Securing ATMs with Privileged Session Manager®

ATMs are computers with powerful system administrator passwords and are increasingly the subject of attack. CyberArk's Privileged Session Manager mitigates the security risks around these sensitive machines, while reducing operational costs and minimizing financial losses.

PSM logs each administrator connecting to the ATM on a named basis and provides detailed activity reports for managers and auditors.

Why CyberArk?

CyberArk is the trusted expert in stopping cyber attacks before they stop business.

The Challenge

Privileged (administrator) accounts exist on all IT systems. They are the most powerful accounts in an organization, with the ability to access the most sensitive data on a daily basis and pose devastating risks if abused. ATM machines are no different and with increasing reports of ATM hack attempts as well as insider misuse, knowing who accessed these machines and what was done on them is crucial. Today, any technical issue on ATMs is solved either by remote connection to the ATM machine or by physical arrival of a technician, often via a third party. The problem with remote management of ATMs is that they do not have a built-in system for securing and storing the passwords that access the ATM, with no personalization of who is using them, nor an audit trail of when and what they were used for. Similarly, the physical arrival of a technician implicates high operational costs, longer time to resolution and manual management of passwords and control, which often results in passwords rarely being changed and known to more people than actually required.

The Solution

CyberArk's Privileged Identity Management (PIM) suite has been implemented by 8 of the 10 largest banks in the world and major financial organizations. Privileged Session Manager (PSM), part of the PIM Suite, protects your most sensitive systems ensuring you have full visibility of who is accessing your systems and furthermore what they are doing with their privileged access. The benefits of PSM to secure ATMs include:

- **Automated password management.** Credentials are automatically changed based on predefined policies and stored in a highly secure Digital Vault, improving operational efficiency.
- **Full accountability and detailed reporting.** PSM logs each administrator connecting to the ATM on a named basis and provides detailed activity reports for managers and auditors.
- **Access control.** Enables segregation of duties (e.g. ATM technicians in the South-West can only access ATMs located in that region). Moreover, PSM streamlines business processes such as approval workflows or one-time access with automatic password replacement upon logout.
- **Secure single sign-on.** Users can remotely connect to ATMs without having to divulge the system's credentials reducing risk of losing control over sensitive passwords.
- **DVR-like playback.** All session activities are recorded and stored in a tamper-proof Vault.
- **Agentless installation.** PSM does not require any installation on the ATMs themselves thus reducing operational risks and overall total cost of ownership.
- **User-friendly web interface.** All users connect to the ATMs via a secure web portal ensuring quick time to resolution from anywhere, at anytime.
- **High Availability/Disater Recovery.** Ensure business continuity of ATMs with built-in redundancy for 99.9% availability.
- **Enterprise-ready.** Integrates with strong authentication systems (e.g. smartcards; fingerprints; biometrics etc) as well as enterprise directories, SIEM, ticketing systems and more.