



# 数据驱动安全思考

董晓琼

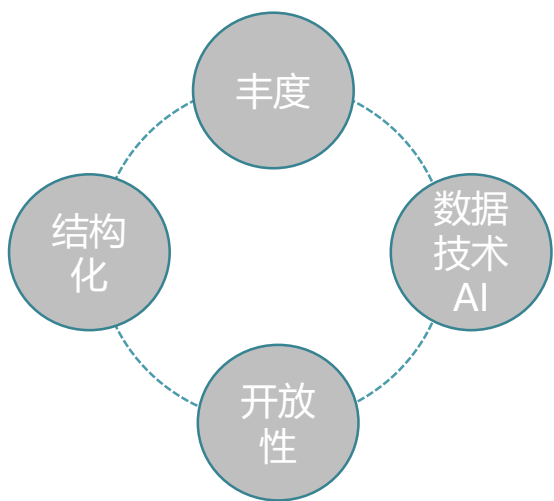


数据优势及行业转变  
数据驱动安全  
安全场景与应用  
数据的闭环与价值



# 数据优势及行业转变

数据的显著优势、丰富的业务场景、及基于数据技术的跨越式发展：重塑传统行业格局，跨越传统企业的技术壁垒。



业务模式的创新  
带动了传统企业-跨越至工业3.0  
AI-传统行业格局的重塑  
- 汽车、金融、医疗健康



# 数据驱动安全是什么？

## 数据驱动安全 非 “情报驱动安全”

定义：在不断变化的组织环境中，为有效地识别和管理动态风险，在组织内部使用的一种方法；



# 安全场景与应用

## UEBA-终端管控场景

**诉求：**员工在-业务系统访问过程中的“异常行为”判断；

**问题：**监控范围大、员工行为关注的业务点和行为差异显著、专家规则极易失效

“变化”中的  
风险识别

### 原始字段

 访问时间

 IP

 url

 流量

### 数据处理



#### 基本统计信息

访问量  
URL数量  
IP数量  
流量相关统计  
访问时间间隔统计



#### IP统计信息

常用IP-C段  
常用IP数量  
全部IP-C段数量  
全部IP数量  
...



#### 功能节点统计信息

用户  
时段  
url  
访问量



#### 行为轨迹

员工-URL 访问  
轨迹



#### 用户历史行为

用户访问分布情况  
(均值、方差、偏  
度、峰度、分位  
数...)



#### 群组历史行为

用户所属群组访问  
分布情况 (均值、  
方差、偏度、峰度、  
分位数...)



#### 功能节点特征

url 访问 top 10  
敏感url  
业务逻辑特征



特征



	主成分1	主成分2	主成分3	主成分4	主成分5	主成分6	主成分7
count	-0.31	0.00	0.15	-0.04	0.12	-0.07	0.05
count_url	-0.26	-0.23	-0.15	0.00	-0.08	0.06	-0.04
count_ip	-0.11	-0.06	-0.04	-0.09	0.19	0.24	-0.04
bytes_cv	-0.14	-0.23	-0.38	-0.18	-0.22	-0.11	-0.05
bytes_kewness	-0.19	-0.26	-0.20	-0.20	-0.20	-0.21	-0.07
bytes_kurtosis	-0.16	-0.19	-0.06	-0.20	-0.11	-0.37	0.29
diff_time_cv	-0.10	-0.16	-0.19	-0.14	-0.01	0.02	-0.28
log_bytes	-0.25	-0.18	-0.05	-0.05	0.04	-0.04	-0.22
urlTop1	-0.21	-0.15	0.19	0.21	-0.09	0.24	0.05
urlTop2	-0.26	0.17	0.08	0.08	-0.17	0.06	-0.03
urlTop3	-0.20	-0.01	-0.17	-0.03	0.01	0.03	0.02
urlTop4	-0.20	-0.16	0.20	0.20	-0.09	0.24	0.03
urlTop5	-0.25	0.21	0.00	0.16	0.14	-0.21	-0.08
urlTop6	-0.26	0.20	0.00	0.20	0.17	-0.23	-0.10
urlTop7	-0.08	-0.21	0.47	-0.30	0.14	-0.03	-0.04
urlTop8	-0.13	0.00	-0.25	-0.14	0.43	0.32	0.19
urlTop9	-0.15	-0.02	-0.25	-0.12	0.40	0.34	0.17
urlTop10	-0.22	0.22	0.05	-0.12	-0.23	0.16	-0.05
url3	-0.19	-0.13	0.09	0.27	-0.18	0.14	0.28
url5	-0.15	-0.09	0.17	-0.04	0.12	0.00	-0.23
url2	-0.26	0.20	0.00	0.20	0.17	-0.23	-0.10
url4	-0.08	-0.21	0.47	-0.30	0.14	-0.03	-0.04
url6	-0.11	0.32	0.05	-0.30	-0.21	0.15	0.10
url7	-0.11	0.32	0.05	-0.28	-0.21	0.18	0.04
url1	-0.21	0.33	-0.01	-0.06	0.07	-0.15	-0.04
user_deviate	-0.01	0.00	0.02	-0.03	0.03	-0.14	0.30
group_deviate	-0.06	0.05	0.02	-0.14	0.12	-0.29	0.55
BL1	-0.09	0.17	-0.03	-0.22	-0.28	0.11	-0.06
BL2	-0.16	-0.09	-0.04	0.24	-0.07	-0.03	-0.07
BL3	-0.11	-0.13	0.02	0.23	-0.22	0.13	0.35

- 取方差贡献度大于1，提取特征主成分。

主成分1	主成分2	主成分3	主成分4	主成分5	主成分6	主成分7
8.07	3.02	2.20	1.74	1.62	1.41	1.00

- 第一主成分：主要与访问量，url数量，流量，url top1-6及个别敏感url相关。可代表常用功能节点访问行为情况。
- 第二主成分主要与敏感url1、url6、url7相关，可代表敏感功能节点访问行为情况。
- 第三主成分主要与流量cv，url top7、敏感url4相关，可代表流量离散度情况。
- 第四主成分，主要与url4-6、BL1、BL2、BL3相关，可代表用户敏感节点业务逻辑情况。

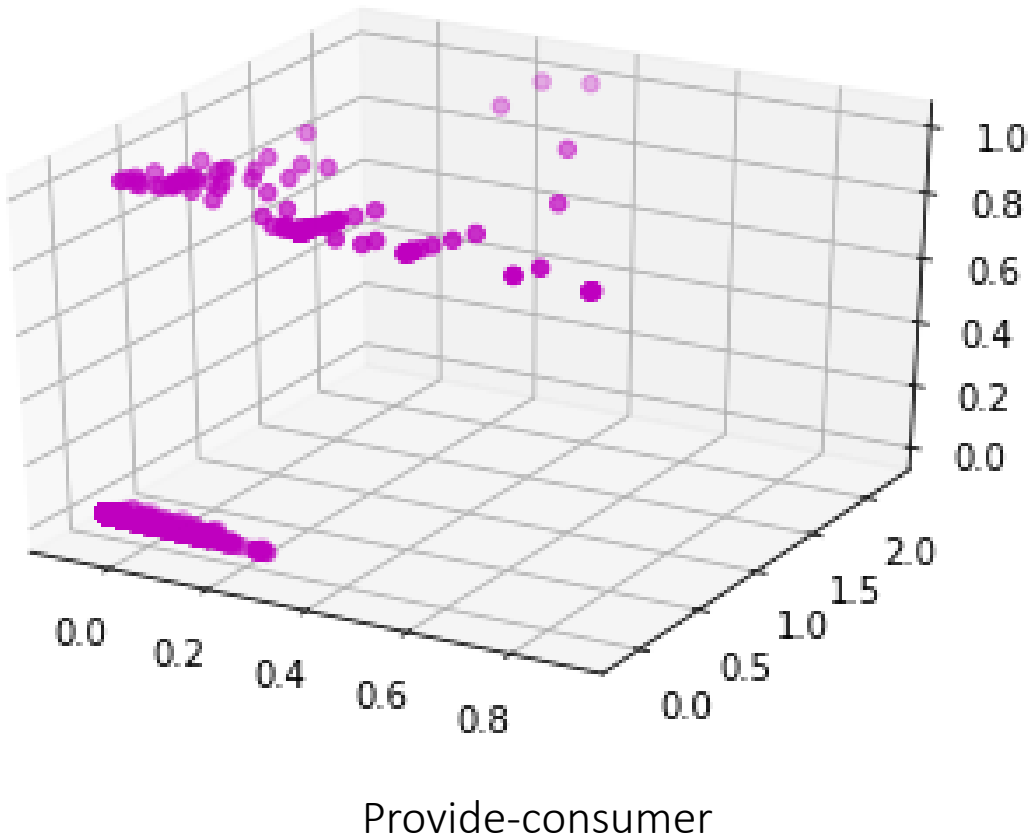
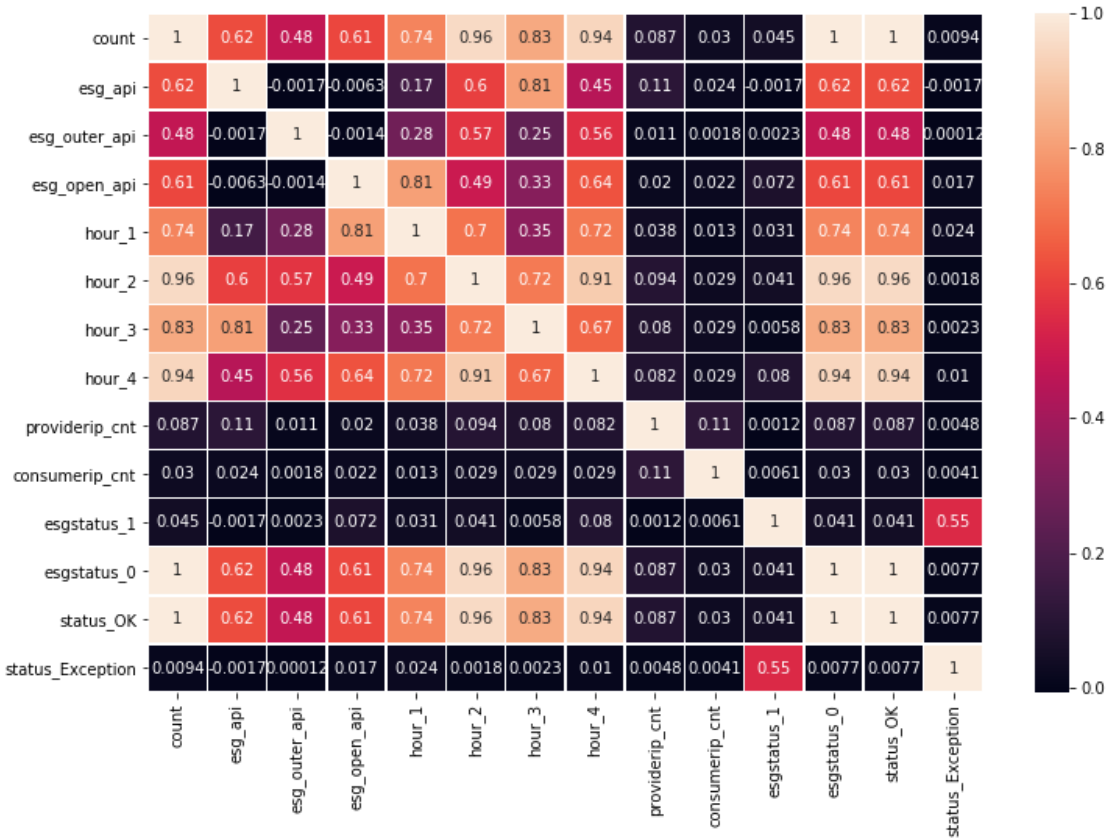
## 特征成分提取

url访问数量异常	user_123456789101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899100								user_123456789101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899100								user_123456789101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899100								user_123456789101112131415161718192021222324252627282930313233343536373839404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899100																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
访问量偏离该用户历史行为	PENG	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31	C32	C33	C34	C35	C36	C37	C38	C39	C40	C41	C42	C43	C44	C45	C46	C47	C48	C49	C50	C51	C52	C53	C54	C55	C56	C57	C58	C59	C60	C61	C62	C63	C64	C65	C66	C67	C68	C69	C70	C71	C72	C73	C74	C75	C76	C77	C78	C79	C80	C81	C82	C83	C84	C85	C86	C87	C88	C89	C90	C91	C92	C93	C94	C95	C96	C97	C98	C99	C100	C101	C102	C103	C104	C105	C106	C107	C108	C109	C110	C111	C112	C113	C114	C115	C116	C117	C118	C119	C120	C121	C122	C123	C124	C125	C126	C127	C128	C129	C130	C131	C132	C133	C134	C135	C136	C137	C138	C139	C140	C141	C142	C143	C144	C145	C146	C147	C148	C149	C150	C151	C152	C153	C154	C155	C156	C157	C158	C159	C160	C161	C162	C163	C164	C165	C166	C167	C168	C169	C170	C171	C172	C173	C174	C175	C176	C177	C178	C179	C180	C181	C182	C183	C184	C185	C186	C187	C188	C189	C190	C191	C192	C193	C194	C195	C196	C197	C198	C199	C200	C201	C202	C203	C204	C205	C206	C207	C208	C209	C210	C211	C212	C213	C214	C215	C216	C217	C218	C219	C220	C221	C222	C223	C224	C225	C226	C227	C228	C229	C230	C231	C232	C233	C234	C235	C236	C237	C238	C239	C240	C241	C242	C243	C244	C245	C246	C247	C248	C249	C250	C251	C252	C253	C254	C255	C256	C257	C258	C259	C260	C261	C262	C263	C264	C265	C266	C267	C268	C269	C270	C271	C272	C273	C274	C275	C276	C277	C278	C279	C280	C281	C282	C283	C284	C285	C286	C287	C288	C289	C290	C291	C292	C293	C294	C295	C296	C297	C298	C299	C300	C301	C302	C303	C304	C305	C306	C307	C308	C309	C310	C311	C312	C313	C314	C315	C316	C317	C318	C319	C320	C321	C322	C323	C324	C325	C326	C327	C328	C329	C330	C331	C332	C333	C334	C335	C336	C337	C338	C339	C340	C341	C342	C343	C344	C345	C346	C347	C348	C349	C350	C351	C352	C353	C354	C355	C356	C357	C358	C359	C360	C361	C362	C363	C364	C365	C366	C367	C368	C369	C370	C371	C372	C373	C374	C375	C376	C377	C378	C379	C380	C381	C382	C383	C384	C385	C386	C387	C388	C389	C390	C391	C392	C393	C394	C395	C396	C397	C398	C399	C400	C401	C402	C403	C404	C405	C406	C407	C408	C409	C410	C411	C412	C413	C414	C415	C416	C417	C418	C419	C420	C421	C422	C423	C424	C425	C426	C427	C428	C429	C430	C431	C432	C433	C434	C435	C436	C437	C438	C439	C440	C441	C442	C443	C444	C445	C446	C447	C448	C449	C450	C451	C452	C453	C454	C455	C456	C457	C458	C459	C460	C461	C462	C463	C464	C465	C466	C467	C468	C469	C470	C471	C472	C473	C474	C475	C476	C477	C478	C479	C480	C481	C482	C483	C484	C485	C486	C487	C488	C489	C490	C491	C492	C493	C494	C495	C496	C497	C498	C499	C500	C501	C502	C503	C504	C505	C506	C507	C508	C509	C510	C511	C512	C513	C514	C515	C516	C517	C518	C519	C520	C521	C522	C523	C524	C525	C526	C527	C528	C529	C530	C531	C532	C533	C534	C535	C536	C537	C538	C539	C540	C541	C542	C543	C544	C545	C546	C547	C548	C549	C550	C551	C552	C553	C554	C555	C556	C557	C558	C559	C560	C561	C562	C563	C564	C565	C566	C567	C568	C569	C570	C571	C572	C573	C574	C575	C576	C577	C578	C579	C580	C581	C582	C583	C584	C585	C586	C587	C588	C589	C590	C591	C592	C593	C594	C595	C596	C597	C598	C599	C600	C601	C602	C603	C604	C605	C606	C607	C608	C609	C610	C611	C612	C613	C614	C615	C616	C617	C618	C619	C620	C621	C622	C623	C624	C625	C626	C627	C628	C629	C630	C631	C632	C633	C634	C635	C636	C637	C638	C639	C640	C641	C642	C643	C644	C645	C646	C647	C648	C649	C650	C651	C652	C653	C654	C655	C656	C657	C658	C659	C660	C661	C662	C663	C664	C665	C666	C667	C668	C669	C670	C671	C672	C673	C674	C675	C676	C677	C678	C679	C680	C681	C682	C683	C684	C685	C686	C687	C688	C689	C690	C691	C692	C693	C694	C695	C696	C697	C698	C699	C700	C701	C702	C703	C704	C705	C706	C707	C708	C709	C710	C711	C712	C713	C714	C715	C716	C717	C718	C719	C720	C721	C722	C723	C724	C725	C726	C727	C728	C729	C730	C731	C732	C733	C734	C735	C736	C737	C738	C739	C740	C741	C742	C743	C744	C745	C746	C747	C748	C749	C750	C751	C752	C753	C754	C755	C756	C757	C758	C759	C760	C761	C762	C763	C764	C765	C766	C767	C768	C769	C770	C771	C772	C773	C774	C775	C776	C777	C778	C779	C780	C781	C782	C783	C784	C785	C786	C787	C788	C789	C790	C791	C792	C793	C794	C795	C796	C797	C798	C799	C800	C801	C802	C803	C804	C805	C806	C807	C808	C809	C810	C811	C812	C813	C814	C815	C816	C817	C818	C819	C820	C821	C822	C823	C824	C825	C826	C827	C828	C829	C830	C831	C832	C833	C834	C835	C836	C837	C838	C839	C840	C841	C842	C843	C844	C845	C846	C847	C848	C849	C850	C851	C852	C853	C854	C855	C856	C857	C858	C859	C860	C861	C862	C863	C864	C865	C866	C867	C868	C869	C870	C871	C872	C873	C874	C875	C876	C877	C878	C879	C880	C881	C882	C883	C884	C885	C886	C887	C888	C889	C890	C891	C892	C893	C894	C895	C896	C897	C898	C899	C900	C901	C902	C903	C904	C905	C906	C907	C908	C909	C910	C911	C912	C913	C914	C915	C916	C917	C918	C919	C920	C921	C922	C923	C924	C925	C926	C927	C928	C929	C930	C931	C932	C933	C934	C935	C936	C937	C938	C939	C940	C941	C942	C943	C944	C945	C946	C947	C948	C949	C950	C951	C952	C953	C954	C955	C956	C957	C958	C959	C960	C961	C962	C963	C964	C965	C966	C967	C968	C969	C970	C971	C972	C973	C974	C975	C976	C977	C978	C979	C980	C981	C982	C983	C984	C985	C986	C987	C988	C989	C990	C991	C992	C993	C994	C995	C996	C997	C998	C999	C1000	C1001	C1002	C1003	C1004	C1005	C1006	C1007	C1008	C1009	C1010	C1011	C1012	C1013	C1014	C1015	C1016	C1017	C1018	C1019	C1020	C1021	C1022	C1023	C1024	C1025	C1026	C1027	C1028	C1029	C1030	C1031	C1032	C1033	C1034	C1035	C1036	C1037	C1038	C1039	C1040	C1041	C1042	C1043	C1044	C1045	C1046	C1047	C1048	C1049	C1050	C1051	C1052	C1053	C1054	C1055	C1056	C1057	C1058	C1059	C1060	C1061	C1062	C1063	C1064	C1065	C1066	C1067	C1068	C1069	C1070	C1071	C1072	C1073	C1074	C1075	C1076	C1077	C1078	C1079	C1080	C1081	C1082	C1083	C1084	C1085	C1086	C1087	C1088	C1089	C1090	C1091	C1092	C1093	C1094	C1095	C1096	C1097	C1098	C1099	C1100	C1101	C1102	C1103	C1104	C1105	C1106	C1107	C1108	C1109	C1110	C1111	C1112	C1113	C1114	C1115	C1116	C1117	C1118	C1119	C1120	C1121	C1122	C1123	C1124	C1125	C1126	C1127	C1128	C1129	C1130	C1131	C1132	C1133	C1134	C1135	C1136	C1137	C1138	C1139	C1140	C1141	C1142	C1143	C1144	C1145	C1146	C1147	C1148	C1149	C1150	C1151	C1152	C1153	C1154	C1155	C1156	C1157	C1158	C1159	C1160	C1161	C1162	C1163	C1164	C1165	C1166	C1167	C1168	C1169	C1170	C1171	C1172	C1173	C1174	C1175	C1176	C1177	C1178	C1179	C1180	C1181	C1182	C1183	C1184	C1185	C1186	C1187	C1188	C1189	C1190	C1191	C1192	C1193	C1194	C1195	C1196	C1197	C1198	C1199	C1200	C1201	C1202	C1203	C1204	C1205	C1206	C1207	C1208	C1209	C1210	C1211	C1212	C1213	C1214	C1215	C1216	C1217	C1218	C1219	C1220	C1221	C1222	C1223	C1224	C1225	C1226	C1227	C1228	C1229	C1230	C1231	C1232	C1233	C1234	C1235	C1236	C1237	C1238	C1239	C1240	C1241	C1242	C1243	C1244	C1245	C1246	C1247	C1248	C1249	C1250	C1251	C1252	C1253	C1254	C1255	C1256	C1257	C1258	C1259	C1260	C1261	C1262	C1263	C1264	C1265	C1266	C1267	C1268	C1269	C1270	C1271	C1272	C1273	C1274	C1275	C1276	C1277	C1278	C1279	C1280	C1281	C1282	C1283	C1284	C1285	C1286	C1287	C1288	C1289	C1290	C1291	C1292	C1293	C1294	C1295	C1296	C1297	C1298	C1299	C1300	C1301	C1302	C1303	C1304	C1305	C1306	C1307	C1308	C1309	C1310	C1311	C1312	C1313	C1314	C1315	C1316	C1317	C1318	C1319	C1320	C1321	C1322	C1323	C1324	C1325	C1326	C1327	C1328	C1329	C1330	C1331	C1332	C1333	C1334	C1335	C1336	C1337	C1338	C1339	C1340	C1341	C1342	C1343	C1344	C1345	C1346	C1347	C1348	C1349	C1350	C1351	C1352	C1353	C1354	C1355	C1356	C1357	C1358	C1359	C1360	C1361	C1362	C1363	C1364	C1365	C1366	C1367	C1368	C1369	C1370	C1371	C1372	C1373	C1374	C1375	C1376	C1377	C1378	C1379	C1380	C1381	C1382	C1383	C1384	C1385	C1386	C1387	C1388	C1389	C1390	C1391	C1392	C1393	C1394	C1395	C1396	C1397	C1398	C1399	C1400	C1401	C1402	C1403	C1404	C1405	C14

# API接口安全监控场景

诉求：应用系统接口-关注是否存在接口异常调用

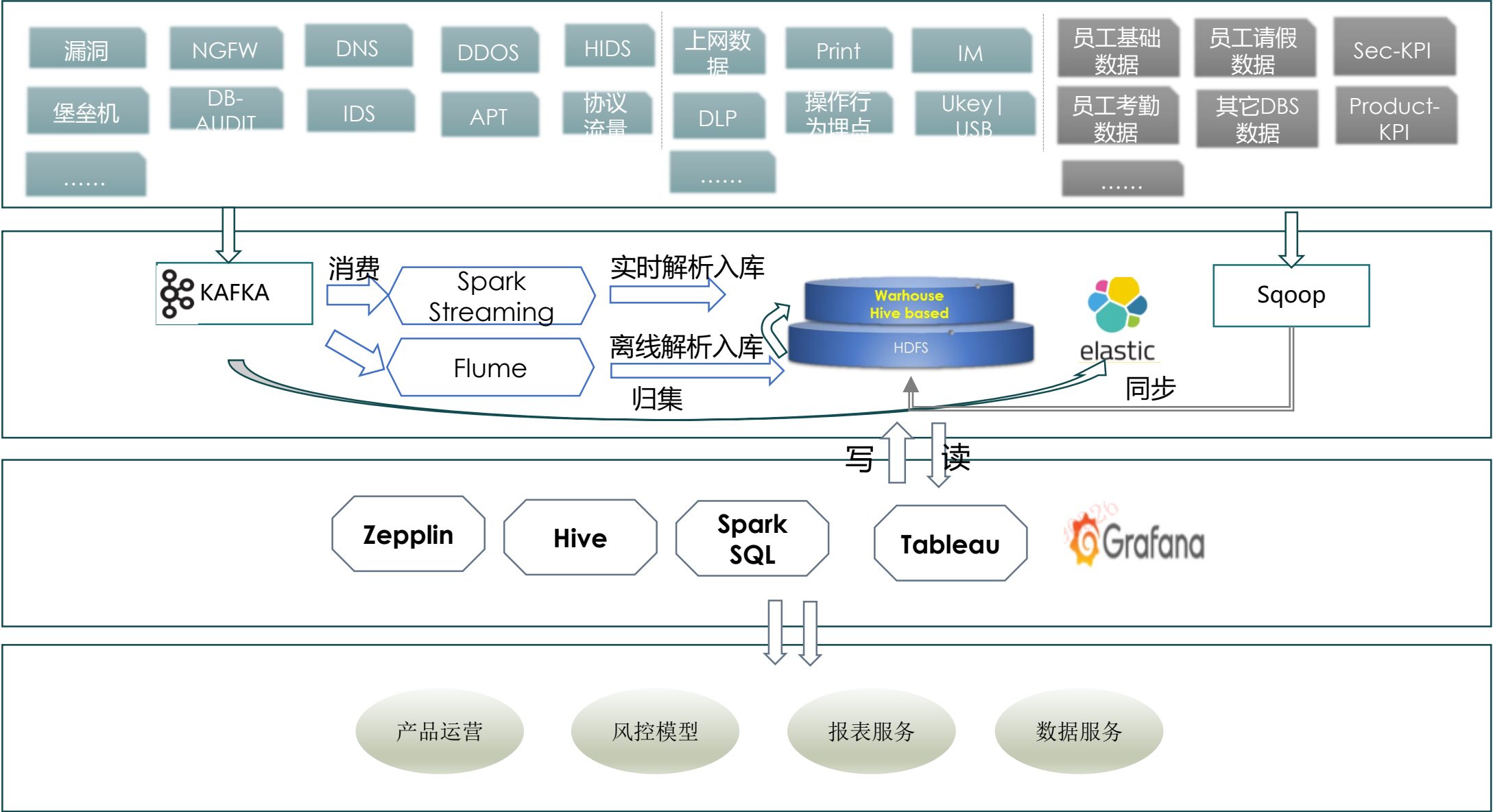
问题：请求量巨大，多基于统计性变量参数，业务模式较为单一，场景相对稳定，寻找一种更为高效、准确的异常预警；







# 数据分析平台





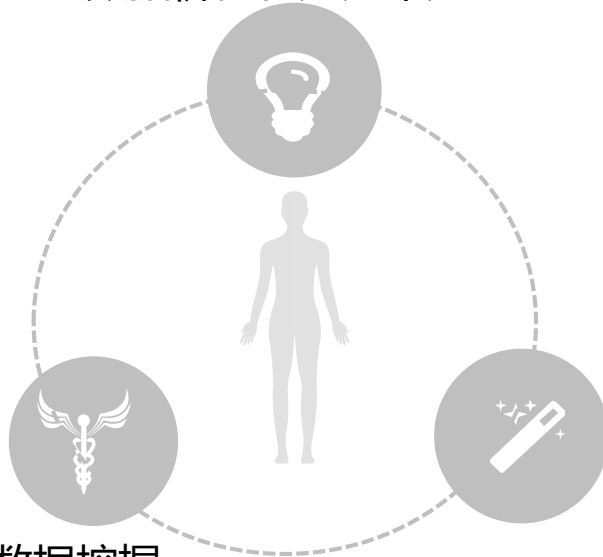
# 有价值的数据闭环与输出

## 数据成本与流动

数据建设的计划投入

聚焦“关注”

数据价值在应用中产生



## 数据与价值闭环管理

数据质量与可用

完整的数据闭环，能让数据挖掘、  
数据分析产生价值；

## 数据价值的输出

结合业务提供有价值数据  
基础数据的积累和循环



Thanks