

Security Event and Log Management Service



Organizations are continuously innovating to provide better services to customers at a faster pace. And most of these services require connecting the enterprise to a growing number of third parties who might include customers, partners, suppliers, service providers, vendors or regulators. This opens up your infrastructure to a number of new risks, in particular intrusion attempts.

Intrusion attempts – both internal and external – are growing at an alarming rate and at the same time are increasingly complex. An organization faces the risk of intrusion from multiple sources on a continuous basis, at multiple points in its network. It can only detect and prevent attacks early if there is continuous monitoring of logs from multiple sources, including firewalls, servers, databases, IDS and physical access logs.

BESECURE offers a complete, managed security event monitoring service for the continuous management of internal and external threats. This is run from a fully-established Security Operations Centre which is ISO27001 certified.



Service Highlights

This service extends security monitoring to your critical servers, network devices, security devices and applications, providing enhanced security coverage while addressing compliance requirements through comprehensive reporting and log archiving capabilities. With pre-defined regulatory reporting capabilities for common industry mandates such as PCI, SOX, COBIT and others – specific insight into your security and compliance posture has never been easier. Event and Log Management service includes:

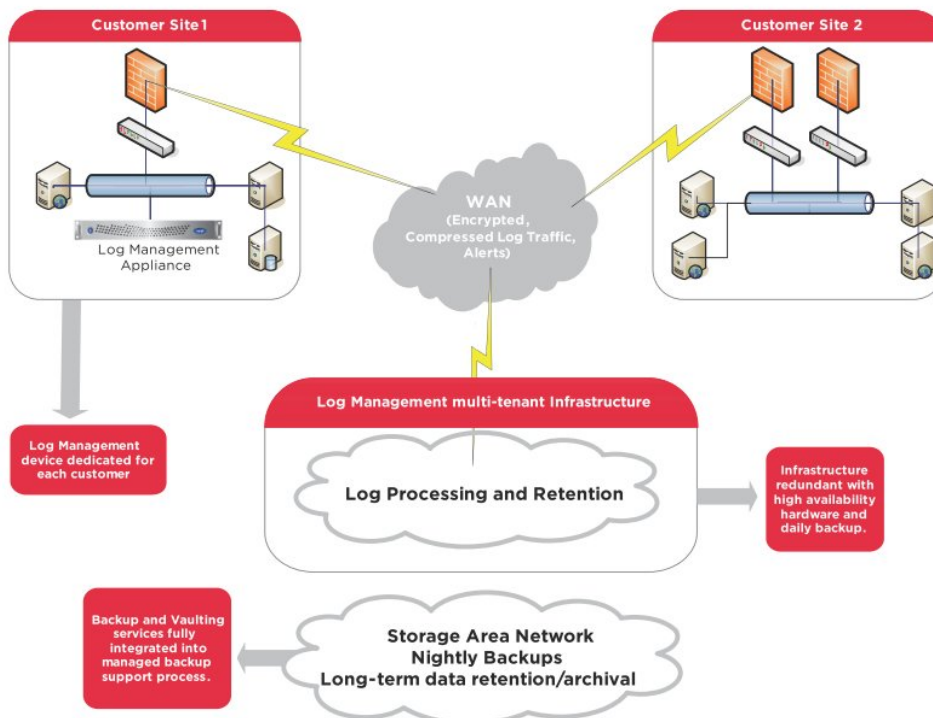
- Attack correlation of logs from multiple sources
- Multi-vendor and platform support
- Support for small and large networks
- Smart utilization of bandwidth
- Incident management
- Historic forensic analysis
- Online reports
- 250+ pre-defined report templates
- Rich visualization

Service Benefits

As part of BESECURE's Managed Security Solutions, Security Event & Log Management service benefits customers in five key ways:

- Preserve 100% of logs in unaltered form, normalize security incidents and trends within BESECURE's correlation environment
- Demonstrate regulatory compliance with actionable reporting, event correlation and archival
- Provide powerful compliance reporting and log search capabilities
- A cost-effective solution to store and process terabytes of logs without investing in a costly SAN infrastructure.
- Provides secure gathering, transmission and storage of all log data, with 90 days of data available online and 12 months of data available in off-site archives

Service Infrastructure



About BESECURE

BESECURE provides compliance services based on legal and regulatory requirements, designs and implements advanced IT security solutions, delivers information security training seminars, provides Managed Security Services, and performs Penetration Tests and Vulnerability Assessments covering all phases of the life cycle of information security.

Services & Solutions

Governance, Risk and Compliance Services

- Information Security Risk Assessments
- Information Security Management Framework Implementations ISO27001
- Enterprise Security Program Reviews & Development
- Enterprise Security Architecture Planning
- Network Vulnerability and Penetration Testing
- Information Security Policies, Standards and Guidelines
- PCI Data Security Standard Consultancy

Managed Security Services

- Managed VPN Security
- Managed Vulnerability Assessment
- **Event and Log Management Service**
- Managed Intrusion Prevention
- Managed Web & Email Content Security

Security Training Services

- Holistic Information Security Practitioner (HISP) Certification Courses
- Security Awareness Program Development
- Information Security Training Planning

