CYBERSECURITY INNOVATIONS POWERED BY AI

BitSecure®

User Entity & Behavior Analytics(UEBA)

AI-driven behavioral analytics with real-time anomaly detection, insider threat identification, and 70% fewer false positives across hybrid and multi-cloud environments.

60%
Faster Threat Detection

70%
Reduction in False Positives

80%
Better Visibility Across Hybrid Environments

THE CHALLENGE

Top 5 Industry Challenges (If UEBA is NOT Implemented)

- **Insider Threats Remain Undetected** -Traditional security tools struggle to identify abnormal user behavior from legitimate accounts. This increases the risk of data theft, sabotage, and misuse by employees, contractors, or compromised users.
- **Delayed Detection of Account Compromise** - Without behavioral analytics, compromised credentials often appear as normal login activity. Organizations may take weeks or months to identify breaches, resulting in major financial and reputational damage.
- **High Alert Fatigue in SOC Teams** - Security teams receive thousands of alerts daily from SIEM tools without contextual intelligence. This leads to analyst burnout, slower response times, and missed critical incidents.
- **Inability to Detect Lateral Movement** - Attackers moving across systems internally often bypass signature-based detection systems. Without UEBA, ransomware and advanced persistent threats (APTs) can spread silently across the environment.
- **Poor Visibility Across Hybrid & Multi-Cloud Environments** -Modern enterprises operate across cloud, on-prem, SaaS, and remote workforce environments. Lack of centralized behavioral monitoring creates blind spots that attackers can exploit.

KEY BENEFITS

Faster Threat Detection & Response
UEBA uses AI/ML-driven anomaly detection to identify suspicious behavior in real time. Organizations can reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) by 40–60%.

Reduced False Positives
Behavioral baselining improves alert accuracy by correlating contextual user activities. Security teams can reduce false positive alerts by nearly 50–70%, improving SOC efficiency.

Improved Insider Threat Detection
UEBA continuously monitors user activities, access patterns, and privileged actions. This helps detect insider threats, compromised accounts, and policy violations before escalation.

Better SIEM & SOAR Effectiveness
UEBA enhances SIEM/SOAR platforms with contextual analytics and risk scoring. SOC analysts gain prioritized alerts, leading to faster investigations and automated containment.

Enhanced Compliance & Risk Management
Continuous monitoring supports compliance requirements for RBI, SEBI, DPDP, ISO 27001, and GDPR. Organizations gain stronger audit visibility and reduced exposure to regulatory penalties.

KEY CAPABILITIES

One Unified Agent

01 Behavioral Analytics & Machine Learning

- AI/ML-driven anomaly detection
- User behavior baselining
- Peer group analysis
- Detection of unusual access patterns
- Adaptive learning for evolving behaviors

02 Insider Threat Detection

- Detection of malicious insiders
- Monitoring privileged user activity
- Unauthorized access identification
- Suspicious login pattern analysis
- Policy violation tracking

03 Real-Time Threat Detection

- Immediate anomaly detection
- Real-time alert generation
- Compromised credential identification
- Lateral movement detection
- Data exfiltration monitoring

04 Identity & Entity Correlation

- Integration with Identity Management systems
- Correlation of user identities across applications
- Device and entity tracking
- Multi-user risk profiling
- Context-aware investigation support

05 SIEM/SOAR Integration

- Seamless API integration
- Works with SIEM, SOAR, and DLP platforms
- Log ingestion from Windows, Linux, Mac, firewalls, databases, and file servers
- Automated incident workflows
- Centralized SOC visibility

06 Multi-Cloud & Hybrid Environment Monitoring

- Cloud and on-prem visibility
- Monitoring across SaaS applications
- Multi-cloud infrastructure support
- Unified analytics dashboard
- Scalable deployment architecture

07 Incident Investigation & Risk Prioritization

- Risk scoring for users/entities
- Investigation timelines
- Threat hunting support
- Granular detection visibility
- Actionable forensic insights

08 Data Exfiltration Prevention

- Monitoring unusual data transfers
- Detection of unauthorized downloads/uploads
- Automated containment actions
- Sensitive data access monitoring
- Early breach indicators detection

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