rf IDEAS

Secure Your Print Environment With WAVE ID® Secure Authentication Readers

WAVE ID® Desktop Mini

WAVE ID® Bio

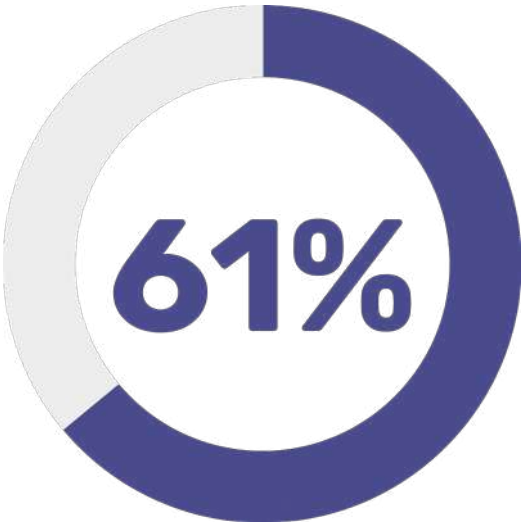
WAVE ID® Mobile Mini

Secure print for a safer network

In 2023, **61%** of organizations experienced data losses related to unsecured printing practices.[1] Printers are often overlooked as a security vulnerability. But with the increasing sophistication of cyberthreats, printers have become potential entry points that must be addressed.

Secure print solutions prevent unauthorized users from accessing network-connected devices and multi-function printers (MFPs). By ensuring that only authorized personnel can release print jobs, these solutions reduce potential data breaches and maintain compliance with regulatory requirements.

With secure print, a contactless credential reader reads an employee's ID badge or mobile credential and securely passes its cryptographic keys to your network's authentication solution. By implementing secure print solutions, your organization can safeguard its data, minimize the risk of data breaches and regain control over your printing environment.



of organizations experienced data losses related to unsecured printing practices in 2023[1]

Why does your organization need secure print?

Secure print offers numerous advantages that not only protect your organization from breaches but also help you avoid regulatory fines, save on printing costs and protect sensitive data. Consider the potential vulnerabilities in your current printer setup — hidden security gaps and inefficiencies could expose your organization to significant risks.

Secure access to network-connected devices

The Cybersecurity & Infrastructure Security Agency (CISA) highlighted the critical nature of print spooler service vulnerabilities in Emergency Directive (ED) 21-04, warning that cyberattacks can exploit these weaknesses to remotely execute code, quickly compromising an organization's infrastructure.[2]

Left unprotected, printers can become a major security vulnerability and prime target for cyberattacks. Securing access to network-connected print devices is essential for preventing unwanted access to your company's network, which can result in malware attacks, data loss, data theft, financial loss and intellectual property loss. Implement secure print solutions to ensure only authorized personnel can release print jobs, safeguard critical information and maintain network security.

Protect sensitive document types

Properly classifying your workforce's ability to reproduce or print documents based on content sensitivity can prevent data breaches. To begin, conduct a document type inventory to discover how many sensitive document types your organization has and where they reside. For example, documents containing personally identifiable information (PII) or confidential business data should be classified accordingly to guarantee they receive the right level of protection.

If your organization handles a high volume of sensitive documents, implementing secure print solutions helps prevent unauthorized access and maintain privacy and compliance with relevant regulations.

Comply with regulations

Do your current printing practices comply with regulatory standards? Depending on your organization's industry and geographic location, regulatory mandates may require stricter control over how sensitive information is handled and printed.

Secure print solutions help organizations comply with mandates by ensuring that sensitive documents are only printed when authorized personnel are present to release the print job. For example, secure print helps healthcare organizations manage patient privacy to comply with HIPAA. For businesses operating in Europe, secure print plays a crucial role in upholding data protection and privacy in accordance with GDPR.

Non-compliance with these regulations can result in significant fines and legal consequences, so you need to consider which regulations apply to your organization and whether your printers meet security standards.

To maintain compliance, adopt a Zero Trust approach — meaning your organization should never automatically trust anything or anyone connected to its systems. This involves deploying identity and access management (IAM) controls and requires continuous verification of identities and access rights, regardless of location within or outside the network.

Reduce printer waste

The cost of printing can quickly add up for organizations. Without authentication measures at the printer, many print jobs may never get picked up. Additionally, paper accounts for **23%** of total municipal solid waste generation,[3] and the pulp and paper sector was responsible for about **2%** of all industrial emissions in 2022.[4]

To unlock cost savings and reduce environmental impact, monitor your organization's printer usage to estimate the percentage of waste and its associated costs. Discover how much paper waste your organization produces to help you make a business case for adopting a secure print solution. By controlling who can print and what they can print, you can minimize unnecessary printing and reduce paper waste.

How to implement secure print

Secure print implementation is easier than you might expect. Follow these steps to secure your organization's print environment and protect sensitive information.

Fleet assessment

The first step in implementing secure print solutions is to assess your current printer fleet. Evaluate the number of print devices your organization has in operation, as well as their makes and models. Consider whether your print fleet operates locally or needs to be deployed across a global, distributed environment. This distinction may impact your choice of print OEM partner and software partner, as a global deployment requires support in all regions.

Next, it's important to know the age of your devices. Older devices may lack the firmware capability to support onboard software agents required for secure print. Additionally, some print devices may not have the front panel monitors required to display a list of print jobs in a person's queue to manage secure print release. If your devices are more than five years old, consider updating your fleet to ensure compatibility with modern secure print solutions.

Make note of workgroup MFP devices and how many workers are utilizing each device. This information will provide insight into the workload distribution and efficiency of your printers. You should also be aware that multi-vendor fleets may have fewer options available from a print management selection perspective. Lastly, understand which print devices require readers to support secure release. Performing a thorough assessment covering all of these points can help define what solutions are most compatible with your current print deployment.

Credential assessment

To identify the right reader for your organization, assess your current credential strategy, including any existing credentials and the software used. In cases where organizations are merging, undergoing acquisitions or transitioning to more secure credentials, the selected reader may need to support at least two credential types for the short term. For example, organizations using basic credentials like HID Prox cards may require a different card reader for secure print than those using more secure credentials. Fortunately, rf IDEAS has readers that can support four different credentials at any one time.

Additionally, consider whether mobile credentials might be a good fit for your organization. These tools are growing in popularity because they offer greater convenience, flexibility and enhanced security features, enabling employees to use their smartphones for secure access.

Software assessment

A number of considerations influence the type of secure print software your organization will select and deploy, including operating systems, virtual desktop requirements, network security, provisioning software and hosting requirements. Additionally, the type of secure print application software used will help determine the readers and configurations needed to ensure compatibility and a seamless deployment.

To ensure success, identify and document interoperability and dependency requirements as your network and supporting software evolve over time. When assessing software, consider if your OEM printer has its own available print management software or if you need to source a third-party, print-managed services partner. rf IDEAS works with a network of secure print-managed solution partners including NT-Ware, PaperCut, myQ, HP Advance, Pharos, Vasion and others.

Organizations remain dependent on printing

of organizations say printing will be very important or critical to their business in the next 12 months[5]

Technical considerations

It's important to carefully evaluate the technical details of your secure print solution before deployment. First, evaluate your existing access control systems and ensure compatibility with third-party readers and credentials. Identify any specific credential requirements for your project, as readers may need configuration, particularly if encrypted credentials are being used.

Next, consider the deployment environment, especially for global implementations, to assess risks like credential duplication. Additionally, conduct a risk assessment to understand regulatory compliance, IT security needs and the level of risk your organization is willing to undertake. This should include factors like geographic location and the number of deployment sites.

Remote reader management utility software

Consider whether remote reader management is right for your organization. Remote reader management allows administrators to manage and monitor credential readers from a centralized, remote location. This is particularly useful for organizations with multiple locations or a large number of devices.

With remote reader management, your IT teams can update firmware, configure settings and troubleshoot issues without needing to be physically present at each device. rf IDEAS has developed remote reader management capabilities, customized to work with leading print OEMs, for seamless firmware and configuration updates. However, it's important to note that some corporate environments may restrict the use of local reader management utilities on PCs within secure environments or may not permit access to cloud-based remote reader management solutions. In such cases, secure configuration cards may be required. rf IDEAS can assist in providing these.

5 reasons to choose rf IDEAS

It's estimated that less than **2%** of business printers are secure.[6] But adopting WAVE ID® readers can significantly enhance the security of your print environment, protecting sensitive information and maintaining compliance with regulatory requirements. Here's why rf IDEAS stands out:

1. Wide range of credential support

rf IDEAS' WAVE ID readers support a wide range of credentials including prox cards, smart cards, mobile credentials, biometric and passkeys. They are available in a variety of form factors from our slim profile reader to OEM embedded options, allowing them to securely and seamlessly integrate into any workspace. Additionally, rf IDEAS has long-standing relationships with print OEM manufacturers such as HP, Ricoh, Xerox, Toshiba, Kyocera and Canon/NT-Ware to enable seamless integration.

2. Proven experience and compatibility

With 30 years of experience supporting access control and credential providers, rf IDEAS ensures that WAVE ID readers work with your existing security infrastructure, the credentials your employees currently use for physical access and emerging credentials like passkeys.

Global Trusted Secure Print Partnerships

hp
TOSHIBA
xerox
RICOH
NTware

3. Consultation and custom solutions

For organizations without existing credential systems, rf IDEAS provides consultation and ultimately solutions for deploying cost-effective card or mobile credentials, securely protecting all devices and data.

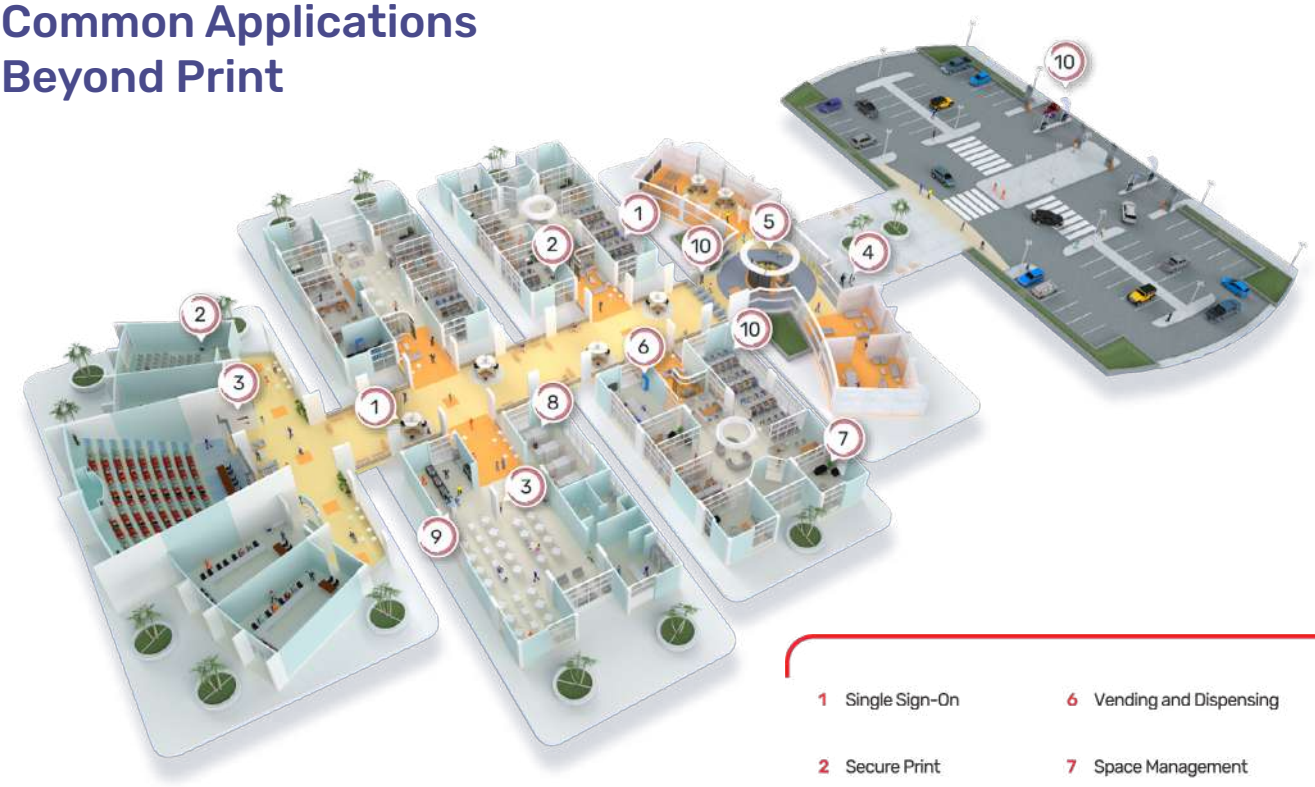
4. Seamless migration and future-proofing

rf IDEAS can assist organizations in the migration from less secure options such as magnetic stripe cards and PIN-based systems to secure credentials such as smart cards and mobile credentials. Many of our newer solutions are “future proof” and can evolve as your credential strategies scale or your needs change.

5. Extending secure authentication

Secure print is just the beginning. Once implemented, your organization can extend secure authentication to other parts of the enterprise, such as logical access control, multi-factor authentication (MFA) and single sign-on (SSO). These solutions help organizations implement Zero Trust security policies, ensuring only authorized users can access critical systems and data.

Common Applications Beyond Print



1 Single Sign-On
2 Secure Print
3 Time and Attendance
4 Mustering
5 Visitor Management
6 Vending and Dispensing
7 Space Management
8 Employee Lockers
9 Cashless Cafeteria
10 Embedded Authentication

Your Secure Print Questions Answered

What are the benefits of using a physical or mobile credential with WAVE ID readers?

rf IDEAS readers support FIDO2[6], enabling seamless and phishing-resistant passwordless authentication while reducing risks associated with lost or stolen passwords. Our readers also save on administrative costs for password resets, leverage existing physical credentials and support NFC mobile wallets for user convenience and flexibility.

How much does it cost to enable secure print?

The cost of enabling secure print varies depending on several factors, including the brand, deployment size and expectations or requirements of the solution. Excluding the reader itself or the purchase of credentials, the software costs can range from monthly fees per device to a one-time capital investment. This depends on your organization's requirements and desired features, such as project or group-based tracking and job logs for audit control.

What type of mobile credentials does rf IDEAS support?

rf IDEAS supports a growing range of mobile credentials, including unmanaged BLE, managed BLE and NFC wallet credentials on both iOS and Android smartphones. Explore the full range of mobile credential access compatibility[7] for WAVE ID.

Get in touch with rf IDEAS today to learn more about how secure print solutions can fortify your cyberdefenses.

rf IDEAS

425 N Martingale Rd, Suite 1680
Schaumburg, IL 60173

1-866-492-8231
Email: sales@rfIDEAS.com // rfIDEAS.com

1. https://quocirca.com/quocirca-print-security-landscape-2023-press-release/
2. https://www.cisa.gov/news-events/directives/ed-21-04-mitigate-windows-print-spooler-service-vulnerability
3. https://www.epa.gov/facts-and-figures-about-materials-waste-and-recycling/paper-and-paperboard-material-specific-data
4. https://www.iea.org/energy-system/industry/paper
5. https://quocirca.com/quocirca-print-security-landscape-2024/
6. https://www.rfideas.com/about-us/blog/fido2-standard-promises-eliminate-risk-passwords
7. https://www.rfideas.com/sites/default/files/2024-07/rf-ideas-wave-id-mobile-credential-offering-overview-b-803-a.pdf