SecureIT®

Endpoint Detection & Response (EDR)

Overview

The Endpoint Detection & Response (EDR) platform provides real-time protection against modern cyber threats through a unified agent that combines next-generation antivirus, behavioral analytics, exploit prevention, and automated remediation. Built for enterprise environments, it delivers continuous monitoring, deep forensic visibility, and rapid containment of known, unknown, and file-less attacks. With centralized management, integrated device and application control, and powerful threat-hunting capabilities, the solution ensures strong on-premise security, high compliance, and complete visibility across all endpoints—while maintaining optimal system performance.

1. Advanced Endpoint Protection

Multi-Layer Malware & Ransomware Defense

- Protection against malware, ransomware, spyware, Trojans, bots, worms & unknown variants.
- Zero-day and file-less attack prevention using behavioral & exploit detection.
- Real-time scanning of files, network shares, email attachments, downloads & archives.
- Identifies malicious executables, compressed/embedded content & suspicious file behaviors.

Unified Lightweight EDR Agent

- Single agent for Anti-Malware, Anti-Ransomware, Exploit Prevention, Device Control, Application Control & EDR.
- Low resource footprint; optimized for performance.
- On-demand scanning with quarantine, delete and clean actions.

On-Premise Deployment

- Complete on-prem architecture with centralized visibility and policy control.

2. Device & Connectivity Control

USB & External Device Protection

- Allow/Block removable storage and peripheral devices based on policy or device ID.
- Block execution of untrusted/unsigned apps from USB.
- Monitor file transfers; automatic threat detection on USB insertion.
- USB tethering restriction for security-sensitive environments.

Wireless & Network Access Control

- Policy-based control of Wi-Fi, Bluetooth & network shares.
- Allow/Block network drives.
- MAC-based device authorization for added control.

3. Endpoint Detection & Response (EDR)

Deep Threat Detection & Forensics

- Advanced detection of kernel exploits, in-memory attacks, and malicious process behavior.
- Forensic snapshot creation for detailed investigation and root-cause analysis.

AI-Driven Investigation

- Automated alert correlation with evidence collection.
- Event prioritization and recommended remediation workflows.

Automated Threat Remediation

- Surgical remediation of threats including memory-based attacks.
- Rollback of malicious or unauthorized changes, including ransomware file recovery.
- Actions: kill process, stop service, isolate endpoint, deregister DLLs, initiate scans.

Proactive Threat Hunting

- IOC/IOA-based hunting across all endpoints.
- Visual process tree, activity history, registry & logon event tracking.
- Hunting for behavioral anomalies like PowerShell execution & abnormal process creation.

Enterprise Threat Intelligence Sharing

- Instant sharing of threat indicators and file reputations across the enterprise.
- Tracks infection origin and lateral movement paths.

4. Application Control & Exploit Prevention

Application Whitelisting/Blacklisting

- Whitelist DLLs, EXEs, scripts (VBS, BAT, Java, COM, SYS etc.).
- Block all unauthorized executables.

Application Integrity Protection

- Prevent tampering/hijacking of trusted applications & system components.
- Protects both disk and memory-resident code.

Exploit & Outbreak Prevention

- Detects exploit techniques and blocks malicious behavior patterns.
- Automated outbreak response based on threat thresholds.

Network Access Governance

- Classifies network activity of applications; blocks unauthorized communications.

5. Reputation-Based Security

File & Web Reputation

- Local and global reputation checks for files & URLs.
- Browser compatibility with Chrome, Edge & Firefox.

Hash-Based Execution Control

- Block or allow files based on hash (IoCs).
- Upload custom IoCs for SOC-driven enforcement.

6. Quarantine & Containment

- Centralized quarantine for suspicious files.
- Admin-driven review, analysis & cleanup actions.
- Automated outbreak containment for rapid response.

7. Centralized Management & Reporting

Unified EDR Management Console

- Single pane for policy, threat monitoring & endpoint management.
- Real-time device health and security posture.

Granular Policy Management

- Grouping by IP, AD, site, OS or department.
- Policy enforcement even when endpoints are offline.
- Unified deployment, updates & configuration.

Reporting, Alerts & Audit

- Reports in HTML, PDF, CSV & Excel formats.
- Dashboards for threats, risks, infected endpoints & compliance.
- Email/SNMP notifications for critical alerts.
- Comprehensive audit trail for admin & endpoint activities.

Log Collection & Integrations

- Centralized logs for device/application control & EDR events.
- SIEM integration via APIs for enhanced analytics & correlation.

8. Platform Compatibility & Support

Supported Platforms

- Windows 10/11, Windows Server 2016–2025.
- Major Linux distributions (32-bit & 64-bit).

Maintenance & Anti-Tamper

- Utility for clean agent uninstallation.
- Anti-tampering prevents unauthorized disable/uninstall.

VELOX SOLUTIONS • INTELLIGENCE THAT SECURES

Mail: bid@velox.co.in

Call: +91 8828297182 | +91 9321420943

Our Presence: India | USA | UK | Dubai | South Africa | Singapore | Indonesia