CYBERSECURITY INNOVATIONS POWERED BY AI

BitSecure®

Log Management

Log Management enables organizations to centralize, monitor, analyze, and secure enterprise log data across IT and security infrastructure, helping reduce incident response times, improve compliance readiness, strengthen cybersecurity posture, and lower operational costs through a scalable and unified log management platform.

80%
Reduction in incident investigation time

70%
Faster threat detection

60%
Reduction in Mean Time to Respond

THE CHALLENGE

Top 5 Industry Challenges (If Log Management is NOT Implemented)

- **Security Incidents Go Undetected** -Without centralized log collection and analysis, security teams lack visibility into suspicious activities across servers, applications, databases, and network devices. This significantly increases the risk of breaches remaining undetected for weeks or months, resulting in financial and reputational damage.
- **Slow Incident Response and Recovery** - IT teams spend valuable hours manually gathering logs from multiple systems during outages or cyber incidents. Longer investigation times directly increase downtime, productivity loss, and business disruption.
- **Compliance and Audit Failures** - Regulatory frameworks such as RBI, SEBI, DPDP, ISO 27001, PCI-DSS, and SOC 2 require log retention, monitoring and reporting. Organizations without centralized logging often struggle to provide audit evidence, increasing compliance risks and penalties.
- **Lack of Operational Visibility** - Organizations cannot effectively monitor application performance, infrastructure health, or abnormal system behavior. This leads to recurring issues, degraded customer experience, and increased operational inefficiencies.
- **Higher Infrastructure and Management Costs** -Using multiple standalone logging solutions creates data silos, duplicate storage requirements, and increased administrative effort.

KEY BENEFITS

Faster Threat Detection & Response
Centralized log monitoring and real-time alerting help identify suspicious activities immediately. Organizations typically reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) by 50–80%.

Improved Security Posture
Continuous collection and analysis of logs from servers, databases, firewalls, IDS/IPS, applications, and cloud platforms improves threat visibility. This can help identify insider threats, malware activity, and policy violations before they become major incidents.

Compliance Readiness
Automated log retention, monitoring, and reporting simplify regulatory audits. Organizations can reduce audit preparation effort by 40–60% while improving compliance accuracy.

Increased Operational Efficiency
Automated log analysis eliminates manual troubleshooting and correlation activities.IT teams typically save 30–50% of investigation time, enabling faster issue resolution and better resource utilization.

Lower Total Cost of Ownership (TCO)
Centralized log storage and management reduce dependency on multiple logging tools and manual processes. Organizations can achieve 20–40% reduction in log management and operational costs over time.

KEY CAPABILITIES

One Unified Agent

01 Log Collection & Ingestion

Centralized Log Collection
- Collects logs from servers, databases, applications, network devices, and security systems.
- Supports heterogeneous IT environments.

Broad Platform Support
- Windows Servers
- Linux (RedHat, Ubuntu, SUSE, CentOS, Debian)
- Hypervisors (VMware, Hyper-V, KVM, Solaris, AIX)

Database Monitoring
Oracle, MS SQL, MySQL, PostgreSQL, MongoDB, Sybase

02 Log Storage & Management

Centralized Repository
- Consolidated storage for all enterprise logs.
- Eliminates fragmented log silos.

Scalable Architecture
- Supports increasing log volumes.
- Suitable for enterprise-scale deployments.

Long-Term Retention
- Facilitates regulatory and forensic requirements.
- Supports historical investigations.

03 Monitoring & Alerting

Real-Time Monitoring
- Continuous monitoring of log collection status.
- Detects anomalies and operational issues.

Automated Alerting
- Security alerts.
- Operational alerts.
- Compliance alerts.

Event Correlation
- Correlates events across multiple systems.
- Improves root cause analysis.

04 Security & Compliance

Threat Detection
- Identification of suspicious activities.
- Detection of unauthorized access attempts.
- Detection of policy violations.

Secure Log Handling
- Encryption of log data.
- Controlled access mechanisms.
- Secure storage practices.

Audit & Compliance Support
- Regulatory reporting.
- Evidence generation for investigations.

05 Integration Ecosystem

Security Integrations
- SIEM, SOAR, DLP
- Vulnerability Management Platforms

IT Operations Integrations
- ITSM
- NMS
- APM Tools

Security Device Integration
Firewalls, WAF, IDS/IPS, NAC, DNS, Proxy Solutions

06 Deployment Flexibility

On-Premises Deployment
- Suitable for regulated industries.
- Complete control over data residency.

Cloud Deployment
- Elastic scalability.
- Faster deployment and expansion.

Hybrid Environments
- Supports modern enterprise infrastructure strategies.

07 Collaboration & Reporting

Cross-Team Visibility
- Security Teams
- IT Operations
- Compliance Teams
- Management

Reporting
- Executive reports.
- Audit reports.
- Operational dashboards.

Knowledge Sharing
- Shared visibility across departments.
- Faster collaborative investigations.

ADD-ON AVAILABLE

Need 24/7 coverage? Add Velox MDR.

- India-based SOC analysts, 24×7×365
- 15-minute SLA for critical incidents
- Seamless activation — no new agent required

LEARN MORE →

THINK CYBER SECURITY... THINK VELOX

Velox Solutions is a Global cybersecurity OEM delivering advanced, AI-powered technologies that strengthen Security Operations and enterprise resilience since 14+ years. Our solutions enable faster threat detection, automated response, and deep visibility across users, endpoints, and infrastructure. Leveraging AI-driven SIEM, SOAR, and behavioural analytics, Velox builds proactive, intelligence-led SOC environments, empowering government and enterprise sectors to stay ahead of evolving cyber threats.

Web
www.veloxworld.com
India
+91 9321943983

Sales
sales@velox.co.in
Marketing
marketing@velox.co.in

©2026 Velox Solutions Pvt. Ltd. All rights reserved. SecureIT, ScanPlus, BitSecure, AssetGrid, PlanetGuard, TrustShields, ScanX, and CodeTrust 360 are Products of Velox Solutions Pvt. Ltd.