CYBERSECURITY INNOVATIONS POWERED BY AI

SecureIT® EDR

Full-spectrum endpoint protection with complete data sovereignty — AI-driven detection, automated response.

98%
Threat detection accuracy across advanced attack scenarios

80%
Reduction in alert noise with AI-driven prioritization

24X7
Continuous endpoint monitoring & threat visibility

THE CHALLENGE

Indian enterprises face a threat landscape that legacy tools were not built for

- **CERT-In mandates 6-hour breach reporting** yet most organisations detect incidents in days, leaving them exposed to regulatory penalties under the DPDP Act and IT Act.
- **Ransomware and supply-chain** attacks are the fastest-growing threat vectors in India's BFSI, manufacturing, and government sectors — and they bypass signature-based defences entirely.
- **Data residency requirements under** RBI, SEBI, and IRDAI prohibit sending sensitive telemetry to foreign cloud infrastructure, disqualifying most global SaaS EDR vendors outright.
- **Lean IT teams** lack the 24/7 SOC capacity to triage thousands of daily alerts while maintaining a compliance posture and managing patch cycles simultaneously.
- **Alert fatigue and fragmented visibility** across endpoints, networks, and users prevent security teams from identifying real threats in time — resulting in delayed response, missed indicators of compromise, and increased dwell time for attackers within the environment.

KEY BENEFITS

- **Detect in minutes, not days**
  AI-driven behavioural engine surfaces threats before damage occurs
- **Meet CERT-In in 6 hours**
  Automated detection timelines and audit-ready incident reports
- **Full data sovereignty**
  On-prem or India-hosted deployment no telemetry leaves your boundary
- **One agent, everything covered**
  EPP + EDR + threat hunting in a single lightweight agent
- **Respond without a full SOC**
  Automated containment and guided response for lean IT teams

KEY CAPABILITIES

One Unified Agent

01 Detect & prevent

- Behavioural AI engine — detects less malware, living-off-the-land attacks and zero-days without signatures
- Static + dynamic analysis — pre-execution and runtime inspection of all types including scripts and macros
- Ransomware kill switch — detects encryption behaviour and halts execution within milliseconds
- MITRE ATT&CK mapping — every detection tagged to technique and tactic for SOC context
- USB & device control — granular peripheral policy per user, group, or endpoint

02 Investigate & hunt

- Attack timeline visualisation— full process tree and kill-chain view from initial access to impact
- Root cause analysis — automated pivot from alert to originating process, le, and user
- Threat hunting queries — pre-built and custom queries across 365-day telemetry retention
- Forensic snapshots — On-demand memory and disk capture for incident response
- IoC search — sweep entire estate for indicators of compromise in real time

03 Respond & contain

- One-click isolation — quarantine a compromised endpoint from the network without touching the host
- Remote shell (RTR) — live investigation and remediation from the console, no VPN required
- Automated playbooks — trigger containment, alert, and ticketing workflows on detection events
- File rollback — restore encrypted or deleted files from protected volume snapshots
- SIEM/SOAR integration — bidirectional API with Splunk, IBM QRadar, and leading SOAR platforms

04 Manage & comply

- CERT-In compliance dashboard — real-time posture view mapped to all 2023 CERT-In directives
- RBI / SEBI audit reports — scheduled PDF reports formatted for regulatory submission
- PDP Act data mapping — endpoint data classification and breach notification workflows
- Multi-tenant console — manage all business units or customer tenants from one pane of glass
- Role-based access control — granular analyst, admin, and read-only roles with full audit log

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