CYBERSECURITY INNOVATIONS POWERED BY AI

ScanPlus®

ATM Online Patch Management

ATM Online Patch Management automates the deployment of security patches and software updates across ATM networks. It helps reduce vulnerabilities, improve compliance, and maintain operational security.

90%
Reduction in Manual Patching Effort

60%
Reduction in ATM Downtime

50%
Lower Incident Recovery Costs

THE CHALLENGE

Top 5 Industry Challenges (If ATM Online Patch Management is NOT Implemented)

- **Increased Exposure to ATM Malware & Cyberattacks** - Unpatched ATMs remain vulnerable to jackpotting, ransomware, OS exploits, and zero-day attacks targeting outdated Windows and third-party applications. This can result in financial fraud, service outages, regulatory penalties, and reputational damage for banks.
- **High Operational Costs Due to Manual Patch Deployment** - Without centralized remote patching, banks rely heavily on field engineers for ATM updates across geographically distributed locations. This increases travel, manpower, maintenance costs, and significantly delays security remediation timelines.
- **ATM Downtime & Customer Service Disruptions** - Manual or poorly coordinated patching often requires ATM shutdowns during business hours. Frequent downtime impacts transaction availability, customer trust, and directly affects transaction revenue.
- **Compliance & Audit Failures** - Banks operating unpatched ATM infrastructure struggle to meet RBI, PCI-DSS, SWIFT CSP, and cybersecurity compliance requirements. Lack of audit trails and patch visibility increases the risk of non-compliance penalties and failed security audits.
- **Inefficient Patch Delivery in Low-Bandwidth Locations** -Remote ATMs connected via VSAT, MPLS, or unstable WAN links face patch failures and incomplete deployments.This creates inconsistent security posture across ATM networks and increases operational risk exposure.

KEY BENEFITS

Centralized Remote Patch Deployment
Enables banks to deploy OS and third-party application patches from a centralized console across ATMs, CRMs, and kiosks. Can reduce manual patch deployment effort by 70–90% while improving rollout speed significantly.

Reduced ATM Downtime
Background patching and scheduled deployment windows ensure updates occur without interrupting ATM operations. Helps reduce ATM service downtime by 40–60% and improves customer transaction availability.

Faster Vulnerability Remediation
Critical security patches can be deployed immediately across distributed ATM infrastructure. This can reduce vulnerability exposure windows from weeks to just a few hours or days.

Optimized for Low-Bandwidth ATM Networks
Supports patch segmentation, resume capability, and lightweight bandwidth-aware transfers for VSAT/WAN environments. Can reduce patch transfer failures by 50–80% in remote branch and rural ATM deployments.

Improved Compliance & Audit Readiness
Provides centralized logs, dashboards, integrity validation, and audit-ready reporting in CSV/PDF/Excel formats. Helps improve compliance visibility and reduces audit preparation effort by 60–75%.

KEY CAPABILITIES

One Unified Agent

01 Centralized Patch Management

- Centralized server for patch deployment and monitoring.
- Unified dashboard for ATM patch visibility.
- Centralized control across ATMs, CRMs, and kiosks.
- Region-wise, branch-wise, and group-wise patch assignment.

02 Multi-Platform & OEM Support

- Supports Microsoft OS patching.
- Supports third-party application patching.
- Compatible with multiple ATM OEMs.
- Single integrated ATM patch management platform.

03 Intelligent Patch Deployment

- Immediate or scheduled patch deployment.
- Background patching without interrupting ATM operations.
- Define maintenance windows for non-disruptive updates.
- Pause, resume, or restart patch jobs dynamically.

04 Low-Bandwidth Optimization

- Operates efficiently on VSAT, WAN, MPLS, and low-speed links.
- Supports bandwidth throttling and custom bandwidth profiles.
- Patch segmentation and progressive download mechanism.
- Resume capability after network interruption or ATM restart.

05 Secure Patch Transfer Mechanism

- Encrypted TCP-based patch transfer.
- Cryptographic checksum validation.
- Integrity verification of transferred patches.
- Automatic packet reassembly and retry mechanisms.

06 Large-Scale File Transfer Capability

- Supports deployment from MBs to TB-scale patch packages.
- Simultaneous transfer → execution → application workflow.
- Lightweight 50KB agent optimized for low CPU/memory usage.

07 Monitoring, Reporting & Compliance

- Real-time patch deployment status dashboard.
- Audit trails, logs, and error reporting.
- Exportable reports in CSV, PDF, and Excel formats.
- Compliance-ready visibility for regulatory audits.

08 Reliability & Recovery Features

- Auto-download resume during network failure.
- Rollback support for failed patch deployment.
- Dynamic job recovery and re-execution.
- High reliability for remote ATM 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