CRYPTOLOG
INFORMATION SECURITY INTELLIGENCE

One of today's critical requirements of each organization is a proper log management system, collecting and analyzing logs to meet the government regulations and industry standards. **CRYPTOLOG** not only ensures government and industry compliance necessities, it provides a unified easy-to-deploy search, analysis and correlation options over log data, adjustable to needs and scale of your IT organization. With an integrated network monitoring platform, **CRYPTOLOG** simplifies identification of potential security threads and forensic investigation from log data.

LOG MANAGEMENT SOLUTION

Each and every device and application, from operating systems to servers on an IT infrastructure, generates event data containing different types of information, such as source and destination IPs, errors, warnings and audit information making tremendous amount of log data. Furthermore, the format, size and frequency of generated logs differs for each source. Accordingly, it is impractical to utilize this information effectively without a unified automated log management system. Meanwhile, government and many regulatory agencies require organizations to collect and store their log data for security purposes. Therefore, an integrated log management scheme which can sparse, collect and store proper logs and also meet the government's regulations as well as required industry mandates, plays an essential role in each organization.

CRYPTOLOG
INFORMATION SECURITY INTELLIGENCE

CRYPTOLOG Highlights

- ✓ Comprehensive log collection from vast varieties of log formats
- ✓ Intuitive user framework for universal control
- ✓ Robust forensic analysis with advanced search engines
- ✓ Scalable in accordance with enterprise size and requirements
- ✓ Exceptional performance
- ✓ Ensuring latest compliance mandates and security regulation
- ✓ Flexible storage options
- ✓ Integrated with CRYPTOSIM's SIEM technology for event correlation
- ✓ Easy deployment for complex topologies
- ✓ Multiple platform compatible

WHY CRYPTOLOG?

CRYPTOLOG is a cost-effective integrated Log Manager which helps you meet regulatory compliance while reducing security risks across a diverse IT environment. With fast and accomplished engines, CRYPTOLOG aggregates and collects wide range of logs and events and provides customizable dashboard to give a comprehensive sketch from total network activities. It normalizes and categorizes events, produces actionable information for further analysis from forensic investigation to anomaly detection.

Widespread Log Workspace

There are varieties of log files from server log file to security logs, containing valuable records on source, destination and sequence of operations or events within specific time. However, aggregating billions of logs from disparate resources into one repository platform is not an easy task. There are varieties of log types i.e. security logs, application logs, domain controller, system logs and so forth; each of which has different contents based on the source of the log file. Furthermore, there are different standardization on the format of each log which makes the parsing process even more burdensome.

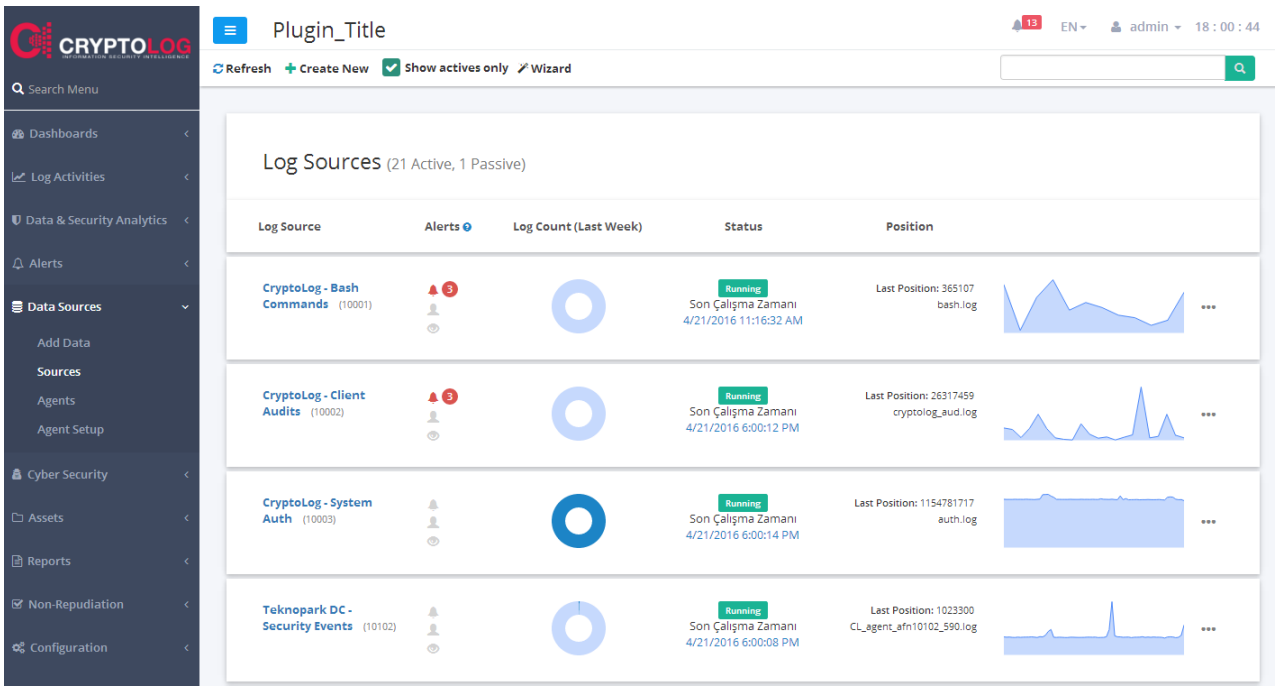
With robust parsing algorithms and powerful collecting engines, CRYPTOLOG overcomes lack of consistency on log formats and provides logging and storage of broad range of log workspace, e.g. OS events, IDS events, application log files, Database transactions, etc. It compresses logs and stores them for analysis, investigation, and data retention requirements. In other words, it collects raw log files from different OS systems (Windows, UNIX and Linux) and normalizes them into unified structure, allowing simpler data analysis. The original log records can be stored separately based on vendor request for lateral archiving or legal regulation purposes.

Table 1 - Log Types Workspace

WebServer Activity Logs	VPN Logs	Framework Logs
Proxy Internet Access and Cache Logs	Windows/LDAP Domain Logs	DHCP Logs
IDS/IPS/IDP Logs	Content Management System Logs	SAN/NAS Object Audit Logs
Firewall Logs	SMSC Gateway Logs	VLAN Access Logs
Router/Switch Logs	Wireless Access Logs	Database Table Logs
MailServer Message Tracking Logs	Oracle Financial Logs	Client/File Server Logs

Simplified Drilldown Analysis

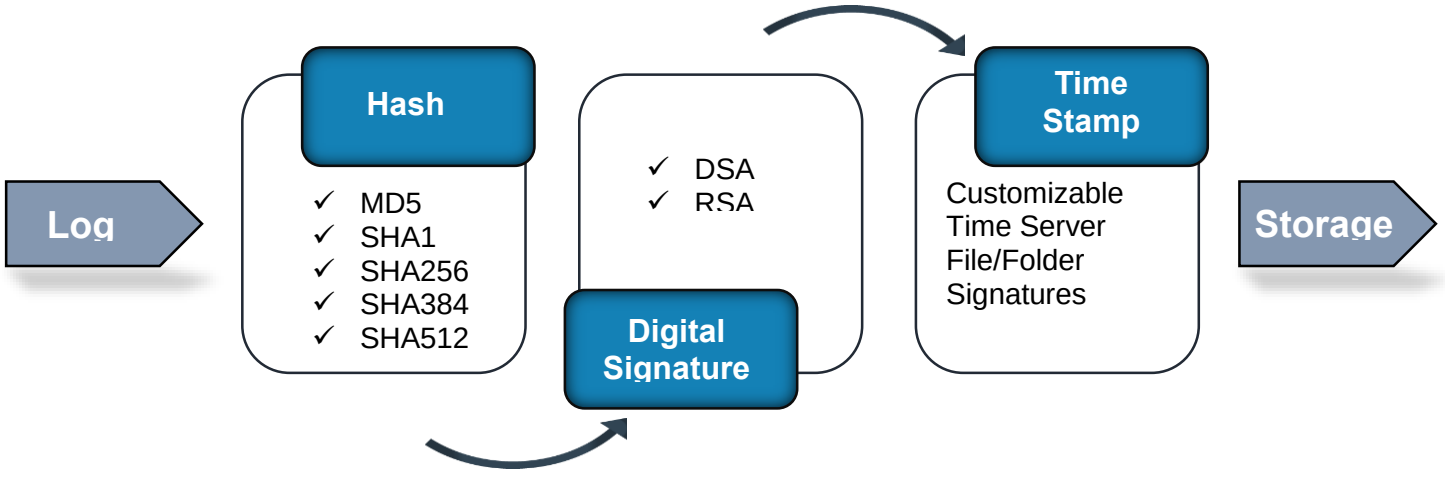
CRYPTOLOG represents total log data trends in an intuitive yet potent centralized user interface, where administrators can monitor and analyze network's events in real-time, without any specific knowledge on log file infrastructure. Pre-defined dashboards with charts and graphs are available based on the required functionality. By one click on each graph or chart, users can drill down to detailed information of the elected actionable log data. In addition, users can customize their own dashboard to inspect peculiar events or activities in more detail. This flexible GUI helps organization not only in monitoring availability and performance but also in determining security anomalies or potential business opportunities over their total IT infrastructure.



CRYPTOLOG
INFORMATION SECURITY INTELLIGENCE

Non-repudiation Efforts Forensic Analysis

Most of IT incidents leave evidence behind in log files and source of the attacks can usually be traced from the information that log file provides. Therefore, log file storages are one the first places they tend to attack. CRYPTOLOG hashes and timestamps all the logs where due to the non-repudiation characteristic of hash functions the source of the attacks can be traced confidently. With advanced query and full text search abilities of CRYPTOLOG, cause or source of a breach can be found and reports based on such queries in logs, can be used as law evidence. Qualified certificates and external timestamp services are available in CRYPTOLOG based on use-cases of organizations. CRYPTOLOG also goes one step further by auditing the auditors' activities and ensures their authentication by sending the logs of CRYPTOLOG to another party for further investigation.



Expandable in Accordance with Enterprise

CRYPTOLOG log manager's architecture and configurations are adaptable to the scale of organizations. It can be applied through a cloud base virtual appliance which remotely collects and analyzes the logs for small scale networks to a single unit software; or using a centralized base with distributed sensors in large scale IT structures. These sensors may only collect the logs and transfer them after compression; or first apply the normalization and then send the analyzed information to central base for further inspections.

Compliance with Internal and External Policies

Internet and IT structures are subject to governments regulations and industry standards and their fast pace changings. Majority of these rules and standards require solid collection and protection of data. CRYPTOLOG with its dynamic storage and search abilities, simplifies organizations effort in achieving and assuring compliance mandates. With myriad build-in rules and reports, CRYPTOLOG ensures organizations of meeting well-known mandates, from Payment Card Industry Data Security Standard (PCI DSS), to Health Insurance Portability and Accountability Act (HIPAA), to Sarbanes–Oxley Act (SOX) and so forth. It also enables organizations to deploy their internal policies by providing role based authorization control over accessing data, reports and searches on software and network. At the same time, CRYPTOLOG satisfies the log storage regulations e.g. Turkish Regulation law 5651 with varieties of compression algorithms and flexible storage options from local storage, to NAS or SAN, to FTP and so forth, based on requirement of the enterprise.

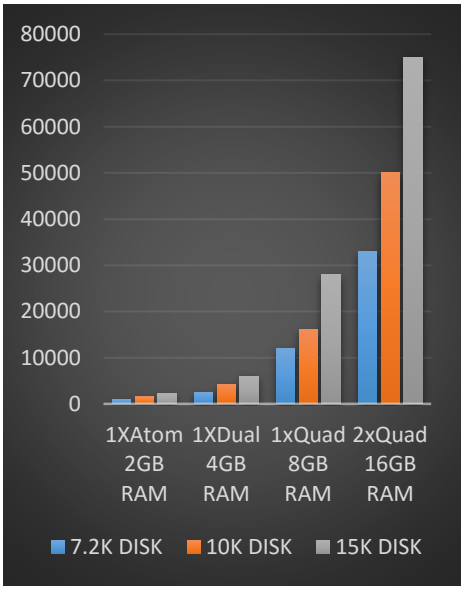


Figure 1 - Hardware Benchmark

Exceptional Performance Efficiency

CRYPTOLOG can captures logs up to a rate of 75000 EPS from more than 800 sources and compress the data by a rate of 1:30 with no additional hardware to system. Queries can be made over archived logs therefore no additional transaction in necessary for reports over archived data. CRYPTOLOG operates on active-passive basis within its grouping substructure, and provides high availability in a minimum of down-time. It also can operate on active-active basis, which allows load sharing in systems to equalize the load stress between subsystems.

CRYPTOLOG
INFORMATION SECURITY INTELLIGENCE

SYSTEM REQUIREMENTS

Supported Operating Systems (both 32-bit and 64-bit)

- Ubuntu 12.04 LTS - Precise Pangolin
- Ubuntu 14.04 LTS - Trusty Tahr
- Ubuntu 16.04 LTS - Xenial Xerus
- Debian 6 - Squeeze
- OpenSuse 11.4, 12.1, 12.2
- Red Hat Enterprise Linux 5.6, 5.7, 6.0
- CentOS 5.6, 5.7, 6.0
- Sun Solaris 10
- OpenSolaris 10.x, 11.x

Virtual Systems;

- Linux KVM-2.6.33 kernel version over (Kernel Virtual Machine)
- Citrix XEN Server 6
- Microsoft Hyper-V Server
- Free Xen Hypervisor 4.1, 4.0
- VMware vSphere Hypervisor 5.0
- VMware ESX & ESXi 3.5, 4.0, 4.1, 5.0, 5.5

EPS (Max)	CPU	RAM	DISK
1.000	1xIntel Atom	2 GB	500 GB 7.2K RPM
2.500	1xIntel Dual Core	4 GB	1 TB 7.2K RPM
12.000	1xIntel XEON Quad Core 3400 Series	8 GB	1 TB 7.2K RPM
33.000	2xIntel XEON Quad Core 56 Series	16 GB	2 TB 10K RPM
50.000	2xIntel XEON Quad Core 56 Series	16 GB	2 TB 15K RPM