CYBERSECURITY INNOVATIONS POWERED BY AI

SecureIT®

Application Whitelisting

Zero-trust application control with cryptographic enforcement, real-time execution blocking, and 100% protection against unauthorized code, malware and ransomware across endpoints and critical systems.

90%
Reduction in Unauthorized Software Execution

60%
Faster Incident Containment

80%
Improvement in Endpoint Visibility

THE CHALLENGE

Top 5 Industry Challenges (if Application Whitelisting is NOT Implemented)

- **Increased Ransomware & Malware Exposure** - Unauthorized applications, scripts, and executables can run freely on endpoints, increasing the risk of ransomware outbreaks and malware persistence. A single infected endpoint can disrupt banking operations, ATM networks, manufacturing systems, or enterprise productivity, leading to massive downtime and recovery costs.
- **Lack of Endpoint Control & Software Governance** - Organizations struggle to identify which applications are running across endpoints, ATMs, servers, or remote systems. This creates shadow IT, policy violations, unlicensed software usage and uncontrolled attack surfaces that increase operational and compliance risks.
- **Higher Probability of Zero-Day & Fileless Attacks** - Traditional antivirus solutions primarily rely on signatures and known threat intelligence. Without whitelisting, unknown or zero-day executables may bypass defenses and execute malicious payloads before detection occurs.
- **Compliance & Audit Failures** - Industries such as BFSI, healthcare, and government require strict endpoint hardening and software execution control. Failure to implement application control can result in non-compliance with RBI, PCI-DSS, SWIFT, ISO 27001, and cybersecurity audit mandates.
- **Operational Downtime & Incident Response Costs** - Security teams spend excessive time investigating unauthorized applications, suspicious processes, and endpoint anomalies.

KEY BENEFITS

Prevents Unauthorized Application Execution
Only approved applications are allowed to run, drastically reducing malware, ransomware, and unauthorized software risks. Organizations can reduce endpoint attack surfaces by up to 70–90% in controlled environments.

Stronger Protection Against Zero-Day Threats
Whitelisting uses a “default deny” security model rather than relying only on known malware signatures.
This significantly improves protection against unknown executables, zero-day attacks, and fileless malware.

Centralized Policy Enforcement
Security administrators can deploy and enforce policies from a centralized console across thousands of endpoints or ATMs. This reduces policy management effort by nearly 50–60% compared to manual endpoint configuration.

Improved Compliance Readiness
Application control supports compliance with RBI, PCI-DSS, ISO 27001, SWIFT CSP, and internal security policies.
Audit preparation time can reduce by 30–40% due to better visibility, reporting, and policy traceability.

Reduced Downtime & Faster Incident Response
Blocking unauthorized executables proactively minimizes endpoint compromise incidents. Organizations can reduce malware-related downtime by 60–80% and improve incident response efficiency substantially.

KEY CAPABILITIES

One Unified Agent

01 Application Control & Execution Prevention

- Application whitelisting using SHA256 hash-based validation.
- Blocks unauthorized executables and scripts.
- Blacklisting support for known malicious applications.
- Default deny execution model.
- Real-time prevention of unknown applications.

02 Multi-Mode Security Operations

- Inactive Mode for monitoring/testing.
- Learning Mode to discover installed applications automatically.
- Protection Mode for strict enforcement and blocking.
- Progressive rollout capability for large enterprises.

03 Policy Management & Governance

- Centralized policy implementation.
- Base policy and update policy creation.
- Policy version control.
- Scheduled and on-demand policy push mechanisms.
- Role-based administrative control.

04 Endpoint & Platform Compatibility

- OS-independent deployment (Windows, Linux, Unix)
- Physical and virtual machine support.
- Offline endpoint enforcement capability.
- ATM endpoint compatibility.
- Remote branch endpoint coverage.

05 Monitoring, Reporting & Visibility

- Real-time dashboards for endpoint status monitoring.
- Policy compliance visibility.
- Alerts through email and SMS.
- Audit-ready reports in PDF, CSV, and Excel formats.
- Historical tracking of application activities.

06 Enterprise Integration & Automation

- SIEM integration support.
- ITSM integration capabilities.
- Active Directory integration for user mapping.
- Automated synchronization and policy deployment.
- Scalable architecture for large enterprise environments.

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

©2026 Velox Solutions Pvt. Ltd. All rights reserved. SecureIT, ScanPlus, BitSecure, AssetGrid, PlanetGuard, TrustShields, ScanX, and CodeTrust 360 are Products of Velox Solutions Pvt. Ltd.