Sponsored by: **HP**

Authors:
Angèle Boyd
Keith Kmetz
Matthew Marden

November 2015

The Business Value of Printer Security

IDC OPINION

According to IDC research, 80% of the companies we surveyed indicated that IT security is important to their business processes, but only 59% of these companies stated that print security is important to their business processes. In addition, senior management is almost 40% more likely to be involved in decision making for overall IT security than for print security. We believe these findings show a lack of attention to print security that may leave businesses vulnerable. IDC research has revealed that there are compelling reasons for businesses to pay closer attention to print security as there are substantial IT and business benefits derived from a secure print environment, such as:

- IDC survey research found that more than half of companies surveyed have experienced an IT security breach that included print security within the past 12 months.
- Any organization's print/document environment is full of vulnerabilities. These vulnerabilities can come from malicious attacks from inside or outside the organization as well as careless usage of printing devices and output. Potential print-related security breaches could occur from the device's network ports, print/copy/scan job interception, print/MFP hard drives and memory (RAM), printed or copied documents left in output trays, or illegal use of secure media (checks, prescriptions), and so forth.
- In-depth enterprise interviews IDC conducted with organizations that have some level of print and related document workflow security revealed two types of enterprises embracing print/document security:
  - Companies with security and compliance concerns embracing an enterprisewide secure IT infrastructure
  - Companies motivated by cost and IT efficiencies gained by security initiatives
- Interviews conducted by IDC with organizations that have initiated a print security program revealed that they have achieved the most significant benefits and business value in three

areas: improved printer security, IT staff efficiencies, and cost reductions. Organizations interviewed reported an impressive collection of achievements for their print and security environments, including:

- Experiencing up to six times fewer printer-related security breaches on average after deploying printer security solutions
- Cutting staff time needed to support their printer environments in half on average after deploying printer security solutions
- Saving an average of 15% on paper, toner, and ink costs

» The manner in which print security solutions are implemented determines not only their effectiveness but also how much employee productivity is impacted. There are key technology, people, and process requirements to consider in order to ensure maximum benefits.

In This White Paper

This white paper is based on primary and secondary research IDC has conducted with regard to IT and print-related security. IDC conducted in-depth interviews from July to September 2015 with individuals responsible for the implementation and management of printer security solutions at 16 organizations. The interviews were designed to enable IDC to understand the quantitative and qualitative impact of the organizations' use of enterprise printer security solutions. Interviews reflected the experiences of a diverse set of organizations. Table 1 provides an overview of the printing environments of the 16 organizations interviewed.

TABLE 1

Firmographics of Interviewed Organizations — In-Depth Interviews

	Average	Median	Range
Number of employees	60,300	20,500	200 to 290,000
Number of IT staff	4,500	610	40 to 25,000
Number of IT users	57,200	19,500	180 to 290,000
Number of total printers	8,800	1,200	4 to 100,000
Number of users who print	50,800	9,000	200 to 280,000
Number of pages printed per year	51 million	10 million	10,000 to 300 million
Industries	Telecom, manufacturing, financial services, publishing, aerospace, biotechnology, education, and healthcare		

n = 16 organizations

Source: IDC's Printer Security Interviews, 2015

IDC supplemented the in-depth interviews with analysis stemming from survey work. Qualified respondents came from over 440 organizations of all sizes and were full-time employees. The respondents had to have knowledge of the printing equipment used at the company as well as knowledge of the company's IT security policies.

Situation Overview

Why Businesses Should Care About Print/Document Infrastructure Security

Most organizations have made IT security a priority for their organizations … and with good reason. The proliferation of computing, mobile, cloud, and other technologies is facilitating an IT environment in which knowledge workers need and demand "anytime, anywhere" access to business information. However, IDC often finds that printing assets and print-related technologies are an overlooked element of an organization's IT security strategy.

So, why should businesses change their existing approach to print security and secure their print devices as they do other technologies (PCs, servers, mobile devices, etc.)? The answer is that an unsecured print infrastructure translates into an overall unsecured IT environment. The risk of printer-related security breaches is higher than one might expect, and there are costly liabilities.

IDC survey research found that more than half of companies in the past 12 months have experienced an IT security breach that included print security.

IDC survey research found that more than half of companies in the past 12 months have experienced an IT security breach that included print security. This vulnerability can come from malicious attacks from inside or outside the organization as well as careless usage of printing devices and output. Potential print-related security breaches could occur from network ports, print/copy/scan job interception, print/MFP hard drives and memory (RAM), printed or copied documents left in output trays, illegal use of secure media (checks, prescriptions), and so forth. In detail:

- Unsecured network ports are an entry point to the company network and information assets.
- Printing confidential documents (e.g., documents with patient information or client financial transactions) on shared printers where the documents sit in the output tray for any period of time is an opportunity for theft of confidential information and regulatory compliance failures.
- Transmitting print/scan data that is not encrypted is practically an invitation to hackers.

Security breaches are costly. There are three types of potential financial liabilities:

- **Company resources used to address the breach.** Companies that suffer a security breach will use significant employee time and costs to "clean up" the incident. Potential revenue-generating opportunities are delayed or cancelled to deal with it.
- **Fines/penalties.** Companies may face a financial penalty for noncompliance (e.g., HIPAA) or lawsuits from a breach of client-customer confidentiality.
- **Company reputation.** In the aftermath of the incident, the organization could still suffer financially because of a tarnished reputation from bad press.

Triggers for Securing Print Infrastructure

Based on in-depth interviews with organizations that have deployed various levels of print security, we found the following triggers for their implementation:

- Security and compliance concerns (including reacting to a breach)
- Proactive security standardization across the IT infrastructure
- Cost savings and IT efficiencies

Security and Compliance Concerns

Security concerns over intellectual property (IP), confidential or restricted information, regulatory compliance, and the need for an enterprisewide, consistent, secure IT infrastructure are key drivers for a print security program. Some organizations are reactively deploying more robust print security programs in response to past incidents or breaches.

Security concerns over intellectual property (IP), confidential or restricted information, regulatory compliance, and the need for an enterprisewide, consistent, secure IT infrastructure are key drivers for a print security program.

In the words of a senior systems director at a financial services company: "Security concerns are everywhere, and the printer is a publicly accessible device that is used for confidential, restricted, and nonconfidential use. Any network devices that deal with confidential/restricted data are subject to security, compliance, and audit requirements; thus we had to do this."

Standardization Across the IT Infrastructure

Security standardization across an organization's overall IT infrastructure is also driving adoption of print and related document security as well as a comprehensive policy for resolving any issues related to the use of this equipment. A vice president of information technology at a publishing company explained: "We wanted policy-driven security, autoresolution, and the foundational security of identity certificates [for printers] consistent with our approach to other infrastructure services."

Cost Savings and IT Efficiencies

Cost savings are one of the ancillary, yet important, benefits of pursuing a secure print and related document security plan.

Any IT initiative that helps cut an organization's operational costs will be attractive to senior management. Cost savings are one of the ancillary, yet important, benefits of pursuing a secure print and related document security plan. While this benefit may not have been the primary driver of adopting a print and document security program, its impact was the top benefit noted by one-third of the survey respondents.

A senior IT director at a financial services company explained: "The need to protect intellectual property and the potential financial impacts related to data security breaches formed the basis of why these solutions were implemented … we are quite certain that the controls which limit thoughtless and unnecessary printing have saved money in both paper and materials cost."

Of course, there are "less direct" cost savings benefits available through a print security initiative as well. Several organizations pointed out that IT efficiencies gained from centralizing and standardizing print and security management have cost benefits. By more actively managing and securing print, IT is freed up to pursue other priority technology needs of the organization. For example, an IT director at a university explained: "We were looking to consolidate cost control and central management control over our printing environment."

Business Value of Printer Security

IDC's in-depth interviews with the 16 organizations using enterprise printer security solutions revealed that they are achieving significant business value through their deployment of these solutions. These interviews — in which IDC asked the organizations to describe their printer environments before and after their deployment of printer security solutions — showed that the organizations are achieving their objectives of creating more secure print environments while still capturing efficiencies in terms of print-related costs and staff time.

» **Security.** Printer environments have become more secure, and costs related to remedying data breaches and ensuring regulatory and auditing compliance have been reduced.

» **IT staff efficiencies.** The amount of staff time needed to manage and maintain the printer environments and create, change, and apply printer-related policy has been reduced, freeing up time for staff to work on other initiatives.

- **Cost savings.** Costs associated with printing have been lowered through improved visibility and changed printing behavior, including savings in terms of printers and supplies for printers.

Risk Mitigation: Improved Printer Security and Compliance

Interviewed organizations reported that they have leveraged their use of enterprise printer security solutions to reduce the impact of printer-related security breaches and make their compliance efforts more efficient and cost effective.

On average, these organizations reported reducing the frequency of printer-related security breaches by up to six times since deploying enterprise printer security solutions.

IDC asked in-depth interview participants about the frequency with which printer-related security and data breaches occur at their organizations and about whether their organizations have experienced what they would characterize as substantial printer-related security breaches. On average, these organizations reported reducing the frequency of printer-related security breaches by up to six times since deploying enterprise printer security solutions. Deployments of print job encryption, user authentication, and pull printing have enabled a level of traceability and accountability that is reassuring and helps prevent breaches from occurring. In addition, printer security has helped complete some organizations' IT infrastructurewide security initiatives, thereby closing remaining vulnerabilities. Interviewed organizations provided examples of printer-related security breaches that they have experienced, including:

- **Printing confidential information with intent to misuse.** An IT director at a manufacturing company explained that his organization lost intellectual property as a result of, among other things, employees printing highly confidential and proprietary information and providing it to the company's competitors.

- **Printing and mishandling secure data.** An IT director at a financial services company explained that employees at his organization were putting designs and other intellectual property at risk by printing indiscriminately or leaving print jobs at the printer.

Interviewed organizations provided several examples of how their use of enterprise print security solutions has helped them minimize the impact of security breaches through printers:

- **Protection of information throughout the printing process.** A vice president of information technology at a publishing company explained: "The solution has become a vital tool to protect the work flow of content and data to and from our printers over the network, ensuring effective trust enabling us to reduce the opportunity for breaches."

- **Prevent unnecessary or improper printing.** An IT director at a financial services company said: "Often sensitive documentation that we distribute internally should never be printed. These solutions help us minimize breaches, a growing number of which occur internally either deliberately or as the result of indiscriminate printing."

As Table 2 shows, although each printer-related security breach can carry costs, significant security breaches are especially important for organizations to avoid because of the substantial costs to remedy them. According to the five interviewed organizations that have experienced what they characterized as a significant printer-related security breach in recent years, the average costs of a significant security breach include productivity losses for 54 employees, 277 hours of time to remedy, and a hard cost of over $500,000 per breach, including fines.

TABLE 2

Impact of Enterprise Printer Security Solutions on Security Breaches — In-Depth Interviews

Security breaches overall	
Average number of breaches per year — before the implementation of printer security	9.9
Average number of breaches per year — with printer security	1.5
Change in number of security breaches	Up to 6 times fewer
Significant security breaches	
Number of interviewed organizations experiencing	5
Average number of employees impacted	54
Average employee time needed to resolve (hours)	277
Total average cost to remedy per breach (including fines)	$521,400

n = 16 organizations

Source: IDC's Printer Security Interviews, 2015

In addition to reducing the frequency of printer-related security breaches, 10 of the 16 organizations interviewed credited their printer security solutions with making their regulatory compliance and auditing efforts more effective and efficient. Improved security and traceability drive these benefits:

» **Improved security:** A director of systems at a financial services company noted: "At the core of implementing this security model is the benefit that you get to build a very robust and secure environment that protects data, documents, increases the confidentiality of design, architecture and securing printers that has significantly helped us to meet our security standards."

» **Traceability and visibility:** A vice president of IT operations at a life science company explained: "We have been able to create an audit trail, prevent interception of data, and show that we have restricted user access to confidential data. Plus our verification and auditing includes risk identification and threat analysis, plus recommended fixes to problems. We get an in-depth overview of system status and can do real-time monitoring — all requirements for compliance."

These improvements have also yielded time and cost savings for the compliance and auditing efforts of the organizations. On average, interviewed organizations reported that their use of printer security solutions is saving them over 200 hours of employee time per year and almost $250,000 per year in related costs, including third-party support costs for audits and compliance.

IT Staff Productivity Benefits

Organizations IDC interviewed reported that they have reduced the time burden of managing and supporting their printer environments since deploying printer security solutions. These efficiencies have been driven by factors such as introducing or extending the use of centralized management capabilities and automation, as well as being able to resolve printer-related issues faster. A senior IT director at a financial services company explained: "There has been a profound impact on staff [from using printer security solutions], both from hours invested in time-consuming activities as well as freeing the team to focus on more strategic activities. The response to printer-related issues is no longer disjointed, but holistic and repeatable." As a result, interviewed organizations told IDC that, on average, their staff have cut in half the time needed to support their printer environments after deploying printer security solutions.

As a result, interviewed organizations told IDC that, on average, their staff have cut in half the time needed to support their printer environments after deploying printer security solutions.

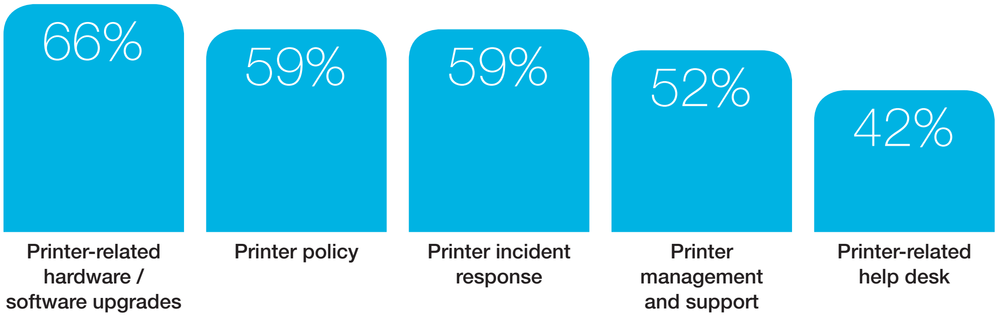
Interviewed organizations reported that printer security solutions have enabled efficiencies for staff members responsible for their printer environments. Staff time savings result from changes such as automation of support and maintenance including through certificate automation, as well as application of other repeatable processes. For example, a vice president at a financial services company employing unique certificate and employee authentication policies explained how his organization has achieved a 60% decrease in the time staff spent monitoring devices: "We're saving IT staff time because profiles can easily be created and pushed out to many devices simultaneously, and we can automate certificate management."

Meanwhile, interviewed organizations are also benefiting from time savings enabled by printer security solutions in creating, applying, and changing printer-related policies. On average, staff at these organizations spend 59% less time on printer-related policy. Beyond staff time savings, more effective implementation of printer-related policy has downstream benefits such as reducing the likelihood of breaches and creating more effective guidelines for printer use.

When printer-related problems arise, interviewed organizations reported that their staff have benefited from features of the printer security solutions such as having (or better leveraging) central consoles and remote access to printers. These factors, in addition to improved printer-related policy, have helped interviewed organizations decrease by an average of 59% and 42%, respectively, the amount of time needed for responding to printer-related incidents and responding to printer-related calls from printer users (see Figure 1). A vice president of IT at a publishing company that was using security solutions that included auto-remediation and managed unique certificates explained the impact on his team's ability to support printers: "There are now fewer issues, and those that exist take less time in aggregate to address. The impact, which is favorable, is that it frees up time for other support and planning activities." An IT director at a financial services company using a printer security management product noted: "Our help desk now has a clear view of printer settings, permissions, and issues and can either act independently or contact a small enterprise printing team for level 2 support."

FIGURE 1

Average Printer-Related Staff Time Savings — In-Depth Interviews



n = 16 organizations

Source: IDC's Printer Security Interviews, 2015

Printing-Related Cost Reductions

Any essential IT initiative that also reduces costs increases its attractiveness. As a result, the ability of interviewed organizations to achieve cost savings through their deployment of printer security solutions has been a substantial value-add. Practices such as employee authentication and pull printing were among the most used by in-depth interview participants (over two-thirds of organizations interviewed are using). These solutions preserve document confidentiality and drive cost savings by requiring print users to take affirmative steps to print documents and by reducing the number of unclaimed or misdirected print jobs. The ability of printer security solutions to serve as a vehicle for reducing printer-related costs is clear enough that several interviewed organizations noted cost optimization as the primary driver for their use of printer security solutions.

Interviewed organizations explained that printer security solutions helped them reduce costs by:

- **Reduced printing by changing printing behavior:** A corporate treasurer at a company in the food industry said: "The pull printing feature we use allows you to send to print but requires you to go and actually put your badge on the printer to actually print it. I think it's reduced at least, from the last numbers I saw, between 21% and 24% the printouts that we used to have before."
- **Providing visibility into printer use:** An IT director at a university reported: "We can now do cost tracking of pages printed to charge back individual departments." With the ability to attribute printing costs on a departmental basis, the university can put the onus on each department to find ways to get its printer users to be as efficient as possible.
- **Decommissioning unneeded or out-of-date printers:** A vice president at a financial services organization noted: "We're reducing the number of unnecessary print jobs as folks know that print activity is monitored, and we are retiring and replacing older print hardware not capable of supporting enterprise print security baselines."

Printer security initiatives have made employees who print more aware about how they use printers and have contributed to printer-related cost savings.

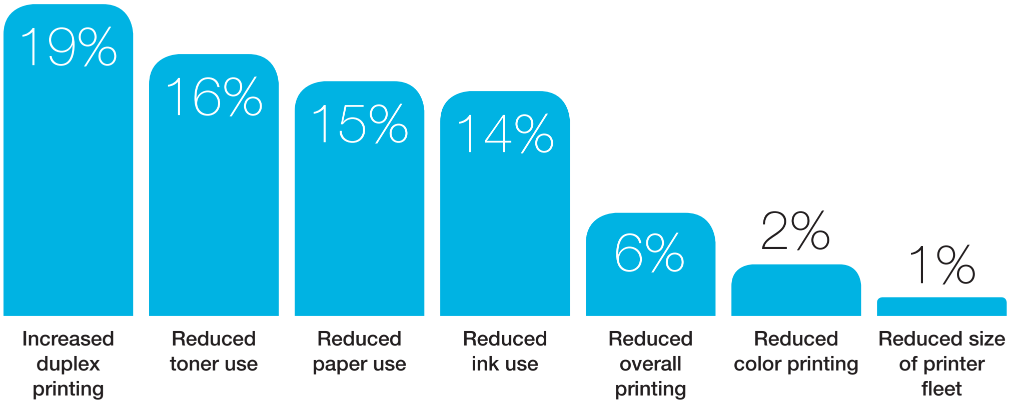
Printer security initiatives have made employees who print more aware about how they use printers and have contributed to printer-related cost savings. On average, in-depth interview participants said that their employees are sending 43% fewer print jobs to the wrong printer. As a result, fewer print jobs are abandoned or repeated. As shown in Figure 2, these types of improvements have contributed to more efficient printer use overall, including printing less overall (6% reduction on average), printing more in duplex (19% increase), and printing slightly less in color (2% reduction). These factors, as well as improved visibility into printer environments, have enabled interviewed organizations to achieve strong cost savings in their printing environments, including the number of printers they deploy and maintain (1%

reduction, or 115 printers on average per organization) as well as the costs associated with paper, ink, and toner (15%, 14%, and 16% reductions, respectively).

FIGURE 2

Average Printer Environment Cost Savings and Printer Efficiencies — In-Depth Interviews

(% efficiency or improvement)



n = 16 organizations

Source: IDC's Printer Security Interviews, 2015

Challenges

With practically any organizational rollout, some challenges can be avoided by planning ahead. The study group's challenges spanned all three phases of a print security rollout: planning, implementation, and post-implementation.

The studied companies reported that they felt a time crunch to develop the strategy and plan. Significant up-front time is needed to achieve the post-implementation reduction in IT's workload. In addition, enforcing employee compliance should be an automated process that encompasses monitoring tools, an escalation process, and remediation to reduce print-related help desk calls.

For an organization's printer users, we note two cautions that should be planned for:

- **Balance tight print security while minimizing employee productivity hit:** Business security needs to be of the highest importance, but an organization should work on a system in a way that has the least adverse productivity impact. For example, some organizations that implement pull printing to address their print security needs may encounter user resistance because of the need to authenticate (i.e., input a password) and then wait for the entire document to be printed. The trade-off in this scenario is the protection of information contained in the document (e.g., no one can view printed documents left unattended in the paper tray) versus waiting for a document to be printed (e.g., printing is initiated only after the user authenticates at the device).

- **Employee training:** Related to employee productivity, the print security plan must include the process and time required to train employees in any new policies and procedures. Businesses should be prepared to provide repeat training and to use different formats to match employee generational and learning style differences.

Essential Guidance

IDC has identified several compelling reasons to incorporate printer and related document workflows into an organizationwide IT security framework. Obviously, one of the core benefits is tied to the provision of a comprehensive IT security program that includes print, but such a plan also has a number of significant benefits beyond security. Two key benefits are notable cost savings and increased IT efficiency.

IDC recommends that an organization bulletproof its print/document security technology. The organization must recognize that this objective can be effectively met only when people and processes are incorporated into the plan's execution.

IDC recommends that an organization bulletproof its print/document security technology.

Technology

With regard to security, implementing technology solutions is basically a black-and-white issue … an organization is either secure or not secure.

IDC recommends that the following capabilities be implemented across the organization as soon as possible. IT personnel and print infrastructure providers should ensure that the following features and capabilities are configured and active for all print devices used throughout the organization:

- Ensure that all networked print devices have the following features or at least have their firmware upgraded to reflect them.

- Make sure that devices use only encrypted communication protocols, and disable the rest.

- Put a system in place that erases or destroys the device's hard drive data as part of removing the device from circulation.

- Support at least one form of user authentication (preferably two or three), and consider the implementation of pull printing for print environments with a high volume of confidential information or compliance requirements.

- Ensure firmware is current and only legitimate firmware is ever loaded.
- Make sure that all printer hard drives are secure (encrypt and erase data on a periodic basis).
- Deploy printed tamper-evident features or use printers with locking drawers for specialty media if the organization's output warrants it. This would secure output that is a potential target for fraud, such as checks, drug/medical prescriptions, and so forth.
- Use a fleet management tool to centrally manage, monitor, and remediate the device to ensure compliance with security policies. In this way, the organization can avoid having to manually configure and maintain each device individually. The tool should allow for simple/easy creation and administration of the security policy, detect when devices are added to the network, provide for unique device certificate management, and log noncompliant incidents and resolve the incidents through an escalation and remediation process. The tool should work with enterprisewide IT security management tools that monitor endpoints for noncompliant incidents and anomalies so that any potential security breaches are identified quickly.
- Make sure that both desktop and mobile device prints and scans (either in motion or at rest) are encrypted to ensure the print-related data is fully protected. This means that even attachments to be printed should be opened and imaged for an additional level of protection. A tool that monitors print and scan content is a key element to ensure the highest level of security and to be compliant with established company policies and industry standards.

People

An organization that is serious about its IT security needs to ensure that the security team includes personnel skilled in securing print devices and related document workflows. This security team can consist of the organization's own internal staff and/or external skilled security resources. The team will be called upon to advise on future print and workflow security issues as well as help with the integration of an enterprisewide IT security plan.

To ensure that securing print devices and related document workflows does not negatively impact employee productivity, the organization should receive input from select employees across the organization as part of the planning process. Involving a change management expert is also recommended, especially if the amount or the nature of changes required is significant. Such an expert can also advise on the rollout and training approach to be used.

Most organizations do not have the necessary knowledge and skill set to adequately secure their print and document infrastructure on their own. Therefore, an organization should consider asking the print device provider about the resources the IT department can leverage. Resources span the security features available in an organization's printer/MFP hardware, security software tools, and security services (e.g., security professional services, security assessments, change management, and expertise in regulatory compliance for specific industries).

Process

It is important that an organization start its security initiative by assessing the current status of its print environment and develop a plan that achieves a level of security consistent with that of the rest of the IT environment. This initiative should include an understanding of the essential security requirements specific to the organization's industry as well as a plan to monitor, escalate, remediate, and enforce these policies on an ongoing basis.

The plan should be reevaluated periodically using data collected during the period to determine if adjustments are needed and to learn from print/document breaches outside the company. Any adjustments will be influenced by the data collected as well as the organization's acceptable level of risk and security spending.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Analyze the Future