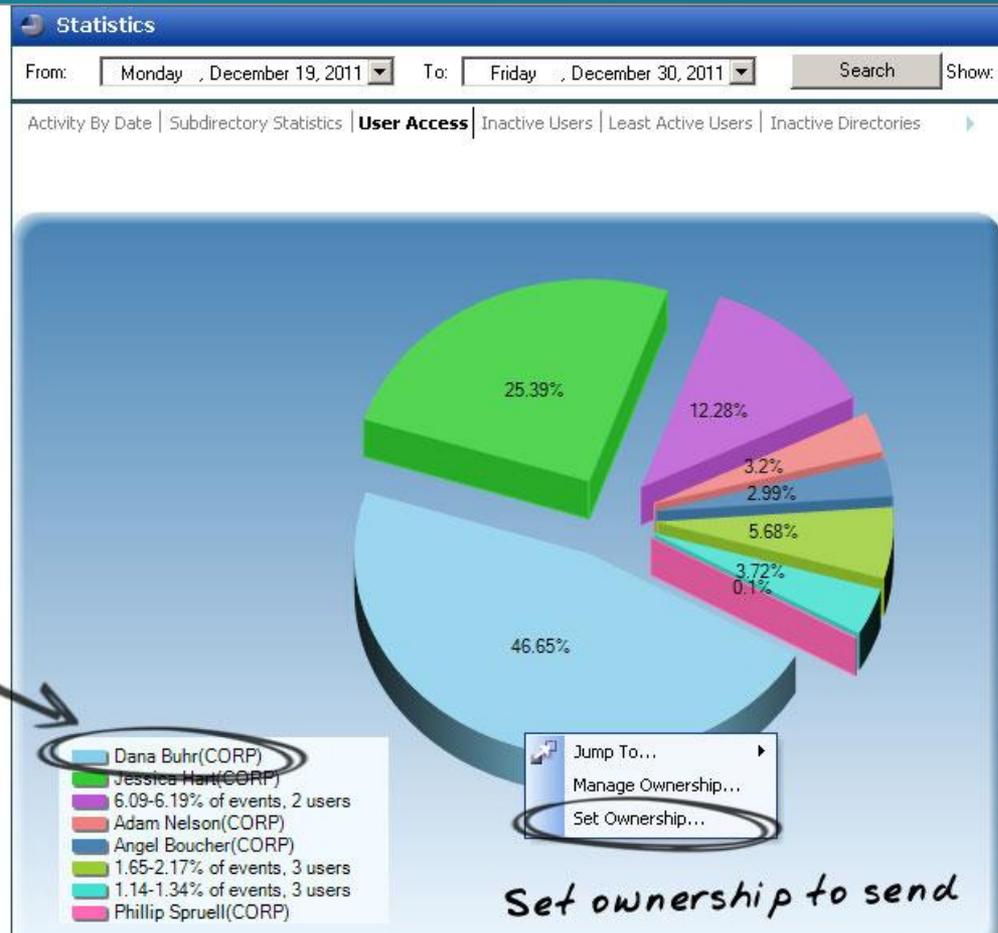
Early Resignation Detection





Who Owns Data?

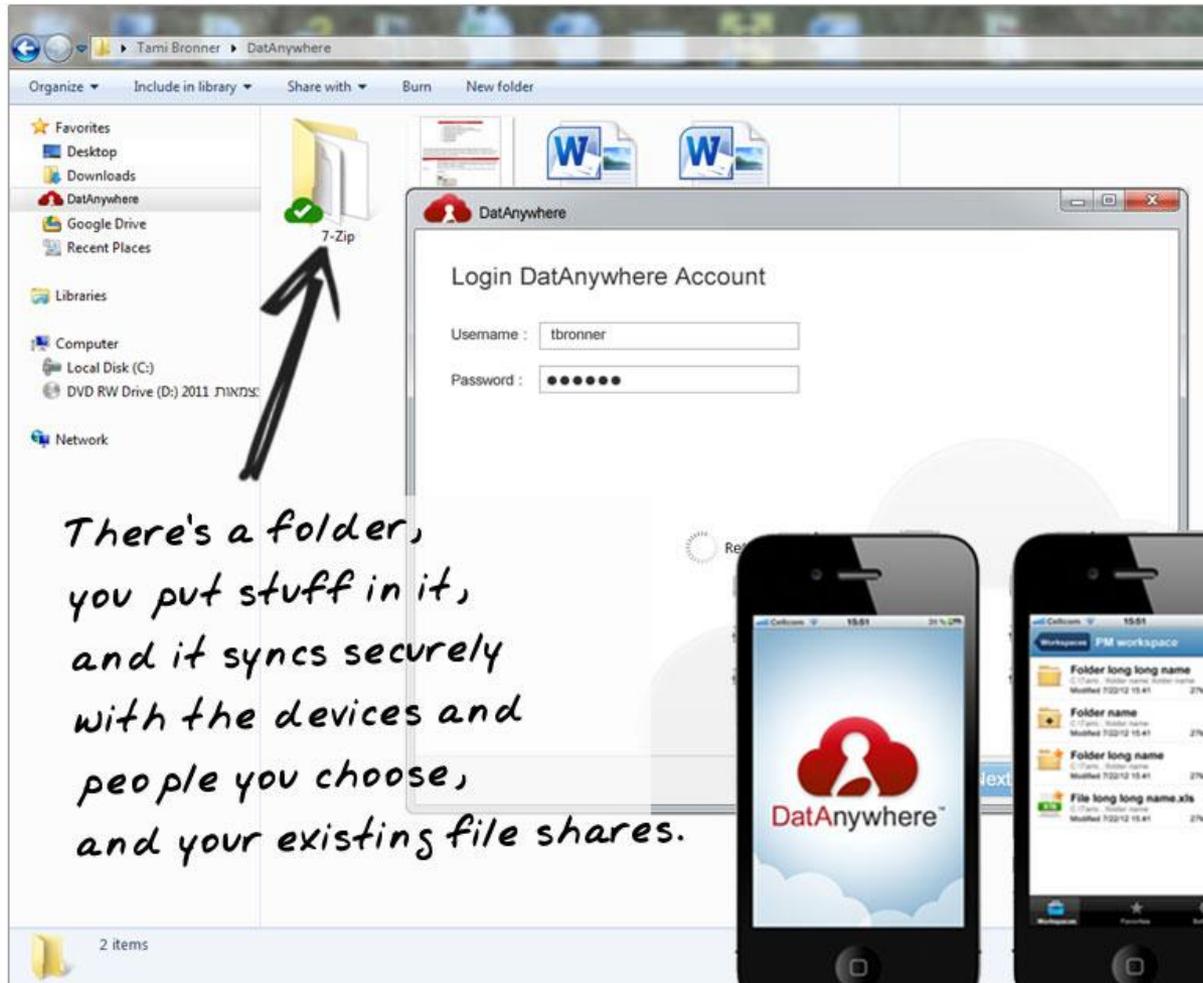
Usage statistics lead us right to the likely owner of any data set.



Set ownership to send automated permissions reports.



DatAnywhere: Your Own Private Cloud



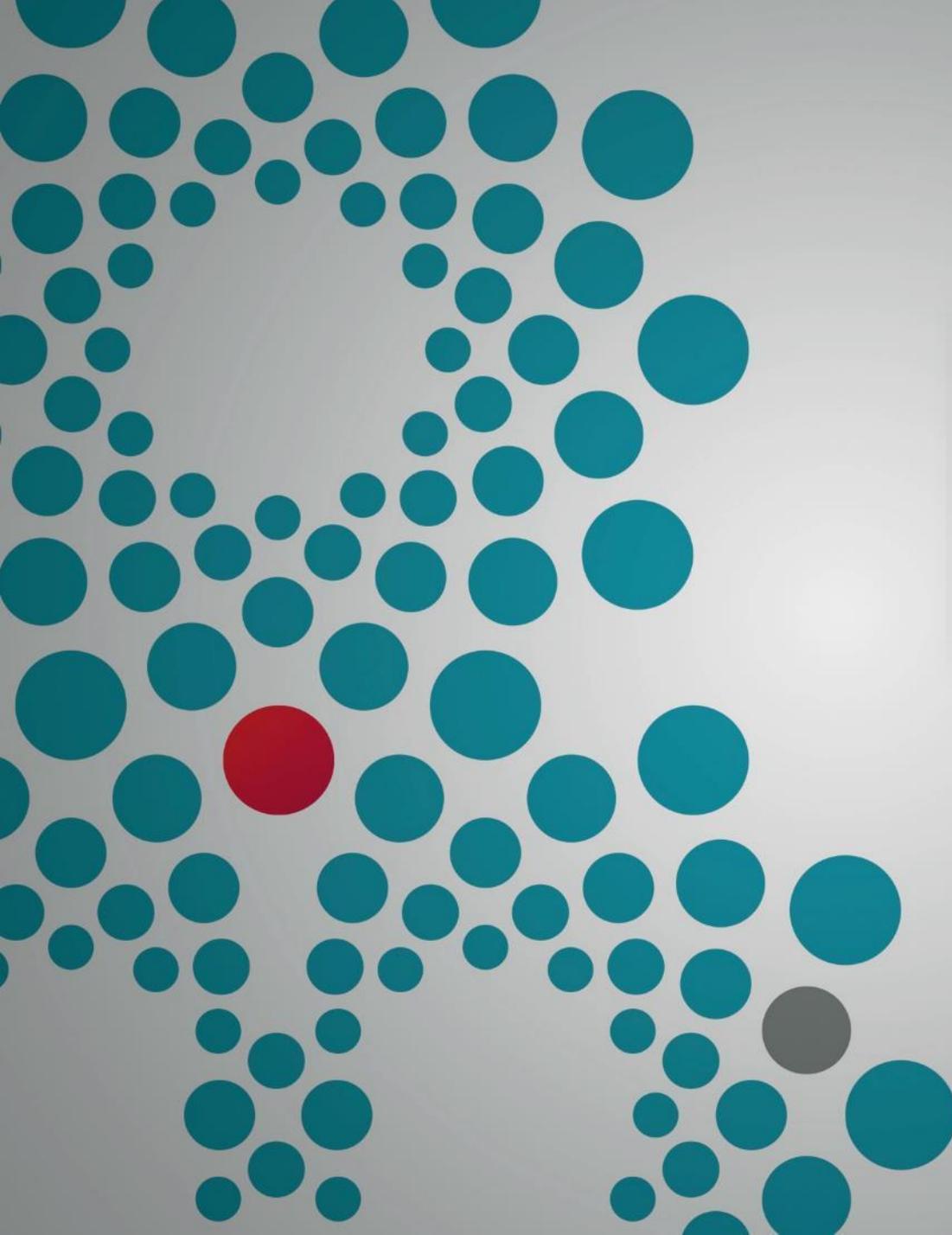
*There's a folder,
you put stuff in it,
and it syncs securely
with the devices and
people you choose,
and your existing file shares.*





Key Questions Varonis Helps Answer

- **WHO** has access to a data set and **WHAT** are they accessing?
- **WHO** should have access to data set?
- **WHICH** data is sensitive?
- **WHO** is the data owner?
- **IS** my sensitive data overexposed and **HOW** do I fix it?
- **WHAT** data is stale and can I archive it?
- **HOW** can I enable secure collaboration without moving my data?
- **HOW** do I provide secure Enterprise Search capabilities?



Q & A

...NO MORE QUESTIONS FOR YOU!



Thank you!

Presented By:

Terry Boedeker, CISSP
Solutions Engineer, Varonis Systems
tboedeker@varonis.com - 503.498.8183

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL