

Insider Threat Analytics & Anomalous Behaviors

By
Carl Miller
Security Strategist

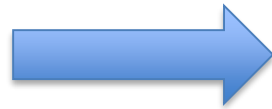


GURUCUL
PREDICTIVE SECURITY ANALYTICS

Too Much Data



**Data
Volume
& Growth**



**Data
Silos &
Expenses**



**Big Data
Lake
Adoption**



Too Few Resources



**Staffing,
Budget
& Talent**



**Alert
Fatigue &
Dead Ends**



**Leverage
Machine
Learning**



Fading Perimeter



**Cloud,
Mobility
& BYOD**



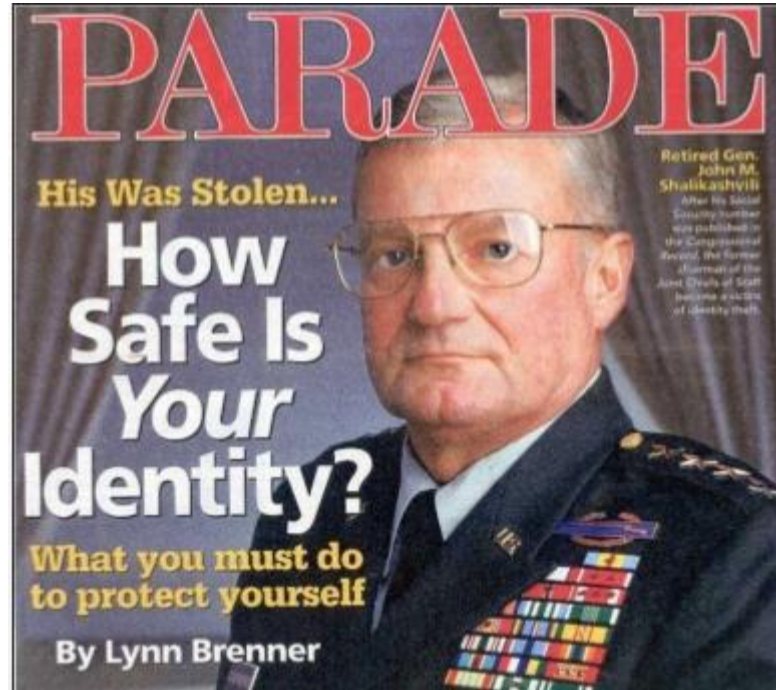
**User
Apps
& Data**



**Identity
Attack
Vector**



New Attack Vector



**Identity
Compromise
& Misuse**



**Evades
Declarative
Defenses**



**Core of
Modern
Threats**



Behavior Anomalies

Solution



**Big Data
& Data
Sources**



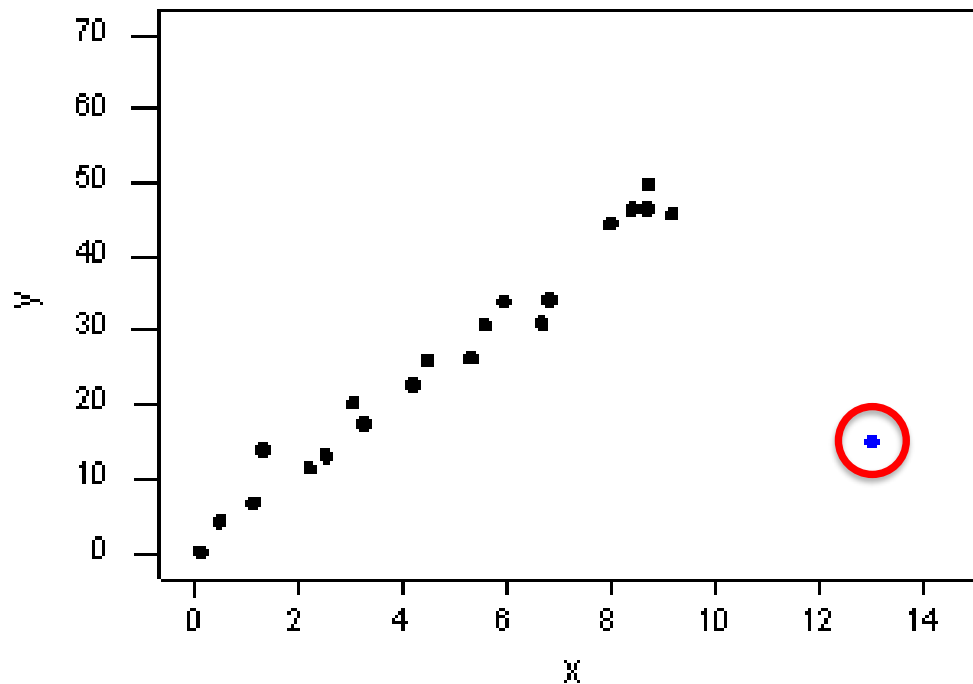
**Machine
Learning
Models**



**Behavior
Analytics &
Risk Scoring**



Anomaly Detection



User
Entity
Peers



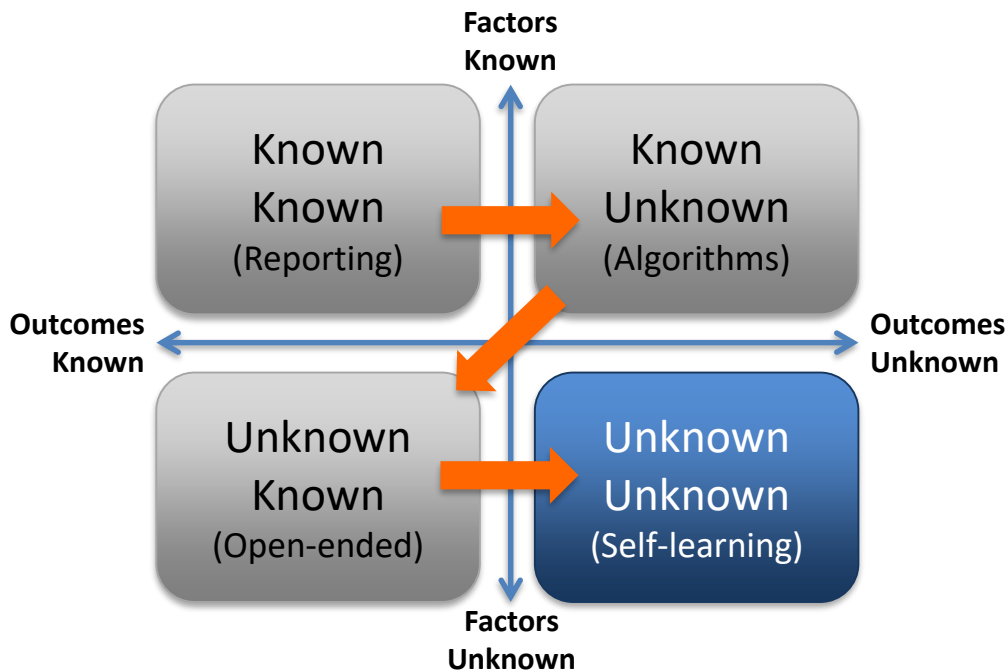
Access
and
Activity



Clustering
w/Outlier
Analysis



Unknown Unknowns



**Declarative
Defenses
& Rules**



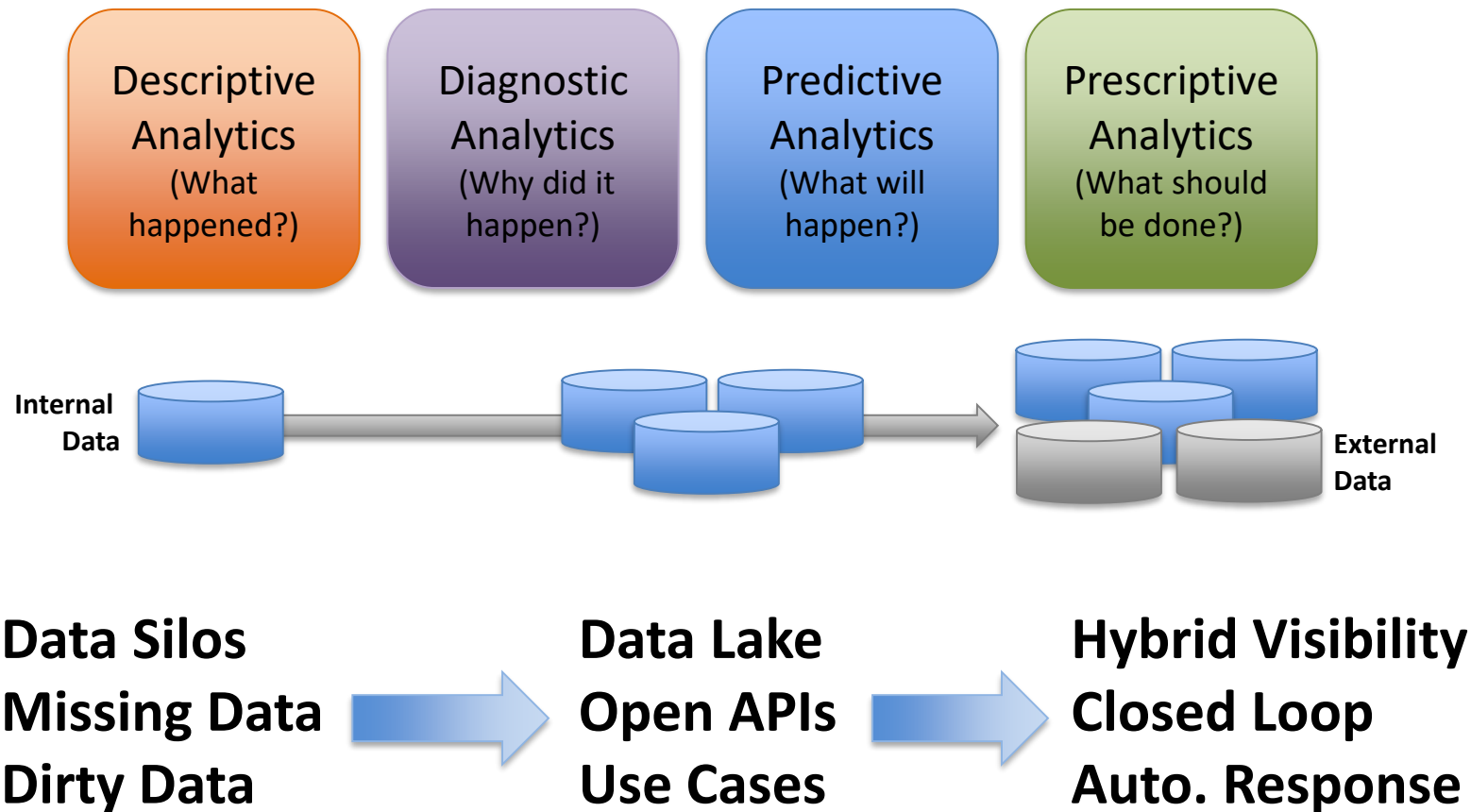
**Correlations
Causality
& Hunting**



**Predictive
Security
Analytics**

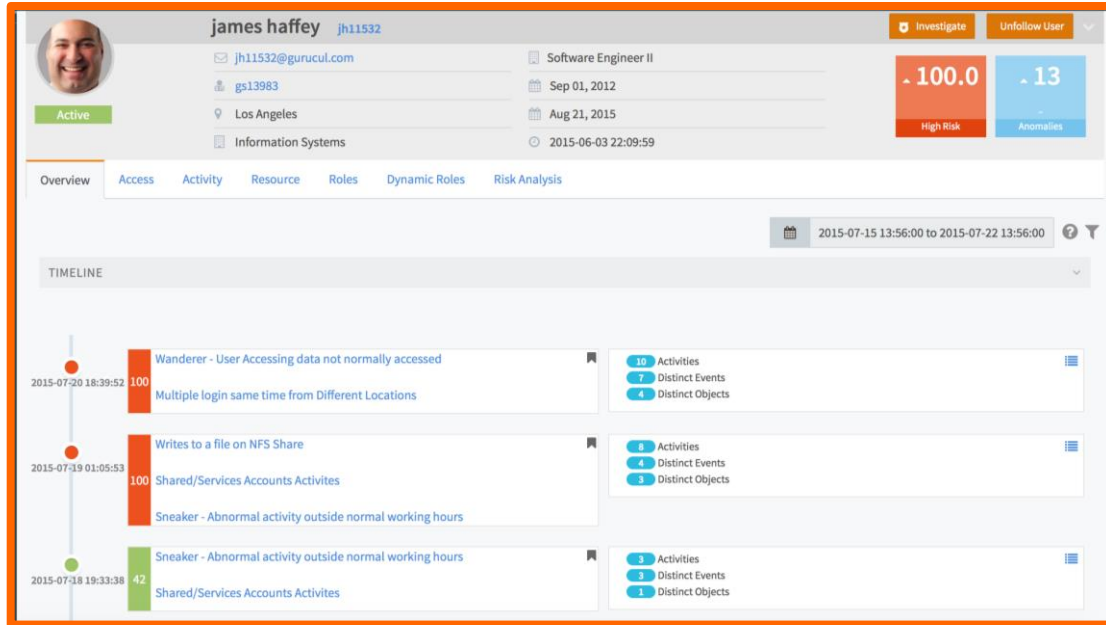


Analytic Maturity Model



User/Entity Behavior Analytics

Solution



Privileged
Access
Abuse



Data
Exfiltration
& Theft



Insider
Threats &
Self-Audits



Identity Analytics (IdA)



**Excess
Access &
Outliers**



**Risk-based
Certs &
Approvals**



**Dynamic
Access
Provisioning**



Privileged Access Analytics

Solution



**Hidden
Privileged
Access**



**Outside
Lists &
Vault**



**Entitlements
Determine
Privileged Access**



Custom ML Models

Solution



**Military
Federal
Financial**



**Private
Data &
Use Cases**

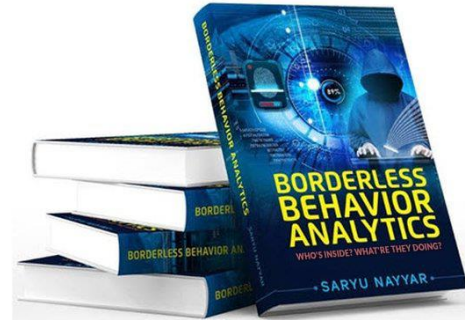


**Custom
Model
Creation**



Thank You!

To Learn more about
behavior analytics:



Available at
amazon

www.borderlessbehavioranalytics.com

