CYBERSECURITY INNOVATIONS POWERED BY AI

ScanPlus®

ATM Terminal Security Solution (ATM-TSS)

Comprehensive ATM protection with cryptographic application whitelisting, full disk encryption, and RBI-compliant security enforcement against jackpotting and malware attacks.

70%
Reduction in Unmanaged Asset Exposure

60%
Faster Vulnerability Prioritization

75%
Better Visibility into Internet-Facing Risks

THE CHALLENGE

Top 5 Industry Challenges (if ATM-TSS is NOT Implemented))

- **Unauthorized USB & Peripheral Device Access** - Without endpoint and USB control, attackers or insiders can connect rogue devices to inject malware or extract sensitive data from ATM systems. This increases the risk of financial fraud, credential theft, and compromise of ATM network integrity.
- **Operational Downtime & Service Disruptions** - Lack of centralized monitoring and remote management causes delayed issue resolution and frequent ATM outages. Downtime directly impacts customer experience, transaction availability, and interchange revenue for financial institutions.
- **Weak Administrative & Access Controls** - Shared passwords, unmanaged admin privileges, and lack of time-based access create opportunities for unauthorized system changes. This leads to insider threats, configuration drift, and increased risk of security breaches across distributed ATM fleets.
- **Non-Compliance with Banking Security Regulations** - Banks and managed ATM service providers must comply with RBI, PCI-DSS, and cybersecurity audit requirements. Without centralized security enforcement, organizations face audit failures, compliance gaps, and increased operational risk exposure.

KEY BENEFITS

Real-Time Threat Prevention
Application whitelisting, sandboxing, USB protection, and OS policy management proactively block unauthorized applications and malware execution. This can reduce malware-related ATM incidents by up to 70–85% across distributed ATM environments.

Reduced ATM Downtime & Faster Resolution
Remote command execution and centralized screen management enable faster troubleshooting without physical site visits. Banks can reduce ATM downtime by 40–60% while improving service availability and operational efficiency.

Stronger Data & System Protection
Full Hard Disk Encryption (FHDE) secures sensitive ATM data even if physical devices are stolen or tampered with. This significantly lowers the risk of data exposure and supports regulatory compliance initiatives.

Improved Compliance & Audit Readiness
Centralized policy enforcement and controlled administrative access simplify compliance reporting and governance management. Organizations can reduce audit preparation effort by nearly 50% through automated policy monitoring.

Lower Operational Costs
A single-agent, centralized dashboard minimizes the need for multiple security tools and reduces field-engineer dependency. Banks and ATM operators can lower operational support costs by 25–40% annually.

KEY CAPABILITIES

One Unified Agent

01 Asset & Network Topology Management

Application Whitelisting

- Allows only approved applications to run on ATM terminals.
- Prevents unauthorized executables and malware attacks.
- Reduces attack surface significantly.

Blacklisting with Sandboxing

- Blocks known malicious applications.
- Sandboxes suspicious files for safe execution analysis.
- Enhances zero-day threat protection.

Auto Run Protection

- Prevents automatic execution of malicious files from removable devices.
- Protects against worm-based and USB-delivered malware.

02 Device & Endpoint Security

USB Protection

- Controls and restricts USB device usage.
- Prevents unauthorized data transfer and malware injection.
- Supports device-level access policies.

Full Hard Disk Encryption (FHDE)

- Encrypts ATM storage devices and sensitive financial data.
- Protects against data theft from stolen or compromised systems.
- Supports compliance requirements.

BIOS Password Management

- Secures BIOS-level configurations.
- Prevents unauthorized boot modifications and hardware tampering.
- Improves physical security posture.

03 Privileged Access & Policy Management

Time-Based Admin Access Management

- Provides temporary elevated privileges for authorized personnel.
- Eliminates permanent admin rights.
- Reduces insider threat exposure.

OS Policy Management

- Enforces centralized operating system security configurations.
- Maintains standardization across ATM fleets.
- Supports compliance and hardening initiatives.

04 Centralized Monitoring & Operations

Remote Screen Management

- Enables centralized visibility into ATM terminal activity.
- Helps troubleshoot issues remotely.
- Reduces field-service dependency.

Remote Run Command Execution

- Allows administrators to execute commands remotely.
- Speeds up incident response and operational maintenance.
- Improves patching and troubleshooting efficiency.

Content Distribution

- Centralized deployment of files, updates and configurations.
- Simplifies ATM software updates and policy rollouts.
- Ensures consistent security posture across branches.

05 Enterprise Security Management

Single-Agent Architecture

- Minimizes system overhead on ATM terminals.
- Simplifies deployment and maintenance.
- Reduces compatibility issues.

Centralized Dashboard

- Unified visibility for security, compliance, and operational monitoring.
- Faster incident correlation and management.
- Improves SOC and ATM operations efficiency.

Real-Time Monitoring

- Continuous visibility into ATM health and security events.
- Enables faster detection of suspicious activities.
- Improves incident response readiness.

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