CYBERSECURITY INNOVATIONS POWERED BY AI

SecureIT®

Extended Detection & Response (XDR)

Extended Detection and Response (XDR) is a cybersecurity approach that integrates and correlates data from multiple security layers (endpoints, networks, servers, and cloud) for better threat detection. It provides centralized visibility and automated response to quickly identify and mitigate advanced cyber threats.

70%
Faster Threat Detection

60%
Reduction in Alert Fatigue

80%
Faster Threat Containment

THE CHALLENGE

Top 5 Industry Challenges (If XDR is NOT Implemented)

- **Fragmented Security Visibility** - Organizations operate multiple security tools (EDR, SIEM, firewall, email security, IAM) in silos, making it difficult to correlate threats across the environment. This leads to missed attack indicators, delayed investigations, and higher breach impact across enterprise infrastructure.
- **Slow Threat Detection & Response** - Without centralized detection and automated correlation, SOC teams spend excessive time investigating alerts manually. This increases Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), leading to larger business disruptions.
- **Increased Risk of Advanced & Multi-Stage Attacks** - Modern ransomware and APT attacks move laterally across endpoints, identities, and networks before triggering payloads. Without cross-domain correlation, organizations struggle to detect attack chains early, increasing operational and financial damage.
- **Alert Fatigue & SOC Inefficiency** - Security teams face thousands of low-context alerts daily from disconnected security products. Analysts spend excessive time triaging false positives instead of focusing on high-priority threats, reducing SOC productivity.
- **Limited Incident Investigation & Threat Hunting** - Traditional tools provide isolated logs without complete attack timelines or contextual analytics. This restricts forensic investigations, proactive threat hunting, compliance reporting, and executive-level cyber risk visibility.

KEY BENEFITS

Faster Threat Detection & Response
XDR correlates endpoint, identity, network, email, and cloud telemetry into a unified detection engine. Organizations can reduce incident investigation time by 50–70% and significantly improve SOC response efficiency.

Improved Detection Accuracy
Behavioral analytics, UEBA, AI-driven correlation, and threat intelligence reduce false positives while improving detection fidelity. Many enterprises experience 40–60% fewer false alerts compared to isolated security monitoring tools.

Automated Containment of Threats
XDR enables automated actions such as host isolation, process termination, account disabling, and IOC blocking. This can reduce ransomware spread time from hours to minutes and minimize operational disruption.

Unified Security Operations
A centralized incident dashboard provides complete visibility across endpoints, users, networks, and cloud workloads. SOC teams can improve analyst productivity by 30–50% through consolidated workflows and automated investigations.

Stronger Cyber Resilience & Compliance Readiness
Continuous monitoring, forensic visibility, attack-chain reconstruction, and risk scoring improve regulatory compliance posture. This supports frameworks such as RBI Cyber Security Framework, SEBI Cyber Resilience Guidelines, DPDP Act, ISO 27001, and PCI-DSS.

KEY CAPABILITIES

One Unified Agent

01 Multi-Source Telemetry Ingestion

Endpoint & Identity Visibility

- Endpoint telemetry collection (processes, memory, registry, network)
- Active Directory log ingestion
- VPN access monitoring
- User authentication tracking

Network & Security Integration

- Firewall log ingestion
- DNS telemetry integration
- Proxy/Web gateway monitoring
- Email security integration

Cloud & Third-Party Integration

- Cloud workload telemetry ingestion
- SIEM integration
- DLP integration
- IAM/security stack interoperability
- Real-time and batch ingestion support

02 Cross-Domain Threat Correlation

Attack Chain Reconstruction

- Multi-stage attack correlation
- Endpoint + identity + network event stitching
- Lateral movement detection
- Kill-chain mapping

Threat Contextualization

- MITRE ATT&CK mapping
- Automated attack narratives
- Incident clustering & deduplication
- Risk-based incident scoring

03 Behavioral & AI-Based Detection

Advanced Analytics

- User & Entity Behavior Analytics (UEBA)
- Machine learning anomaly detection
- Time-sequenced behavioral analysis
- Baseline deviation monitoring

Insider & Advanced Threat Detection

- Rare process execution detection
- Rare authentication detection
- Insider threat behavior modeling
- Policy deviation detection

04 Network-Aware Threat Detection

Advanced Network Monitoring

- Command & Control (C2) beaconing detection
- DNS tunneling detection
- Suspicious encrypted traffic analysis
- East-west lateral traffic monitoring

Data Protection & Threat Prevention

- Data exfiltration detection
- Geo-location anomaly detection
- IP/domain reputation analysis
- VPN misuse detection

05 Threat Intelligence Integration

Intelligence Enrichment

- Global threat intelligence feed integration
- IOC ingestion (IP, Domain, URL, Hash)
- Automatic IOC enrichment
- Reputation-based correlation
- Open Standards & Sector Intelligence

Open Standards & Sector Intelligence

- STIX/TAXII support
- Financial sector-specific threat intelligence
- Dark web credential monitoring (optional)

06 Centralized Incident Management

SOC Operations Enablement

- Unified incident dashboard
- Case management workflows
- Alert prioritization
- SLA tracking

Investigation & Reporting

- Evidence aggregation
- Full forensic timelines
- Executive summary generation
- Incident escalation workflows

07 Automated Response & Orchestration

Automated Containment

- Endpoint isolation
- Process termination
- Enterprise-wide IOC blocking
- User account disabling

Security Automation

- Playbook automation
- Conditional response workflows
- Bulk containment actions
- Credential reset automation

08 Advanced Threat Hunting

Threat Hunting Capabilities

- Cross-domain query engine
- Historical telemetry search
- IOC-based retrospective hunting
- Suspicious authentication hunting

Custom Analytics

- Custom detection rule creation
- Scheduled hunting jobs
- Exportable hunting reports
- Data exfiltration hunting

09 Attack Visualization & Security Analytics

Attack Visibility

- Interactive attack graphs
- Multi-host attack timelines
- Endpoint-centric attack visualization
- User activity mapping

Enterprise Risk Analytics

- Risk heatmaps
- Department-wise risk scoring
- Branch-level security posture view
- Security trend analysis dashboards

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