SECNOLOGY

SECNOLOGY VS COMPETITORS

TURN DATA INTO ACTIONS

	ARCHITECTURE - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Architecture Bottleneck	No	Yes
2	Speed & Performance	High	Low
3	High Availability (Active-Passive)	Very Easy	Very Complex
4	High Availability (Active-Passive)	Yes	No
5	Multi Site High Availability	Yes	No
6	Cost of High Availability	No Cost	Additional Cost
7	Scalabilty	Unlimited	No
8	Flexibility	Yes	No
9	Supported Devices	All	Predefined List
10	Adherence to the SQL DB as well as to the O.S.	No	Yes
11	Simultaneous Concurrent Data Access	Yes	No
12	Additional Software Required	No	Yes for Backup
13	Software Data Corruption	No	Possible
14	Disk Space Overhead	20% of Originals	up to 900% originals
15	Dedicated Platforms required	No	Yes
16	Compatible with your Filer, NAS, or SAN	Yes	Depends on Brands
17	Choice of your Storage Device	Yes	No Choice
18	Choice of your Data Storage Location	Yes	No Choice
19	Full Features Virtualization Support	Yes	No
20	Support of Acceleration Protocols	Yes	No
21	Daily Data Volume Processing	No Limit	Limited
22	Global Data Volume Capacity	No Limit	Limited
23	Ability to Process History	Yes	No
24	Raw Log Retention	All Events	Only Matched Events
25	Data Retention Period	No Limit	Maximum 3 months
26	Data Accessibility Period	Unlimited	Limited
27	Product Installation	1 minute	Many Hours
28	Project Deployment	Few Days	Many Weeks
29	Autonomy regards other IT dept.(DBA)	Yes	No
30	Stealth Environment Integration	Yes	No
31	Continuous Handholding required	No	Yes

TURN DATA INTO ACTIONS

	EVENT COLLECTION - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Supported Collection via OPSEC Protocol	Yes	Some of Them
2	Supported Collection via NETFLOW Protocol	Yes	Some of Them
3	Supported Collection via SFLOW Protocol	Yes	Some of Them
3	Supported Collection via JFLOW Protocol	Yes	Some of Them
4	Supported Collection via POP3 Protocol	Yes	Some of Them
4	Supported Collection via UDP Protocol	Yes	Some of Them
5	Supported Collection via TCP Protocol	Yes	Some of Them
6	Supported Collection via CIDEE Protocol	Yes	Some of Them
7	Supported Collection via SNMP Protocol	Yes	Some of Them
8	Supported Collection via SYSLOG Protocol	Yes	Yes
9	Supported Collection via FTP Protocol	Yes	Some of Them
10	Supported Collection via ODBC Protocol	Yes	Some of Them
11	Supported Collection via SSL Protocol	Yes	Some of Them
12	Supported Collection via Remote Agents	Yes	Some of Them
13	Keep Raw Events	Yes	No
14	Keep Parsed Events	Yes	Yes
15	Real-Time Collection	Yes	Yes
16	On-Demand or Scheduled Collection	Yes	No
17	Links between Devices & Collectors	Direct or Indirect	Direct Mandatory
18	Windows & Linux Collectors	Yes	Some of Them
19	Windows & Linux Agents	Yes	Some of Them

	PARSING - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Graphical Parser	Yes	No
2	Development Toolkit required	No Need	Mandatory
3	Log Format Support	All	Predefined List
4	RegExp Parsing	No Need	Mandatory
5	Off-Line Parsing	Yes	No
6	Required Fields	Only Selected Fields	All Fields required
7	Log Normalization	Not Mandatory	Mandatory
8	Log Aggregation	Not Mandatory	Mandatory
9	Impact on Column Log Format Modification	Parser Modification	Database Modification
10	Impact on Field Log Format Modification	Parser Modification	Events Loss
11	Unstructured Data Format Support	Yes	No
12	Virtual Field Support	Yes	No
13	Data Masking	Yes	No
14	Event Categorization	Multiple	Only Once
15	Pattern Event Categorization	Yes	No

TURN DATA INTO ACTIONS

	DATA MANAGEMENT - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Parallel Reports Generation	Yes	No
2	Data Policy Segregation	Yes	No
3	Multiple Data Retention Periods	Yes	No
4	Simultaneous Concurrent Data Access	Yes	No
5	Real-Time Rule Processing	Yes	No
6	Regulatory Compliance	Unaltered raw Logs	Altered raw Logs
7	External Applications Support	Yes	No
8	Raw Log Integrity	Yes	No
9	Raw Data Encryption	Yes	No
10	Raw Data Compression	Yes	No
11	Raw Data Confidentialy	Yes	No
12	Raw Data Integrity	Yes	No
13	Raw Data Availability	Yes	No
14	Raw Data Accessibility	All Time	Limited Timeframe
15	Rule-Based Policy Log Segregation	Yes	No

	DATA PROCESSING - KEY DIFFERENTIATORS	SECNOLOGY	COMPETITORS
1	Available Fields for Correlation	All + Metafields	Only Few
2	Correlation between many Giga Logs File	Yes	No
3	Visual Correlation	Yes	No
4	MetaEvent Support	Yes	No
5	MetaGraph Support	Yes	No
6	Cold and Hot Data Processing	Cold & Hot	Only Hot
7	UnMatched Events Investigation	Yes	Impossible
8	Data Archive/Restore	No	Mandatory
9	Active/Restore Service Impact	None	Down Time
10	Archive & Restore Images Compability	Yes	Very Complex
11	Specific Backup/Recovery	No	Mandatory
12	Restore & Roll Back	Immediate	Very Complex
13	Dependencies with 3rd Party Applications	No	Yes
14	Event Log Synchronization	Yes	No
15	Event Data Mining	Yes	No

Corporate Headquarters
747 El Granada Boulevard Suite 2547
El Granada, CA 94018
(415) 762-1820
info@secnology.com

EMEA Office
22 rue Victor Hugo
78350 Jouy-En-Josas, France
+33 (0)1 4645-4610
emea@secnology.com