VARONIS

Fighting a different battle than
conventional cybersecurity companies

Varonis Intro

Q1, 2020

What if security started with data?

SUSTAIN — We'd efficiently sustain our secure state

PREVENT — Only the right people would have access

DETECT — We'd monitor it for abuse

DATA — We'd know where our sensitive data lives

VARONIS

For many data stores…

Windows

Office 365

Unix/Linux

SharePoint

Exchange

NAS

Box

VARONIS

Many questions

Is my data at risk?

Am I compliant?

Can I detect a breach?

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

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

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

…Lots more questions…

VARONIS

THREE USE CASES

DATA PROTECTION
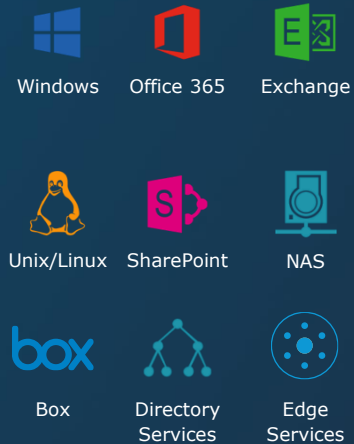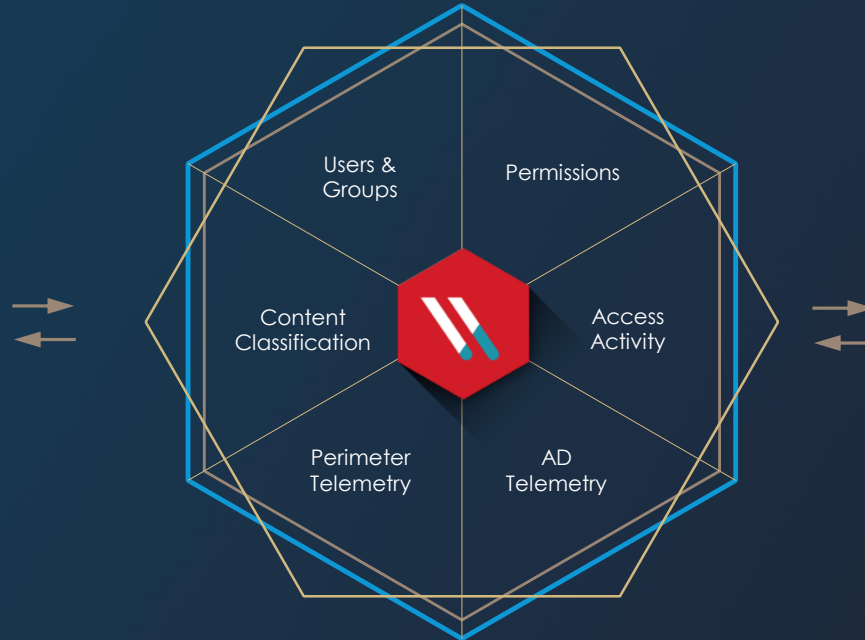
COMPLIANCE

THREAT DETECTION & RESPONSE

ONE PLATFORM

VARONIS

Varonis Data Security Platform

Varonis Data Security Platform

ENTERPRISE DATA STORES AND INFRASTRUCTURE

Windows

Office 365

Exchange

Unix/Linux

SharePoint

NAS

Box

Directory Services

Edge Services

ANALYTICS & AUTOMATION

Users & Groups

Permissions

Content Classification

Access Activity

Perimeter Telemetry

AD Telemetry
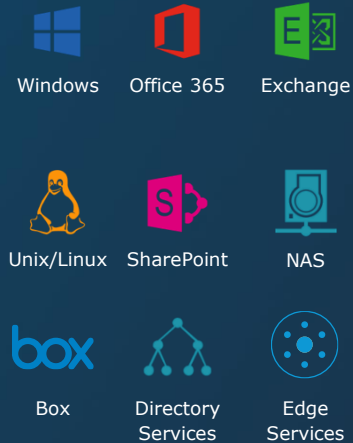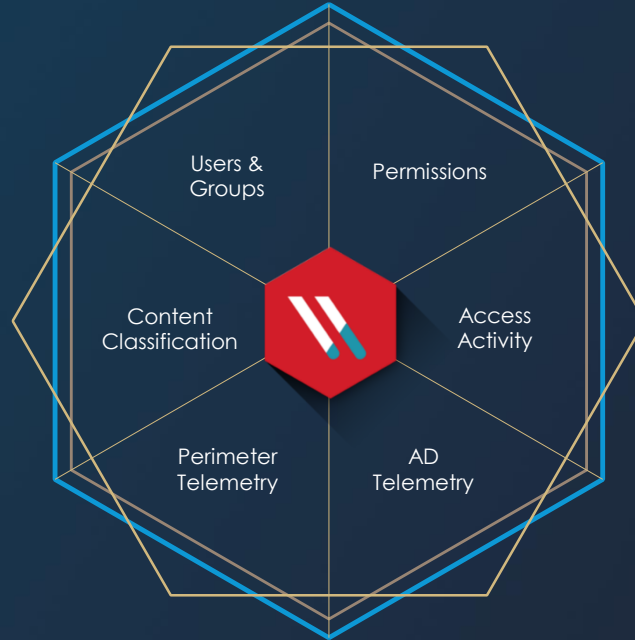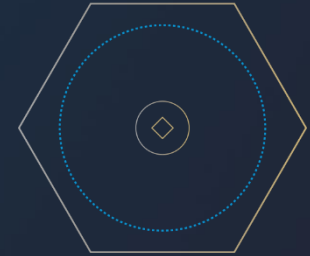
RISK ASSESSMENT

- 90 minute install
- Minimal hardware required
- Free

VARONIS

Operational Journey

RISK ASSESSMENT

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

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

COMPLIANCE

PCI, HIPAA, GDPR, SOX, ITAR, GLBA

THREAT DETECTION & RESPONSE

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

VARONIS

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?

Ecosystem

CLOUD

VARONIS DCAP
THREAT DETECTION & RESPONSE
CLASSIFICATION
RIGHTS MANAGEMENT
CASB
DLP

DATA
Data Stores
Cloud Applications
Email

THREAT DETECTION & RESPONSE
IDENTITY IAM
OKTA

DIRECTORY SERVICES & DNS
Azure AD
Public DNS

EDR/NGAV
MOBILE SECURITY
DLP

ENDPOINTS
Workstations
Mobile Devices

GATEWAYS

VPN   Email Gateway   Web Proxy   Next Gen Firewall

THREAT DETECTION & RESPONSE
IDS/IPS
DLP

ON-PREM

NETWORK
INFRASTRUCTURE

IDS/IPS
NAC

DATA
Data Stores
Databases
Email

VARONIS DCAP
THREAT DETECTION & RESPONSE
CLASSIFICATION
RIGHTS MANAGEMENT
DATABASE SECURITY
DLP

DIRECTORY SERVICES & DNS
Active Directory
LDAP

THREAT DETECTION & RESPONSE
IDENTITY IAM
PAM

ENDPOINTS
Workstations
Mobile Devices

EDR/NGAV
MOBILE SECURITY
DLP

SECURITY
OPERATIONS

SIEM
ORCHESTRATION
MGMT.
THREAT HUNTING