CYBERSECURITY INNOVATIONS POWERED BY AI

BitSecure®

SIEM

SIEM converts massive security data into real-time intelligence, detecting threats faster, automating response, and ensuring compliance at scale.

90%
Improved Security Visibility

85%
Faster Threat Detection

80%
Reduction in False Positives

THE CHALLENGE

Enterprises face a threat landscape that legacy tools were not built for

- **No Centralised Security Visibility** - Logs remain scattered across devices, applications, and networks with no correlation. This creates blind spots, allowing threats to go undetected for long periods.
- **Delayed Threat Detection & Response** - Without real-time correlation and alerting, incidents are identified too late. This increases breach impact, downtime, and recovery costs.
- **Compliance & Audit Failures** - Organizations fail to maintain centralised log storage and reporting required by regulations. This leads to audit failures, penalties, and regulatory risks (RBI, ISO, etc.).
- **Inability to Detect Advanced Threats (APT/Insider)** - Traditional tools fail to detect sophisticated, multi-stage, or insider threats. Without behaviour analysis and correlation, these threats remain hidden.
- **High Operational Burden on Security Teams** - Manual log analysis and a lack of automation slow down security operations. This increases SOC workload, inefficiency, and the cost of security management.

KEY BENEFITS

- **Real-Time Threat Detection & Correlation**
  SIEM collects and correlates logs across all systems to detect suspicious patterns instantly.
- **Centralised Log Management & Visibility**
  Aggregates logs from servers, endpoints, firewalls, and applications into a single platform.
- **Faster Incident Response with Automation (SOAR)**
  Automated workflows, runbooks, and alert escalation reduce manual intervention.
- **Advanced Threat Detection (UEBA + Threat Intelligence)**
  Uses behavioral analytics and threat intelligence to detect unknown and insider threats.
- **Compliance & Reporting Readiness**
  Provides historical log storage, reporting, and audit trails for regulatory compliance.

KEY CAPABILITIES

One Unified Agent

01 Log Collection & Aggregation

- Collects logs across the entire IT ecosystem
- Multi-source collectors
- Centralised log repository for analysis

02 Event Correlation & Security Scoring

- Correlates events using rules + machine learning
- Assigns security scores based on risk and behaviour
- Identifies attack patterns across systems

03 Real-Time Monitoring & Alerting

- Continuous monitoring of security events
- Alert escalation via dashboard, email, SMS
- Detects anomalies

04 Incident Management & Tracking

- Out-of-the-box correlation rules
- Incident prioritisation and tracking
- Attack history monitoring
- Historical data analysis for trend detection

05 UEBA (User & Entity Behavior Analytics)

- Detects anomalous user and system behaviour
- Identifies insider threats and compromised accounts
- Uses behavioural baselines for advanced detection

06 SOAR (Security Orchestration, Automation & Response)

- Automated workflows and response playbooks
- Runbooks for repetitive security tasks
- L1/L2 task automation to reduce manual workload
- Bi-directional integration with security tools

07 Threat Intelligence Integration

- Integrates external threat feeds
- Correlates malicious IPs, domains, and indicators
- Enhances detection accuracy and reduces false positives

08 Flexible Deployment (Agent-Based & Agentless)

- Agent-based for deep visibility
- Agentless for easy deployment
- Unified setup supporting both approaches

KEY CAPABILITIES

One Unified Agent

09 Dashboards & Visualization

- Customizable dashboards for real-time monitoring
- Pattern recognition and anomaly visualization
- High-level and granular visibility for SOC teams

10 Automated Response & Business Impact Tracking

- Automated remediation actions
- Tracks ALE (Annual Loss Expectancy) and business impact
- Measures effectiveness of security controls

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 →

VELOX®

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