VARONIS

Fighting a different battle than
conventional cybersecurity companies

# Varonis Operational Journey: l'approccio data-centrico alla Sicurezza informatica

Security Summit Roma, 5 Giugno 2019

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

# About Varonis

- Started operations in 2005
  - VRNS on Nasdaq
- More than 6,000
- Data-centric security software
- Built by world-class cyber security experts (not through acquisitions)


> Varonis works across the whole organization. It works with our infrastructure, our Active Directory, it works with all the hardware and software we have.

-- Wade Sendall, VP of IT, The Boston Globe

# For many data stores…

Windows

Office 365

Unix/Linux

SharePoint

Exchange

NAS

Box


VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

# Many questions

## Is my data at risk?

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

## Am I compliant?

- Where is my regulated data?
- Should I delete it?
- Can I prove compliance?

## Can I detect a breach?

- Is anyone stealing it?
- From which devices and locations?
- Can I investigate quickly?

# THREE USE CASES

DATA PROTECTION

COMPLIANCE

THREAT DETECTION & RESPONSE

ONE PLATFORM

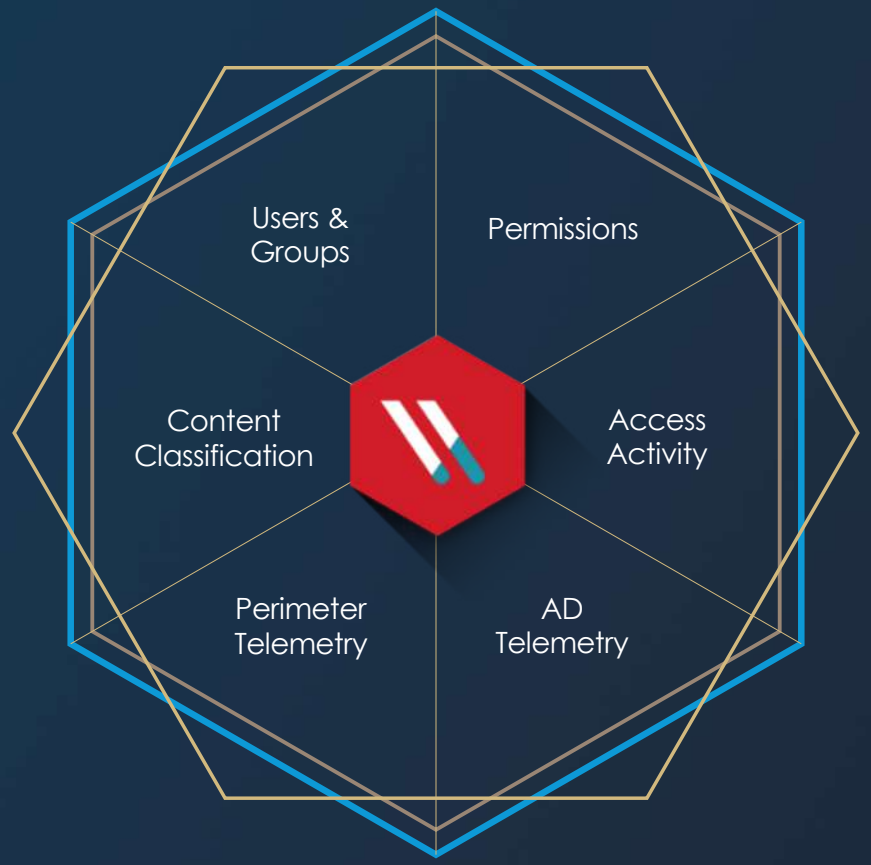
VARONIS

# Varonis Data Security Platform

## ENTERPRISE DATA STORES AND INFRASTRUCTURE

Windows
Office 365
Exchange
Unix/Linux
SharePoint
NAS
Box
Directory Services
Edge Services

## ANALYTICS & AUTOMATION




## USE CASES

DATA PROTECTION

COMPLIANCE

THREAT DETECTION & RESPONSE

VARONIS

# Ecosystem

**VARONIS DCAP**
**THREAT DETECTION & RESPONSE**
**CLASSIFICATION**
RIGHTS MANAGEMENT
CASB
DLP

**THREAT DETECTION & RESPONSE**
IDENTITY IAM
OKTA

EDR/NGAV
MOBILE SECURITY
DLP

CLOUD

DATA
Data Stores
Cloud Applications
Email

DIRECTORY SERVICES & DNS
Azure AD
Public DNS

ENDPOINTS
Workstations
Mobile Devices

SECURITY OPERATIONS

GATEWAYS

VPN Email Gateway Web Proxy Next Gen Firewall

**THREAT DETECTION & RESPONSE**
IDS/IPS
DLP

SIEM
ORCHESTRATION
MGMT.
THREAT HUNTING

ON-PREM

NETWORK INFRASTRUCTURE

IDS/IPS
NAC

DATA
Data Stores
Databases
Email

DIRECTORY SERVICES & DNS
Active Directory
LDAP

ENDPOINTS
Workstations
Mobile Devices

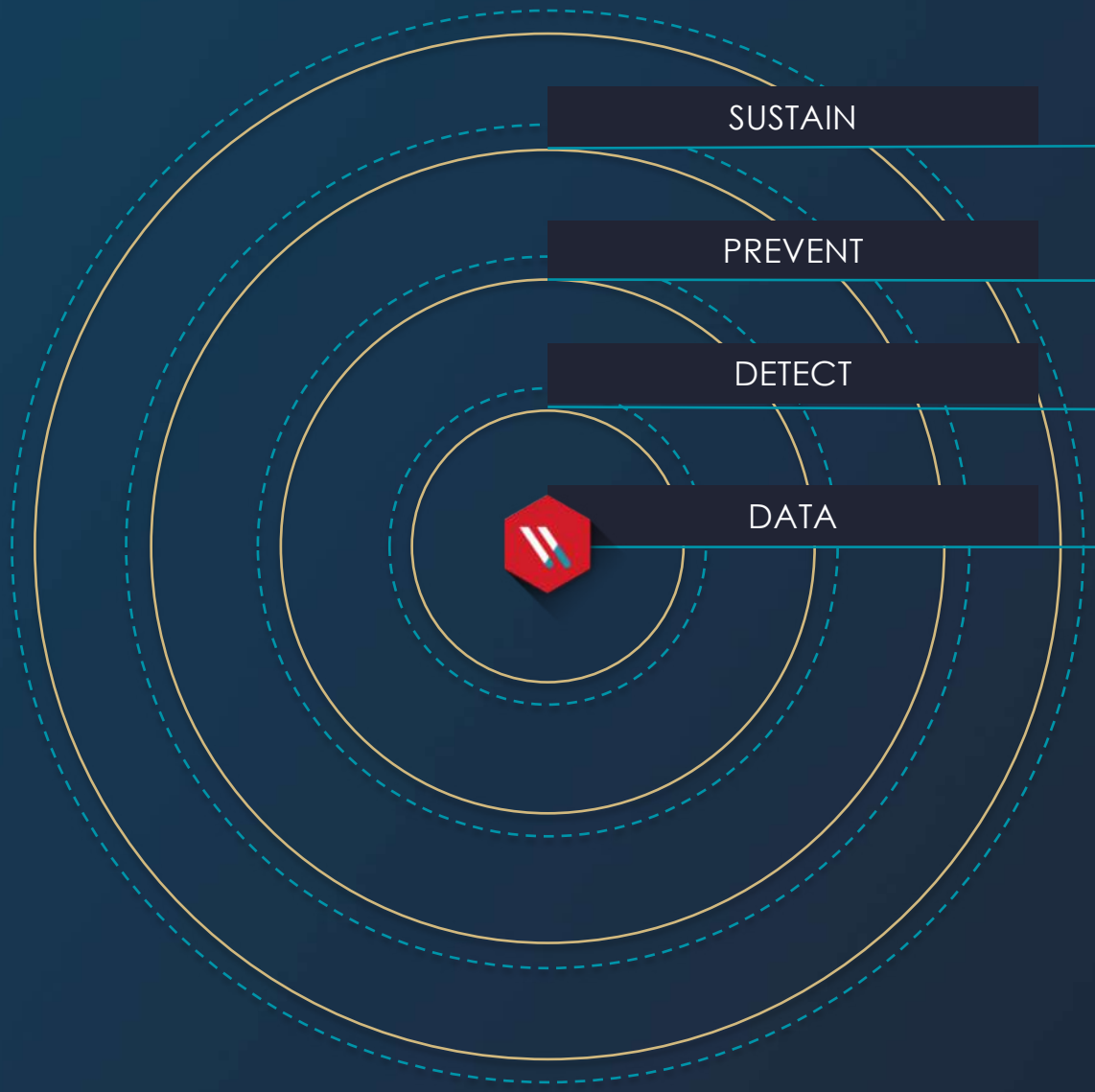
**VARONIS DCAP**
**THREAT DETECTION & RESPONSE**
**CLASSIFICATION**
RIGHTS MANAGEMENT
DATABASE SECURITY
DLP

**THREAT DETECTION & RESPONSE**
IDENTITY IAM
PAM

EDR/NGAV
MOBILE SECURITY
DLP

VARONIS

# What if security started with data?




We'd efficiently sustain our secure state

Only the right people would have access

We'd monitor it for abuse

We'd know where our sensitive data lives

# 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

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

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

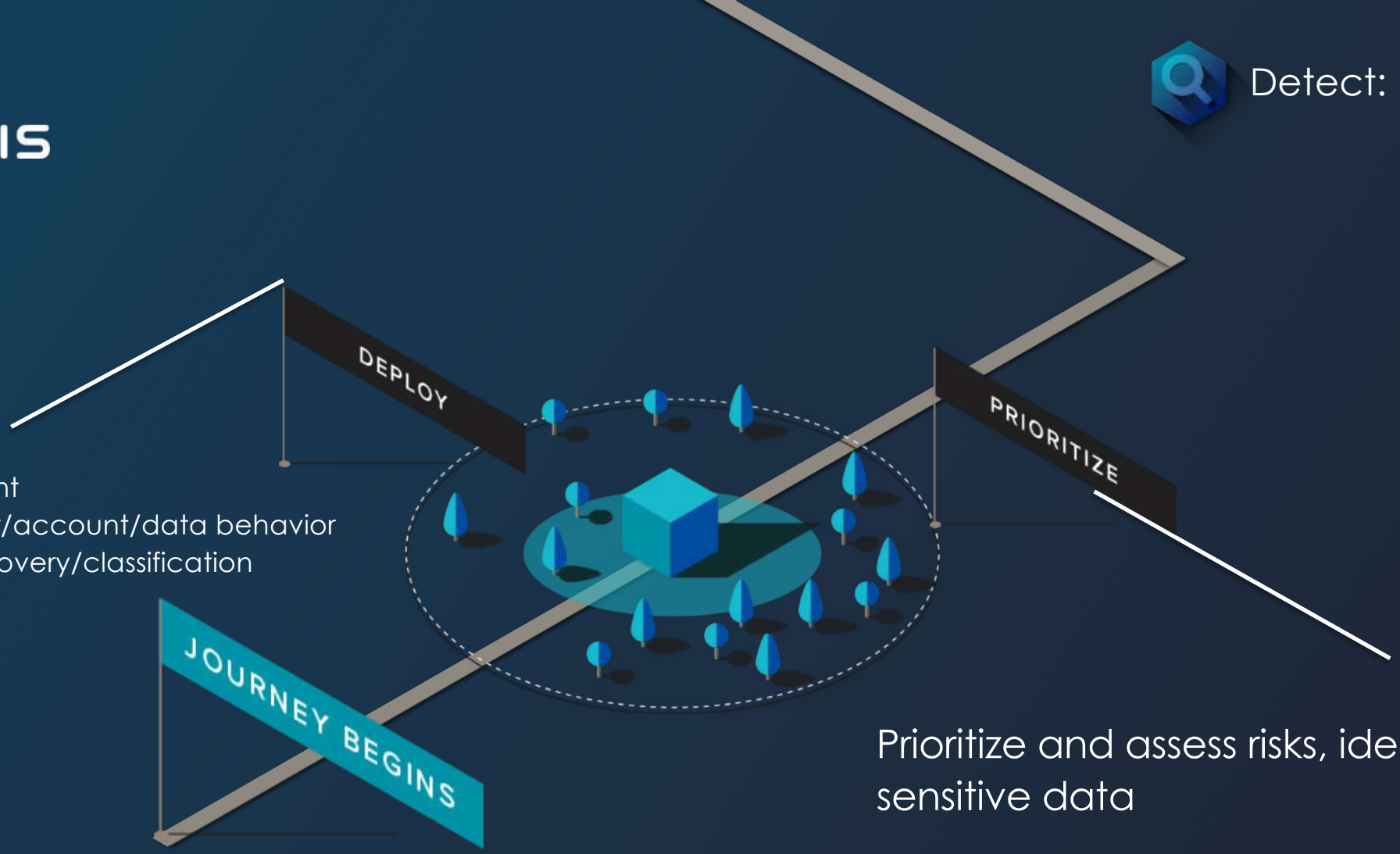
2. OPERATIONALIZE
- Tune alerts
- Automate response
- Test incident response plans

VARONIS

# Detect: Prepare

## Deploy Varonis

- Map your environment
- Begin monitoring user/account/data behavior
- Start automated discovery/classification




- Can be accomplished quickly
- Requires: DA, DCF, DS

## Prioritize and assess risks, identify sensitive data

- Prioritize scope by sensitivity, staleness,
- department criticality, etc.
- Review Incident Response Procedure,
- SOC capabilities and toolsets

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

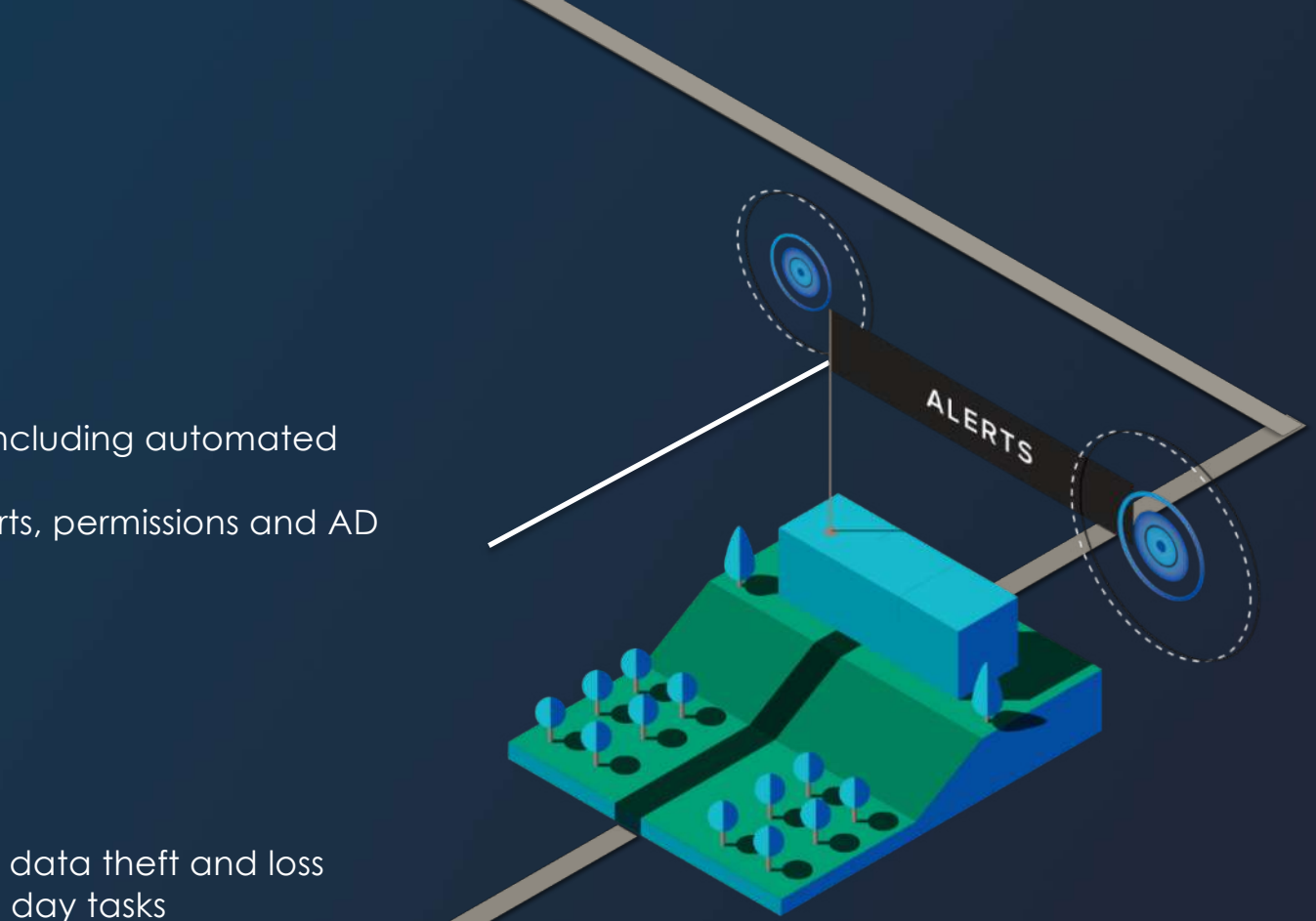
## Steps

- Prioritize and create incident response plan for alerts, including automated responses
- Train staff on day to day management, including reports, permissions and AD management, finding lost files, etc.
- Identify known data owners demarcation points
- Identify known data retention and disposition policies

## Benefits

- Incident response plans and automation reduce risk of data theft and loss
- Staff becomes more operationally efficient with day to day tasks

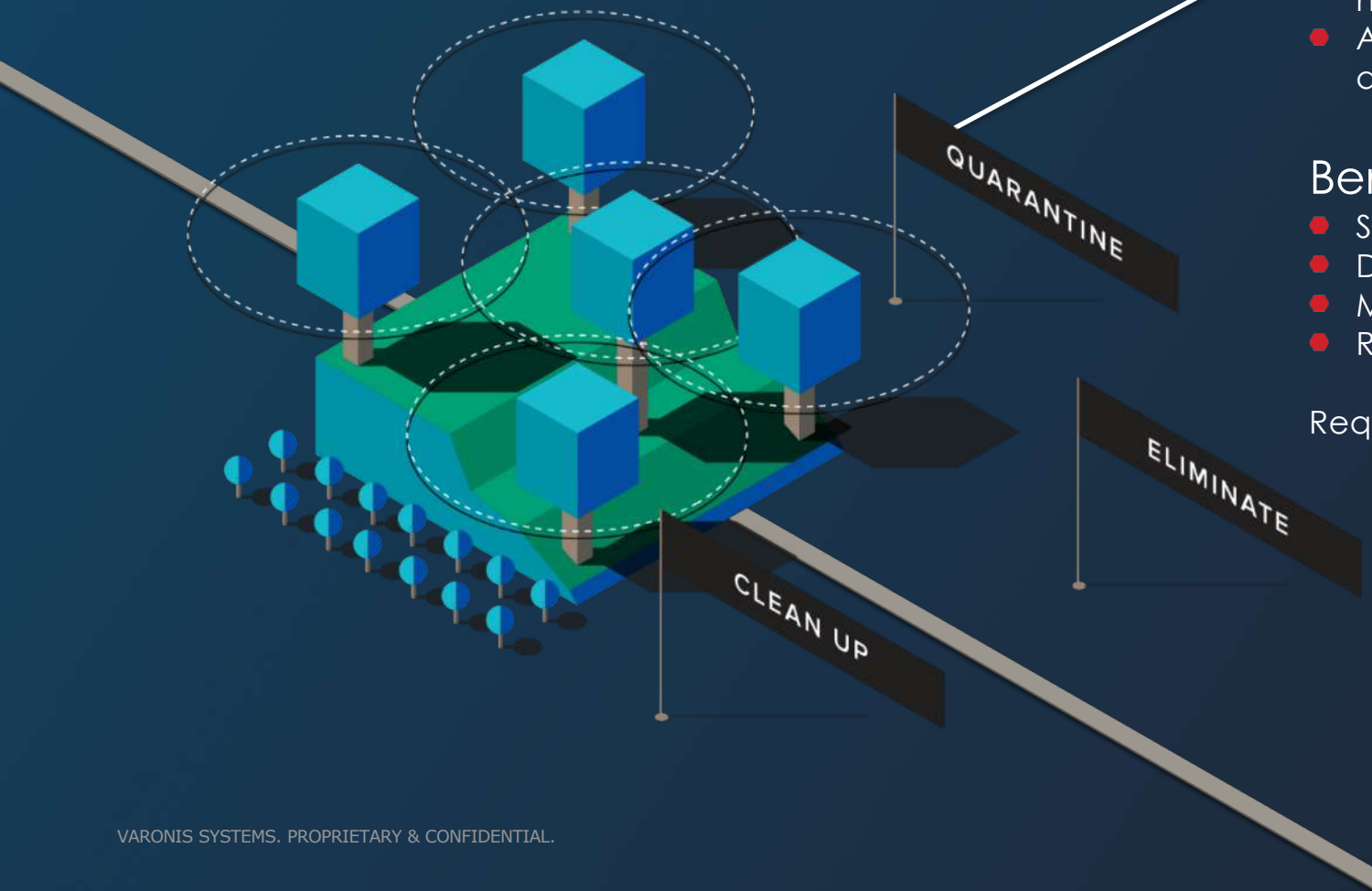
Requires: DA, DCF, DLS




Detect: Operationalize

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS




## Steps

- Fix inconsistent/broken ACL's
- Eliminate global access groups around sensitive data
- Eliminate remaining global access groups
- Address AD artifacts (empty, unused security groups, non-expiring passwords, etc.)
- Address retention/disposition by quarantining, archiving, and deleting stale data

## Benefits

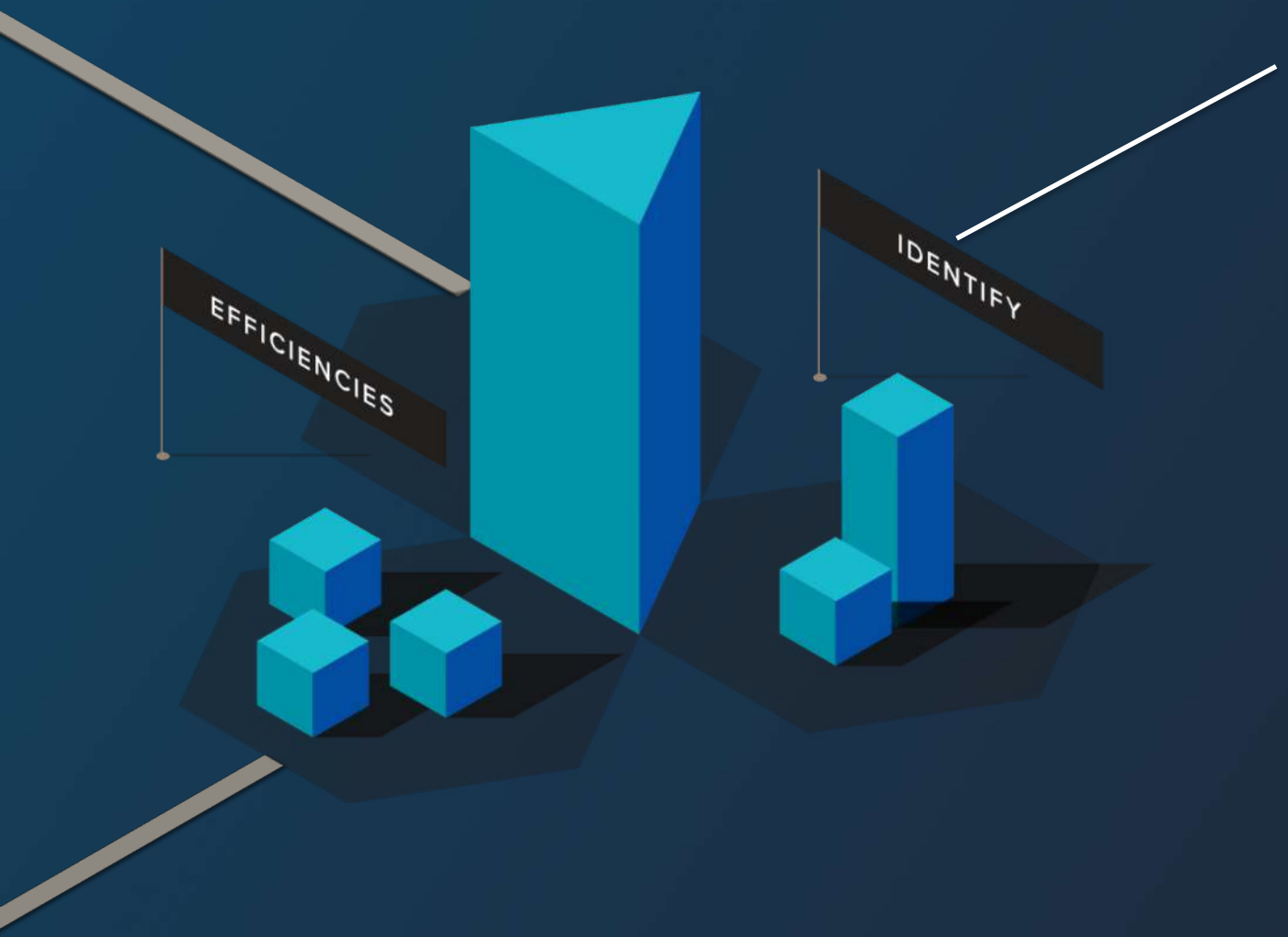
- Significant risk reduction
- Defensible position with respect to compliance
- More efficient usage of storage
- Reduced complexity increases operational efficiency

Requires: DA, DCF, AE, DS

Prevent: Fix

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

# Prevent: Transform




## Steps

- Identify folders that need owners (demarcation points)
- Identify and confirm data owners
- Simplify permission structure - (read/write), consistent inheritance
- Initiate entitlement reviews to prune residual access
- Prune residual unnecessary access

## Benefits

- Dramatic increase in operational efficiencies
- Better service for end users (faster access to data)
- Reduced complexity and risk

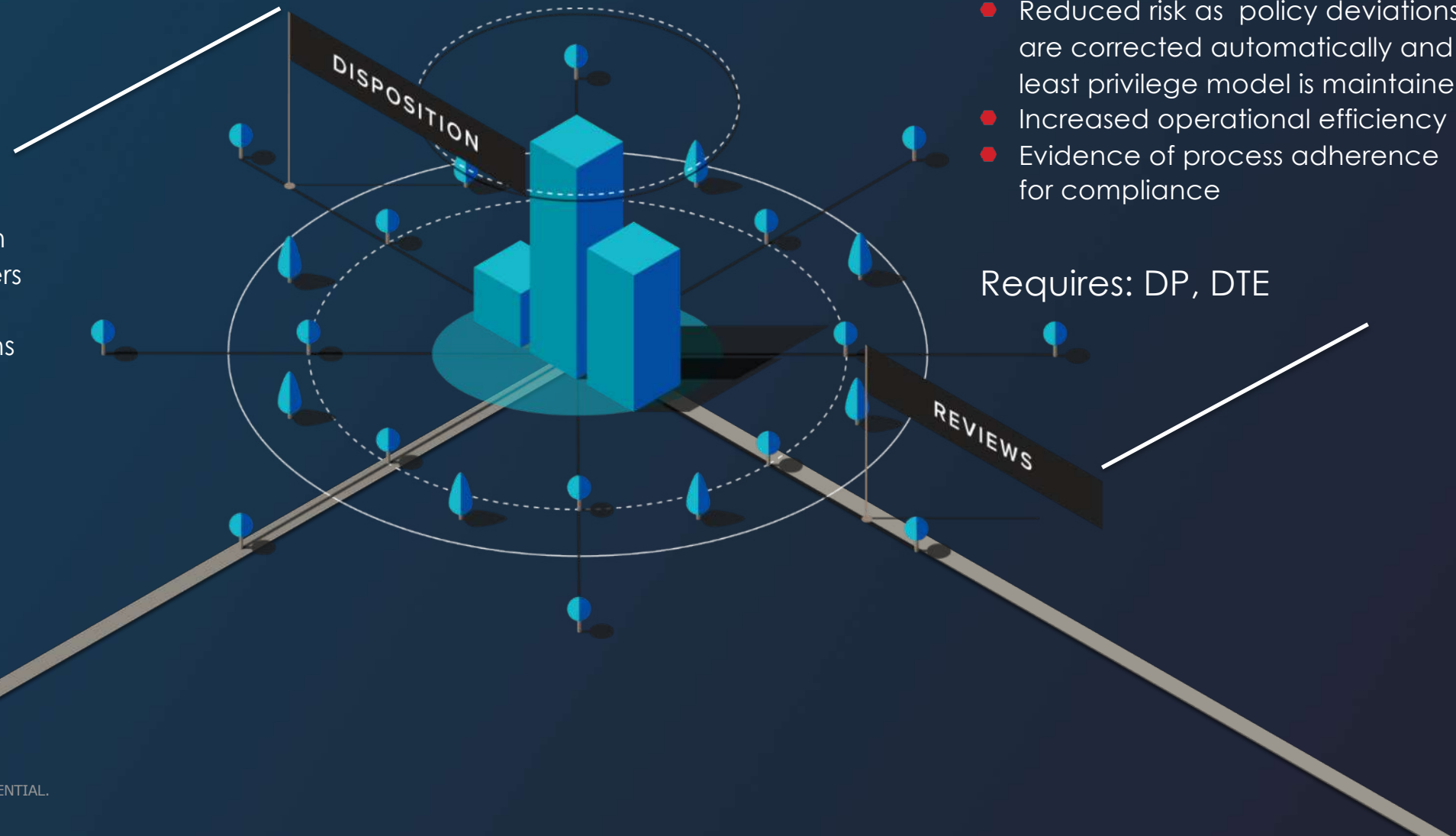
Requires: DA

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

# Sustain: Automate

## Steps

- Implement authorization workflow via data owners
- Automate disposition, quarantining, permissions enforcement
- Automate periodic entitlement reviews




## Benefits

- Reduced risk as policy deviations are corrected automatically and least privilege model is maintained
- Increased operational efficiency
- Evidence of process adherence for compliance

## Requires: DP, DTE

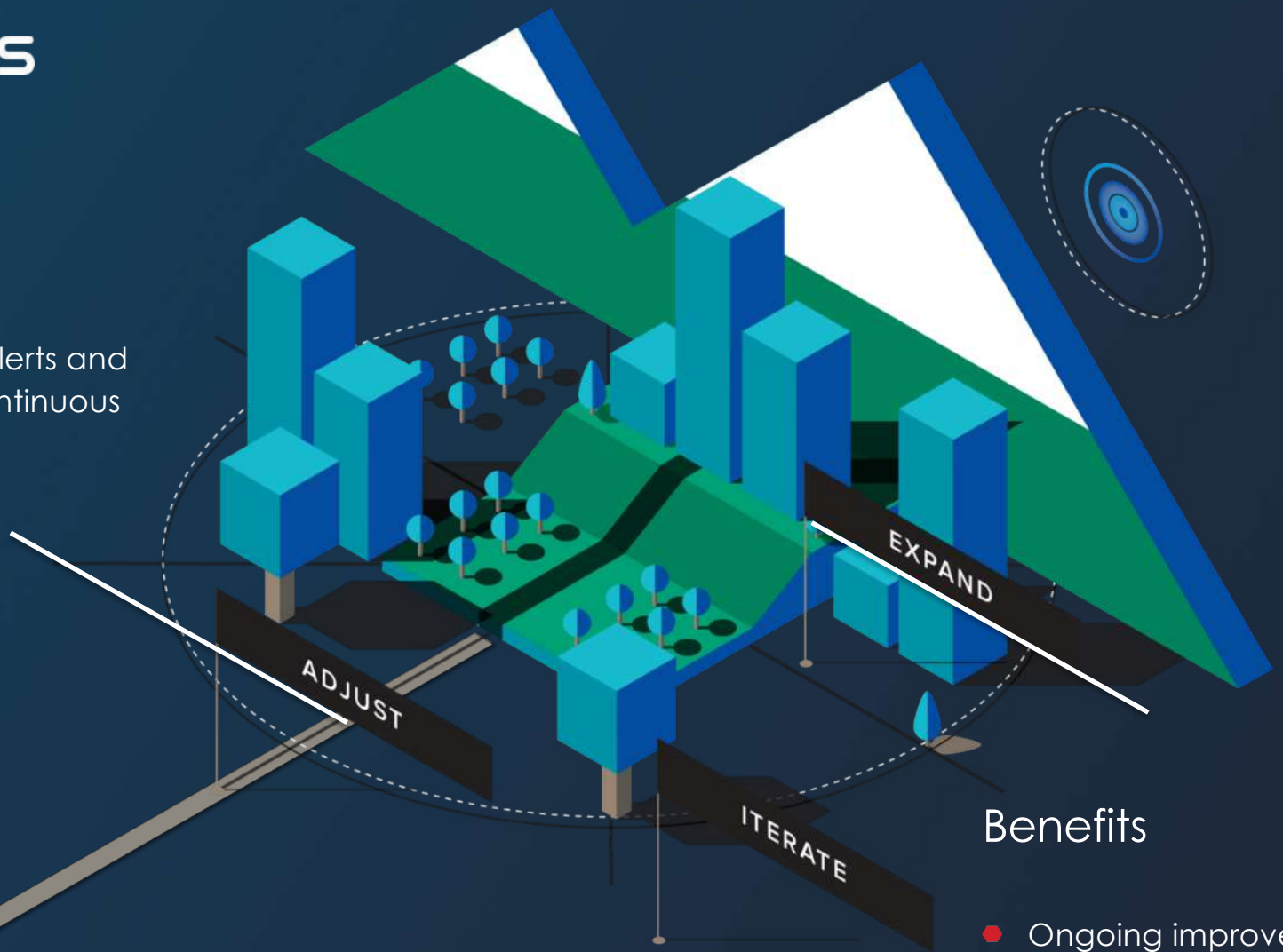
VARONIS SYSTEMS PROPRIETARY & CONFIDENTIAL.

VARONIS

# Sustain: Improve

## Steps

- Regularly review risks, alerts and processes to ensure continuous improvement




## Benefits

- Ongoing improvements in risk reduction and operational efficiency

Requires: DA, DCF, DLS, AE, DP, DTE

RONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

# Journey of Value

VARONIS

Risk Reduction
Efficiency Gains

## DETECT: 1. Prepare

Deploy Varonis

Prioritize and assess risks | DA, DCF

## 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, DCF, 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, DCF

## PREVENT: 4. Transformation

Identify folders that need owners | DA

Identify data owners | DA

Simplify permissions structure | DA

Initiate entitlement reviews to prune residual access | DA

## SUSTAIN: 5. Automation

Implement authorization workflow via Data Owners

Perform periodic entitlement reviews | DA, DP

## SUSTAIN: 6. Improve

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

VARONIS

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

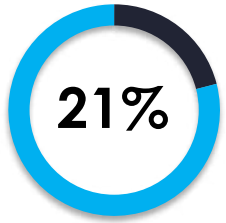
# Comprehensive Risk Assessment

- 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?

# Data Risk Report Findings

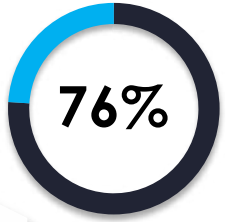
**41%** had at least 1,000 **sensitive files** opened to every employee

**58%** have over 100,000 **sensitive folders** opened to every employee



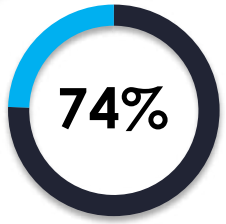

of folders are opened to **global group access**

Statistics from over 130 organizations




of folders contain **stale data**

**34%** of **user accounts** are enabled but inactive

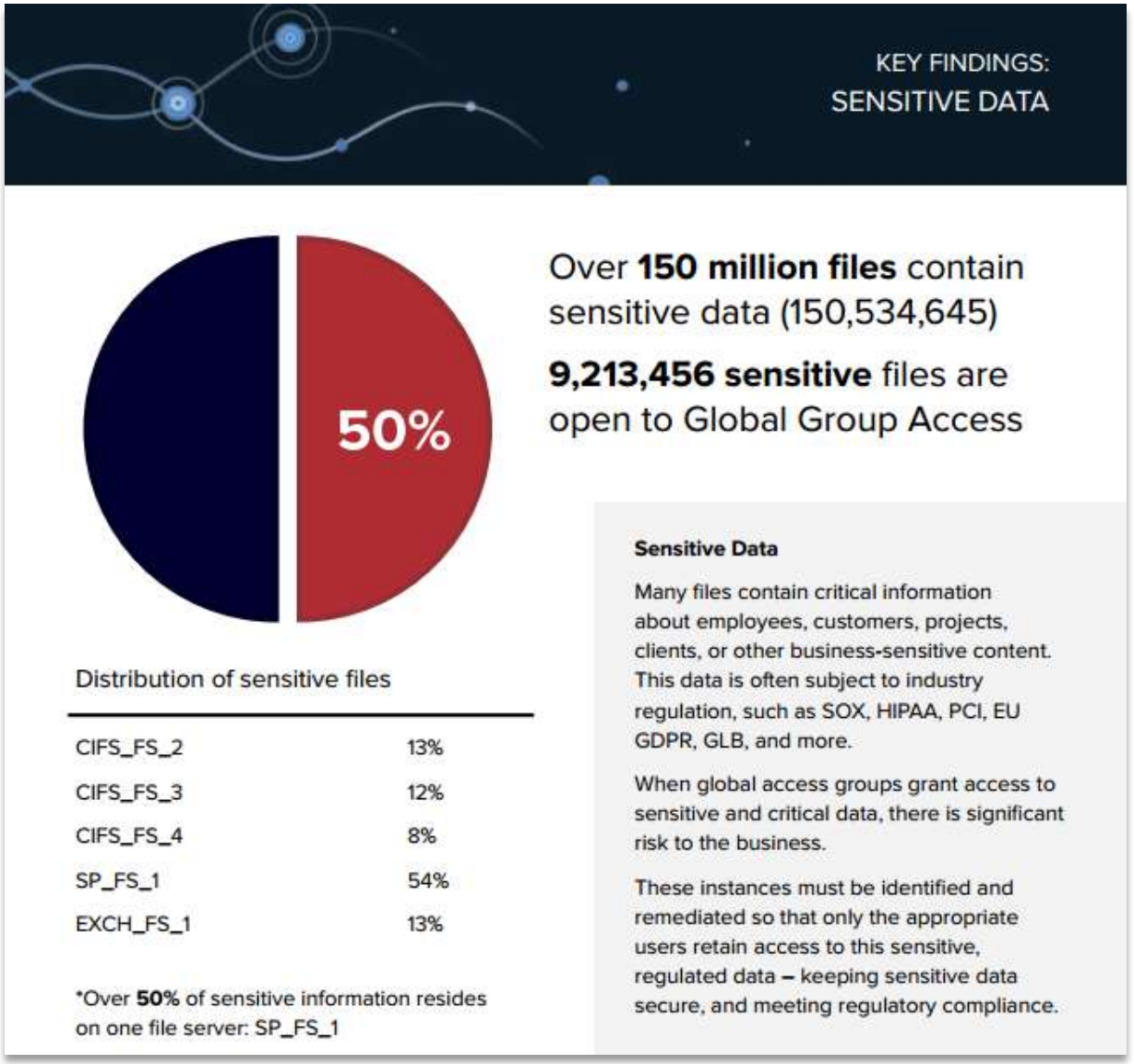



of companies have **over 1,000 stale, sensitive files**

The 2018 Global Data Risk Report captures findings of Data Risk Assessments performed on 130 organizations—a representative sample from many industry segments and sizes.

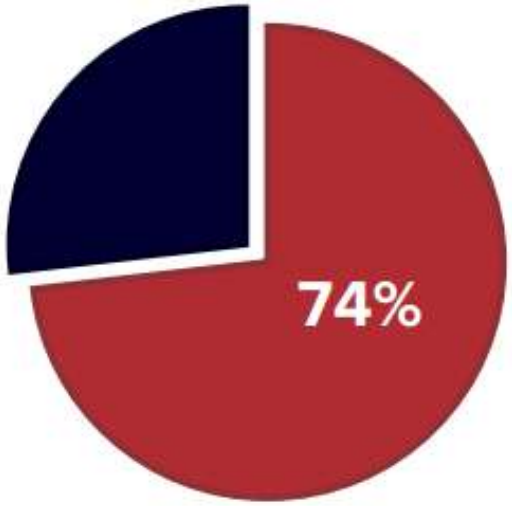
# Sensitive Data

- Where does my sensitive data live?
- How much of it is over-exposed?
- What kind of sensitive data do I have? (PCI, SOX, PII, etc.)



# Global Access

- Which data is open to everyone?
- Which data is open to everyone *and* is also sensitive?




Over **66.5 million folders** with global group access

66,502,975 of 90,348,156

Distribution of global group access

| | |
|---|---|
| CIFS_FS_2 | 11% |
| CIFS_FS_3 | 7% |
| CIFS_FS_4 | 20% |
| SP_FS_1 | 44% |
| EXCH_FS_1 | 18% |

**Global Group Access**

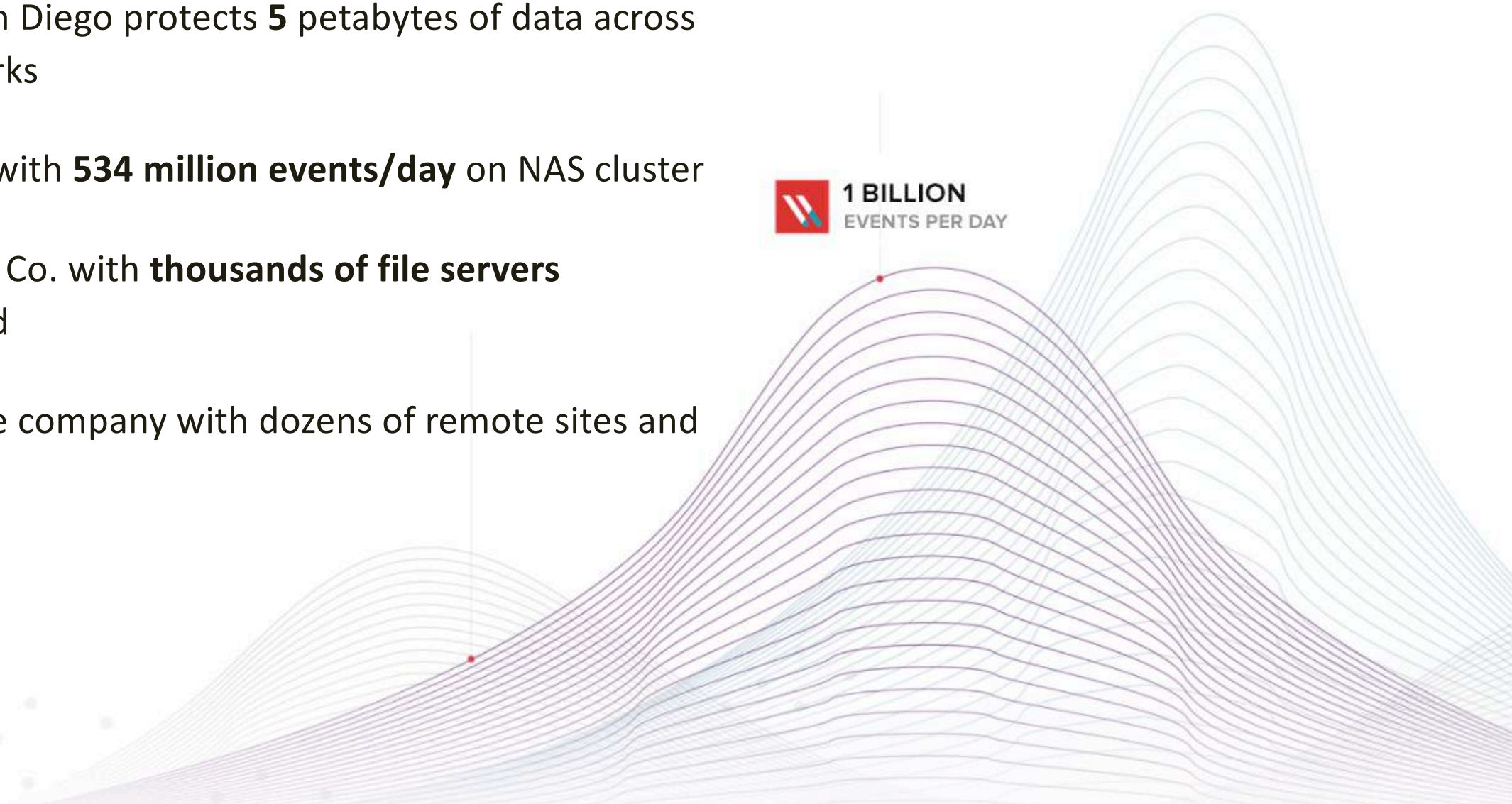
These include groups such as Everyone, Domain Users, and Authenticated Users.

Global access groups will allow anyone within an organization to access data with these access controls.

Data should generally never be accessible to global access groups like Everyone, Domain Users, or Authenticated Users. Data that is open to everyone is most vulnerable and at-risk for loss, theft or misuse.

# Built to Scale

- City of San Diego protects **5** petabytes of data across **24** networks
- Financial with **534 million events/day** on NAS cluster
- Insurance Co. with **thousands of file servers** monitored
- Aerospace company with dozens of remote sites and domains



VARONIS

Fighting a different battle than conventional cybersecurity companies

# Grazie!

Security Summit Roma, 5 Giugno 2019

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.