Datiphy Smart Data UEBA

Data-Centric View of UEBA

V1.4
Decemer18, 2019

Agenda

1. About Datiphy
2. UEBA Technology & Products
3. Datiphy UEBA Technology
4. Value Proposition

datiphy™
Know Your Data

About Datiphy

Company Mission:

- Provide a solution that will provide in-depth visibility and identify high-risk behaviors to every piece of sensitive data within an organization

Market:

- Data Centric Audit & Protection (**DCAP**)
- User & Entity Behavior Analysis (**UEBA**)
- Threat Intelligence **(TI)**

Solution:

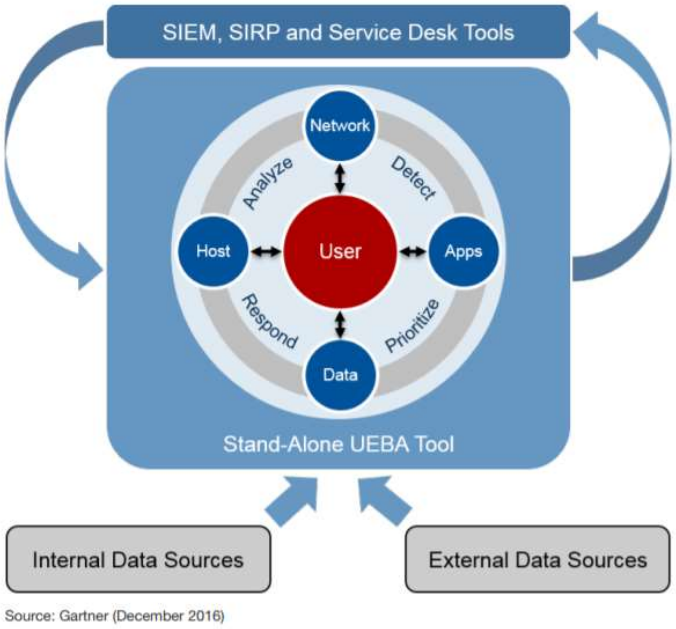
- Using **DatiDNA™** technology to incorporate user behaviors & data analytics to produce threat models

What is UEBA Used For?

UEBA is the abbreviation of “User and Entity Behavior Analytics”.
The primary objectives of UEBA is:

- Detect - Rapidly identify attack with alerts/notifications .
- Prioritize - Prioritize alerts for risk professional to take actions. Improve alert management by correlating/consolidating alerts from existing systems
- Respond - Streamline alerts and incident investigations to reduce incident investigation time. Provide contextual information from various data sources to expedite the investigator’s response time.
- Analyze - Apply analytics across a variety of data sources in near real time and on a frequent basis (hourly, daily).

What Features UEBA are Equipped with ?



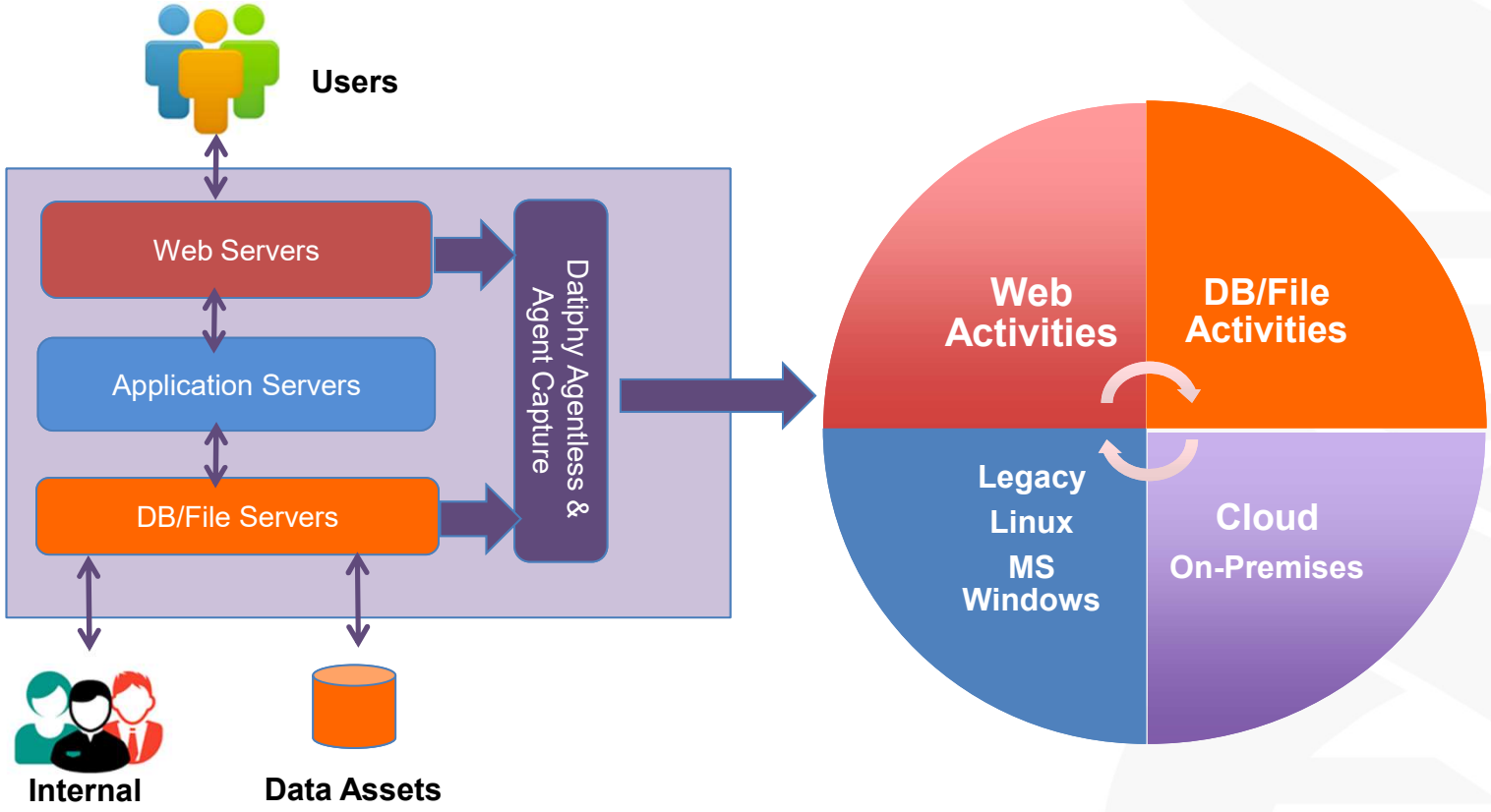
Source: Gartner (December 2016)

- UEBA solutions should be able to understand any type of structured data and non-structured information needed for its analysis
- UEBA product that only ingests logs may miss important activity, especially if it does not have full visibility into the endpoint device used by the user.
- UEBA brings machine learning and statistical analysis to security monitoring, generating risk scores for evaluated events and entities

Datiphy and End System UEBA Comparison

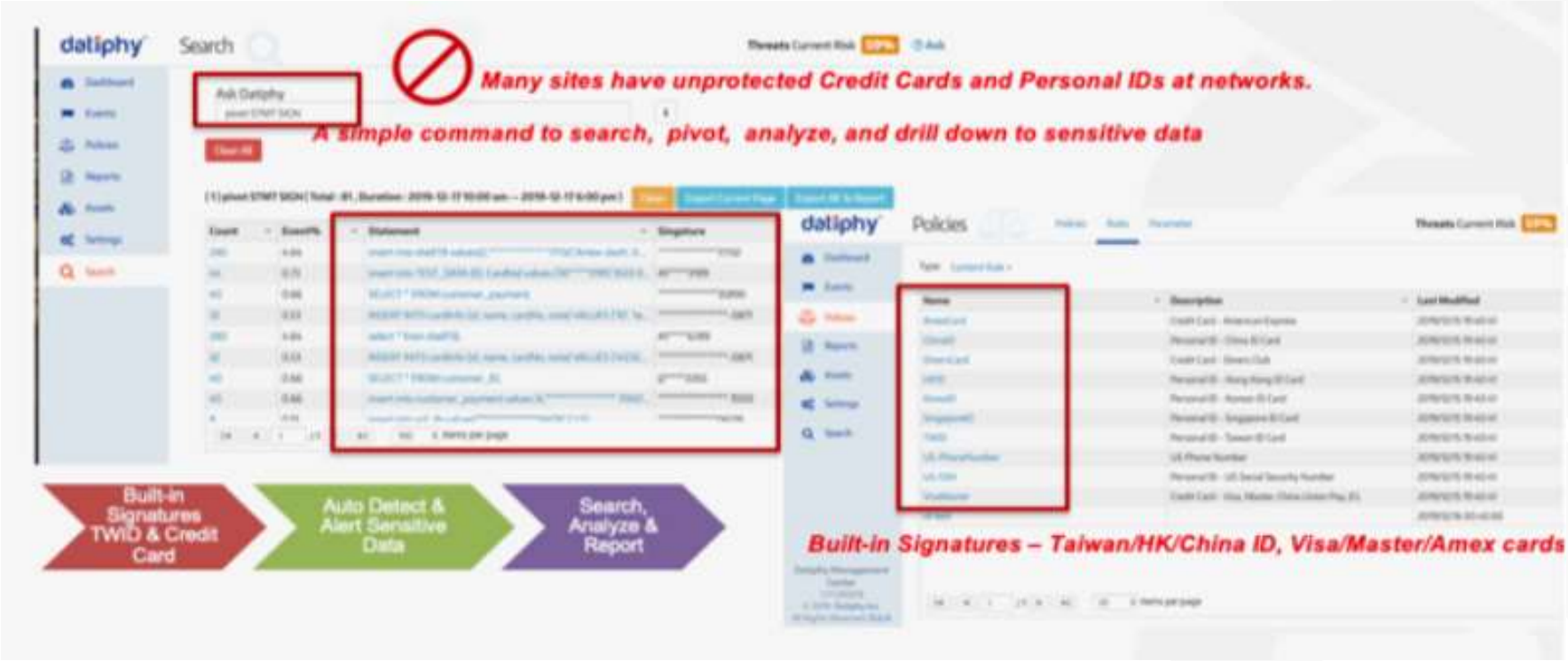
Solutions	Datiphy Smart Data UEBA	End System UEBA
Features	User and Data Behavior Analytics to Audit/Block both external and internal threats (Users and Internal Admins)	End System (Users) Breach Scan User Behavior Analytics
Technology	Audit Data → Data Behavior → Data Intelligence AI on User and Data Behaviors	End System Virus Scan --> Breach/Vulnerability Scan AI on User Behaviors
Environment	Cover Entire Enterprise Infrastructure (On Premises & Cloud) (End Users, Web, Application, DB Layers)	Cover End Systems (on Premises & Cloud)
Deployment	Datiphy Management Center (with Agents)	End Systems and Management Console
Integration	Seamless Integration by REST API and Connectors: Splunk, SIEM, ELK, PowerBI, Hadoop, Log Manager, etc.	Log Manager

Datiphy Enterprise Environment

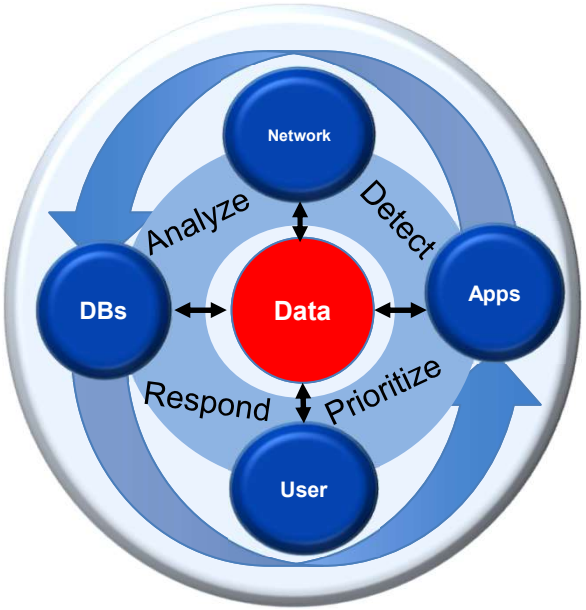


Detect and Prevent APT (Advanced Persistent Threats)

Detect and protect Sensitive Data



Datiphy provides Data-Centric View of UEBA



- Data-Centric Protection
  - Who, when, where, what, how?
- Auto Data & Assets Inventory
  - New assets discovery
  - Assets map
- User & Data Profiling
  - User/Data Behavior Modeling
  - Machine Learning & Pattern Matching
  - User & Data Behavior Correlation
- Data Auditing & Compliance
  - Audit events
  - Data integrity and non-repudiation
  - Compliance to regulations (GDPR, PCI DSS, HIPAA…)

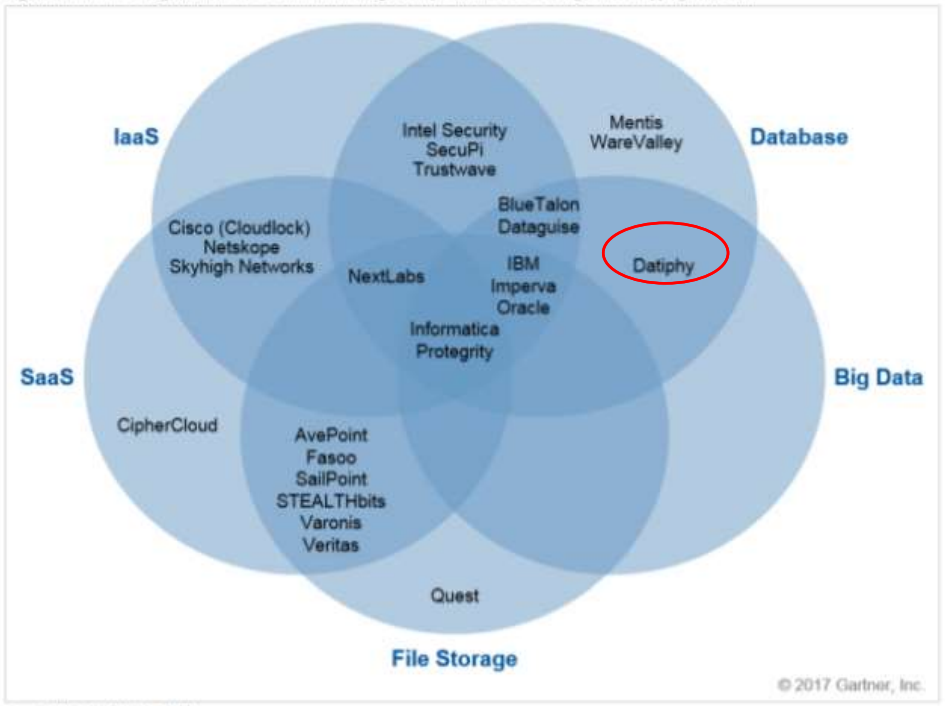
Gartner lists Datiphy as UEBA Representative Vendor

Datiphy Enterprise focuses on monitoring structured and unstructured data in databases (both on-premises and in cloud services) using a combination of agents deployed on hosts, in the cloud or at the network layer. The solution is deployed on the customer's premises as the management server along with the agents. Datiphy Enterprise has preconfigured threat intelligence rules, as well as risk metrics included out of the box. Pattern matching and machine learning are used to profile users and entities, and to detect specific threats against databases.

Domains: Data exfiltration, external threats

Gartner lists Datiphy as (DCAP) Data-Centric Auditing and Protection Representative Vendor

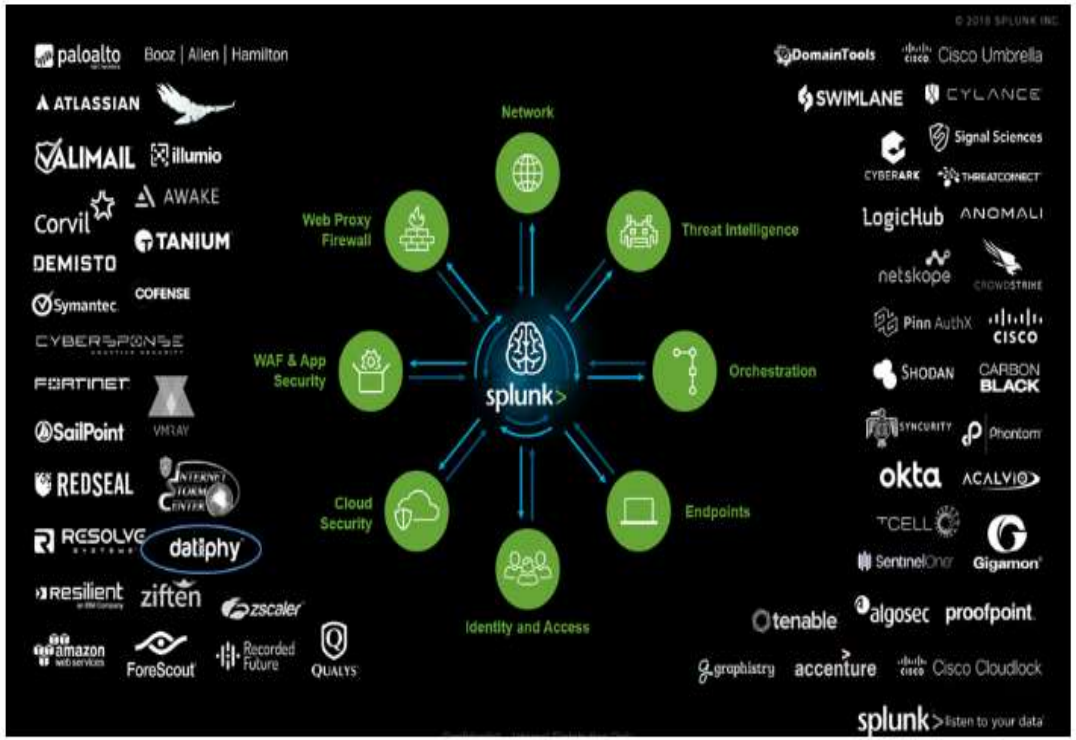
Figure 2. Schematic Diagram for the DCAP Market Showing a Sample of Vendor's Coverage of Overlapping Data Silos



Source: Gartner (March 2017)

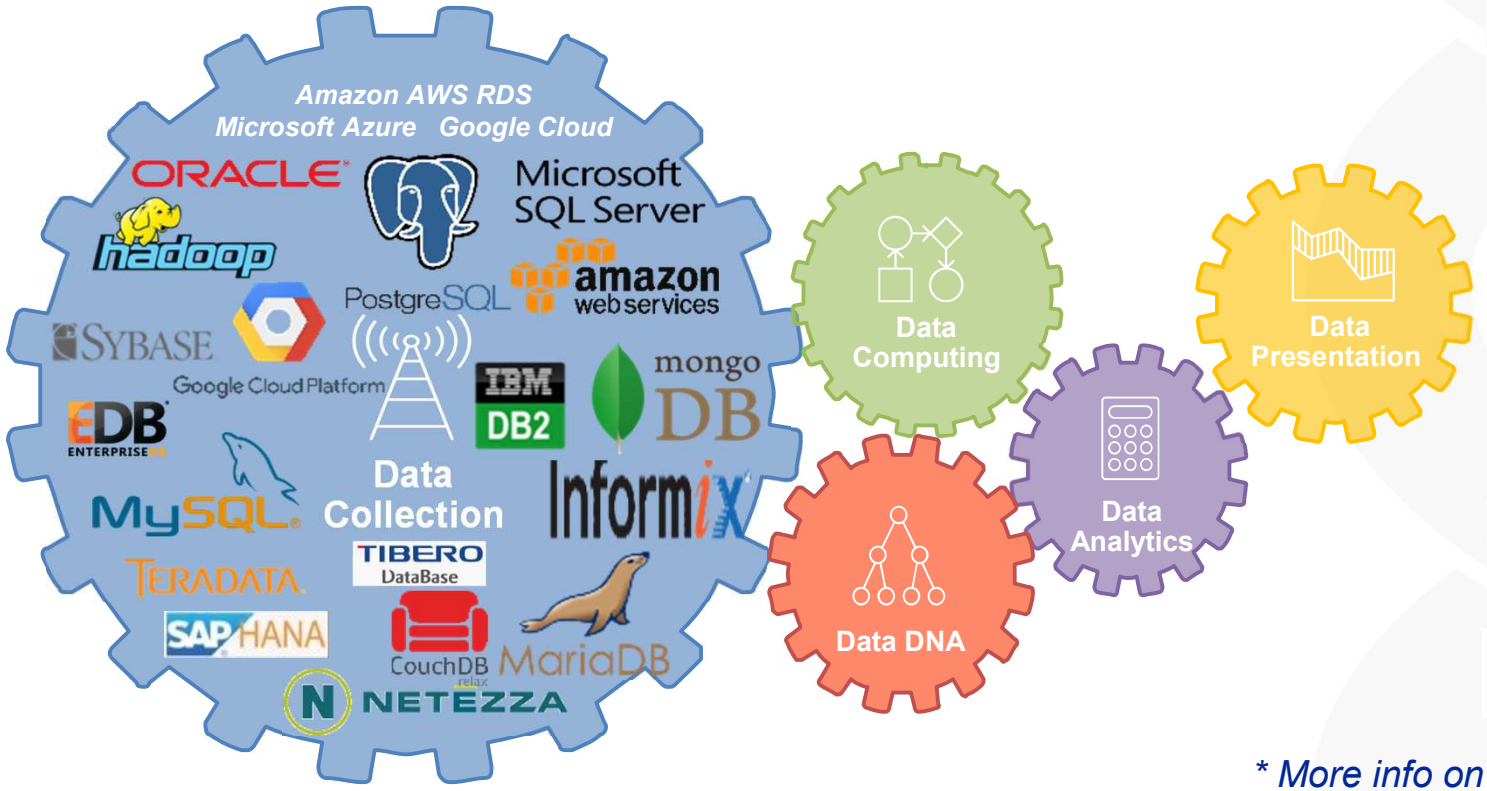
Adaptive Response Action Framework-

Timely respond to threats



Datiphy partners with AWS and Splunk in the Adaptive Response Action Framework using patented machine learning technology to provide data-centric UEBA solutions for enterprise customers.

Datiphy Smart Data UEBA Process

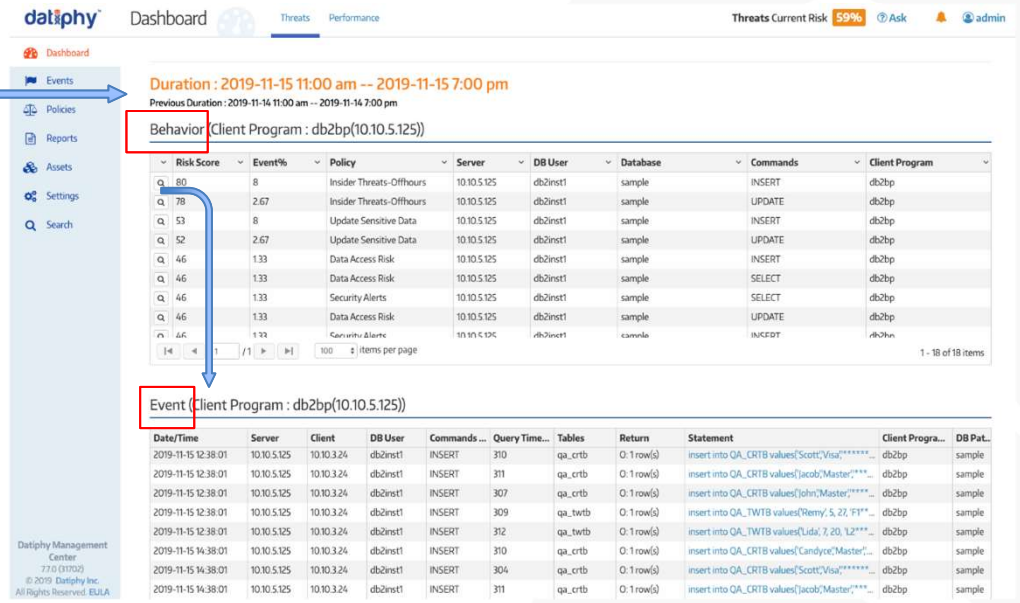


datiphy
tableau
Power BI
splunk>
elastic
hadoop
kafka
logstash

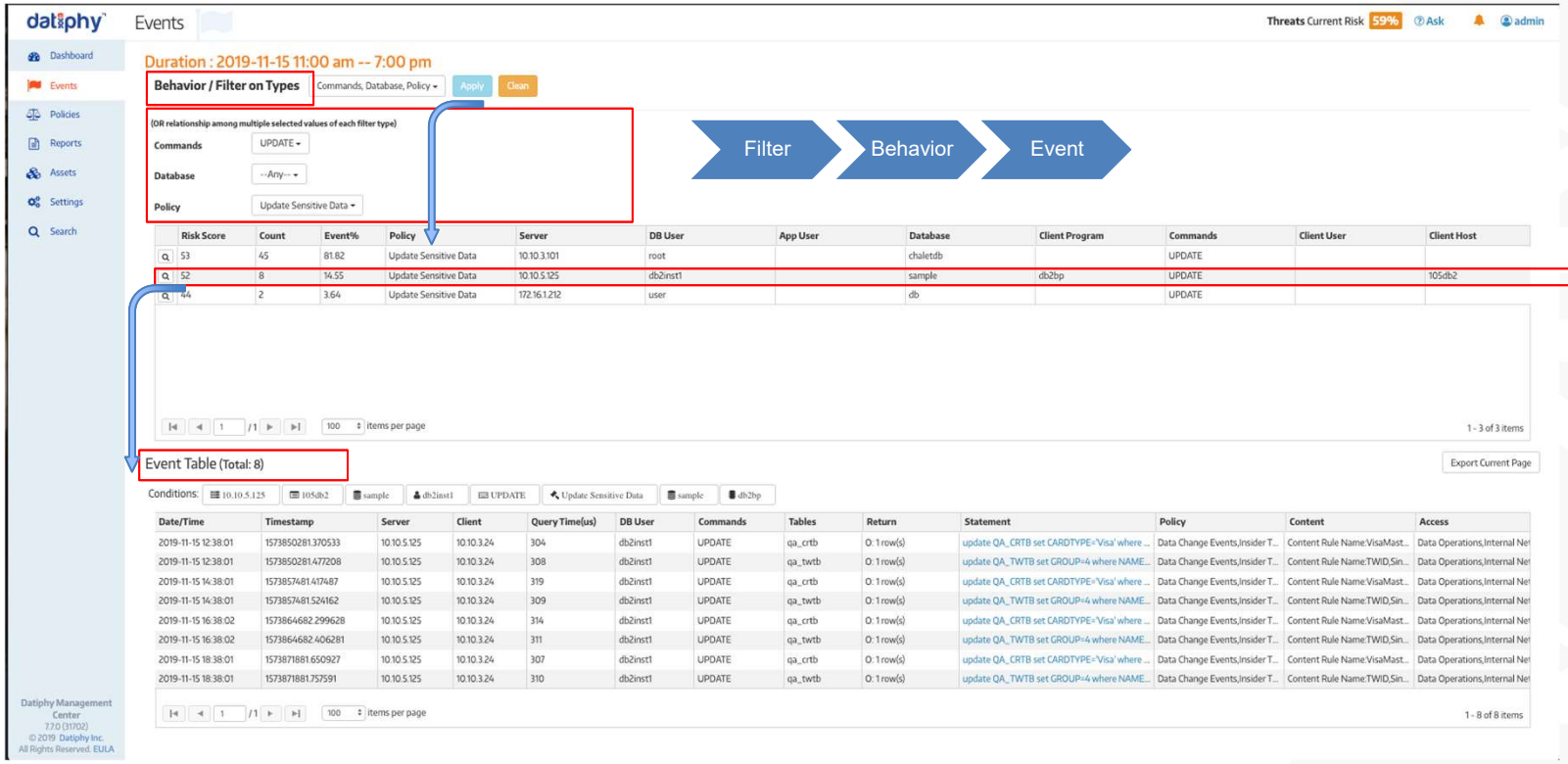
** More info on www.datiphy.com*

Dashboard – Showing Risk and Behaviors

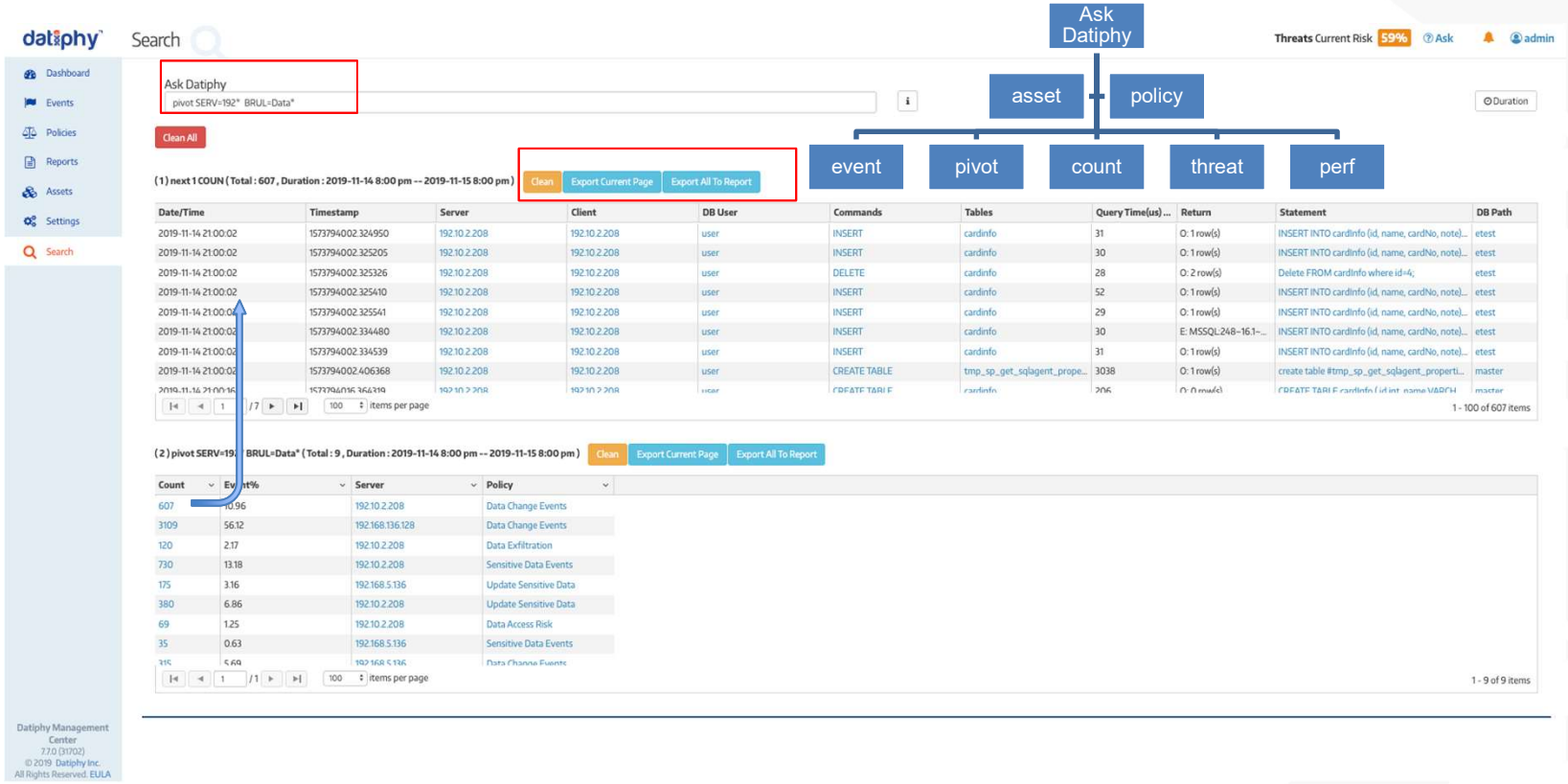
Trend → Risk View → Behavior → Event → Report



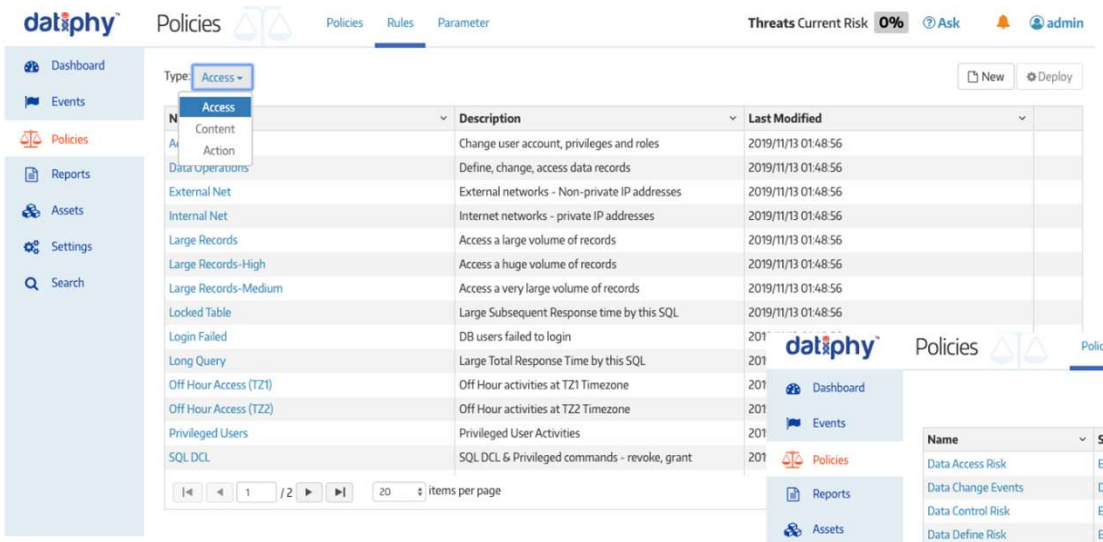
Drill down to Events details

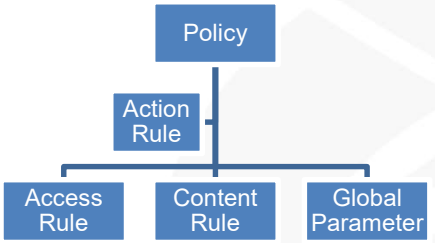


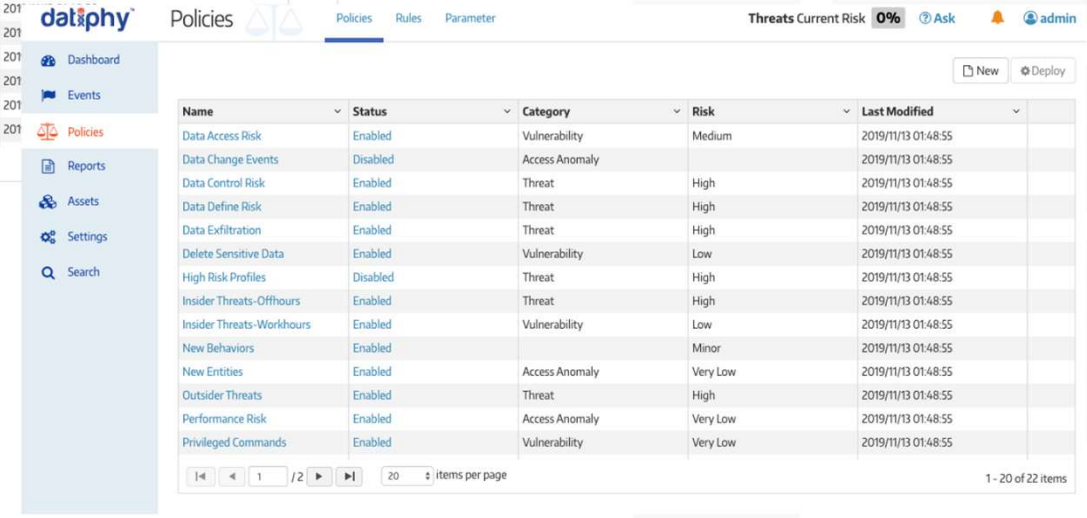
Search and Analytics – Correlate Users and Data



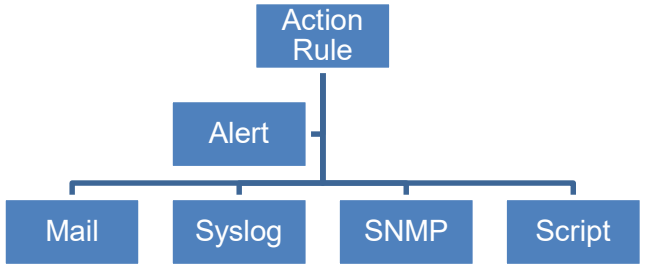
Policies and rules

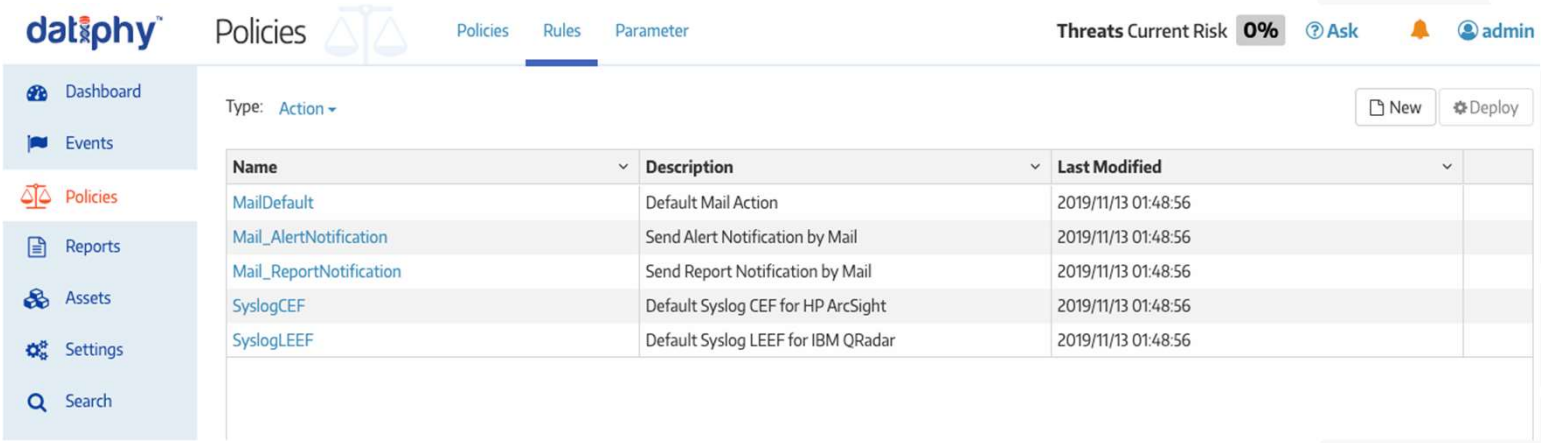




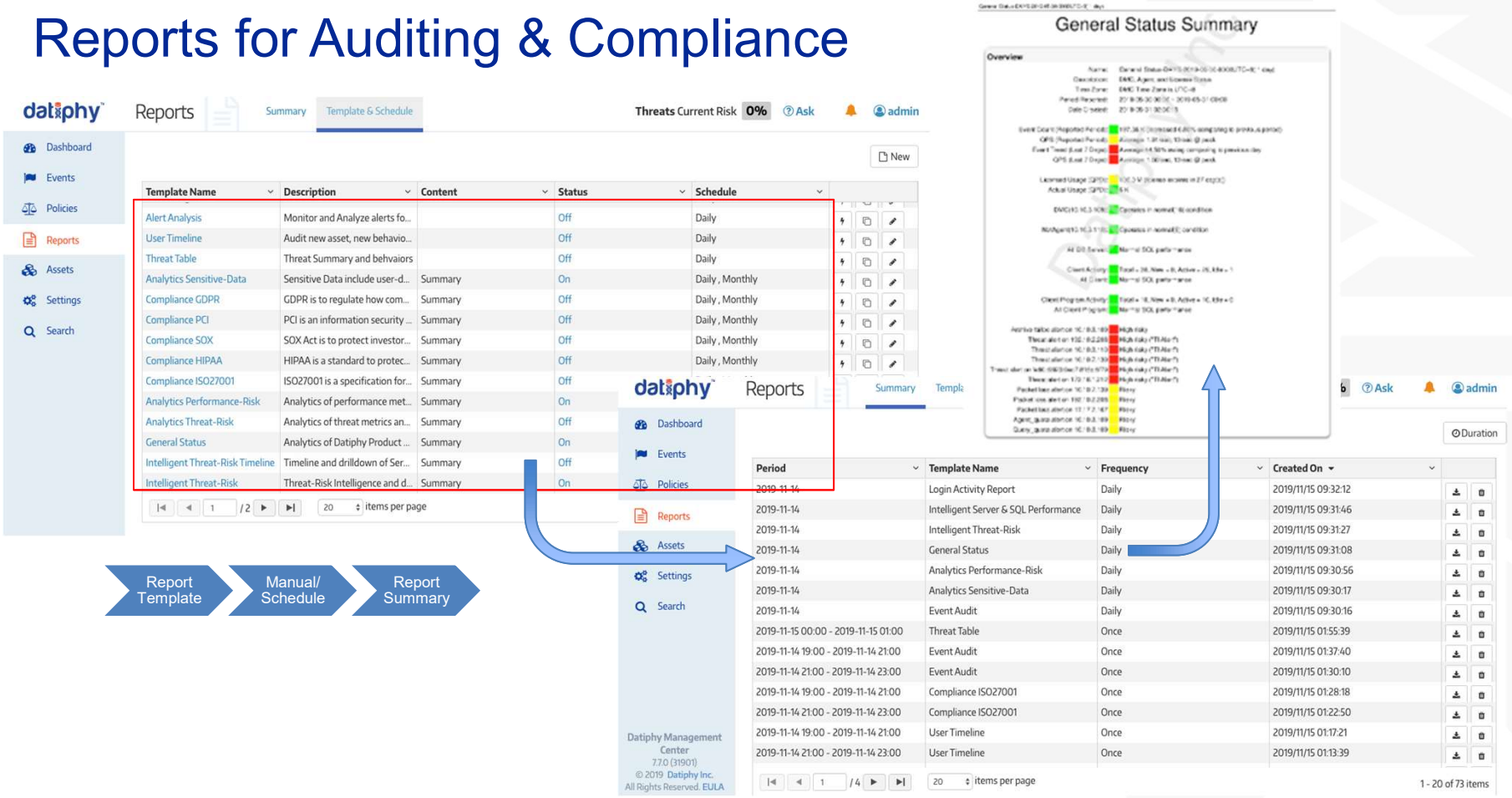


Alerts and Actions





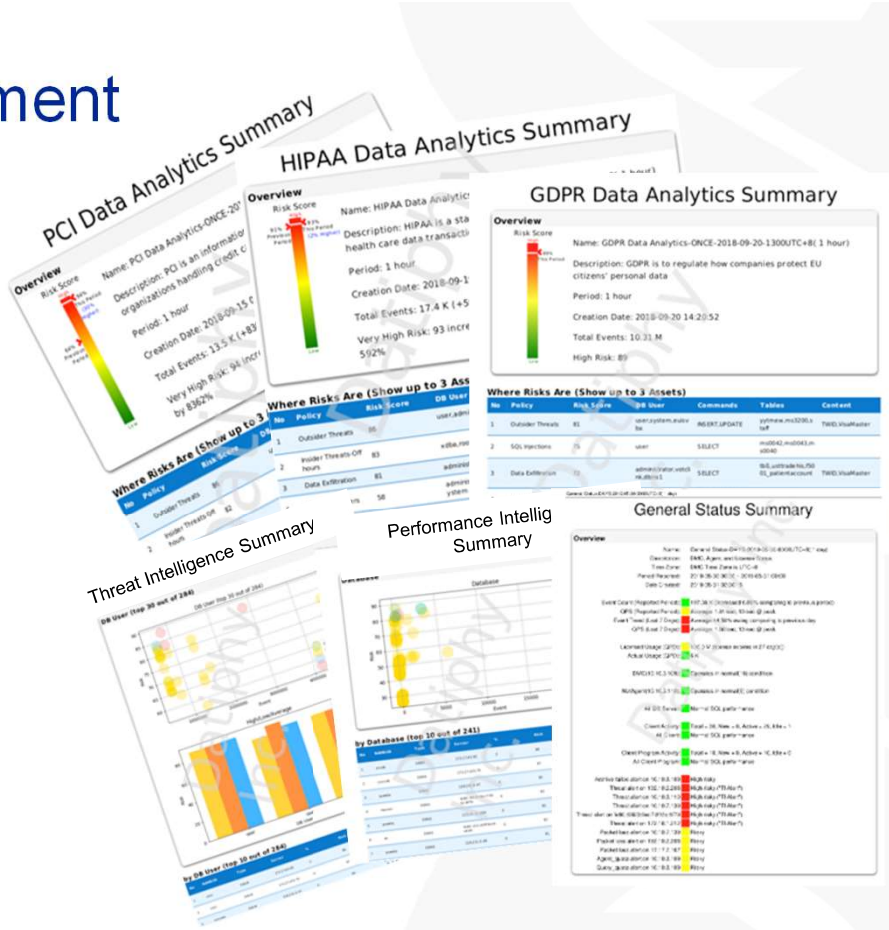
Reports for Auditing & Compliance



Intelligence Reports for Management

One-page Executive Summary:
Pinpoint Risks on What, Who, Where, When and How

Report Type	Templates
Compliance	GDPR, HIPAA, PCI, ISO27001, FSI Audit, Personal Data Audit .
Security	Threat Intelligence, Security Audit
Performance	Performance Intelligence Capacity Planning, Performance Audit
Operation	Asset, Status, Timeline, ..



Value Proposition

- Gartner list as DCAP(Data-Centric Auditing & Protection) & UEBA (User Entity Behavior Analysis) representative vendor
- 10+ US Patent Technology
- RD and support in both San Jose and Taiwan
- Centralized Management of hybrid databases
- Machine Learning Technology for Behavior Modeling
- Threat Intelligence and Risk Management
- Customer Reference in all industries