

Fighting a different battle than conventional cybersecurity companies



Varonis Intro

Q1, 2020

What if security started with data?



For many data stores...





Office 365



Unix/Linux





Exchange





NAS

Вох



Many questions

Is my data at risk?



- Is my data exposed?
- Who does it belong to?

Am I compliant?



- Where is my regulated data?
- Should I delete it?

...Lots more questions...

Can I detect a breach?



- Is anyone stealing it?
- How hard is it to recover from a breach?



THREE USE CASES



DATA PROTECTION



COMPLIANCE



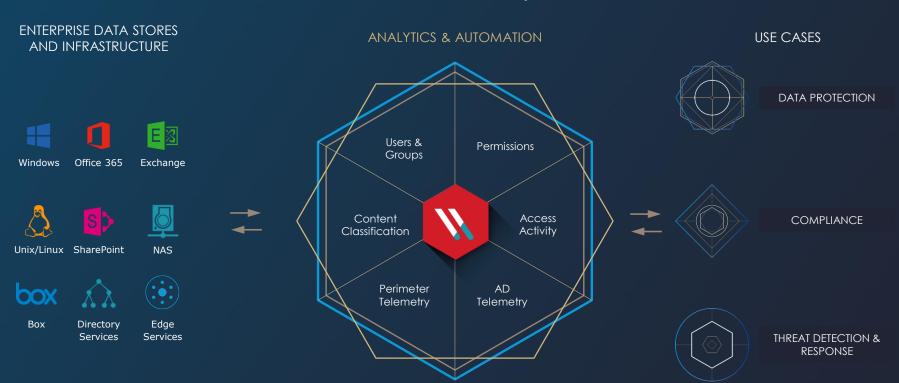
ONE PLATFORM



THREAT DETECTION & RESPONSE



Varonis Data Security Platform





Varonis Data Security Platform

ENTERPRISE DATA STORES AND INFRASTRUCTURE



Windows Office 365

Exchange

NAS



Unix/Linux SharePoint

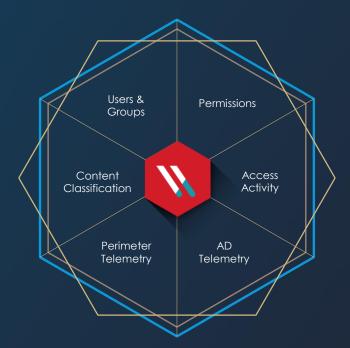


Box



Edge Services

ANALYTICS & AUTOMATION



RISK ASSESSMENT



- 90 minute install
- Minimal hardware required
- Free



Services

Operational Journey



DATA PROTECTION

1. OPERATIONALIZE

- Train
- Report
- Apply labels
- Index

2. FIX

- Eliminate issues
- Archive stale data
- Eliminate global access
- Quarantine sensitive data

3. TRANSFORM

- Simplify permissions
- Identify and assign owners

4. SUSTAIN

- Automate authorization
- Automate retention



RISK ASSESSMENT



- Discover privileged accounts
- Classify sensitive data
- Baseline activity
- Prioritize risk



COMPLIANCE

PCL HIPAA, GDPR, SOX, ITAR, GLBA



1. INTEGRATE

- Confirming Privileged Account Discovery
- Enable alerts and methods
- Connect to SIEM
- Create Incident Response Plans

2. OPERATIONALIZE

- Tune alerts
- Automate response
- Test incident response plans





Start With A Data Risk Assessment

- Valuable reports quantify risk and diagnose issues such as:
 - What kind of sensitive data do I have? (PCI, SOX, PII, etc.)
 - Where is sensitive data overexposed?
 - Who has access to what?
 - Where are users acting strangely or maliciously?
 - What's being used and what's not?

GLOBAL GROUP ACCESS:

Global groups allow everyone in an organization to access these folders. Global groups are groups such as Everyone, Damain Users, and Authenticated Users.

Overexposed data is a common security vulnerability. IT professionals estimate it takes about 6-8 hours per folder to locate and manually remove global access groups. They must identify users that need access, create and apply new groups, and populate them

RISK SUMMARY: Low

- Excessive access is one of the primary causes of data breaches
- Overexposed sensitive and critical data is a significant security risk
- · Outdated user permissions are a target for exploitation and malicious use

RECOMMENDED ACTIONS:

- Remove global access group permissions to identify folders open to global groups
- Place active users in a new group
- Replace the global access group with the new group on the ACL

Key Findings: Global Access Groups

66.5 million folders with global group access

DISTRIBUTION OF GLOBAL GROUP ACCESS

GROUP ACCESS

Key Findings: User Activity

USER ACTIVITY

- 182,335 file modifications
- 65,120 file deletions
- 22,965 permission changes

750,000+

Of Sensitive Files With Open Access

Key Findings: KPIs

9.213.456 Sensitive Files With Open Access

hat Contain Sensitive Data





horized attempts to gain access to or modify assets often signal malware, insider threats, or

- al user behavior (compared to their baselines) ate potential account hijackina, data ation, and attempts at compromising data
- al access to sensitive data suggests that data sk and prone to a security incident

MMENDED ACTIONS:

or user behavior and file activity

and alert on security violations, suspicious vior, and unusual activity

lish incident response plans and investigation asses to pursue potential security violations



950,534.645 Files Contain Sensitive Data

User Accounts with Non-Expiring Passwords

1.182

User Accounts with Non-Expiring Passwords



Ecosystem







GATEWAYS

VPN Email Gateway

Web Proxy

Next Gen Firewall



THREAT DETECTION & RESPONSE

IDS/IPS
DLP

SIEM ORCHESTRATION MGMT. THREAT HUNTING

ON-PREM

CLOUD



NETWORK INFRASTRUCTURE

IDS/IPS





RIGHTS MANAGEMEN DATABASE SECURITY DLP



Active Directory LDAP



IDENTITY IAM PAM

ENDPOINTS

Workstations

Mobile Devices

EDR/NGAV MOBILE SECURITY DLP