

TECHNICAL DATASHEET



Automate Log Compliance, Simplify Security Event Management

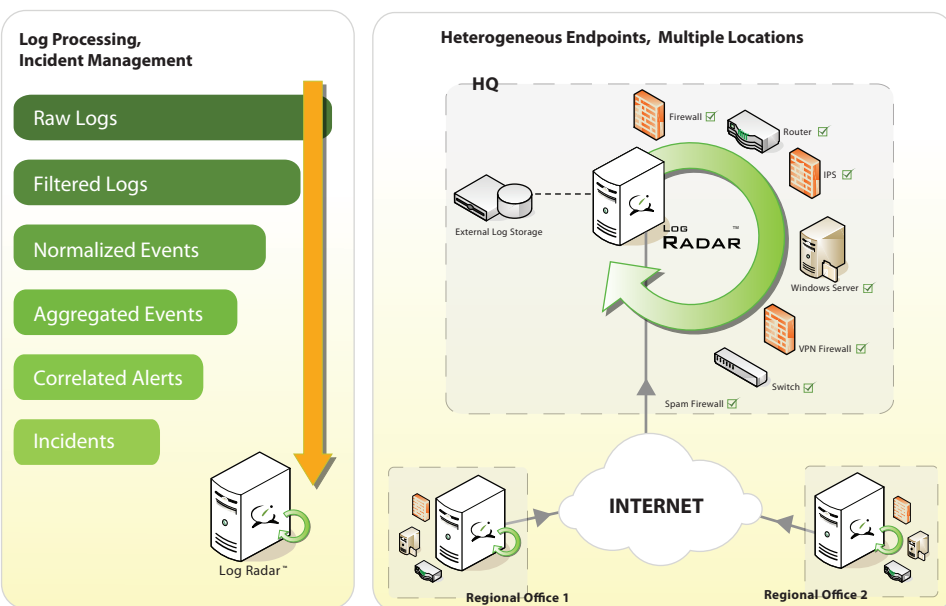
Highlights :

- ✓ Get up-to-date network overview by viewing real-time log details on interactive dashboards
- ✓ Web-based Centralized Management Console
- ✓ Log Consolidation from heterogeneous sources -e.g. Windows Servers, Firewall, IDS/IPS, VPN
- ✓ Normalization of logs instantly deciphers raw logs into easily understandable language
- ✓ Identifies the root cause of non-conforming activities promptly and effectively
- ✓ Upholds top service level performance with instant alert upon threat identifications
- ✓ Analyzes your Windows Server and PC logs and identifies possible brute force attacks
- ✓ Automated sorting and categorization of attacks naming convention from heterogeneous sources
- ✓ Simplifies Standard Compliance with 200+built-in report templates for ISO 27002 , PCI DSS, HIPAA, SOX etc.
- ✓ Flexibility of generating distributed reports at multiple branches, as well as centralized reports at HQ
- ✓ Frees up technical human resource with computerized processing of security log
- ✓ Accepts SYSLOG and SNMP integration

TecForte® Log Radar™

Log Radar™ is a robust and easy-to-use Security Information and Event Management (SIEM) software solution that provides essential real-time security intelligence to help decipher hacker/virus behavior, combat security threats and meet regulatory compliance requirements across the entire IT infrastructure.

Log Radar™ provides powerful security intelligence across heterogeneous network devices that have an impact on an organization's security framework.



Log Radar™ automatically collects and correlates logs from variety of heterogeneous multi-vendor network devices including routers, switches, firewalls, VPNs, IDS/IPS systems, proxy servers, spyware, antivirus, SPAM and content filtering web security appliances. This information helps to eliminate false positives, identify security breaches and corporate violations, improve security operations and delivers the necessary tools to meet ISO27001, SOX, HIPAA and PCI DSS compliance.

Log Radar™ helps minimize incident response time and maximize the ability to take preventative actions by providing advanced security event monitoring, correlation and historical reporting. The end result improves security operations and protects IT assets by helping organizations centrally manage information risk and take proactive steps to minimize security breaches and meet compliance mandates.

Real-time Monitoring and Alerting

Heterogeneous Real-time Monitoring

Monitors security event data across the entire network in real-time.

Real-time Correlated Alerting

Allows the creation and definition of any number of alerts to reduce false positives and identify blended attacks.

Real-time Event Manager

Presents a view of security event data from various heterogeneous and multi-vendor network devices. Prioritizes the actions based on business impact of each event, allowing for corrective actions before an incident occurs.

Monitoring Dashboard

Provides a quick, consolidated view of the environment.

Web-based Interactive Dashboard



Compliance Management

Log Archiving for Compliance

Automatically compresses, encrypts and archives log files for investigative analysis and regulatory compliance.

Compliance Monitoring

Provides centralized monitoring and alert correlation for real-time investigation of security incidents with regulatory compliance implications.

Compliance Reports

Offers detailed reports specific to ISO27002, SOX, HIPAA and PCI DSS.

Scalable Search

Searches hundreds of GB of log data across multiple devices to aid in investigative analysis.

Activity Investigation

Identifies anomalies and employee corporate policy violations.

Automated Asset Discovery



Supported Systems & Devices

Log Radar™ provides out-of-the-box support for a broad range of heterogeneous endpoints, including support for:

- Microsoft Servers and workstations
- Antivirus / Antispam products
- Firewall / Web Filtering products
- VPN products
- IDS / IPS
- Routers and Switches

Log Radar™ can be easily extended to monitor other products, systems and devices. Please contact us for more information on how Log Radar™ can assist in supporting your environment and specific requirements.

Advanced Security Intelligence

Event Drilldown

Provides advanced on-the-fly event drill-down with correlation and analysis of significant security events to enable quick resolution of security incidents.

User-definable Event and Threat-Level Classifications

Classify events and threat levels based on unique requirements.

Recommended System Requirements:

| Model | Requirements |
|----------------------------|---|
| Processor | Intel Xeon Quad Core 2.5 GHz or higher |
| Memory | 4 GB |
| Operation System | Server 2003 64 - bit |
| Disk Space for Application | 390 MB |
| Disk Space for Logs | Subject to traffic volume and log rotation policy |

Security Reporting

Reporting Portal with Powerful Drilldown
Access to over 300+ interactive reports.

Correlated Reporting

Offers a holistic view and understanding of hacker and virus activity by correlating data across all network devices instead of looking at each device data separately.

Intrusion and Rules-based Reporting

Attack and rules-based reports provides a comprehensive understanding of the intrusions and rule violations.

Protocol and Web Usage Reporting

Provides a firm handle on protocol and web usage patterns.

SPAM, Spyware and Antivirus Reporting

Generates reports on malware activities.

Vulnerability Reporting

Integrates and reports on vulnerability data derived from your network.

Content Categorization Reporting

Generates reports to help understand web usage patterns.

Automated Report Generation and Distribution

HTML display, and automatic e-mail distribution of reports in PDF, Excel formats.

Top Attackers Report





Network and System Log Management in Government Ministries and Agencies

Governments around the world are continuously seeking for effective and sustainable ICT practice to keep its computer systems in top notch condition. In many ways, a Government environment is much more complex than any corporate environment, as there is a strong need to balance the freedom of information and internet with national security.

“34% of total security incidents reported by the Government Ministries and Agencies could not be investigated due to the lack in log activation & management.”

- According to MAMPU (Malaysian Administrative Modernisation and Management Planning Unit)

- GCERT (Government Computer Emergency Response Team): Reference: MAMPU 702-11/1/7 Jld. 3 (48)]

As new computer threats and risks are being discovered, there is a valid reason for the Government Ministries, Agencies and GLCs to continue adding layer upon layer of security solutions to beef up its defenses. – However, with this addition of more and more system devices and security products comes the responsibility of managing them! - And monitoring such a highly complex security measures and its enormous amount of Network and System Logs have been recognized by Governments in the world to be one of the biggest headaches in today's ICT security management!

A Central Network and System Log Management Application is required to eliminate human-intensive, complex and costly log management process; and to deliver a clear and comprehensive ministry-wide overview of the entire network & system security condition in real time. Furthermore, the application would assist to collect electronic evidence, probe deeper and solve technical problems to help the judicial process and national security.

“With the recognition of the critical importance in ICT security, MAMPU encourages use of locally developed security products are preferred over foreign makes to help spur local ICT security development.”

- (MyMIS 2.6)

Main Function of Log Radar™ Central Network and System Log Management System

Log Radar™ is enabling the ICT administrator to regain full control over their ICT Security Systems by delivering tremendous value and insight towards maintaining security health, rapid threat identification and improved system availability & uptime – via centralized log data collection, analysis and correlation.

- » To comply to MAMPU policies in log management and pass stringent system audits
- » To strengthen on Government's effort to battle internal abuse and external hacking
- » To increase productivity, integrity, availability of its computer network infrastructure
- » To mitigate guesswork and fire-fighting in the current security controls

About TecForte®

TecForte® is a Malaysia based R&D centre for Central Security Management Solution (since 2004). Its pioneer status has also won the award of MSC status. Log Radar™ has been implemented by Malaysia Custom Immigration & Quarantine (CIQ) Complex, MAVCAP, TOT Thailand, Central Bank of Thailand, TelBru (Telekom of Brunei), etc. Currently, it is undergoing world class security certification, CC EAL2.



TecForte Sdn Bhd
Parcel No 2A-13-2, Plaza Sentral Phase II,
Jalan Stesen Sentral 5, Kuala Lumpur Sentral
50470 Kuala Lumpur, Malaysia

| | |
|-------|--|
| Tel | : +6(03) 2264 3164 |
| Fax | : +6(03) 2264 3064 |
| Email | : info@tecforte.com |
| URL | : www.tecforte.com |



Online and Phone Support Available

All Rights Reserved. TecForte © 2010