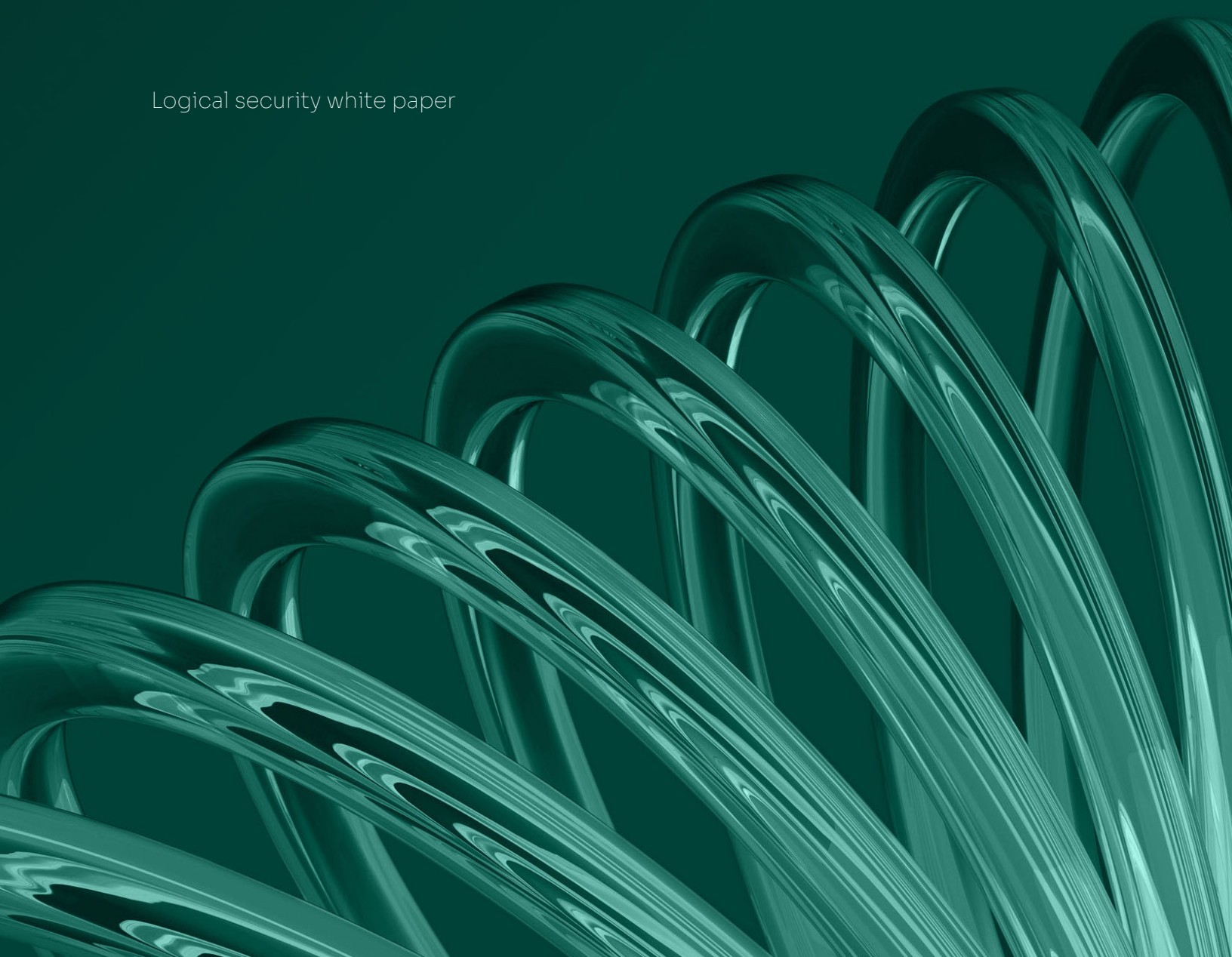


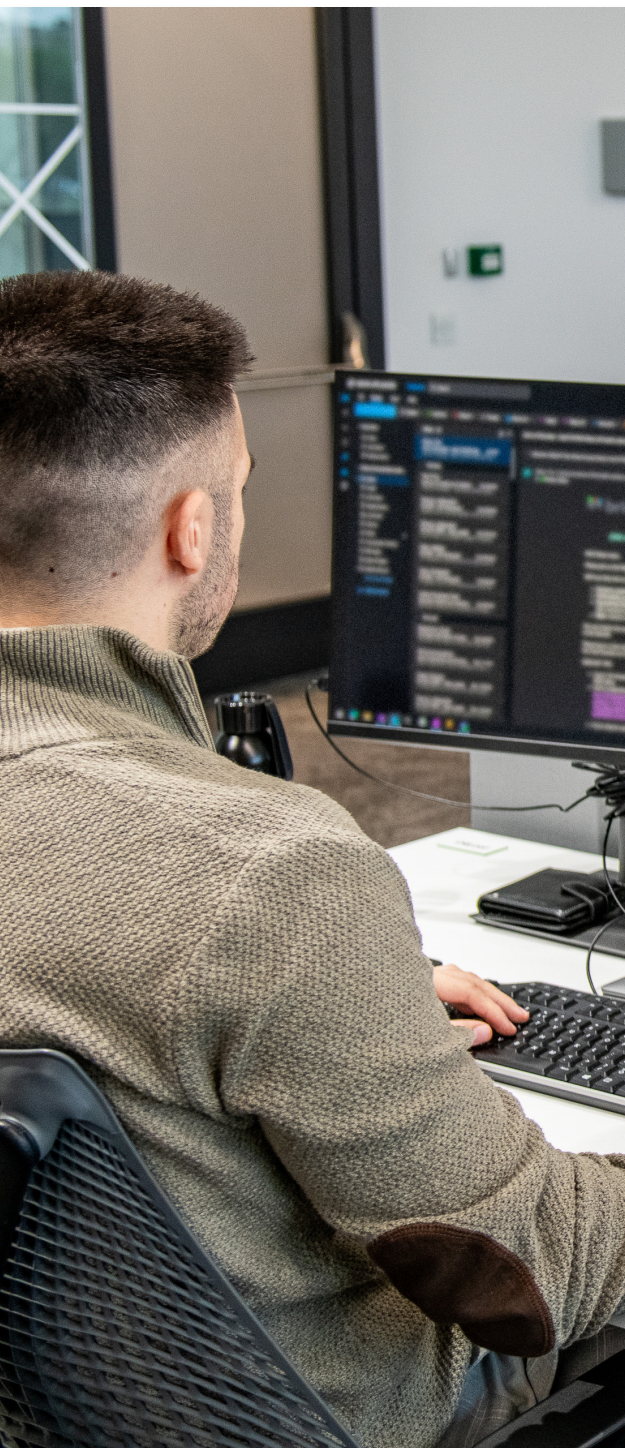


Best practices for password management

Securing your ATM network and
protecting your investment

Logical security white paper





Introduction

While traditional physical attack vectors are a significant and material threat to ATM operators, financial institutions (FIs) are continuing to see “logical” attacks—cyberattacks that exploit vulnerabilities in software, systems or network protocols to gain unauthorized access or cause harm—as a threat.

These threats often include the use of electronic devices or malware to trigger an unauthorized cash dispense from the ATM. And such threats are growing, with the FBI and the US National Vulnerability Database (NVD) reporting significant yearly increases in ATM crime. Europol, as well, has published clear guidance on mitigating the risk of ATM logical and malware attacks as these attacks increase.

Europol also recognizes that logical attacks have become big business. Its European Cybercrime Centre’s annual report, Internet Organized Crime Threat Assessment (IOCTA), takes an in-depth look at the online criminal ecosystem, with key findings and emerging threats and developments in cybercrime.

As more and more reports of cyber-attacks hit the headlines every day, deploying robust, intelligent and proactive software and network security measures should be a top priority for every FI.

This white paper outlines password management techniques that can help. It expands upon password policies outlined in our white paper on 15 rules for logical security, in which we stressed the importance of ensuring a well-defined password policy as part of our layered approach to logical security. Here, we’ll go into more detail about BIOS and Windows password management—and about the risks of doing nothing.

P@ssw0rd is not more secure than password

Passwords are everywhere. They are fundamental to ensuring against security breaches as part of the digital age. But industry advice can be conflicting. Strong password guidance is widely defined and has been clear for some time. Passwords must include a mix of upper and lower case, be a mix of numbers and letters and include a special character. While these policies are still true today, Splashdata compiled a “most popular password of the year” list and concluded that “123456” and “password” remain the top two most used passwords. So, we have a problem. We know that robust passwords are a must, but as we try to adhere to this, password hygiene becomes a bigger issue. As we make passwords more complex, there becomes a need to catalogue our multiple passwords somewhere, which in turn brings the risk of compromise.



Password fatigue—it’s a thing!

Continually having to create and keep track of an ever-growing number of passwords has led to two common trends: writing down and re-using passwords. When we consider the powerful computer programs that hackers use to reveal passwords, we’re back to the threat of an attack. If you add in the need to reset passwords periodically, it’s no surprise that people resort to shortcuts.

The impact of doing nothing

Doing nothing is not a realistic option. Not only would it increase the risk of exposure to ransom attacks and the accompanying financial impact, but brand reputation is also at stake too. We know BIOS and Windows admin default passwords become widely known, and yet many FIs often don’t update them—leaving themselves at risk and open to attacks. If customers perceive that a FI is giving security less of a priority across their ATM channel or taking fewer precautionary measures, they tend to lose trust and take their financial business elsewhere.



Taking the proactive approach

So how do FIs ensure they are taking the right security approach for their network and their customers? The best approach is to establish an adequate operational password policy for all passwords. We recommend using an account management system such as Microsoft Active Directory to manage accounts centrally. We also recommend these guidelines:

- ALL default passwords MUST be changed as per PCI 4.0 requirement 2.2.
- User account passwords must be unique per ATM and per account. This gives maximum protection at each ATM, as a successful attack at one ATM cannot then lead to a successful attack at another ATM.
- User passwords should be at least 14 characters long and must not contain more than two consecutive characters from the username.
- User passwords must contain at least three of the following four features:
 - English uppercase alphabet characters (A-Z)
 - English lowercase alphabet characters (a-z)

- Base 10 digits (0-9)
- Non-alphanumeric (“special”) characters (e.g. !@#\$%)
- User and administrator account passwords must be changed a minimum of every 90 days as required by PCI DSS 4.0 requirement 8.3
- BIOS passwords are often limited by length and complexity. Nonetheless, BIOS passwords should be as complex as the BIOS allows. NCR Atleos has solutions designed to maximize the security of BIOS passwords.

Implementing a password manager

Implementing a password manager for both BIOS and Windows® passwords should be the first step. Password managers can create and facilitate robust and varied passwords; by implementing them, FIs can put their IT management team back in control of securing their ATM networks.

How NCR Atleos can help

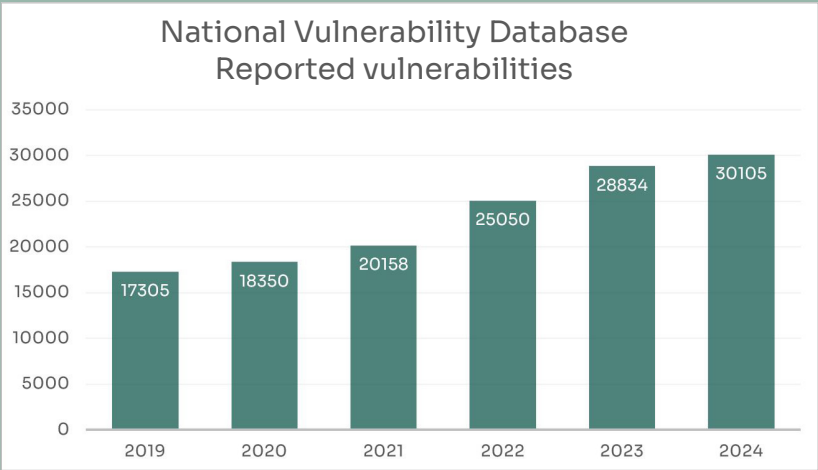
NCR Atleos is uniquely positioned to help FIs efficiently implement the guidelines we have shared here. As the owner and operator of the world’s largest ATM network, we have a unique perspective on the global ATM threat environment and security best practices to combat them. These security capabilities are available to our customers as part of our industry-leading ATM as a Service.

Security is deeply integrated into our standardized software platform. This approach includes data, application, host, network and perimeter defence solutions that operate over and above OEM (original equipment manufacturer) software. The NCR Atleos security platform is built on the strongest technology including advanced cyber intelligence and forensic research. Our operating model addresses information security as a global independent function and includes strategies to prevent large-scale data loss.

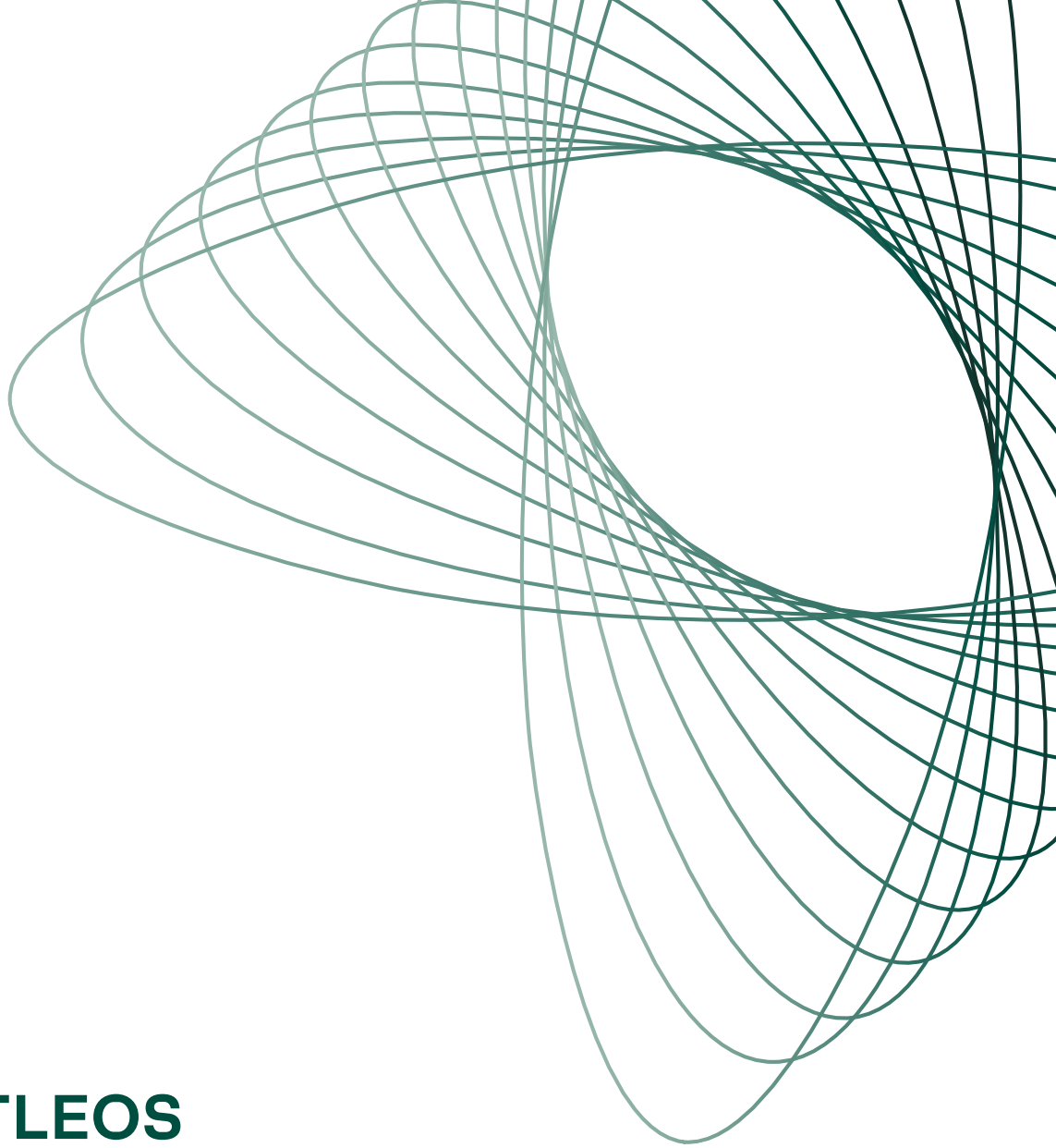
We invest millions of dollars each year and dedicate significant resources to maintaining the highest levels of channel security. Our security teams are in regular contact with law enforcement officials and industry bodies at all levels around the world to proactively engage and thwart emerging threats.

As a result, we can enable our FI customers to offer their own customers industry-leading device availability in a highly secure environment.

To learn more, visit [Endpoint Security Software | NCR Atleos](#)



Source: NIST-National Vulnerability Database



NCR ATLEOS

Contact us at [NCRAtleos.com](https://ncratleos.com) today

NCR Atleos (NYSE: NATL) is a leader in expanding self-service financial access, with industry-leading ATM expertise and experience, unrivalled operational scale including the largest independently-owned ATM network, always-on global services and constant innovation. NCR Atleos improves operational efficiency for financial institutions, drives footfall for retailers and enables digital-first financial self-service experiences for consumers. NCR Atleos is headquartered in Atlanta, Georgia, with 20,000 employees globally.

For more information check out our website
Endpoint Security Software | NCR Atleos

NCR Atleos Corporation

864 Spring St NW

Atlanta, GA 30308

© 2024 NCR Atleos Corporation

ncratleos.com