CYBERSECURITY INNOVATIONS POWERED BY AI

SecureIT®

Anti-APT

Anti-APT solution capabilities outlined in the attached datasheet, including network-wide threat detection, sandboxing, lateral movement detection, threat intelligence integration, Active Directory attack detection, and automated investigation capabilities.

90%
Reduction in successful advanced attack execution

70%
Faster threat detection by continuously rescanning traffic

60%
Reduction in incident investigation time through packet capture retention

THE CHALLENGE

Top 5 Industry Challenges (If ITOM is NOT Implemented)

- **Undetected Advanced Attacks** - Sophisticated attackers can remain hidden inside the network for months, silently stealing sensitive data, intellectual property, or customer information before being discovered.
- **Long Dwell Time of Threats** -The longer attackers remain undetected, the greater the financial damage, operational disruption, and regulatory exposure. Recovery costs can increase significantly over time.
- **Lateral Movement Across Infrastructure** - Once attackers compromise a single system, they can move across servers, endpoints, Active Directory, and critical assets without triggering traditional security controls.
- **Data Exfiltration & Ransomware Risk** - Organizations may suffer data theft, ransomware deployment, and business disruption, resulting in revenue loss, reputational damage, and customer distrust.
- **Slow Incident Investigation & Response** - Security teams lack the visibility and forensic evidence needed to understand attack paths, delaying containment and increasing business impact.

KEY BENEFITS

Early Detection of Advanced Threats
Detects both known and previously unknown attacks across the network, reducing breach exposure by up to 70–90%.

Reduced Threat Dwell Time
Continuous rescanning and threat intelligence updates help identify hidden threats significantly faster, reducing attacker presence from months to days.

Accelerated Incident Response
Detailed attack context, PCAP storage, and behavioral analysis can reduce investigation time by 50–70%.

Protection Against Zero-Day & Unknown Malware
Advanced sandboxing detects suspicious behavior beyond signatures, improving detection rates for emerging threats and evasive malware.

Enhanced Security Operations Efficiency
Automated detection, threat intelligence sharing, and integrated response capabilities reduce analyst workload by 40–60% while improving threat visibility.

KEY CAPABILITIES

One Unified Agent

01 Advanced Threat Detection

Multi-Layer Threat Identification
- Detects malware, exploits, hacking tools and suspicious behaviors
- Identifies social engineering-based attacks
- Detects policy violations and malicious activities
- Monitors attacker activity across the entire attack lifecycle

Known & Unknown Threat Detection
- Signature-based detection
- Behavioral analytics
- Reputation-based analysis
- Zero-day and unknown malware identification

02 Advanced Sandboxing

Malware Analysis Engine
- Executes suspicious files in an isolated sandbox environment
- Detects malware evasion techniques
- Analyzes malicious behavior patterns
- Supports multiple file formats

Customizable Sandbox
- Mimics customer endpoint environments
- Improves detection accuracy
- Reduces false positives

03 Network-Wide Visibility

Infrastructure Monitoring
- Perimeter security monitoring
- Internal network monitoring
- WAN visibility
- DMZ monitoring
- Server farm monitoring

Deep Traffic Inspection
- Inspection of 100+ protocols
- Up to 4 Gbps inter-VLAN traffic inspection
- Packet-level analysis
- Full session visibility

04 Lateral Movement Detection

East-West Traffic Monitoring
- Detects attacker movement within the network
- Tracks compromised accounts and systems
- Identifies privilege escalation attempts
- Agentless detection architecture

Active Directory Protection
- Detects attacks targeting Active Directory
- Identifies suspicious authentication activity
- Monitors credential abuse
- Detects domain compromise attempts

05 Threat Intelligence & Analytics

Threat Intelligence Integration
- Knowledge-base driven detection
- Continuous intelligence updates
- Threat intelligence sharing via REST APIs
- Custom threat intelligence import/export

Security Analytics
- Infection analysis
- Command & Control (C&C) detection
- Asset discovery
- Data discovery

06 Investigation & Forensics

Incident Investigation
- Stores raw network traffic
- Retains malicious communication PCAPs
- Malware behavioral records
- Session-level attack details

Reporting & Visibility
- Out-of-box security reports
- Threat dashboards
- Attack trend analysis
- Executive reporting

07 Automated Security Operations

Integrated Security Controls
- Automatic threat blocking
- Vulnerability protection
- Application control
- EDR integration
- Threat containment workflows

Security Automation
- SOC integration
- API-driven orchestration
- Automated intelligence sharing
- Incident workflow support.

08 Enterprise Deployment & Scalability

Platform Support
- Windows
- Linux/Unix
- macOS

Performance & Scale
- 65 parallel virtual analysis instances
- Up to 40,000 samples analyzed daily
- Scalable storage architecture (2 TB to 8 TB+)
- On-premises deployment with data residency

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