

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



datiphyTM
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:

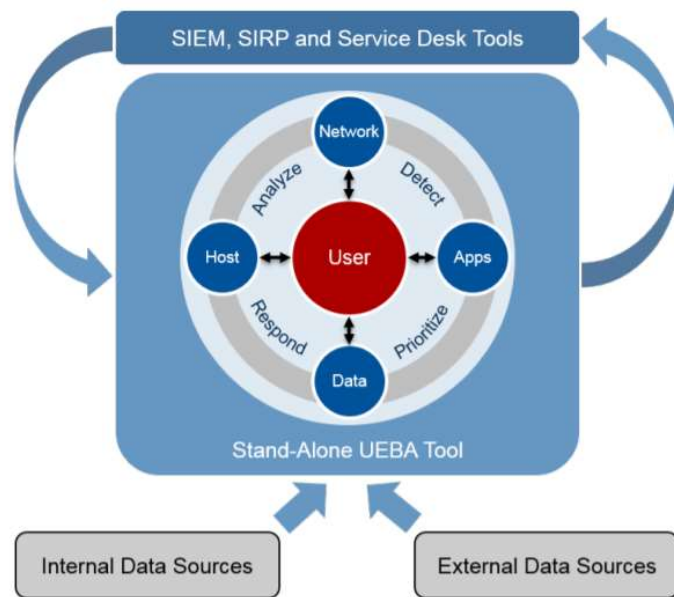
- Using **DatiDNA™** technology to incorporate user behaviors & data analytics to produce threat models

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?



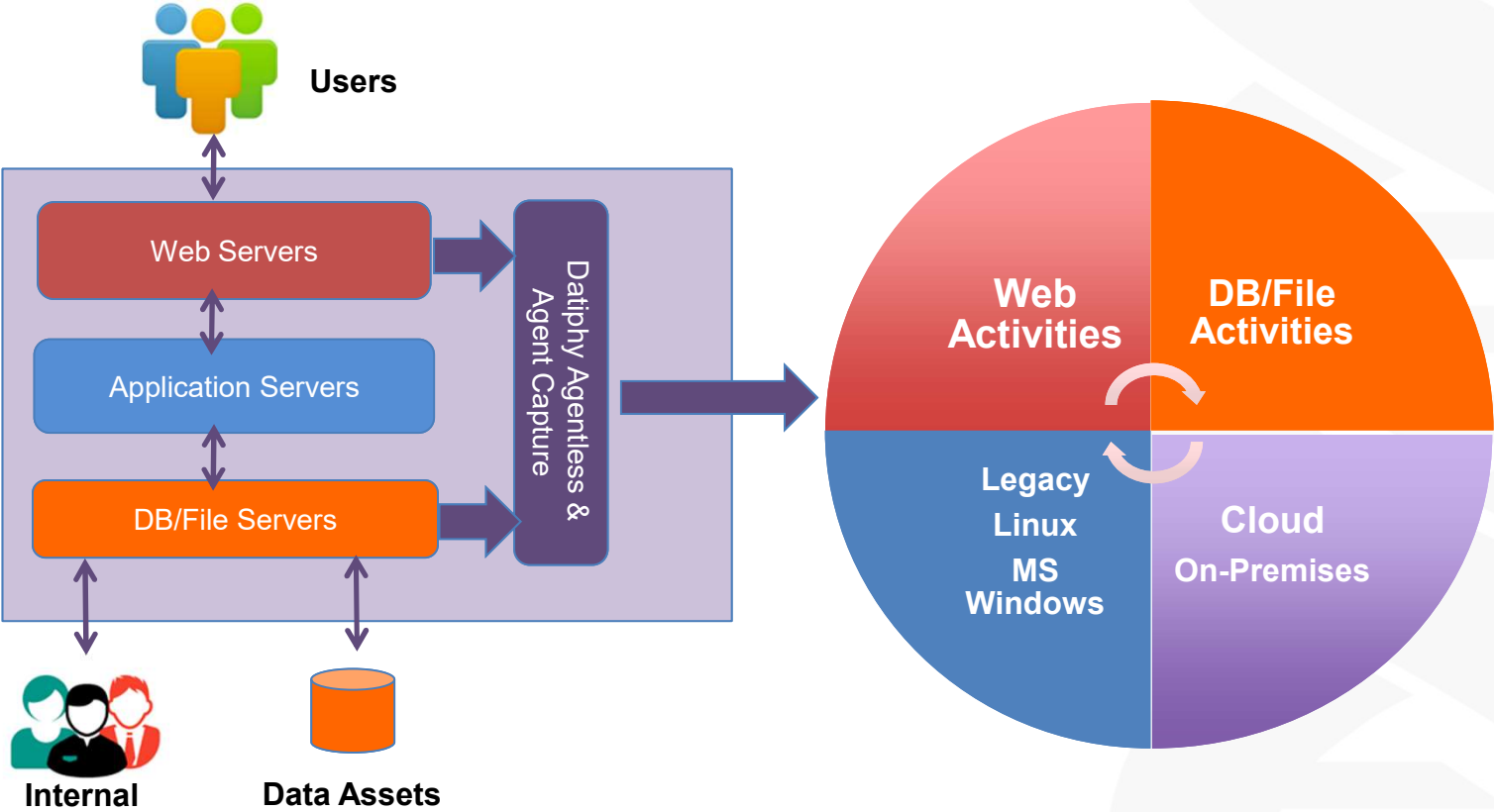
Source: Gartner (December 2016)

- 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

Many sites have unprotected Credit Cards and Personal IDs at networks.

A simple command to search, pivot, analyze, and drill down to sensitive data

Search Command: `Ask DathiPhy show:TWID:SIGN`

Results Table:

Event	Severity	Statement	Signature
200	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000
100	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000
100	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000
100	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000
100	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000
100	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000
100	CRITICAL	Account: TWID: SIGN: (S) CardNo: 1234567890123456	0000000000000000

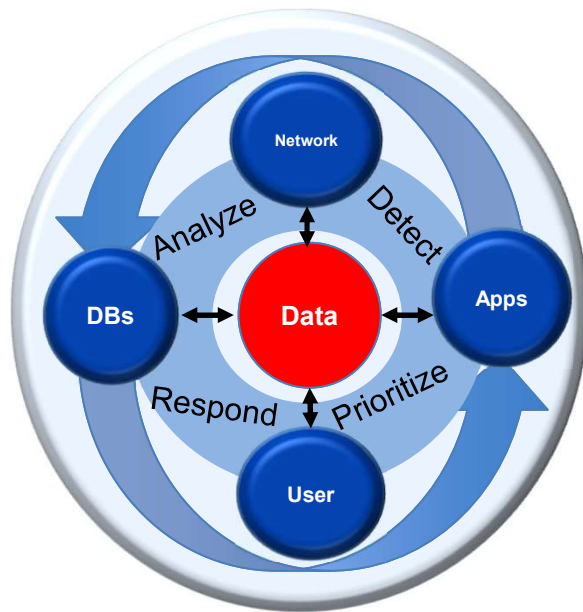
Polices Table:

Name	Description	Last Modified
Credit Card - American Express	Credit Card - American Express	2019/12/19 10:40:00
Personal ID - China ID Card	Personal ID - China ID Card	2019/12/19 10:40:00
Credit Card - Other Card	Credit Card - Other Card	2019/12/19 10:40:00
Personal ID - Hong Kong ID Card	Personal ID - Hong Kong ID Card	2019/12/19 10:40:00
Personal ID - Korea ID Card	Personal ID - Korea ID Card	2019/12/19 10:40:00
Personal ID - Singapore ID Card	Personal ID - Singapore ID Card	2019/12/19 10:40:00
Personal ID - Taiwan ID Card	Personal ID - Taiwan ID Card	2019/12/19 10:40:00
US Phone Number	US Phone Number	2019/12/19 10:40:00
Personal ID - US Social Security Number	Personal ID - US Social Security Number	2019/12/19 10:40:00
Credit Card - Visa/Master/China UnionPay JCB	Credit Card - Visa/Master/China UnionPay JCB	2019/12/19 10:40:00

Built-in Signatures – Taiwan/HK/China ID, Visa/Master/Amex cards

Workflow: Built-in Signatures TWID & Credit Card → Auto Detect & Alert Sensitive Data → Search, Analyze & Report

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...)

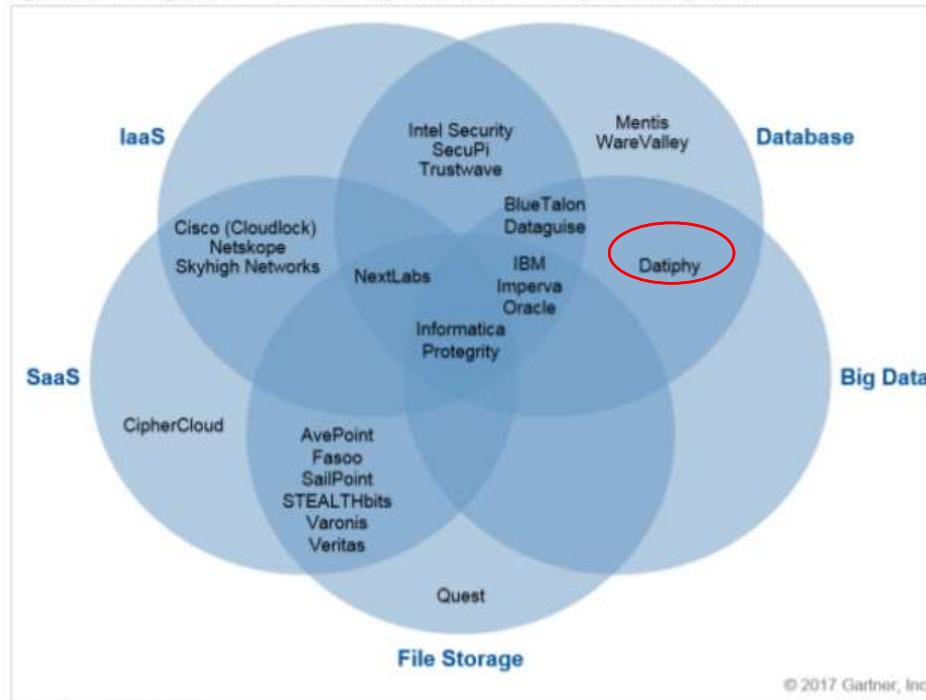
Gartner lists Datiphy as UEBA Representative Vendor

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



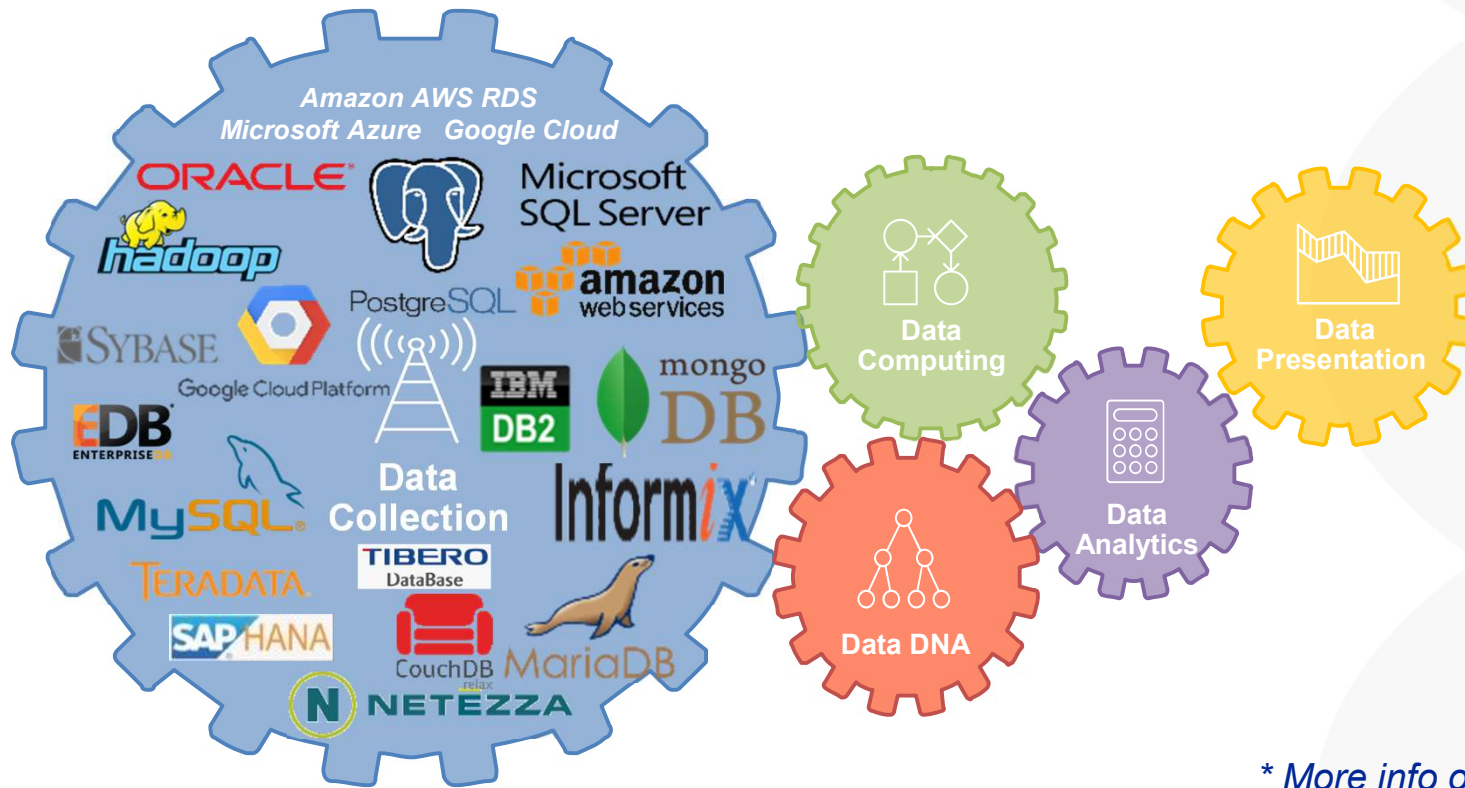
Source: Gartner (March 2017)

Adaptive Response Action Framework- Timely respond to threats



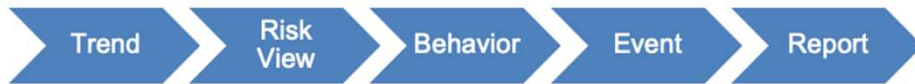
Datiphy partners with AWS and Splunk in the Adaptive Response Action Framework using patented machine learning technology to provide data-centric UEBA solutions for enterprise customers.

Datiphy Smart Data UEBA Process



* More info on www.datiphy.com

Dashboard – Showing Risk and Behaviors



Behavior (Client Program : db2bp(10.10.5.125))

Risk Score	Event%	Policy	Server	DB User	Database	Commands	Client Program
80	8	Insider Threats-Offhours	10.10.5.125	db2inst1	sample	INSERT	db2bp
78	2.67	Insider Threats-Offhours	10.10.5.125	db2inst1	sample	UPDATE	db2bp
53	8	Update Sensitive Data	10.10.5.125	db2inst1	sample	INSERT	db2bp
52	2.67	Update Sensitive Data	10.10.5.125	db2inst1	sample	UPDATE	db2bp
46	1.33	Data Access Risk	10.10.5.125	db2inst1	sample	INSERT	db2bp
46	1.33	Data Access Risk	10.10.5.125	db2inst1	sample	SELECT	db2bp
46	1.33	Security Alerts	10.10.5.125	db2inst1	sample	SELECT	db2bp
46	1.33	Data Access Risk	10.10.5.125	db2inst1	sample	UPDATE	db2bp
46	1.33	Security Alerts	10.10.5.125	db2inst1	sample	INSERT	db2bp

Event (Client Program : db2bp(10.10.5.125))

Date/Time	Server	Client	DB User	Commands ...	Query Time...	Tables	Return	Statement	Client Progra...	DB Pat.
2019-11-15 12:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	310	qa_crtb	0.1 row(s)	insert into QA_CRITB values('Scott','Visa','*****')	db2bp	sample
2019-11-15 12:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	311	qa_crtb	0.1 row(s)	insert into QA_CRITB values('Jacob','Master','**')	db2bp	sample
2019-11-15 12:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	307	qa_crtb	0.1 row(s)	insert into QA_CRITB values('John','Master','**')	db2bp	sample
2019-11-15 12:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	309	qa_twitb	0.1 row(s)	insert into QA_TWITB values('Henry','5, 21, F1**')	db2bp	sample
2019-11-15 12:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	312	qa_twitb	0.1 row(s)	insert into QA_TWITB values('Lida','7, 20, 12**')	db2bp	sample
2019-11-15 14:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	310	qa_crtb	0.1 row(s)	insert into QA_CRITB values('Candice','Master','**')	db2bp	sample
2019-11-15 14:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	304	qa_crtb	0.1 row(s)	insert into QA_CRITB values('Scott','Visa','*****')	db2bp	sample
2019-11-15 14:38:01	10.10.5.125	10.10.3.24	db2inst1	INSERT	311	qa_crtb	0.1 row(s)	insert into QA_CRITB values('Jacob','Master','**')	db2bp	sample

Drill down to Events details

datiphy Events Threats Current Risk **59%** Ask admin

Dashboard | Events | Policies | Reports | Assets | Settings | Search

Duration: 2019-11-15 11:00 am -- 7:00 pm

Behavior / Filter on Types Commands, Database, Policy - Apply Clear

(OR relationship among multiple selected values of each filter type)

Commands: UPDATE - Database: --Any-- Policy: Update Sensitive Data -

Filter → **Behavior** → **Event**

Risk Score	Count	Event%	Policy	Server	DB User	App User	Database	Client Program	Commands	Client User	Client Host
53	45	81.82	Update Sensitive Data	10.10.3.101	root		chaletdb		UPDATE		
52	8	14.55	Update Sensitive Data	10.10.5.125	db2inst1		sample	db2bp	UPDATE		105db2
46	2	3.64	Update Sensitive Data	172.16.1.212	user		db		UPDATE		

1 - 3 of 3 items

Event Table (Total: 8) Export Current Page

Conditions: 10.10.5.125 105db2 sample db2inst1 UPDATE Update Sensitive Data sample db2bp

Date/Time	Timestamp	Server	Client	Query Time(us)	DB User	Commands	Tables	Return	Statement	Policy	Content	Access
2019-11-15 12:38:01	1573850281.370533	10.10.5.125	10.10.3.24	304	db2inst1	UPDATE	qa_crtb	0: 1 row(s)	update QA_CRTB set CARDTYPE='Visa' where ...	Data Change Events,Insider T...	Content Rule Name:VisaMast...	Data Operations,Internal Net
2019-11-15 12:38:01	1573850281.477208	10.10.5.125	10.10.3.24	308	db2inst1	UPDATE	qa_twrb	0: 1 row(s)	update QA_TWTRB set GROUP=4 where NAME...	Data Change Events,Insider T...	Content Rule Name:TWD,Sin...	Data Operations,Internal Net
2019-11-15 14:38:01	1573857481.417487	10.10.5.125	10.10.3.24	319	db2inst1	UPDATE	qa_crtb	0: 1 row(s)	update QA_CRTB set CARDTYPE='Visa' where ...	Data Change Events,Insider T...	Content Rule Name:VisaMast...	Data Operations,Internal Net
2019-11-15 14:38:01	1573857481.524162	10.10.5.125	10.10.3.24	309	db2inst1	UPDATE	qa_twrb	0: 1 row(s)	update QA_TWTRB set GROUP=4 where NAME...	Data Change Events,Insider T...	Content Rule Name:TWD,Sin...	Data Operations,Internal Net
2019-11-15 16:38:02	1573864682.299628	10.10.5.125	10.10.3.24	314	db2inst1	UPDATE	qa_crtb	0: 1 row(s)	update QA_CRTB set CARDTYPE='Visa' where ...	Data Change Events,Insider T...	Content Rule Name:VisaMast...	Data Operations,Internal Net
2019-11-15 16:38:02	1573864682.406281	10.10.5.125	10.10.3.24	311	db2inst1	UPDATE	qa_twrb	0: 1 row(s)	update QA_TWTRB set GROUP=4 where NAME...	Data Change Events,Insider T...	Content Rule Name:TWD,Sin...	Data Operations,Internal Net
2019-11-15 18:38:01	1573871881.650927	10.10.5.125	10.10.3.24	307	db2inst1	UPDATE	qa_crtb	0: 1 row(s)	update QA_CRTB set CARDTYPE='Visa' where ...	Data Change Events,Insider T...	Content Rule Name:VisaMast...	Data Operations,Internal Net
2019-11-15 18:38:01	1573871881.757591	10.10.5.125	10.10.3.24	310	db2inst1	UPDATE	qa_twrb	0: 1 row(s)	update QA_TWTRB set GROUP=4 where NAME...	Data Change Events,Insider T...	Content Rule Name:TWD,Sin...	Data Operations,Internal Net

1 - 8 of 8 items

Dati Management Center 77.0 (31702) © 2019 Dati Inc. All Rights Reserved. EULA

Search and Analytics – Correlate Users and Data

The screenshot displays the Datiphy Search and Analytics interface. At the top, the search query is "Ask Datiphy" with a sub-query "pivot SERV=192* BRUL=Data*". A hierarchical diagram shows "Ask Datiphy" branching into "asset" and "policy", which further branch into "event", "pivot", "count", "threat", and "perf".

The first table, titled "(1) next 1 COUN (Total : 607, Duration : 2019-11-14 8:00 pm -- 2019-11-15 8:00 pm)", lists individual events with columns for Date/Time, Timestamp, Server, Client, DB User, Commands, Tables, Query Time, Return, Statement, and DB Path.

Date/Time	Timestamp	Server	Client	DB User	Commands	Tables	Query Time(us)	Return	Statement	DB Path
2019-11-14 21:00:02	1573794002.324950	192.10.2.208	192.10.2.208	user	INSERT	cardinfo	31	O: 1 row(s)	INSERT INTO cardinfo (id, name, cardNo, note)...	etest
2019-11-14 21:00:02	1573794002.325205	192.10.2.208	192.10.2.208	user	INSERT	cardinfo	30	O: 1 row(s)	INSERT INTO cardinfo (id, name, cardNo, note)...	etest
2019-11-14 21:00:02	1573794002.325326	192.10.2.208	192.10.2.208	user	DELETE	cardinfo	28	O: 2 row(s)	Delete FROM cardinfo where id=4;	etest
2019-11-14 21:00:02	1573794002.325410	192.10.2.208	192.10.2.208	user	INSERT	cardinfo	52	O: 1 row(s)	INSERT INTO cardinfo (id, name, cardNo, note)...	etest
2019-11-14 21:00:04	1573794002.325541	192.10.2.208	192.10.2.208	user	INSERT	cardinfo	29	O: 1 row(s)	INSERT INTO cardinfo (id, name, cardNo, note)...	etest
2019-11-14 21:00:02	1573794002.334480	192.10.2.208	192.10.2.208	user	INSERT	cardinfo	30	E: MSSQL248-161-...	INSERT INTO cardinfo (id, name, cardNo, note)...	etest
2019-11-14 21:00:02	1573794002.334539	192.10.2.208	192.10.2.208	user	INSERT	cardinfo	31	O: 1 row(s)	INSERT INTO cardinfo (id, name, cardNo, note)...	etest
2019-11-14 21:00:02	1573794002.406368	192.10.2.208	192.10.2.208	user	CREATE TABLE	tmp_sp_get_sqlagent_prope...	3038	O: 1 row(s)	create table #tmp_sp_get_sqlagent_propert...	master
2019-11-16 21:00:16	1573794016.364214	192.10.2.208	192.10.2.208	user	CREATE TABLE	cardinfo	206	O: 0 row(s)	CREATE TABLE cardinfo (id int name VARCHAR	master

The second table, titled "(2) pivot SERV=192* BRUL=Data* (Total : 9, Duration : 2019-11-14 8:00 pm -- 2019-11-15 8:00 pm)", is a pivot table showing counts and event percentages for different servers and policies.

Count	Event%	Server	Policy
607	10.96	192.10.2.208	Data Change Events
3109	56.12	192.168.136.128	Data Change Events
120	2.17	192.10.2.208	Data Exfiltration
730	13.18	192.10.2.208	Sensitive Data Events
175	3.16	192.168.5.136	Update Sensitive Data
380	6.86	192.10.2.208	Update Sensitive Data
69	1.25	192.10.2.208	Data Access Risk
35	0.63	192.168.5.136	Sensitive Data Events
115	2.10	192.168.5.136	Data Change Events

Policies and rules

The screenshot displays the datiPHY interface with the 'Policies' tab selected. The top navigation bar shows 'Threats Current Risk 0%' and user 'admin'. The left sidebar contains navigation options: Dashboard, Events, Policies, Reports, Assets, Settings, and Search.

The main content area shows a list of policies with columns for Type, Description, and Last Modified. A dropdown menu is open for the 'Type' column, showing options: Access, Content, and Action.

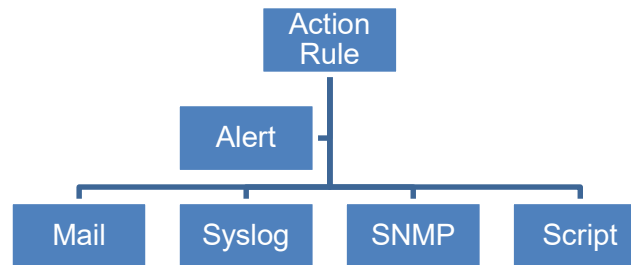
Type	Description	Last Modified
Access	Change user account, privileges and roles	2019/11/13 01:48:56
Content	Define, change, access data records	2019/11/13 01:48:56
Action	External networks - Non-private IP addresses	2019/11/13 01:48:56
Data operators	Internet networks - private IP addresses	2019/11/13 01:48:56
External Net	Access a large volume of records	2019/11/13 01:48:56
Internal Net	Access a huge volume of records	2019/11/13 01:48:56
Large Records	Access a very large volume of records	2019/11/13 01:48:56
Large Records-High	Large Subsequent Response time by this SQL	2019/11/13 01:48:56
Large Records-Medium	DB users failed to login	2019/11/13 01:48:56
Locked Table	Large Total Response Time by this SQL	2019/11/13 01:48:56
Login Failed	Off Hour activities at TZ1 Timezone	2019/11/13 01:48:56
Long Query	Off Hour activities at TZ2 Timezone	2019/11/13 01:48:56
Off Hour Access (TZ1)	Privileged User Activities	2019/11/13 01:48:56
Off Hour Access (TZ2)	SQL DCL & Privileged commands - revoke, grant	2019/11/13 01:48:56
Privileged Users		
SQL DCL		

Below the policy list is a table of risk items:

Name	Status	Category	Risk	Last Modified
Data Access Risk	Enabled	Vulnerability	Medium	2019/11/13 01:48:55
Data Change Events	Disabled	Access Anomaly	High	2019/11/13 01:48:55
Data Control Risk	Enabled	Threat	High	2019/11/13 01:48:55
Data Define Risk	Enabled	Threat	High	2019/11/13 01:48:55
Data Exfiltration	Enabled	Threat	High	2019/11/13 01:48:55
Delete Sensitive Data	Enabled	Vulnerability	Low	2019/11/13 01:48:55
High Risk Profiles	Disabled	Threat	High	2019/11/13 01:48:55
Insider Threats-Offhours	Enabled	Threat	High	2019/11/13 01:48:55
Insider Threats-Workhours	Enabled	Vulnerability	Low	2019/11/13 01:48:55
New Behaviors	Enabled		Minor	2019/11/13 01:48:55
New Entities	Enabled	Access Anomaly	Very Low	2019/11/13 01:48:55
Outsider Threats	Enabled	Threat	High	2019/11/13 01:48:55
Performance Risk	Enabled	Access Anomaly	Very Low	2019/11/13 01:48:55
Privileged Commands	Enabled	Vulnerability	Very Low	2019/11/13 01:48:55

The diagram on the right shows a hierarchy: 'Policy' is the root, which branches into 'Action Rule', 'Content Rule', and 'Global Parameter'. 'Action Rule' further branches into 'Access Rule'.

Alerts and Actions



datiphy™ Policies ⚖️ Policies Rules Parameter Threats Current Risk **0%** 🔍 Ask 🔔 👤 admin

Type: Action 📄 New ⚙️ Deploy

Name	Description	Last Modified
MailDefault	Default Mail Action	2019/11/13 01:48:56
Mail_AlertNotification	Send Alert Notification by Mail	2019/11/13 01:48:56
Mail_ReportNotification	Send Report Notification by Mail	2019/11/13 01:48:56
SyslogCEF	Default Syslog CEF for HP ArcSight	2019/11/13 01:48:56
SyslogLEEF	Default Syslog LEEF for IBM QRadar	2019/11/13 01:48:56

Reports for Auditing & Compliance

The screenshot displays the Datiphy Reports management interface. At the top, there are tabs for 'Summary' and 'Template & Schedule'. The main area is divided into three sections:

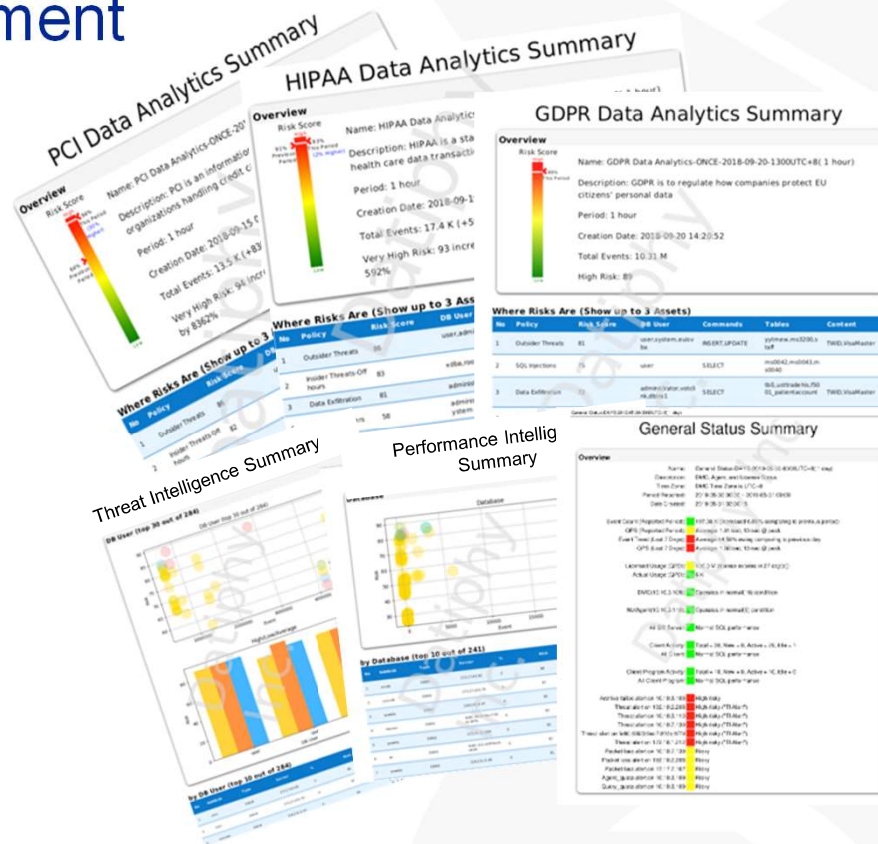
- Template List:** A table listing various report templates with columns for Template Name, Description, Content, Status, and Schedule. A red box highlights the 'General Status' and 'Intelligent Threat-Risk' templates.
- General Status Summary Preview:** A detailed report card for the 'General Status' template, showing an overview of system health, compliance metrics, and risk levels with color-coded indicators.
- Report List:** A table showing a list of generated reports, including columns for Period, Template Name, Frequency, and Created On. A red box highlights the 'General Status' report in this list.

Navigation arrows at the bottom left indicate the workflow: Report Template → Manual/Schedule → Report Summary.

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