Our mission is to help enterprises realize value from their unstructured data.

AI and machine learning what does it all really mean

November 2018

Ben Hui bhui@varonis.com

Do you Remember this

- Expo 86
- "The Future of Transportation"
- Represented the "Impossible"

Our Shortcomings

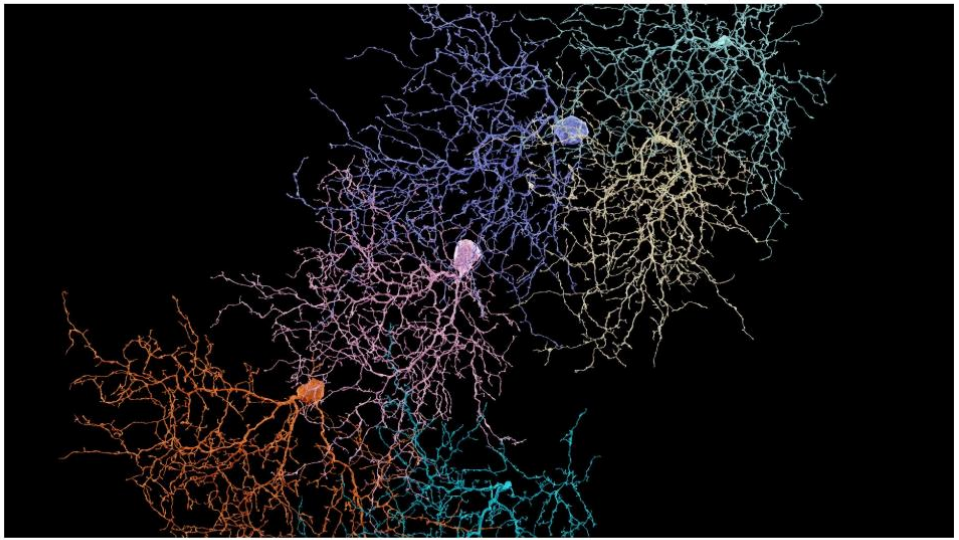
George Armitage Miller (February 3, 1920 – July 22, 2012

Miller (1956) magic number 7

- 1. **limited capacity** (only about 7 items +/- 2 can be stored at a time)
- 2. **limited duration** (storage is very fragile and information can be lost with distraction or passage of time)

What Machines can't do

Sebastian Seung's Quest to Map the Human Brain



Several distinct neurons in a mouse retina that have been mapped by volunteers playing a game developed by Sebastian Seung. Photo Illustration by Danny Jones. Original Images from EyeWire.

- Even with AI and Machine Learning, Algorithms
- Most of the mapping is completed using a mobile game developed to allow users to connect the neurons together

Mapping the 100 Trillion connections between neurons of the human brain to try and understand how memory is persisted

Example raw capture of a single VPN login sequence

- Info spread across events
- Not consecutive
- Not consistent between vendors

```
Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Key Exchange number 1 occurred for user with NCIP 172.16.248.93
Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with ESP transport mode.
Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Starting dsagentd session.
Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with SSL transport mode.
Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: Session started for user with IPv4 address 172.16.248.93, hostname OSHEZAF-LT
Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Agent login succeeded for oshezaf/VaronisCertificate from 84.229.120.164 with Pulse-Secure/8.3.3.1021 (Windows 10) Pulse/5.3.3.1021.
Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[] - Host Checker realm restrictions successfully passed for oshezaf/VaronisCertificate , with certificate 'CN=Ofer Shezaf, OU=Herzliya, OU=IL, OU=Users, OU=Varonis, DC=varonis, DC=com'
Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.120.164] oshezaf(VaronisCertificate)[] - Primary authentication successful for oshezaf/CertificateServer from 84.229.120.164
Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.120.164] oshezaf()[] - Host Checker policy 'Varonis' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user 'oshezaf'.
Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.120.164] oshezaf()[] - Host Checker policy 'Domain' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user 'oshezaf'.
```

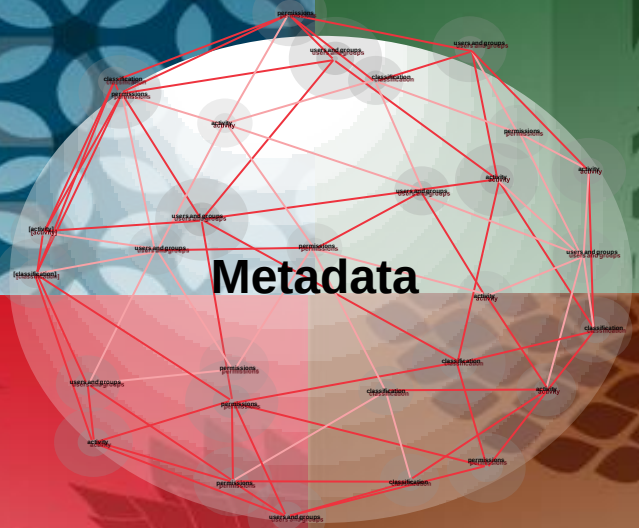
The Ingredients for Inside-Out Security

User and Group Information

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

Permissions Information

knowing who can access what data



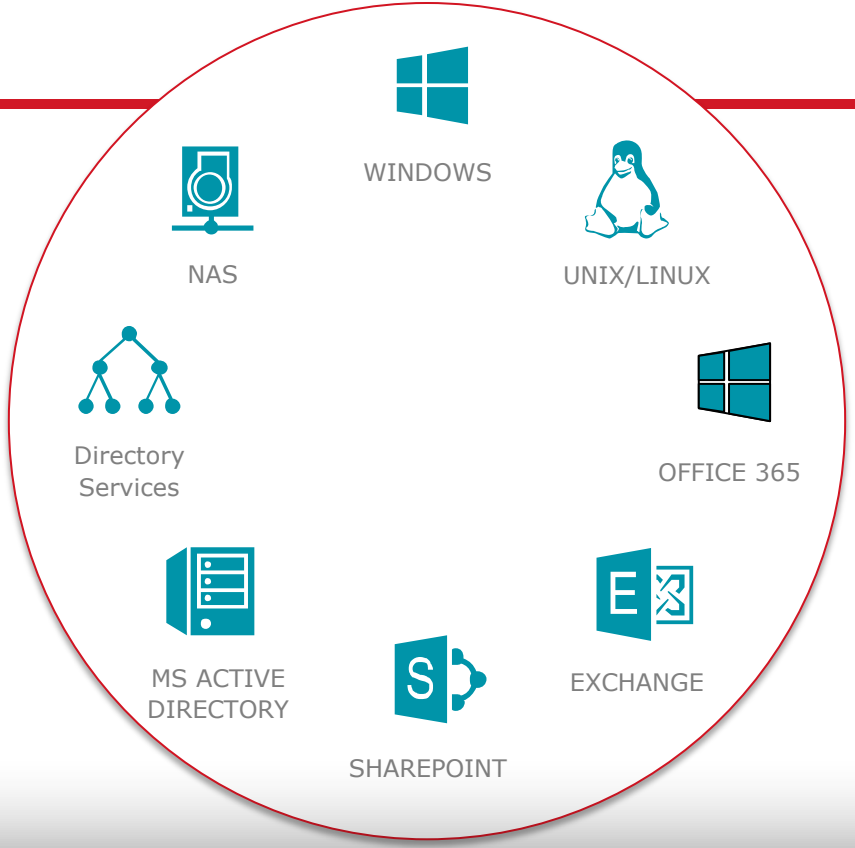
Access Activity

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

Content Information

knowing which files contain sensitive and important information

- APT's
- C&C Servers
- Malware
- Exfiltration
- Credential Stuffing
- Botnets



VPN

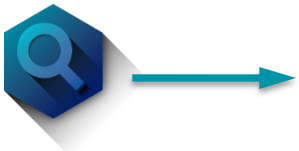
PROXY

DNS

And put them in context with core data stores

Journey of Value

Risk Reduction
Efficiency Gains



DETECT: 1. Prepare

Deploy Varonis

Prioritize and assess risks | DA, DCE

DETECT: 2. Operationalize

Create incident response plan based on alerts, including automation | DLS

Train staff on the basics - managing perms and finding lost files | DA

PREVENT: 3. Fix

Fix broken ACL's | DA, AE

Eliminate global access to sensitive data | DA, DCE, AE

Eliminate remaining global access groups | DA, AE

Eliminate unnecessary AD artifacts (unused security groups, non-expiring passwords, etc.) | DA

Quarantine/archive/delete stale data | DA, DTE

PREVENT: 4. Transformation

Identify folders that need owners | DA

Identify data owners | DA

Simplify permissions structure | DA, DP

Provide owners reports about their data | DA

SUSTAIN: 5. Automation

Automate authorization workflow via Data Owners | DP

Automate periodic entitlement reviews | DP

Automate disposition, quarantining, policy enforcement | DLS, DTE, DCE

SUSTAIN: 6. Improve

Regularly review risks, alerts and processes to ensure continuous improvement | DA, DP, DLS, DCE, DTE

DA | DatAdvantage
DLS | DatAlert Suite
DCE | Data Classification Engine
AE | Automation Engine
DTE | Data Transport Engine
DP | DataPrivilege

VARONIS

Methodology Framework and Operational Plan

Varonis is the only vendor who provides an industry proven methodology for implementation and sustainability. And we have 6500+ live deployments of the Varonis platform to prove it.

Map directory services, permissions and file systems, discover sensitive data, audit all file system activity, baseline normal behavior, detect suspicious behavior

Lock down sensitive data, fix Active Directory/file system issues, eliminate global access and prune unnecessary access, simplify permissions structure, identify data owners

Continuously monitor all user and file system activity, automatically catch and correct deviations from policy and trusted state

Permissions Gathering – The Basics Are Not So Basic

DETECT

If it were easy, everyone could do it

- Crawl an entire data structure quickly and efficiently
  - One customer with 2.5PB of data on a single clustered NAS has entire permission scans completing in hours
  - Hourly incremental scans to pick up only deltas
- Calculations are done on who has access to what AND where global access is present
- Metadata captured for analysis of key metrics, such as open access to sensitive and/or stale data

VARONIS

Monitoring Unstructured Data Across Disparate Platforms

DETECT

Centralized Data Security Platform

Quickly monitor event activity across an organization's many data platforms, including on premise and in the Cloud

- Identify insider threats, privilege escalation, and ransomware attacks
- Build context around the data and activity with the collected metadata
- Detect anomalies, correlate intelligently and prioritize for action high-priority incidents, all within one platform
- Enrich the alerting with additional context, including sensitive data identification, device source information, time of day, Proxy logs, VPN logs, DNS logs and peer analysis

VARONIS

Directory Services Monitoring

DETECT

More than simply gathering Active Directory events, provide intelligence

- Automatically Detect and add Domain Controllers for Monitoring
- Aggregate individual events into a single human readable event
- Aggregation of events prior to consolidation to reduce bandwidth
- Alerting on high risk AD objects such as privileged groups and GPO objects
- Baseline analysis to identify anomalous activity, such as an accumulated increase in lock-out events across administrative accounts

VARONIS

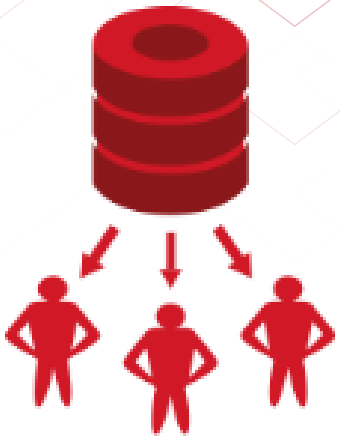
Account Discovery

DETECT

We understand your accounts

Varonis automatically detects and categorizes your accounts as Service / Admin / Executive / User

- We collect and understand your organizational structure based on AD group membership and attributes, data access permissions, and data usage patterns.
- Threat detection takes account type into consideration to spot privilege escalation
- Alerting on anomalous activity on sensitive accounts, such as executives



VARONIS

What's Happening in your Email

DETECT

Securing email systems includes knowing who's accessing critical mailboxes and what actions they're performing

- Provide complete visibility into who has access to mailboxes, through either Administrative permissions, or delegated rights
- Identify misconfiguration, such as Open Access on mailboxes or public folders
- Track DatAlert Analytics identified VIP/Executive accounts separately, such as when an Administrator is reading an Executives mailbox
- Current and historical reporting on Exchange resources, such as mailboxes & public folders, for on premise and in Office 365

VARONIS

Analytics Engine

DETECT

You need to know what normal looks like before you can detect potential abnormalities

- 80+ Threat Models which use a proprietary Analytics Engine to baseline normal user behavior across data shares, and Active Directory, to detect and help quickly mitigate threats to your data and organization.
- Dedicated team analyzing new threats ensures an organization is prepared to deal with new crypto malware and ransomware threats
- Clean, normalized alerts can be forwarded to a SIEM
- Alert workflows including taking actions

VARONIS

Sensitive Data Identification with Context

DETECT

Knowing where your sensitive data resides is the first step to securing it

- Extensive list of predefined patterns and regulatory aligned rules such as PCI / PII / PHI
- Selective scanning of document parts, such as header/footer
- Flexible custom rule creation including proximity matching, pairing of dictionaries and custom regular expressions or strings
- Content type detection for documents with no extensions
- Contextual data to assess and prioritize risk, such as sensitive data with open access or anomalous activity
- True incremental scanning after initial scan, based on event activity

VARONIS

Pre-Built GDPR Patterns

- **All 28 EU countries** :
  - National Identification Numbers:
    - ID/PIC/PIN
    - SSN
    - TIN
    - VAT
  - Vehicle
    - Driver's License
    - License Plates
  - Phones
    - Landline
    - Mobile
  - Banking
    - IBAN

- Generic patterns –
  - Credit Cards
  - Email Address
  - IP Address
  - Date of Birth
  - Blood Type

Device Name Resolution

DETECT

Knowing where a threat is coming from speeds up mitigation and recovery

- Device Name and Device IP Address information captured through event collection along with Active Directory Service event collection
- Enriches alerting, by providing additional context as to whether the alert was triggered from a system not typically utilized by the alerted user
- Name and IP address details available as variables for alert workflow, such as logging off, session control, or integrating with a SIEM or NAC workflow
- Directory Services event capture identifies resources accessed, even those not monitored by Varonis

Security Intelligence

DETECT

Incident Identification, Triage & Response

- Gather event information from all monitored platforms
- Baseline, correlate, and detect anomalous events, to identify and respond to incidents
- Provide Hunting capabilities vs simply reacting to incidents
- Prioritize clean-up efforts to reduce the most at risk data sets
- Automation to ensure security standards are maintained

VARONIS

Comprehensive Reports Engine

DETECT

Prebuilt reporting to quickly realize value and simplify administration

- Over 150+ prebuilt reports, customizable utilizing 100s of filter types and output columns, optimized for output performance
- Customized reports may be created and saved for individual or organizational use
- Reporting may be run ad-hoc, or through automated subscriptions delivered by email or created on a file share, in various formats including PDF, Excel, CSV, XML, TIFF, Web Archive
- Query API for external querying of the most common reports

Flexible Event Archival and Retrieval

DETECT

Retrieving event details quickly and easily is key to investigations

- Recent events stored in optimized local store for quick retrieval
- Medium term events available for querying and reporting
- Long term events archived to a location of your choosing, for perpetual storage of all event activity for auditing or analysis
- Selectively restore events for a specific time frame and/or set of users
- Decommission servers but maintain event information

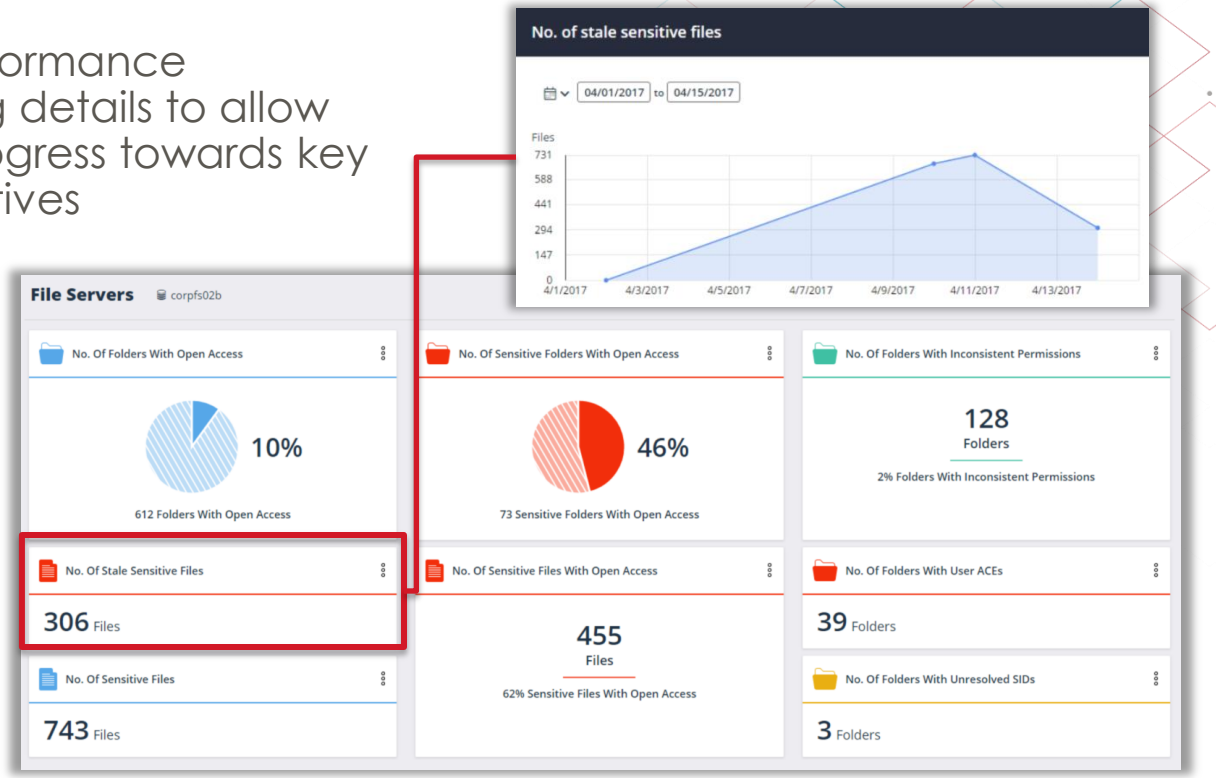
VARONIS

KPI Dashboards

PREVENT

Dashboards include Key Performance Indicators (KPIs) with trending details to allow organizations to measure progress towards key risk-reduction business objectives

- Removal of global access to sensitive content
- Removal or archival of stale sensitive files
- Remediation of shares with inconsistent permissions, unresolved SIDs or User ACEs



VARONIS

Permissions Modeling and Commit Engine

PREVENT

- The Varonis platform is in a unique position to model and simulate permission changes, by correlating users & group membership with prior access events
- The Varonis Commit Engine allows changes across the various monitored platforms, with multiple dependencies to be performed in the order required, preventing errors which can occur when executed manually
- Changes can be submitted immediately or at defined date/time such as afterhours or during a change window, and executed from the optimal Varonis server
- Back-out capabilities are built in, so if you're not satisfied with the results, they can quickly be undone

VARONIS

Automated Remediation of Broken and Inconsistent ACLs

PREVENT

You can't fix it if you don't know it's broken

- Broken and inconsistent ACLs can lead to inadvertent access
- Find and fix broken and inconsistent ACLs automatically
- A necessary step prior to any remediation or clean-up efforts
- Fix inconsistent permissions all the way down the folder tree, not just at the top level

Automated Global Access Group Remediation

PREVENT

How much of your data is wide open to all users in your organization? We can find and fix it automatically.

- Automatically locate folders where a global access group has been granted and safely remove it for immediate risk reduction.

- During the remediation process, our analytics engine accurately determines which users actually need access to the data and automatically creates the appropriate access for just those users.

VARONIS

Integration with Security Ecosystem

SUSTAIN

splunk>partner+

RSA

CYBERARK

DELL

boldonjames
A QinetiQ Company

EMC² BUSINESS PARTNER Technology Connect SELECT

FireEye

hp

ArcSight
An HP Company

LogRhythm
The Security Intelligence Company

Hitachi Data Systems

Quantum
ADVANTAGE PARTNER

McAfee

NetApp Compatible

https://www.varonis.com/tap

VARONIS

AI Nothing to fear here

- Expo 86
- "The Future of Transportation"
- Represented the "Impossible"