KYOCERA

kyoceradocumentsolutions.co.uk

Kyocera: Major Player in the Modern Age of Document Security

Mastering print and data security is crucial in an era of remote working and increased cybersecurity threats.

Table of Contents

Introduction

With the rise of smart technologies like Artificial Intelligence (AI) and the Internet of Things (IoT), the possibilities to transform the way we work and interact have become endless.

The digital era offers tremendous opportunities, but many industries have now entered unexplored waters. It has quickly become apparent that security needs to be the foundation upon which everything is built.

Without a robust and agile approach to data and systems protection, growth plans are essentially built on sand foundations, and any short-term success is likely to be undone sooner rather than later.

Our lives have never been so connected, and we have never been so mobile. While we enjoy unprecedented freedom to innovate and collaborate to create a better, more sustainable world, we are now facing an unprecedented wave of security threats. Threats that are not only increasing in volume, but in complexity and intelligence.

These threats are forcing business leaders across the world to look inward, to examine where immediate improvements are needed.

This period of immense disruption poses many challenges, but it also provides today's businesses with the chance to build vital cybersecurity capacities at the very heart of their digital transformation strategy.

Those who fail to do so might not get a second chance.

1. Building a Secure Future

It is widely thought that there are two types of companies in today's business world: those that know they've been compromised, and those that don't know.

A global pandemic has seen a tremendous acceleration of trends which were already in motion. With the rise of automation and other digital solutions, data security and document solutions have become intertwined, and can no longer be viewed as separate entities.

Nor can security be considered the sole responsibility of the IT department: in the digital era, a new approach is required. Security solutions need to be robust and interconnected. There can be no gap areas.

In recent years, businesses have demanded more streamlined services that help boost efficiency while ensuring maximum data protection. However, with the onset of COVID-19, the way of working changed in an instant for millions of employees across the globe.

Now, with staff spread out across towns and cities, the number of potential points of cyber-attack has grown exponentially. As a result, today's businesses need a professional and comprehensive set of printing and IT solutions they can trust.

It's a time for doers. A time for all leaders across all industries to practice what they preach.

Recent results from International Data Corporation (IDC), the premier global provider of market intelligence, advisory services, and events in ICT, show that Kyocera Document Solutions is one such company.

Upon completion of a rigorous print and document security solution market assessment, **Kyocera has been awarded "Major Player" status in the IDC MarketScape[1].**

In this eBook we will examine the current state of play with regards to security in the printing and document solutions market. We will highlight emerging trends, as well as the threats and opportunities they pose for companies.
The role of leaders like Kyocera will be integral to digital transformation as we continue to move towards smarter workspaces and greater mobility.

Our industry expertise combined with cutting-edge technology and industry-recognised robust print and document security solutions and services has cemented our reputation as a trusted security advisor in the industry.

Now, we are here for you.

1. Source: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019—2020 Vendor Assessment, Doc #US44811119, Dec 2019.

2. The Digital Transformation — A New Era With New Needs

Document Solutions security threats

The number and complexity of threats facing the security of our data continues to rise rapidly. For many companies, the task of bolstering security has been complicated further by the sudden shift to remote working. The following are just some of the principal threats that all organisations need to be aware of:

Unauthorised access to print data
A third-party goes to the printer and accesses documents that belong to someone else.

Print data disclosure
Accessing the print data from memory, file system, print jobs and hard drives when printers are decommissioned.

Unauthorised configuration changes
Someone changes the printer configuration to route the print jobs elsewhere.

The printer as an attack point
A compromised printer can be used to attack other applications, execute arbitrary malicious code or threaten other systems.

Print job manipulation
This includes replacing the print content for others, inserting new content in print jobs, and deleting logs.

Cloud printing risks
This approach is susceptible to middleman attacks or someone trying to gain access to the enterprise network through cloud printing channels.

Given the ferocious pace at which the coronavirus evolved in early 2020, many organisations were forced to implement remote working.

Employees were given their laptops or computers to take home, where the security of a company's data and information went from being protected in one secure place to an open arena replete with an increasing number of malicious security threats.

This was music to hackers' ears. They are all too aware that they only need to find one weak link in the security chain in order to do untold damage.

For many businesses, that weak link continues to be their print and document infrastructure.

Thus, the onus for ensuring the safety of an organisation's data has been shifted towards each individual employee working from home, and print and document management infrastructure is one of the most vulnerable to security risks.

With employees across the globe now working from home, the focus has turned to ensuring they can continue to print, scan, fax and share documents in a secure and efficient manner.

This will require a consistent, homogenous approach. Employees using multi-brand printers across a team not only increases costs due to the inability to purchase supplies in bulk, but it only serves to significantly increase the risk of a data breach.

Without device consistency, there is significantly less control. Without a mechanism to monitor an entire fleet from one place, companies will continue to lag behind professional hackers.

3. Getting it Right

Finding the sweet spot between optimal mobility and maximum security is one of the great challenges facing today's companies who suddenly find themselves in uncharted waters.

However, as mentioned in the introduction of this eBook, 2020 simply marks an acceleration of trends that were already a part of our daily lives.

After in-depth research, **IDC's 2019–2020 Vendor Assessment report** concludes that "a majority of organizations place a notable difference on the level of importance associated with IT security compared with print and document security."

They detail how many IT managers and Chief Information Security Officers (CISOs) still assume that systems put in place to protect the network would extend to other connected peripherals. They warn that security around network perimeter is "crumbling," and "every device connected to the network is now an endpoint security risk, printers and MFPs included."

Those who continue to underestimate these risks will pay dearly in the long run. IDC state that the result of a security breach to the print and document infrastructure is no different to that of any other security lapse: downtime costs, fines associated with corporate governance and regulatory compliance, as well as damage to reputation. Therefore, the need for a printing fleet assessment from experts has never been greater.

According to a study by Gemalto, 66% of consumers surveyed said they wouldn't do business with a company that had sensitive information exposed due to a data breach.

4. Kyocera: Leading the Way

Nowadays, the biggest change in printing is the shift away from locally-hosted servers to the Cloud.

Well aware of the growing shift towards mobility, Kyocera provides robust, versatile solutions to meet the changing needs of the modern enterprise.

This holistic approach to print security focuses on four key areas: device-level protection, authentication, software or SaaS, and consulting services. Leveraging its portfolio of owned-IP software as well as partner solutions, Kyocera's wide range of security capabilities — which include data encryption, device and print management, and malware protection — has been earmarked as core strengths by IDC. These not only help bolster content security and data privacy, but also ensures data integrity.

Device authentication has taken center stage in recent times and is an area where Kyocera continues to excel. Its user identification feature for MFPs allows administrators to manage user activity, and IT departments are able to authorize specific users for registered access. **Multi-step authentication** via pin numbers and card readers provide users with extra protection for their valuable documents.

Convenience is a requisite in today's fast-paced business world and companies now demand a one-stop-shop service. Security solutions is no different, and is an area where Kyocera continues to excel.

Combining device-level security features and a wide range of software solutions that support its print and document security capabilities, Kyocera customers enjoy a standardized service to ensure maximum security for the entire print and document infrastructure.

This consequently creates several positive spin-off effects such as more agile processes and increases in both efficiency and productivity, while helping customers adhere to security compliance and meet key industry standards.

This comprehensive approach to security and compliance has earned Kyocera the industry-wide reputation as a trusted security advisor.

As more and more companies transition to the Cloud, Kyocera continues to aggressively expand in servers, firewalls, and virus protection solutions to provide total network support and security capabilities.

Leveraging its expertise in Cloud technology, Kyocera has positioned itself as the prime partner for the secure (SHA-2) transition to virtual networks, cloud hosting for documents and cloud services for applications in multiple locations.

With SHA-2 384-bit encryption, our devices communicate directly with the Cloud for optimal efficiency.

5. Take Back Control of Your Security

Agile operations weave security into the fabric of the organization. Stand-alone solutions lead to needless inefficiencies and increased downtime.

When it comes to your information, Kyocera's streamlined approach helps you quickly find your documents securely. This is important considering that **70% of the overall task time is spent actually looking for the document**.

Moreover, as we continue to see the volume of ransomware surge, strong backup capabilities will prove to be a competitive advantage.

Looking at Kyocera on a device level, administrators are immediately alerted to any suspicious activity, be it an unauthorised user who attempts to access a Kyocera MFP or three failed attempts whereby the user's access is immediately blocked.

Multi-factor authentication is becoming increasingly popular among companies who have integration with outside third parties or customer base. People don't want hardware to be a vulnerability or launchpad for an attack, and this extra step ensures versatile printing and scanning without compromising on security.

With the increase in the number of devices accessing shared networks on the go, companies must be able to easily control access permissions and track who has been using a given device.

6. Meet the Solutions

By working closely with reputable vendors such as **Google, Microsoft** and **OnBase**, Kyocera is able to combine its own expertise with those of specialized solutions providers to ensure customers are using the most secure products.

+ **Microsoft Connector** is a business application created to simplify document scanning and sharing from a network-connected Kyocera HyPAS-enabled MFP to an existing installation of Microsoft SharePoint, Exchange, and/or OneDrive for Business.

+ With Kyocera's **OnBase Connector** you can further leverage your existing OnBase investment by scanning, indexing and routing documents into the enterprise content management application directly from your HyPAS-enabled Kyocera MFP — facilitating the secure collaboration and exchange of information.

+ **Kyocera Fleet Services** allows you to regularly update your device firmware to prevent vulnerabilities while its audit log function enhances compliance. Remote management maximizes your print fleet's potential without the need for costly onsite visits. With the rise of remote working, being able to monitor multiple devices across multiple locations will prove to be invaluable.

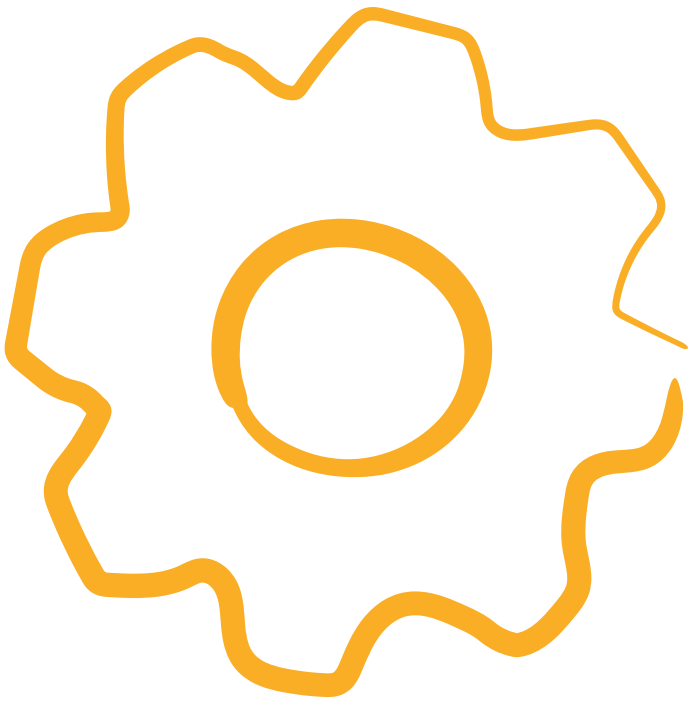
Kyocera develops MFPs and printers with three key security attributes in mind. In order to ensure that customers can use Kyocera products securely, product developers prioritize these attributes, which you should keep in mind at all times. They are:

Confidentiality means that only those who are authorized to access information assets can view, download, print or edit these information assets. To maintain confidentiality, Kyocera prevents unauthorized access to data and documentation.

Integrity demands that information assets must be accurate and correct. To maintain integrity, information assets must be protected against unauthorized alteration by a malicious third party.

Availability ensures that content must be accessible when authorized users need to access it, while maintaining confidentiality and integrity. To ensure availability, information assets must be available at the exact timing when an authorized user wishes to use it.

These are the pillars upon which businesses will build sustainable success.



7. Achieve Real Results

Going that extra mile for our customers is what defines Kyocera.

Customer success is our source of pride. One such example is a US-based healthcare provider who wanted to implement measures to meet HIPAA regulations. Failure to do so would have resulted in a potential fine and damage to the company reputation.

Having previously relied on multi-brand devices, the company elected a comprehensive Kyocera approach to their document management system in the form of 22 TASKalfa devices and DMConnect software.

This standardized and centralized strategy was underpinned by a Card Authentication Kit which allows users to use their HID cards for access to the MFP when copying, scanning and retrieving stored print jobs, and a Data Security Kit to add an additional level of security when it came to Personal Health Information (PHI). The end-user now has a very easy and efficient way to scan documents as well as securely store then release print jobs at any device.

Kyocera Net Manager's server-based application has also provided a way to hold print jobs on a server, allowing the user to release their print job on any machine. This also provided the organization with better control over Patients Health Information (PHI) by avoiding sensitive information being printed and then sitting in the exit tray waiting to be retrieved.

Kyocera's industry-leading End of Life Sanitisation process ensures device information is cleared completely. This includes address books, IP addresses, applications, as well as the hard drive and entire RAM. Kyocera provides a seven-time data overwrite and low-level format of the HD and memory which is unrivalled. This can all be done by users who pre-configure the end of life date for the device and receive a printed certificate to confirm that the process has been completed. Once this is done, the device is unusable and a notification is shown on the machine screen to confirm that the device is ready for removal.

These are just some examples of how Kyocera can provide the secure solutions that organizations need. Whether it is required for compliance or just to offer greater protections to data or even as a promise to clients, Kyocera solutions can provide the perfect fit to enhance your document and print security.

8. Working Together for a Secure Future

Data is now considered as one of the most important assets at a company's disposal. Safeguarding this information in the age of increased mobility is a major challenge for today's businesses.

Despite the rapid pace of change and uncertainty about what the future holds, we can conclude the following with regards data security in the digital age:

+ **Security threats continue to grow:** Companies can no longer rest on their laurels when it comes to security. As the volume and complexity of these threats continues to increase, companies must realize that protecting their employees and customers from cyberthreats is a continuous battle which requires the usage of the latest technologies.

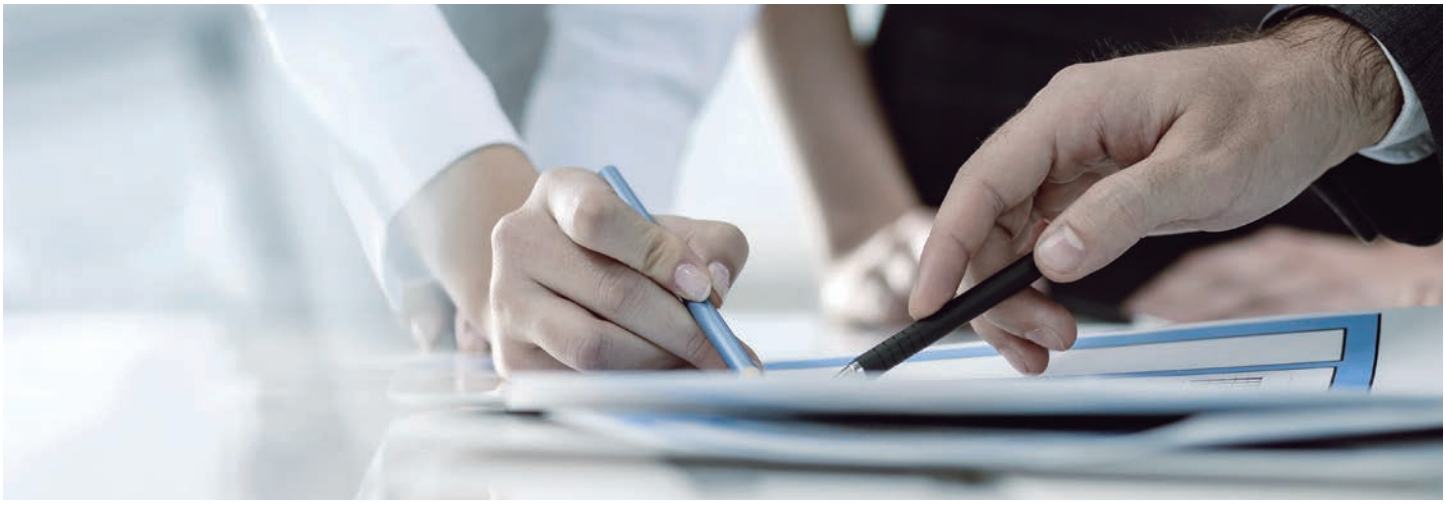
+ **Outdated attitudes towards security:** As per IDC's 2019—2020 Vendor Assessment report, many business leaders place a notable difference on the level of importance associated with IT security compared with print and document security. Those who follow this mindset are destined to learn the hard way of the importance of secure print security.

+ **A one-size-fits-all solution no longer suffices:** Every company is unique and security solutions must be tailored to their needs and current capabilities. A printing fleet assessment is a useful way to identify strengths and weaknesses, as well as obvious security vulnerabilities.

+ **The Confidentiality, Integrity, Availability approach:** To maintain **Confidentiality**, we prevent unauthorised access to information assets. To ensure **Integrity**, information assets must be protected against unauthorised alteration by a malicious third party. **Availability** means that information assets must be accessible when authorised users need to access them, while maintaining confidentiality and integrity.

+ **The benefit of a Trusted Partner:** In an age of increasing uncertainty, expertise is key. Businesses today need reliability and demand long-lasting quality. By leveraging its wealth of experience, Kyocera is the ideal digital transformation partner.

To achieve sustainable success, today's businesses must have security at the very heart of their overall business strategy. During these uncertain times, it will be the robust, agile approach based on innovation and collaboration that will last the test of time.



With its comprehensive approach to print and document security, Kyocera has positioned itself as a trusted security advisor for the SMB sector.

Source: IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2019–2020 Vendor Assessment, Doc #US44811119, Dec 2019

Kyocera Document Solutions has championed innovative technology since 1934. We enable our customers to turn information into knowledge, excel at learning and surpass others. With professional expertise and a culture of empathetic partnership, we help organizations put knowledge to work to drive change.

KYOCERA Document Solutions (U.K.) Limited
Eldon Court, 75-77 London Road
Reading, Berkshire RG1 5BS
Tel: 0333 015 1855

KYOCERA

kyoceradocumentsolutions.co.uk