Secure printing: The foundation of multi-layered security

Sponsored by ELATEC, October 2023

QUOCIRCA

Market context

The hybrid work environment has expanded the exploitable attack surface, and multiple layers of security are required to protect it from external and internal threats. Implementing secure print solutions is an easy way to ensure neither network data nor printed documents fall into the wrong hands. RFID readers and mobile authentication technology solutions help organisations implement secure print policies and seamlessly enable user authentication across multiple identification platforms.

Businesses of all sizes are facing a rising tsunami of cybersecurity risks. In today's cloud- and AI-driven hybrid work era, the threat landscape is complex and constantly evolving, with new, more sophisticated cyber threats emerging daily – whether these involve malware, phishing, or ransomware attacks. Meanwhile, security teams are dealing with a whole new raft of security threats, misconfigured access points, weak passwords, lack of identity and access management (IAM), and failure to use multi-factor authentication.

Quocirca's Print Security Landscape, 2023 report reveals that the volume of overall security incidents has increased in the past year for 61% of organisations, rising to 70% in the US and 66% in business and professional services organisations. Yet, just 38% of organisations use a secure print solution (such as pull-printing) to ensure documents are only released to authorised users.

The impact of a data breach can be severe, if not catastrophic. With end points representing the most common attack vector and cyber-attacks continuing to grow in sophistication, organisations are finding it harder to detect and defend against cybersecurity threats. Meanwhile, the most common threat is from insiders – with the majority of data breaches caused by human error.

'Just 38% of organisations use secure printing to release documents to authenticated users.'

Print security is non-negotiable

Today's smart MFPs have several points of vulnerability – in addition to the printed output that can fall into the wrong hands without the right controls, devices can be attacked and become access points to the wider network.

However, for many organisations, securing a diverse printer fleet that may include multiple brands, legacy devices, and a patchwork of software and drivers can be challenging. The risk is exacerbated in today's distributed hybrid work environments, where MFPs are shared among more users, sometimes in settings that involve more than one company or are away from standard controllable locations, such as in an employee's home.

Meanwhile, a multi-vendor environment may not incorporate consistent security controls, and a fragmented approach to cloud printing may create further security risks around access and authentication. Similarly, organisations may already have access token systems in place and be unwilling to burden employees with additional cards.

The insider threat and data protection

Awareness of the importance of data protection has never been higher, thanks to vigorous public information campaigns around privacy legislation such as the GDPR and CCPA. However, businesses often focus disproportionately on mitigating external malicious threats. The risk of employee error or insider threat is frequently overlooked, even though it is statistically much more likely, hence the relatively low proportion of organisations that have implemented secure printing.

Many organisations still need to be educated on the print-related data breach risk and encouraged to address it through user-friendly secure printing solutions. Spearheading a programme for education and awareness of the solutions that can help businesses mitigate print-related data breach risk is an important role and opportunity for suppliers.

© Quocirca 2023

Home printers, particularly those that were purchased by employees, may not meet corporate security standards or be monitored through centralised security tools. Remote workers may be accessing data from unsecured home or public Wi-Fi networks.

Yet, print security remains low on the agenda compared to top priorities such as cloud and email. This lack of priority – or complacency – is leaving businesses vulnerable given that paper is one of the least secure mediums in the workplace. While device attacks are rare, the likelihood of paper documents being accessed by unauthorised recipients is increasingly prevalent. Quocirca's research revealed that, on average, 27% of IT security incidents relate to paper documents, and overall, 61% of organisations have experienced a paper-related data breach. This has led to an average print data breach cost of $970,000 – the financial consequences of a data breach can be severe for businesses of any size.

The complexity of securing the print infrastructure is putting more pressure on already-stretched IT teams. According to Quocirca's research, 39% of IT decision-makers believe print security has become harder to manage.

It is, therefore, perhaps unsurprising that just 19% of ITDMs are completely confident that their print infrastructure is protected from security breaches and data losses. This drops to just 11% among SMBs.

Mitigating the risk with multi-layered print security

Fortunately, these risks can be mitigated in simple and effective ways. Secure printing is a key element of a broader multi-layered, integrated approach to print security. Quocirca's Print Security Maturity Index reveals that organisations classed as security leaders (defined as those that have implemented a range of measures, including security assessments, pull-printing, and formal print security policies) are seeing lower levels of data loss and have higher confidence in the security of their print infrastructure.

Advanced secure printing solutions ensure that documents are only released to authorised users, when the user authenticates at the device via RFID card, smartphone mobile credential, or biometrics. This allows organisations to ensure employees have a consistent way of releasing documents across distributed environments and overcome some of the inherent risks associated with using basic PINs or weak password credentials alone.

With just 38% of organisations reporting that they have implemented secure printing, advanced secure printing solutions based on RFID technology offer a clear opportunity to mitigate the growing risk of print-related data breaches.

Security and convenience with ELATEC RFID readers

ELATEC, a global provider of universal RFID, NFC, and Bluetooth® Low Energy (BLE) readers, is well established in the print security market. Its RFID readers offer convenient user authentication and access control across a wide range of locations, equipment, and systems. The readers integrate with leading MFP brands and print software, allowing employees to authenticate at devices with the same RFID cards they use to enter the building, which eliminates the need for new systems. This overcomes the risks associated with using passwords or PINs to release print jobs. The card can also be implemented as part of many existing smartphone apps.

© Quocirca 2023

With RFID card and smartphone credentialing systems, users simply wave their ID card or smartphone over the reader to release the print job. The reader connects with the print management software system to authenticate and match the user with the print jobs they sent. All of this is recorded in case a forensic investigation around information loss is required. Usage and volume of consumables used can also be monitored and tracked for chargeback purposes.

Such an identity management platform is extensible. For example, ELATEC supports mobile credentials and access solutions that can be integrated into existing secure identity systems. Examples include building information management (BIM) systems, for unlocking doors or clocking into a building, as well as single sign-on (SSO) systems for logging onto a computer network or accessing applications. The solutions leverage standard device technologies and are universally accessible, easy to deploy, and simple to manage.

Further security capabilities involve the location of the user and printer. For example, if a user is logged as being in one part of a building and trying to free up a print job in another, the system can flag this as a likely problem and put a hold on the print job until the issue between location and action can be resolved. Different security approaches can be applied based on location – for example, an employee may be able to print a document while in the office, but not when at home or in a public environment. Certain documents may only be printable in a secure print room, which enables much greater control over what information is made available, even within the organisation.

Privacy and regulation compliance

According to the UN Conference on Trade & Development, 71% of countries worldwide have data protection and/or privacy regulations in place. Many of those that do not are in the process of implementing them. In the US, individual states have enacted their own privacy regulations.

While the detail varies between jurisdictions, fundamental privacy regulations make businesses liable for protecting the data they collect, manage, and share.

The print network represents a major channel for sharing and managing data. Therefore, implementing a secure printing solution should be viewed as a fundamental step to ensure compliance with data protection regulations.

Failure to adequately protect data across the digital and physical print network can result in heavy fines, legal action, and reputational damage that, in the most severe cases, can affect the business's survival.

As such, an RFID approach can enable a well-rounded security strategy, blending in location, time, user credentials, application access, and information type, while bringing together all aspects of security that an organisation needs – not just at a simplistic IT level. For example, even if a malicious actor gains entry to an IT environment, using RFID tokens integrated into SSO systems and protecting information flows and print job processes prevent them from accessing important information.

As an extra layer of security, the RFID signal can be encrypted, making the solution much more secure than a password or PIN system. The transponder signal cannot be easily cloned or hacked, and employees are much less likely to share their corporate ID card or phone than a printer password or PIN. Even when a card is mislaid or stolen, it can be easily deleted from the access database, and the physical card will be inactive.

The path forward

The threat landscape is set to become more complex, with advanced cyber-attacks likely to result in far-reaching financial and business impact. Therefore, ensuring resilient and secure print infrastructure as part of the overall IT and business information environment, while supporting efficiency, is a business imperative.

Printing remains a key element of the IT infrastructure, and organisations must treat print security as any other end point on the network. RFID access control and mobile authentication will enable IT teams to balance security with productivity in today's evolving hybrid workplace.

© Quocirca 2023

About Quocirca

Quocirca is a global market insight and research firm specialising in the convergence of print and digital technologies in the future workplace.

Since 2006, Quocirca has played an influential role in advising clients on major shifts in the market. Our consulting and research are at the forefront of the rapidly evolving print services and solutions market, trusted by clients seeking new strategies to address disruptive technologies.

Quocirca has pioneered research in many emerging market areas. More than 10 years ago we were the first to analyse the competitive global market landscape for managed print services (MPS), followed by the first global competitive review of the print security market. More recently Quocirca reinforced its leading and unique approach in the market, publishing the first study looking at the smart, connected future of print in the digital workplace. The Global Print 2025 study provides unparalleled insight into the impact of digital disruption, from both an industry executive and end-user perspective.

For more information, visit www.quocirca.com.

Usage Rights

Permission is required for quoting any information in this report. Please see Quocirca's Citation Policy for further details.

About ELATEC

ELATEC is a global developer and manufacturer of authentication solutions. Its market-leading RFID and mobile credential readers are integral to secure printing. They enable touchless user authentication, authorisation, and access control for secure print release, usage tracking, and billing. These universal readers are compatible with all major transponder technologies and are pre-certified for use in as many as 110 countries worldwide.

The standard for secure printing, ELATEC readers offer plug-and-play simplicity, the contactless convenience of RFID card or smartphone user authentication, and the cost-saving future proofing of remote or configuration card programmability.

The company was founded in 1988 and currently has 22 two locations worldwide. ELATEC Inc.'s headquarters are in Palm City, Florida, and ELATEC GmbH's headquarters are in Munich, Germany.

For more information, visit www.elatec.com.

Disclaimer:

© Copyright 2023, Quocirca. All rights reserved. No part of this document may be reproduced, distributed in any form, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Quocirca. The information contained in this report is for general guidance on matters of interest only. Please note, due to rounding, numbers presented throughout this report may not add up precisely to the totals provided, and percentages may not precisely reflect the absolute figures. The information in this report is provided with the understanding that the authors and publishers are not engaged in rendering legal or other professional advice and services. Quocirca is not responsible for any errors, omissions, or inaccuracies, or for the results obtained from the use of this report. All information in this report is provided 'as is', with no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this report, and without warranty of any kind, express or implied. In no event will Quocirca, its related partnerships or corporations, or its partners, agents, or employees be liable to you or anyone else for any decision made or action taken in reliance on this report, or for any consequential, special, or similar damages, even if advised of the possibility of such damages. Your access and use of this publication are governed by our terms and conditions. Permission is required for quoting any information in this report. Please see our Citation Policy for further details.