NCR ATLEOS

Logical Security

15 rules to protect against logical attacks

NCR Atleos's security model takes a layered approach across multiple aspects of physical and logical security in order to provide coverage across all areas. Having the different layers and types of security in place ensures the maximum level of protection for multiple attack vectors to mitigate risk.

These principles apply regardless of operating system environment or vendor, although specifics of implementation may differ.

These guidelines are not optional. They are essential to protecting the ATM in today's environment.

Rule 1: BIOS security

- BIOS must be configured to boot only from the primary hard drive
- BIOS updates must be reviewed & tested before deployment
- Operations must be password protected
- UEFI Security Boot should be configured

Rule 2: Password management

- Change all default passwords
- Implement unique account passwords per ATM
- Change passwords every 90 days
- Enforce passwords of at least 14 characters using mixed character types
- Apply the maximum BIOS password complexity supported

Rule 4: Firewall

- Allow only authorised ATM connections
- Configure firewall rules by application, opening only the ports each program requires
- Block inbound connections by default
- Explicitly approve apps that require inbound access
- Use NCR Atleos Base/Enhanced OS Hardening guidance

Rule 6: Deploy anti-malware

- Use an allowlisting solution to block all unauthorised and unknown software
- Deploy anti-virus to detect & remove known malware
- Keep anti-virus signatures current and review scan reports regularly
- Run regular scans during low-usage periods
- Activate incident response procedures if malware is detected

Rule 3: Encryption

- Apply end-to-end encryption across entire ATM network
- TLS 1.2 with certificate pinning minimum (no SSL or early TLS)
- Never transmit unencrypted cardholder data
- Use secure certificates, ciphers, and authentication
- Consider cryptographic MAC-ing

Rule 5: Remove unused services & applications

- Follow the principle: **"If you don't use it, disable it"**
- Remove unnecessary software
- Regularly review & clean the software stack
- Block non-removable executables with allowlisting tools

Rule 7: Patching

- Regularly update all software with the latest security patches
- Prevent exposure to known vulnerabilities
- Apply Microsoft security updates to protect the ATM operating system
- Maintain PCI DSS alignment with vendor-supplied security patching

Rule 8: OS Hardening

- Lock down OS to essential functions only
- Disable auto-run from external media
- Use restricted user accounts
- Block unauthorised keyboard & input activity
- Restrict file, registry and device access
- Apply strict system policies & control

Rule 9: Role-based access control

- Restrict access to business need only
- Assign permissions based on specific user roles
- Limit access to only required functions per role
- Avoid remote desktop access
- Enforce multi-factor authentication (MFA) for remote access

Rule 10: Hard Disk Encryption

- Fully encrypt all disk drives
- Prevent access to data if the disk is removed, stolen or booted externally
- Ensure data remains unreadable and tamper-resistant
- Enable centralised key management & remote control
- Support secure data deletion (crypto-erase) where needed

Rule 11: ATM-dispenser communication

- Encrypt communication to prevent black box attacks
- Accept only authenticated commands from ATM software
- Set appropriate authentication levels
- Keep dispenser firmware & platformware software up to date
- Disable diagnostic and unauthorised configuration functions

Rule 12: Penetration test

- Conduct independent annual penetration testing to identify vulnerabilities, misconfigurations and weaknesses

Rule 13: Deploy software distribution tool

- Use secure software distribution to enable remote updates, patching and rapid malware response across the ATM estate

Rule 14: Consider the physical environment

- Deploy ATMs in secure locations with appropriate physical & network protection controls

Rule 15: Align with enterprise security best practices

- Apply enterprise-wide security controls to reduce risk and protect the ATM environment

A layered approach is essential to protecting ATM environments against logical threats which continue to evolve, including malware, DMA and man-in-the-middle. Each layer works with other to mitigate risk. By consistently applying these 15 rules, organisations can significantly strengthen resilience, prevent jackpotting instances, and maintain compliance.

They should not be considered optional, but rather critical to safeguarding ATM operations against monetary loss.