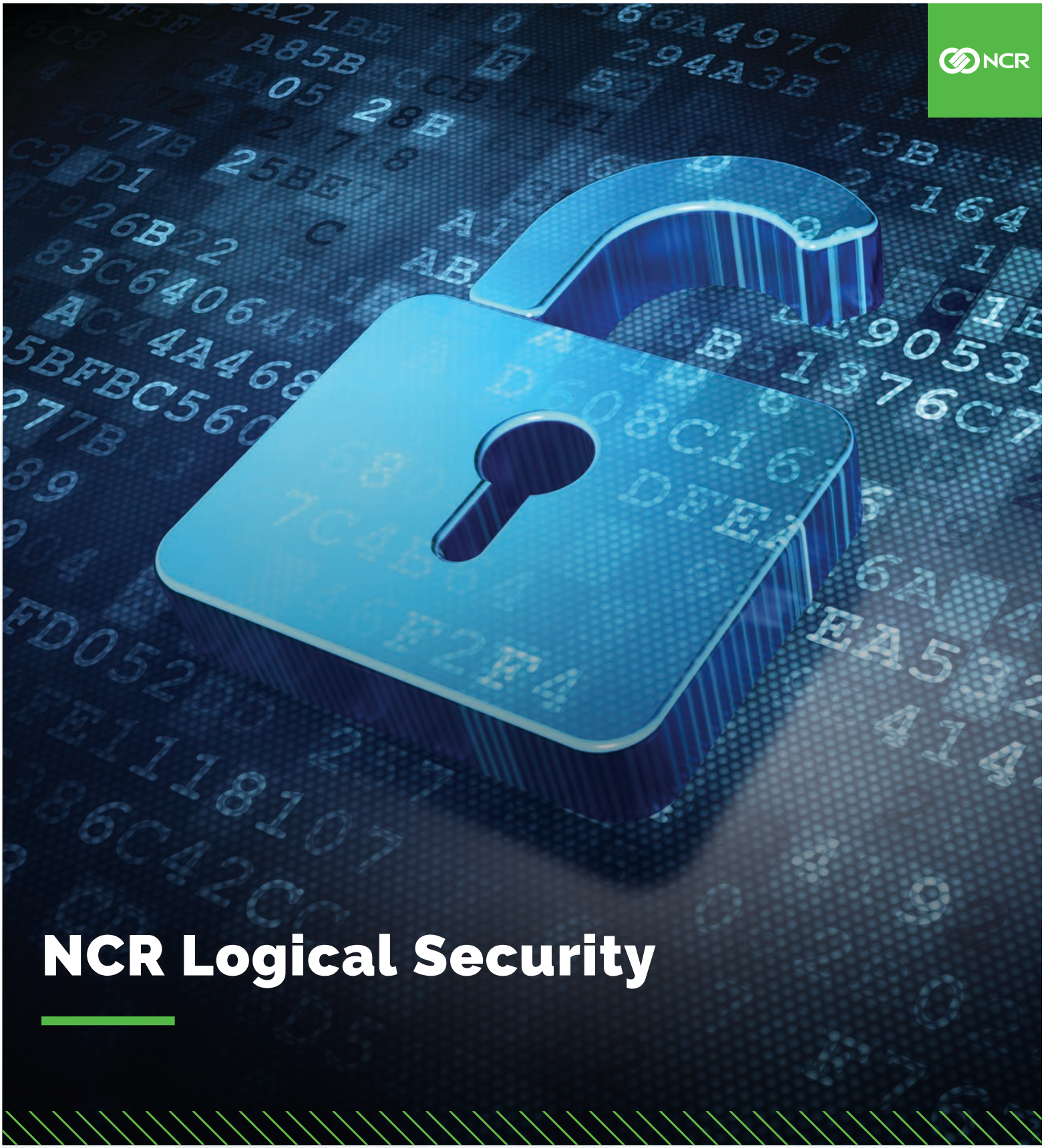


NCR Logical Security

Security requirements to help protect against logical attacks

An NCR Whitepaper

Introduction

For far too many years, to reduce costs, security has played a minor role in the purchasing decision of ATMs, but with the increase in criminal attacks on ATMs and pressure from industry bodies such as PCI and EMV, security and compliance is no longer an optional extra.

This document describes the primary activities required to be performed to maximise the security and integrity of an ATM estate.

NCR's security model defines a layered approach, this provides the best protection from a variety of attack vectors and having all the security layers in place maximises the security of your ATM estate.

NCR Secure Minimum Configuration

This paper defines the minimum security configuration requirements for an NCR ATM. The majority of the recommendations may also be relevant for other vendor ATMs.

This document defines the minimum security configuration requirements for an NCR ATM. The majority of the recommendations may also be relevant for other vendor ATM's.

All NCR ATM's MUST be configured as per the guidelines explained in this document. These minimum security requirements are necessary to defend/protect against currently known attacks on an ATM. All of the requirements provide protection to the different layers within the environment complementing each other to provide a secure holistic coverage across all the layers.

If one layer has a weakness, then the other layers will mitigate the risk of that weakness being exploited. If all the layers of protection are not applied then it may allow compromise of another layer.

The layered approach to security and the importance of having the layers is critical to preventing attacks on the ATM environment. These guidelines are not optional; they should be viewed as mandatory to protect your ATM in today's environment.

NCR Secure: Software Configuration and Implementation Guidelines

RULE 1: Secure the BIOS

The UEFI firmware/BIOS is a set of programs, typically in firmware (PROM, EEPROM or flash memory), that enables a computer's CPU to communicate with peripheral devices. The BIOS provides start-up Power-On Self-Test (POST) and then bootstraps the operating system on power-on or bus-reset. The BIOS consists of code (typically operating CPU in real mode) and configuration settings. The configuration settings are used to control the operation of the BIOS programs and also the hardware parameters that are exposed to the operating system.

Securing the BIOS is fundamental to the security of the ATM. Administration of the BIOS must adhere to the following principles:

- During normal operations, you should configure the BIOS to boot from the primary Hard Disk only. All other bootable mechanisms should be removed from the boot order
- BIOS updates must be reviewed and tested before deployment
- Editing of BIOS settings must be password protected
- UEFI Secure Boot, where at all possible, (Windows 10) to protect against boot vector attacks

To manually configure the ATM BIOS on your NCR ATMs, please contact your NCR Account Manager for a copy of Manually Securing the BIOS.

NCR recommends the use of Secure Boot and NCR SECURE Remote BIOS Update.

NCR SECURE Remote BIOS Update:

- Remotely, through software distribution, secures and updates the BIOS for most NCR cores
- Configures boot from primary Hard Disk only
- Sets a customer specific BIOS password
- Allows remote update of
  - ATM boot order
  - ATM BIOS Password

RULE 2: Establish An Adequate Operational Password Policy For All Passwords

It is up to each and every ATM deployer to ensure that they implement a secure user account and password policy. Banks should use an account management system that will allow them to manage accounts centrally, e.g., Microsoft Active Directory. Moreover, they should ensure that all passwords are secure.

- ALL default passwords MUST be changed
- User account passwords must be unique per ATM and per account. This provides maximum protection at each ATM, as a successful attack at one ATM cannot lead to a successful attack at another
- NCR recommends user passwords be at least 14 characters long and must not contain more than two consecutive characters from the user name
- User passwords should also be complex and must contain at least three of the following 4 categories
  - English uppercase alphabet characters (A-Z)
  - English lowercase alphabet characters (a-z)
  - Base 10 digits (0-9)
  - Non alphanumeric characters (for example !@#$%)
- User and Administrator account passwords must be changed every 90 days (as required for PCI DSS Certification)
- BIOS passwords are often limited by length and complexity. Nonetheless, BIOS passwords should be as complex as the BIOS allows.

RULE 3: Implement Communications Encryption

Transmission of sensitive cardholder data across ALL networks must be encrypted. Cyber criminals may be able to intercept transmissions of cardholder data over networks, so it is important to prevent their ability to view this data. Encryption is one technology that can be used to render transmitted data unreadable by any unauthorized person.

PCI DSS Requirement 4.1 states to use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission.

SSL and early TLS encryption have been shown to have weaknesses that can be exploited and must not be used as a security control to meet PCI requirements.

As a minimum the PCI DSS guidance below should be followed for migrating away from SSL and early TLS.

- Since June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place
- New implementations must not use SSL or early TLS as a security control
- Existing implementations must migrate to a secure TLS version (currently 1.1 or later)
- All use of SSL and early TLS as a security control must be stopped

NCR Secure TLS Encrypted Communications supports TLS version 1.2 and is stronger when combined with the environment hardening guidelines provided in this document.

Never send unencrypted cardholder data by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

NCR Recommends NCR Secure TLS Encrypted Communications, with MACing enabled for all message fields.

RULE 4: Install And Maintain A Firewall

The ATM firewall must be configured to only allow known, authorized incoming and outgoing connections necessary for an ATM environment; the connections must be configured per program rather than per port.

For example, the default configuration of the Windows 7 (and newer) firewalls blocks all incoming communication connections. Any applications that require incoming connections must be explicitly configured. All outgoing communications are allowed by default.

Detailed configuration options for the Windows firewalls and more are provided within **the NCR Base/Enhanced OS Hardening products**. For further information, please refer to the documentation for your firewall product.

RULE 5: Remove Unused Services And Applications

It is recommended that you remove any unused services and applications from the system to reduce the attack surface area. By adopting the principle of, "If you don't use it, disable it," you remove potential points of attack.

For example, if your application does not use output caching, you should disable the ASP.NET output cache module. Thereafter, if future security vulnerabilities are found in this module, your application is not vulnerable.

The following table lists **examples** of the recommended applications that should be removed from the ATM software stack if they are not used. However, you should review your software stack to determine if there are further binaries that can be removed:

Application	File Name	Description/ Purpose
Address Resolution Protocol	arp.exe	Display/edit network address
File Attribute	attrib.exe	Display/edit file attributes
File Transfer Protocol	ftp.exe	Transfer files between two hosts
NetBios over TCP/IP	nbtstat.exe	Display network information
Network Statistics	netstat.exe	Display network information
Name Server Lookup	nslookup.exe	Display network information
Remote Copy Program	rcp.exe	Copy files
Registry Editor	regedit.exe	Display/edit Windows registry
Registry Editor	regedt32.exe	Display/edit Windows registry
TCP/IP Route Command Application	route.exe	Display/edit network settings
Remote Shell Application	rsh.exe	Execute command on remote computer
Terminal Emulation Protocol	telnet.exe	Connect to a remote computer

RULE 6: Deploy An Effective Anti-Malware Mechanism

Anti-malware software will:

- Maintain the integrity of your ATM software stack and prevent malicious software compromising your ATM.

An effective white-listing solution will provide online protection beyond known malware threats. For example, memory protection, zero-day attacks and threat alerting.

NCR Recommends NCR Secure Solidcore Suite

NCR Secure Solidcore Suite:

- is more effective that anti-virus software alone in preventing known and unknown malware from executing.
- is an active whitelisting application for increased malware protection
- prevents execution of malware copied onto an environment
- prevents unauthorised software from execution
- alerts on execution of unauthorised software and malware.
- provides runtime memory protection
- protects against zero-day attacks, known, and unknown threats
- can evaluate its own status, and send alerts if its agent becomes disabled

To complement NCR Secure Solidcore Suite you should use a traditional reactive signature-based Anti-Virus (AV) solution to ensure any known malware copied onto your ATM is removed.

Major points to consider when deploying Anti Virus

- Anti-Virus only protects and cleans up known malware and is as effective as its last set of signatures, these signatures must be kept up to date
- Scan reports/logs must be reviewed regularly to determine if the ATM is infected or not
- AV should be run on a weekly basis on an ATM to detect if known malware exists

AV on an ATM should be configured to:

- Run in silent mode with no pop-ups
- Do not have the AV running in real-time mode, do not check log files too frequently because they are updated too often
- If the AV software is running in the background, consider process priorities
- Put the ATM out of service prior to scanning and run during quiet periods
- Update the signature files prior to running the scan

If NCR Secure Solidcore Suite Alerts or AV scan reports indicate malware has been found, best practice malware incident procedures must be followed, which may include the following:

- Containment and eradication of the malware is essential; it must be quarantined or deleted if possible
- Recovery of the ATM to restore normal functionality, the ATM should be reimaged, with a known master image
- Samples of the original hard disks must be removed for forensic analysis

RULE 7: Establish A Regular Patching Process For All Software Installed

Keep all software running on the ATM up to date with the latest NCR and other vendor security patches for all software. This ensures attackers don't take advantage of known vulnerabilities within the deployed software.

Weaknesses may allow malware to be installed onto the ATM or allow attackers access to the ATM software stack. If a vulnerability within the software stack has been addressed by a patch which has been installed onto the ATM, then it will no longer be exploitable.

Keeping up to date with Microsoft security hotfixes ensures attackers don't take advantage of known vulnerabilities within the operating system. The unpatched vulnerabilities may allow malware to be installed onto the ATM or allow attackers access to the ATM software stack.

NCR can provide a Managed Services offering that deploys Microsoft Windows hotfixes to your ATM estate on a quarterly basis.

PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met.

A substantial number of ATMs still run Windows 7, and support for Windows 7 from Microsoft ceased on the 14th January 2020. Migration away from windows 7 to a supported operating system such as Windows 10 must take place as soon as possible.

Without critical Windows security updates, your ATM may become vulnerable to harmful viruses, spyware and other malicious software, which can steal cardholder data or damage your business data and information.

RULE 8: Hardening The Windows Operating System (OS)

The Windows operating system must be hardened to restrict the privileges and behavior of the ATM to allow only the functions necessary for a self-service environment. This consists of setting up a locked down OS environment on a standalone ATM based on the following high level requirements:

- Disable Windows Auto-play
  - Auto-play is a feature of Windows operating systems, which allows software to run from removable media as soon as it is detected on a USB, DVD or CD. Disabling the auto-play feature within the operating system will prevent malware being automatically run when it is detected on removable media
- Implement a locked-down user account for automatically running self-service application functionality, with the minimum privileges and no interactive desktop access
- Implement a keyboard disabler to block keypresses being interpreted within the locked down account
- Apply file, folder and registry permissions to restrict the access the minimum required for the ATM to function
- Apply computer and user policies to restrict to the minimum functionality required for the ATM application to function correctly and securely

All the above configuration options and many more are provided within **NCR Secure Base OS Hardening and NCR Secure Enhanced OS Hardening**.

NCR Recommends NCR Secure Base (or Enhanced) OS Hardening

These protect the operational security of an ATM, creating a secure, locked down environment to protect the ATM's assets. The secure environment encompasses a comprehensive set of security features including: preventing the automatic running of programs on removable media, providing a locked down account for automatically running self-service functionality, controlling access to external devices and running of software, which effectively locks down the runtime environment of the ATM at the registry level. 500+ settings are automatically set when the software is installed in 'Secure Mode'. These settings are a balance between the minimum settings required to operate an ATM in a stand-alone environment,
and the industry-accepted system hardening standards. These include, but are not limited to:

- Center for Internet Security (CIS)
- Microsoft Windows Security Baseline using Security Compliance Toolkit
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards Technology (NIST)

RULE 9: Implement Role Based Access Control

The more people who have access to cardholder data environment, the greater risk there is that a consumers account will be used maliciously. Restricting access to those with a legitimate business reason for the access helps an organiszation prevent mishandling of cardholder data, and protect against ATM jackpotting

For all users accessing the ATM environment, their user account permissions should be based on the roles they have and they should be given only the access permissions required based on the role. For example, branch staff who need to change the printer paper needs only the level of privilege needed to effectively perform that assigned task. Once all roles and corresponding access needs are defined, individuals can be granted access accordingly.

Restrict functionality allowed via remote control desktop access to ATMs and if remote access is required then role based access control must also be implemented. PA-DSS requirement 10.1 must be enforced for that access which means multi-factor authentication with at least two of the methods below be used for all remote access to the payment application environment.

Authentication methods for all users:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

Payment application vendors must provide instructions for configuring the application to support multi-factor authentication.

NCR PA-DSS compliant applications provide guidance on how to meet this requirement.

RULE 10: Deploy A Remotely Authenticated Hard Disk Encryption Solution

Deploying full hard disk encryption protects the integrity of the ATM hard disk and offline attacks. This means the ATM is protected against:

- Malware attacks when the ATM hard disk is offline
- Attackers reverse engineering software on the ATM hard disk
- Attackers harvesting data from the ATM hard disk
- Hard disk being seen when ATM is booted from removable media
- Hard disk being removed from the ATM and mounted as a secondary drive
- The core is removed from the ATM

NCR Recommends NCR Secure Hard Disk Encryption

- Protects against attackers installing malware offline onto the ATM hard disk
- Renders the contents of the hard disk unreadable to protect against offline attacks, reverse engineering of code or data harvesting
- Provides a centralized encryption status of the ATMs being managed
- Prevents attackers deriving or harvesting the decryption keys locally to circumvent encryption technology
- Remote authentication prevents the encryption key being derived or harvested from the local hard disk.

RULE 11: Protect Communication Between The ATM Core And The Dispenser

Encrypting the communications between the ATM core and the dispenser will prevent black box attacks. If attackers attempt to send commands to the dispenser directly, the dispenser will recognize these commands as invalid. Only commands from the ATM software stack will be authenticated and processed by the dispenser.

NCR Recommends for NCR SelfServ ATMs

- Enable NCR Dispenser Software Security with Dispenser Protection Authentication Level set to Physical Authentication (Level 3) and set the appropriate authentication sequence
  - For S1 Dispensers set the Dispenser Authentication Sequence to Level 2
  - In high risk areas, or on high risk ATM models, set Dispenser Authentication Sequence to the highest level for both S1 and S2 dispensers
- Ensure the latest XFS Dispenser Security Updates are deployed and apply additional layers of protection, e.g., disable diagnostic dispense (for S1), disable SYSAPP configuration of settings.

RULE 12: Perform A Penetration Test Of Your ATM Annually

It is a best practice to have a penetration test performed on your ATM by an organization external to your company. It should be done against a full software stack, network access points and physically hardened environment per the recommendations in this document. At a minimum, follow the PA-DSS requirements for ensuring applications are not vulnerable to common coding vulnerabilities.

The test should comprise various simulated attacks in an attempt to find misconfiguration, weaknesses and vulnerabilities that could be exploited by an attacker in a production level ATM. The penetration test will allow you to identify any areas that need addressed to ensure your ATM is optimally secure.

RULE 13: Deploy A Software Distribution Tool That Will Assist In Maintaining The Confidentiality, Integrity And Availability Of Your ATMs

A software distribution capability with built-in security controls, role based account control, authorization and authentication is an essential layer that will help you maintain the confidentiality, integrity and availability of your ATMs.

To meet rule 7, it is essential to have remote software distribution capabilities.

If malware is found or suspected to be on an ATM, software distribution will expedite the clean-up and update malware signature files across an ATM estate. This will help put the ATMs into a more secure state, prevent attacks occurring and help limit damage to those ATMs that may be compromised.

NCR Recommends Vision Software Distribution

RULE 14: Consider The Physical Environment Of ATM Deployment

The physical environment that an ATM is deployed within and the ATM type will influence the risk of an ATM being attacks. Lobby ATMs (e.g. P77 or 6622) should not be deployed in 24/7 unattended environments without compensating physical security controls. A "through-the-Wall" ATM may be more suitable for these locations.

NCR Recommends:

Through-the-wall ATMS, which may be more suitable for unattended environments.

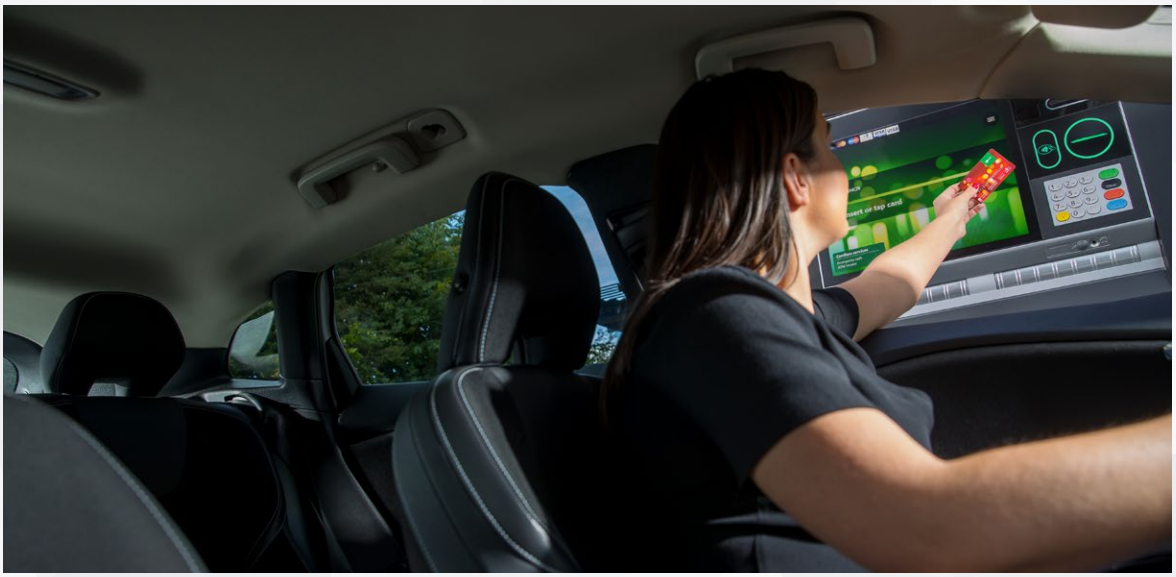
UL-rated, pick-resistant, Top Box locks SelfServ ATMs as a configuration option or upgrade kit with appropriate key management.

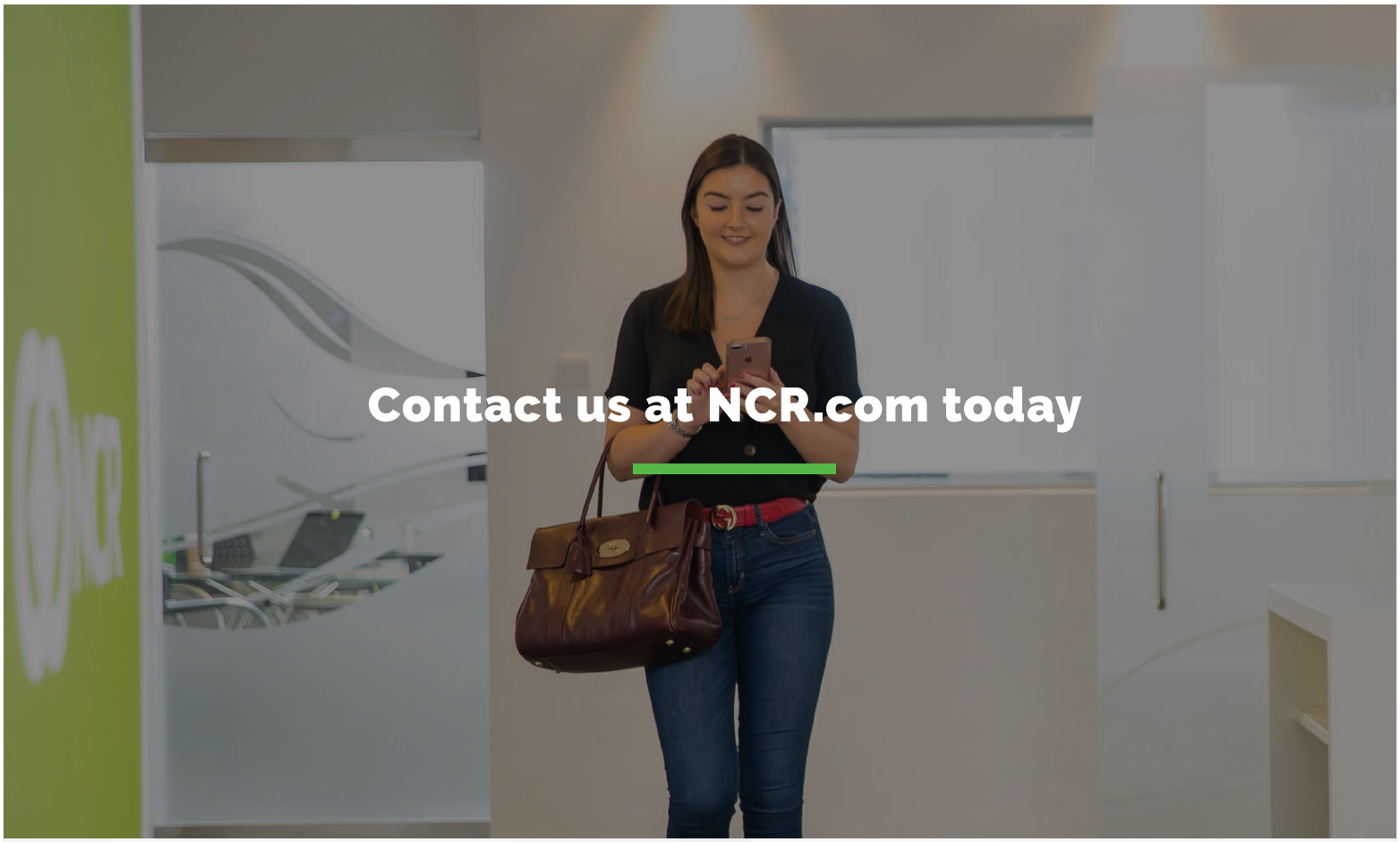
RULE 15: Consult An Enterprise Security Specialist To Assess And Deploy Industry Best-Practice Security Controls Within Your Enterprise

Ensure you follow industry best-practices within your wider organization to minimize the risk of a compromise occurring within your enterprise, for example:

- Security Awareness Training for employees to minimize the risk of spear phishing and other social engineering attacks
- A robust patching process is in place across the FI's enterprise
- Role-based access control
- Network Intrusion Detection/Prevention systems. Creating custom rules to detect and respond to unusual traffic behavior, e.g., block and alert on any ATM to ATM traffic
- Network Access Control for endpoint authentication to only allow authorized authenticated devices (ATMs) and applications access to the network and services.

NOTE: These are just examples. Your enterprise security specialist should advise on best-practice controls.





Contact us at NCR.com today

Why NCR?

NCR Corporation (NYSE: NCR) is a leading software and services-led enterprise provider in the financial, retail, hospitality, small business and telecom and technology industries. We run key aspects of our clients' business so they can focus on what they do best. NCR is headquartered in Atlanta, Ga., with 34,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.