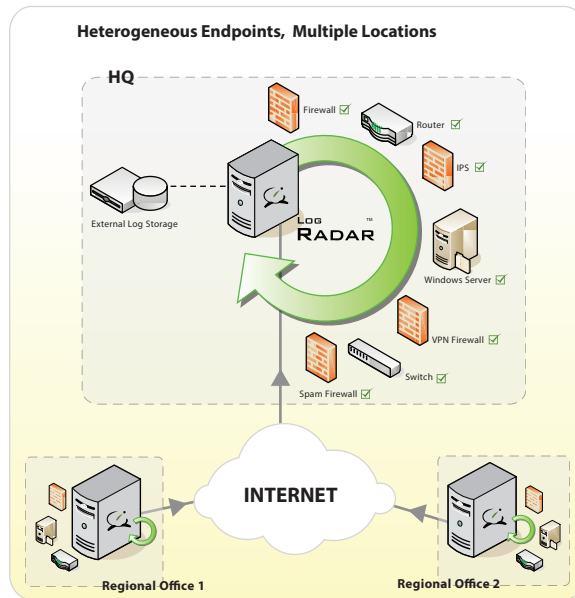
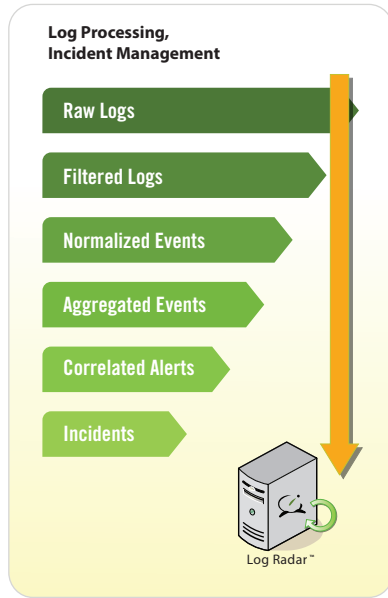




Do It The Log Radar™ Way

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



Top Attackers Report



Real-time Monitoring and Alerting

Heterogeneous Real-time Monitoring
Monitoring 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 Report
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
Generates reports on malware activities. Identifies anomalies and employee corporate policy violations.

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.

Automated Asset Discovery



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.



Tecforte Sdn Bhd (680593-P)
A-18-3, Tower A, Level 18, Northpoint Office,
Mid Valley City, No. 1 Medan Syed Putra Utara,
59200 Kuala Lumpur, Malaysia.

Tel : +6(03) 7960 5009
Fax : +6(03) 7960 5010
Email : info@tecforte.com
URL : www.Tecforte.com

