TIBCO LogLogic ST Appliances

BENEFITS

PROTECT IN REAL TIME
Set real-time alerts for events such as brute force password attacks, denial of service, account hijacking, and virus outbreak using baselines and trending and develop precise recommendations for threat removal by correlating internal and external patterns for known and unknown threats.

SPEED RESOLUTION
Resolve underlying security issues within seconds by tracking all user activity using advanced root-cause analysis and forensics workflow—or use the open API to integrate with other analytic solutions or with service-desk management systems.

INCREASE ROI
Deploy in hours, not weeks; avoid maintenance of complex rules; and practically eliminate false positives using an accurate security information and event manager with a unique taxonomy design.

SEE EVERYTHING
Track all user activity such as geography, rights and configuration changes, asset misuse, and proxy bypass using a browser-based security information management interface and out-of-the-box reports for access control, policy information, and network, database, IDS, email, Web, and legacy system activity.

SCALE AS NEEDED
Collect up to 250,000 events per second per appliance using a distributed architecture that scales across deployments and enables centralized data aggregation and search, and high-capacity storage for up to 10 years.

AT A GLANCE:
TIBCO LogLogic® ST storage appliances provide the fastest, most scalable IT data warehouse available, supplying an historical end-to-end view of your infrastructure for in-depth analysis of events past and present—and their root cause. ST appliances provide simply the best way of doing long-term forensics using IT data.

HIGH CAPACITY INTELLIGENCE
Storage is the single most significant addition you can make to your infrastructure to gain visibility and control and deliver improved security, greater compliance, and the information you need to plan and operate an optimized IT service.

LogLogic IT data warehouses—the ST line of appliances—eliminate waste by centralizing all IT data and auto-identifying the incoming stream whether from our Universal Collector or some other source. All data is then normalized and indexed, enabling you to benefit from lightning-fast searches and reports.

Open-forwarding technology means ST appliances can act as a warehouse for all vendors' analytic engines, adding scalability and resilience to a solution you may have already purchased. Front-ending your analytic solution with a LogLogic data warehouse lets you see everything that is happening within your infrastructure.
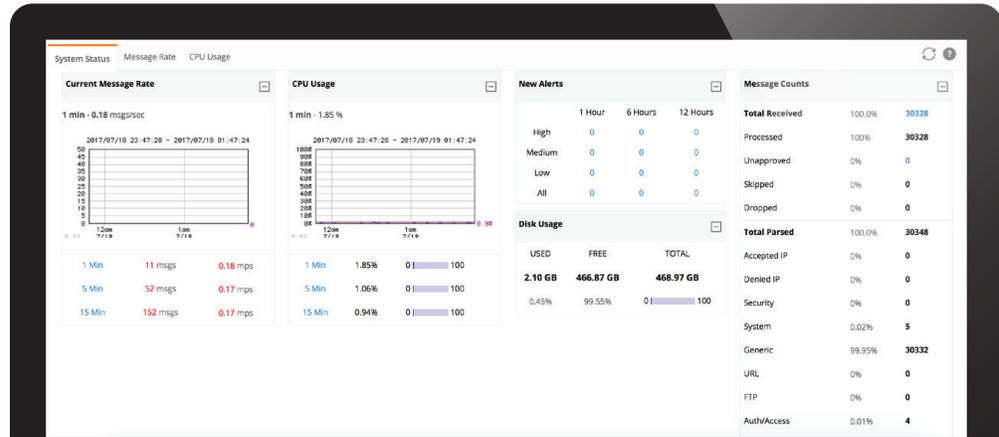
ATTRIBUTES & CAPABILITIES

BETTER, LONG-TERM FORENSICS
With all data available for analysis, you can see not only that someone successfully breached your security or that your data is currently out of compliance with PCI, but also answer a very key question: "What else happened?"

FASTER, SCALABLE
With sustained data ingest, indexing, and storage of up to 150,000 messages per second (MPS) and peak performance of up to 250,000 MPS, you can address denial-of-service attacks and chatty firewalls—at an order of magnitude faster than competitive products.

NAS- AND SAN-AWARE
Centralized, real-time access to up to 10 years of archived data with fully automated data-retention and deletion-policy controls supplies virtually unlimited scalability.

SIMPLE CONTROL
Appliances are managed as a peer group, allowing you to remotely control multiple appliances as if they were one device.

FAST SEARCH
Distributed indexing lets you search through everything, and quickly and easily see the data that is most important, regardless of what physical appliance it's stored on. Log Management Intelligence now supports fast and powerful searches by being able to combine index searches with regex patterns.

FLEXIBLE TAGGING
With custom parsing you can tag your own sources and rapidly present any data, even using RegEx if desired.

OPEN FORWARDING
LogLogic LX and ST data management appliances are unusual in their ability to forward to multiple analytics engines simultaneously so you can make best use of your data, and your past investments, too. The appliances can be integrated with LogLogic Compliance Manager to provide index reports.

ACCESSIBLE, AUDITABLE, AND IMMUTABLE
Automated retention, on-demand verification, compressed raw data storage, immutable data stores, and connectivity to write-once-read-many (WORM) data storage drives provide enterprise-class storage options.

ADMINISTRATIVE MONITORING
For added security, all administrative actions are logged, even those made to the appliances themselves.

	ST1025	ST2025-SAN	ST4025	ST2025-SANR1	ST4025R1	ST2025-SANR2	ST4025R2	ST4035	ST2035-SAN
Peak messages per second (MPS)	120K	235K	250K	235K	250K	235K	250K	250K	235K
Sustained MPS	75K	150K	150K	150K	150K	150K	150K	150K	150K
Supported Devices	16K	16K	16K	16K	16K	16K	16K	16K	16K
Raw Storage (HDD)	1 TB	1 TB*	8 TB	8 TB*	32 TB	8 TB*	32 TB	32 TB	8 TB*
Raw Storage (SSD)	--	--	--	6 TB	6 TB	6 TB	6 TB	7.5 TB	7.5 TB
Maximum Retention (Raw and index data)	10 years	10 years	10 years	10 Years	10 Years	10 years	10 years	10 years	10 years

* extensible via SAN and network file storage.
  Other ST models' storage is also extensible via NAS.